

Замкнутые маршруты и алгоритмы сегментации изображений

А. Малистов, И. Иванов-Погодаев, А. Я. Канель-Белов

А. Алгоритмы

Пусть у нас в распоряжении имеется книга из n страниц. На каждой странице книги написано какое-нибудь слово. Кроме того, у нас есть карточка, на которой также написано одно слово. За одну операцию разрешается открыть любую страницу в книге и прочитать слово, которое там написано. За какое число операций можно гарантированно выяснить, есть ли слово на карточке в книге? Ясно, что за n операций это можно сделать, прочитав все страницы в книге.

Пусть теперь известно, что слова в книге расположены по алфавиту. Теперь выяснить, записано ли слово в книге можно за $\lceil \log_2 n \rceil$ операций. Сначала мы открываем книгу на середине. Если слово, написанное на странице совпадает с искомым, то на этом процедуру поиска можно завершить. Если слово оказывается по алфавиту больше нашего, то вторую половину книги можно выкинуть. Если слово оказывается по алфавиту меньше нашего, то первую половину книги можно выкинуть. Таким образом мы сократили книгу в два раза. Далее мы будем повторять операцию до тех пор, пока не останется одна страница. Такой алгоритм известен под названием *бинарный поиск*.

Таким образом, на специально подготовленном массиве данных можно производить поиск гораздо быстрее. В современных компьютерных базах данных может храниться до миллиарда разных записей. Обычный поиск вынуждал бы компьютер просматривать их все. С помощью бинарного поиска мы можем найти необходимую информацию всего за 30 операций.

Пусть имеется компьютер с памятью, состоящей из ячеек. Каждая ячейка имеет адрес. Адреса нумеруются последовательно, начиная с нуля. Каждая ячейка может хранить целые числа, ограниченные по модулю некоторым положительным числом L . Значение L зависит от входных данных решаемой на компьютере задачи. Кроме того, компьютер имеет конечное число регистров для проведения арифметических операций. Алгоритмом называется пронумерованная последовательность разрешенных операций. Разрешены операции чтения чисел из памяти в регистр и записи из регистра в память, арифметические операции (сложение, умножение, вычитание, целочисленное деление, взятие остатка). За одну операцию также можно сравнить значение двух чисел, и, в зависимости от результата, перейти к любому шагу алгоритма. Временем работы алгоритма называется число операций, которые алгоритм выполняет для решения задачи. Объёмом памяти, необходимым для работы алгоритма, называется максимальный адрес ячейки, которая была задействована.

Рассмотрим следующую задачу. Требуется выяснить, есть ли в массиве размера n два одинаковых числа. Эту задачу можно решить за $n(n-1)/2$ сравнений для каждой пары чисел. Но кроме операций сравнения, потребуется организовать два цикла, в котором один вложен в другой. Для каждого цикла нужна переменная-счётчик, которая на каждой итерации увеличивается на единицу. Эти дополнительные операции производятся компьютером, поэтому, чтобы оценить общее время работы алгоритма, необходимо их также учитывать. Количество вспомогательных операций для двух циклов не будет превышать $C_1 n^2$ для некоторой константы C_1 , а, значит, число всех операций, включая сравнение, не превышает $C_2 n^2$ для некоторой константы C_2 . Ча-

сто при анализе времени работы алгоритмов константы не учитывают, говоря, что алгоритм работает за $O(n^2)$ (произносится O -большое от n^2).

Более формально, пусть имеется задача, в которой по набору входных данных нужно вычислить некоторый ответ. Обычно, чем сложнее входные данные, тем дольше работает алгоритм. Пусть с входными данными связан некоторый целочисленный параметр n , например, количество чисел в массиве, число вершин в графе и т.п. Этот параметр n часто называют функцией длины входа. Для каждого фиксированного значения n вход алгоритма может быть различным. Будем говорить, что алгоритм выполняется за $O(f(n))$, если существуют такие константы C и n_0 , что для всех $n > n_0$ число операций, которые выполняет алгоритм на любом входе длины n , не превышает $Cf(n)$. Таким образом, выяснить, есть ли в массиве размера n два одинаковых числа, можно за $O(n^2)$ операций. Есть алгоритм, который позволяет это сделать за $O(n \log n)$ операций¹. Время работы алгоритма также может зависеть от размера ячейки L . Если существует многочлен от двух переменных $p(n, \log_2 L)$ такой что время работы алгоритма и объём используемой памяти для любого входа длины n и размера ячейки L не превосходит $p(n, \log_2 L)$, то такой алгоритм называют *полиномиальным*. Если существует многочлен $p(n)$ такой, что время работы алгоритма и объём используемой памяти для любого входа длины n не превосходит $p(n)$, то такой алгоритм называют *сильно полиномиальным*. Например, алгоритмы, работающие за $O(n^4)$ или $O(n \log n)$ — сильно полиномиальные.

Обозначения с O -большое можно легко обобщить на случай с несколькими переменными. Например, для графа с V вершинами и E рёбрами работа алгоритма за $O(EV^2 \log V)$ означает, что существуют такие константы C , V_0 и E_0 , что для всех $V > V_0$ и $E > E_0$ число операций, которые выполняет алгоритм на любом входе с V вершинами и E рёбрами, не превышает $CEV^2 \log V$. Обычно в графах V и E обозначают множества вершин и рёбер, а для количества вершин и рёбер используются обозначения $|V|$ и $|E|$. Внутри записи с O -большим мы будем писать просто V и E , так как это не вводит в заблуждение. Запись $O(V^2E)$ означает то же, что и $O(|V|^2|E|)$.

► **A1.** Предложите алгоритм, который выясняет есть ли в массиве размера n два одинаковых числа и работает за $O(n \log n)$ операций.

В алгоритмах разрешается использовать дополнительную память для хранения промежуточных данных. Объём необходимой памяти можно также оценивать, используя нотацию с O -большое. Существуют алгоритмы, быстрые, но использующие много памяти, а также алгоритмы, которые требуют мало дополнительной памяти, но работают долго. В зависимости от задачи, применяются разные типы алгоритмов. Если не оговорено иное, мы считаем, что для алгоритма доступно $O(n)$ дополнительной памяти (для графов $O(E + V)$). Это означает, что для алгоритма существует константа C такая, что дополнительной памяти требуется меньше, чем Cn ($CV + CE$ для графов).

► **A2.** Предположим, что нет ограничений на использование памяти. Предложите алгоритм, который выясняет есть ли в массиве размера n два одинаковых числа и работает за $O(n)$ операций.

Пусть $G = (V, E, w)$ — некоторый взвешенный ориентированный граф, где V — множество вершин графа, $E = \{(u, v) \mid (u, v) \in V\}$ — множество рёбер графа, $w: E \rightarrow \mathbb{R}$ — функция, сопоставляющая каждому ребру вес. В компьютерной памяти описание графа может занимать $3|E| + 2|V|$ ячеек. В первой ячейке записано число вершин графа $|V|$, во второй ячейке записано число рёбер $|E|$, а далее идут $|E|$ троек ячеек, в каждой

¹ В обозначениях с O -большое мы будем опускать основание логарифмов, так как логарифмы с разным основанием отличаются константным множителем и $O(\log_2 n)$ означает то же самое, что и, например, $O(\log_{10} n)$.

тройке для каждого ребра $e = (i, j)$ графа записаны номер исходящей вершины i , номер входящей вершины j и вес $w(i, j)$.

Маршрут $s \rightsquigarrow t$ между вершинами s и t называется последовательность вершин $s = v_1, v_2, \dots, v_n = t$, где для любого $i = \overline{1, n-1}$ существует ребро $(v_i, v_{i+1}) \in E$, направленное из v_i в v_{i+1} . *Длиной маршрута* $s \rightsquigarrow t$ называется сумма весов всех его рёбер. *Кратчайшим маршрутом* между вершинами s и t называется такой маршрут, длина которого минимальна среди всех возможных маршрутов из s в t . Кратчайшим расстоянием между вершинами от s к t будем считать длину кратчайшего маршрута между ними. Кратчайшие маршруты определены тогда и только тогда, когда в графе нет отрицательных по весу циклов. По умолчанию мы считаем, что все веса ребер в графе **положительны**.

► **A3.** Пусть все веса в графе равны 1 (невзвешенный граф). Пусть s, t — некоторые вершины графа. Предложите алгоритм, который находит кратчайшее расстояние от s до t за время $O(E)$.

► **A4.** Пусть все веса в графе равны 1 (невзвешенный граф). Пусть s, t — некоторые вершины графа. Предложите алгоритм, который находит кратчайший путь от s до t , то есть последовательность номеров вершин s, u_1, u_2, \dots, t за время $O(E)$.

Пусть s — некоторая вершина графа $G = (V, E, w)$. *Деревом кратчайших путей* для вершины s называется подграф $T_s = (V_s, E_s, w)$ исходного графа $G = (V, E, w)$ такой, что 1) V_s — множество вершин, достижимых из s , 2) T_s — дерево с корнем в s , 3) Для всех вершин $u \in V_s$ путь из s в u в дереве совпадает с одним из кратчайших путей в графе G из s в u .

► **A5.** Доказать, что для любой вершины s в графе $G = (V, E)$ существует дерево кратчайших путей T_s .

► **A6.** Пусть $G = (V, E, w)$ — произвольный взвешенный ориентированный граф. Пусть s — некоторая вершина графа. Предложите алгоритм, который находит дерево кратчайших путей T_s и кратчайшие расстояния от s до каждой вершины графа G за время $O(V^2)$.

Рассмотрим граф-дерево. У каждой вершины дерева, кроме корня, существует ровно один родитель и, возможно, несколько дочерних вершин (потомков). У корня только дочерние вершины. Разделим все вершины дерева на слои. *Первый слой* дерева будет включать в себя только корень. *Второй слой* дерева будет включать потомков корня. *Третий слой* дерева будет включать потомков вершин второго слоя. И далее $(i + 1)$ -ый слой дерева будет включать потомков вершин i -ого слоя.

Двоичным (или бинарным) деревом назовём дерево, у каждой вершины которого не более двух потомков. Все вершины двоичного дерева можно пронумеровать следующим образом. Вершина первого слоя (корень) получает номер 1, вершины второго слоя получают номера 2 и 3 (слева направо), вершины третьего слоя получают номера 4, 5, 6 и 7, и так далее, вершины i -ого слоя получают номера от 2^{i-1} до $2^i - 1$. Если в соответствующем месте вершина отсутствует, то ее номер пропускается и не присваивается никаким другим вершинам.

Назовём бинарные деревья *почти полными*, если все их k вершин имеют номера от 1 до k , то есть ни одного номера не было пропущено. Предположим, что с каждой вершиной дерева связано некоторое целое число, которое будем называть ключом, и дополнительный набор данных конечного размера. Почти полное бинарное дерево называется *неубывающей бинарной кучей*, если ключ в любой вершине не больше, чем ключи его потомков. Минимальный элемент в неубывающей бинарной куче, очевидно, можно найти за $O(1)$ операцию. Он находится в корне.

- **A7.** Предложите алгоритм, позволяющий добавить один элемент в кучу за $O(\log k)$ операций и сохранить основное свойство кучи.
- **A8.** Предложите алгоритм, позволяющий удалить минимальный элемент из кучи за $O(\log k)$ операций и сохранить основное свойство кучи.
- **A9.** Предложите алгоритм, позволяющий изменить значение ключа произвольного элемента кучи за $O(\log k)$ операций и сохранить основное свойство кучи.
- **A10.** Пусть $G = (V, E, w)$ — взвешенный ориентированный граф. Пусть s — некоторая вершина графа. Предложите алгоритм, который находит дерево кратчайших путей T_s и кратчайшие расстояния от s до каждой вершины графа G за время $O(E \log V)$.

В. Планарные графы

Пусть $G = (V, E)$ — планарный граф. Каждой вершине v сопоставлена точка на плоскости с целыми координатами (x_v, y_v) . Будем считать, что все рёбра в рассматриваемых планарных графах представлены на плоскости непересекающимися отрезками.

- **V1.** Докажите, что в планарном графе $|E| < 3|V|$.

В дальнейшем нам потребуется следующая теорема Жордана. Принимаем её без доказательства.

Теорема Жордана для многоугольников. Дан многоугольник (ребра не пересекаются). Доказать, что этот многоугольник разбивает плоскость на две связные области и является их границей.

Выберем на плоскости точку H , не лежащую ни на одном ребре, включая вершины планарного графа G . Для любого ребра AB углом вращения $\omega(AB)$ вокруг точки H называется ориентированный угол AHB (от $-\pi$ до π). Для любого маршрута $w = e_1 e_2 \dots e_m$, где $e_i \in E$, углом вращения $\omega(w)$ называется сумма $\omega(e_1) + \omega(e_2) + \dots + \omega(e_m)$.

- **V2.** Доказать, что для любого замкнутого маршрута $v_1 v_2 v_3 \dots v_m v_1$, где $v_i \in V$ угол вращения вокруг H , равен $2\pi n$, где n — целое число. Число n называется индексом вращения маршрута относительно H .

Выберем в планарном графе вершину s . Далее будем рассматривать маршруты, начинающиеся в вершине s , которые назовём s -маршрутами. s -петлёй будем называть замкнутый s -маршрут.

- **V3.** Дана s -петля с индексом вращения $n > 1$ вокруг точки H . Доказать, что существует s -петля с индексом вращения $n - 1$ вокруг точки H .

С. Кратчайшие замкнутые маршруты вокруг одной точки

Основные задачи проекта будут посвящены алгоритмам поиска кратчайших замкнутых маршрутов с заданной стартовой вершиной s при различных дополнительных ограничениях:

1. Количество точек, вокруг которых мы хотим найти петли: одна H или две H_1, H_2
2. Ориентированный/неориентированный граф
3. Поиск полиномиального алгоритма или быстрого за $O(V \log V)$.
4. Поиск кратчайшего маршрута среди всех с ненулевыми индексами или с заданными индексами вращения.

Пусть имеется одна точка H , вокруг которой мы будем прокладывать замкнутые маршруты с заданной стартовой точкой s . Во всех задачах ниже нужно установить, существует ли алгоритм поиска маршрута с указанными свойствами.

- ▶ **C1.** Неориентированный граф, нужно найти кратчайший замкнутый s -маршрут с ненулевым индексом за $O(V \log V)$ операций.
- ▶ **C2.** В ориентированном графе нужно найти кратчайший замкнутый s -маршрут с ненулевым индексом за $O(V \log V)$ операций.
- ▶ **C3.** Неориентированный граф, нужно найти кратчайший замкнутый s -маршрут с заданным индексом k за $O(V \log V)$ операций. Считаем, что $|k| < 100$.
- ▶ **C4.** Ориентированный граф, нужно найти кратчайший замкнутый s -маршрут с заданным индексом k за полиномиальное число операций. Считаем, что $|k| < 100$.
- ▶ **C5.** Ориентированный граф, нужно найти кратчайший замкнутый s -маршрут с заданным индексом k за $O(V \log V)$ операций. Считаем, что $|k| < 100$.

Д. Кратчайшие маршруты вокруг двух точек

Пусть теперь имеются две точки H_1 и H_2 . Пути вокруг них (если их рассматривать как траектории) характеризуются уже двумя индексами вращения. У нас по-прежнему есть стартовая точка s . Во всех задачах ниже нужно установить, существует ли алгоритм поиска маршрута с указанными свойствами.

- ▶ **D1.** Неориентированный граф, нужно найти кратчайший замкнутый s -маршрут с заданными индексами (k, n) за $O(V \log V)$ операций. Считаем, что $|k| < 100$, $|n| < 100$.
- ▶ **D2.** Ориентированный граф, нужно найти замкнутый s -маршрут с заданными индексами (k, n) за полиномиальное число операций. Считаем, что $|k| < 100$, $|n| < 100$.
- ▶ **D3.** Ориентированный граф, нужно найти замкнутый s -маршрут с заданными индексами (k, n) за $O(V \log V)$ операций. Считаем, что $|k| < 100$, $|n| < 100$.

Е. Кратчайшие маршруты без старта

Теперь нет выделенной стартовой точки. То есть требуется найти кратчайший замкнутый маршрут, не обязательно проходящий через заранее выделенную вершину. По-прежнему, нужно установить, существует ли алгоритм поиска маршрута с указанными свойствами.

Решетчатый граф — это граф, вершины которого соответствуют точкам на плоскости с целыми координатами, $(x = 1, \dots, n; y = 1, \dots, m)$, и вершины которого соединены ребром, если соответствующие точки находятся на расстоянии 1. Для ориентированного случая, две точки на расстоянии 1 соединены в обоих направлениях, возможно с разными весами.

- ▶ **E1.** Существует ли алгоритм поиска кратчайшей петли вокруг H в ориентированном решётчатом графе за время $O(V^{\frac{3}{2}} \log V)$?
- ▶ **E2.** * Попробуйте найти алгоритм поиска кратчайшей петли вокруг H в ориентированном решётчатом графе за время $O(V \log V)$.
- ▶ **E3.** * Попробуйте найти алгоритм поиска кратчайшей петли вокруг H в ориентированном планарном графе за время $O(V^{\frac{3}{2}} \log V)$.

Enclosing walks and image segmentation algorithms

A. Malistov, I. Ivanov-Pogodaev, A. Kanel-Belov

A. Algorithms

Consider a book with n pages. Every page contains some word. Moreover, there is a card with a single word. Using one operation we can look an arbitrary page and read a word. How many operations are required to find the word from the card in the book? It is clear that n tests are sufficient to look up all the pages in the book.

Suppose that all the words in the book are sorted in alphabetical order. Now $\lceil \log_2 n \rceil$ operations are sufficient to check for the existence the word in the book. First of all, we can check the midpage of the book against our word and eliminate half of the book from further consideration. The *binary search* algorithm repeats this procedure, halving the size of the remaining portion of the book each time.

So, we can make a search faster using specially prepared data. Modern computer data bases contain billions records. The linear search algorithm must look up all the records. We can find any record using 30 operations with the binary search algorithm.

Consider the computer operating the memory with some registers. A register is a location with both an address and a content — a single integer number x ($|x| < L$, L is a positive integer). L depends on input data of our problems. Address is an integer more or equal to zero. The following operations are permitted: addition, subtraction, multiplication, integer division, modulo operation, comparison and conditional branch, which may or may not cause branching depending on the comparison result. The *running time* of an algorithm is the number of operations or “steps” executed. The memory capacity used by an algorithm is the maximal address of memory unit used.

Consider an n -element linear array. Are there exist two equal elements in the array? We can solve this problem using $n(n-1)/2$ comparisons — for every pair of elements. Algorithm needs some additional operations except the comparisons. For example, this is an increment for the loop variables. The number of additional operations is less than $C_1 n^2$ for some constant C_1 . Thus, the number of all operations is less than $C_2 n^2$ for some constant C_2 . They often describe the running time of algorithm ignoring the constant factors. They say that the running time of the algorithm is $O(n^2)$ (big O notation).

Suppose that we want to compute result using some input parameters. Usually, more complex input increases algorithm’s running time. Let n be a some integer which depends on the input. For example, n is array size or number of nodes etc. This parameter is called “input length function“. There are different inputs for fixed n . We say that an algorithm has a running time $O(f(n))$ if there exist some constants C, n_0 such that for any $n > n_0$ the number of operations executed less than $Cf(n)$ for any input of length n . Thus one can find two equal numbers in array of size n using $O(n^2)$ operations. There is an $O(n \log n)$ algorithm which solves this problem¹. The running time of an algorithm can depend on the size L of the memory unit. An algorithm is *polynomial* if there is a polynomial $p(n, \log_2 L)$ such that the runing time and memory used are less than $p(n, \log_2 L)$ for any input. An algorithm is *strong polynomial* if there is a polynomial $p(n)$ such that the runing time and memory used are less than $p(n)$ for any input. For exapmle, $O(n^4)$ algoritms and $O(n \log n)$ algorithms are strong polynomial.

O -notations can be easily extended to multiple variables case. For example, for graph with V vertices and E edges, the running time $O(EV^2 \log V)$ means that there exist constants C, V_0 and E_0 such that for all $V > V_0$ and $E > E_0$ the number of operations

¹ We will use baseless log inside of big O notation. The thing is that two logarithms with different bases are just scalar multiples of each other.

executed less than $CEV^2 \log V$. Usually V is a set of vertices and E is a set of graph edges. $|V|$ and $|E|$ are sizes of these sets. We will write just V and E inside of big O notation. $O(V^2E)$ and $O(|V|^2|E|)$ are the same.

► **A1.** Describe an $O(n \log n)$ algorithm that determines whether or not there exist two equal elements in the array of size n .

An algorithm can use additional memory to store temporary data. The size of required memory can be estimated via O notation. There are many fast algorithms that require much memory. To the other side, there are many low memory algorithms that require much time to perform. Unless otherwise stated, any algorithm has an $O(n)$ memory capacity (or $O(E + V)$ for graphs). This means that, for the algorithm, there is a constant C such that this algorithm requires memory amount less than Cn . (or $CV + CE$ for graphs).

► **A2.** Suppose that there are no memory restrictions. Describe an $O(n)$ -algorithm that determines whether or not there exist two equal elements in the array of size n .

Let $G = (V, E, w)$ be an weighted directed graph. V is a set of its vertices, $E = \{(u, v) \mid (u, v) \in V\}$ is a set of graph edges, $w: E \rightarrow \mathbb{R}$ is a weight function. Graph description can hold $3|E| + 2$ memory units. First cell holds the number of graph vertices $|V|$, second cell holds the number of graph edges $|E|$. The next cells holds $|E|$ triplets for each edge. Each triplet is the index of outgoing vertex i , the index of incoming vertex j and weight $w(i, j)$.

A walk $s \rightsquigarrow t$ from s to t is a sequence $s = v_1, v_2, \dots, v_n = t$ such that for any $i = \overline{1, n-1}$ there exists an edge $(v_i, v_{i+1}) \in E$ from v_i to v_{i+1} . The weight of a walk $s \rightsquigarrow t$ is sum of all edges weights. A shortest walk from vertex s to vertex t is any walk $s \rightsquigarrow t$ with minimal weight. The shortest distance from s to t is the weight of a shortest walk from s to t . Shortest walks are well defined if and only if the graph G contains no negative-weight cycles. Unless otherwise stated, only **positive-weight** graphs are considered.

► **A3.** Suppose that all weights of the graph G are equal to 1 (unweighted graph). Let s, t be two vertices of the graph G . Describe an $O(E)$ algorithm that searches for the shortest distance from vertex s to vertex t .

► **A4.** Suppose that all weights of the graph G are equal to 1 (unweighted graph). Describe an $O(E)$ algorithm that searches for the shortest walk from vertex s to vertex t . Output of this algorithm is a sequence s, u_1, u_2, \dots, t .

For any vertex s there is a *shortest-paths tree* $T_s = (V_s, E_s, w)$ such that 1) T_s is a subgraph of G , 2) s is the root of T_s , 3) V_s contains vertices reachable from s , 4) for all $v \in V_s$, the path from root s to v in T_s is the shortest path from s to v in G .

► **A5.** Prove that for any vertex s there is a *shortest-paths tree* T_s .

► **A6.** Let $G = (V, E, w)$ be an weighted, directed graph. Let s be a some vertex. Describe an $O(V^2)$ algorithm that searches for the shortest-paths tree T_s and shortest distances from vertex s to all other vertices.

Consider a tree. Each vertex except the root has a unique parent and probably some children. The root has children only. Let us divide all the vertices by the levels. Level 1 contains the root only. Level 2 contains the children of the root. Level 3 contains the children of the verices from level 2 etc. Level $(i + 1)$ contains the children of the verices from level i .

Binary tree is a tree in which each node has at most two children. We can enumerate all the vertices of the binary tree by the following way. The vertex of level 1 (the root)

has index 1. The vertices of level 2 have indices 2, 3. The vertices of level 3 have indices 4, 5, 6 and 7, and so on. The vertices of level i have indices from 2^{i-1} to $2^i - 1$. If some vertex is absent then its index is skipped.

A binary tree is called an *almost complete* binary tree if all the levels (maybe except the last one) is completely filled. Suppose that each tree node contains some integer (*key*) and an additional data of fixed size. A *binary heap* is a almost complete binary tree such that the key at every node is less than (or equal to) the key at its left child and the key at its right child. It is clear that the element with minimal key can be found using $O(1)$ operations.

- ▶ **A7.** Describe an $O(\log k)$ algorithm that pushes a single element into the binary heap and retains the heap property.
- ▶ **A8.** Describe an $O(\log k)$ algorithm that eliminates the minimal element from the binary heap and retains the heap property.
- ▶ **A9.** Describe an $O(\log k)$ algorithm that changes the key of the minimal element of the binary heap and retains the heap property.
- ▶ **A10.** Let $G = (V, E, w)$ be the weighted, directed graph. Let s be some vertex. Describe an $O(E \log V)$ algorithm that searches for the shortest-paths tree T_s and shortest distances from vertex s to all other vertices.

B. Planar graphs

Let $G = (V, E)$ be a planar graph. Every vertex v corresponds to some point on the plane with coordinates (x_v, y_v) . We assume that all the edges in considered planar graphs has nonintersection segments representation on the plane. All edges intersect only at endpoints.

- ▶ **B1.** Prove that for any planar graph $|E| < 3|V|$.

Further, we need Jordan's Theorem. You can use this theorem without proof.

Jordan's Theorem for polygons. Given the polygon, prove that this polygon divides the plane into an "interior" region bounded by the polygon and an "exterior" region containing all of the nearby and far away exterior points.

Consider a point H that does not belong to any edge or the vertices of the planar graph G . *The winding angle* $\omega(AB)$ for given edge AB around the point H is a signed angle AHB ($-\pi < \omega(AB) < \pi$). For any walk $w = e_1 e_2 \dots e_m$ ($e_i \in E$), *the winding angle* is a sum $\omega(e_1) + \omega(e_2) + \dots + \omega(e_m)$.

- ▶ **B2.** Prove that for any closed walk $v_1 v_2 v_3 \dots v_m v_1$ ($v_i \in V$), the winding angle around the point H is equal to $2\pi n$ (n is some integer). n is *the winding index* of the walk around H .

Fix some vertex s in the planar graph G . Further we will only consider walks that start in s . Let us call them s -walks. s -loop is a closed s -walk.

- ▶ **B3.** Consider a s -loop of winding index $n > 1$ around point H . Prove that there is a s -loop of winding index $n - 1$ around H .

C. Shortest closed walks around single point

In the sequel, we shall focus on the problem of the shortest closed walk of non-zero winding number with some source vertex s under different following conditions:

1. The number of points we want to enclose by loop: single point H or two points H_1, H_2
2. Directed or undirected graphs

3. Polynomial algorithms or fast $O(V \log V)$ algorithms.
4. Finding the shortest walks with non-zero winding index or finding the shortest walks with fixed winding index.

Given a weighted digraph $G = (V, E)$ embedded in the plane P , let H be a point of the plane P , let $s \in V$ be a source vertex. We want to find a shortest closed walk $s \rightsquigarrow s$ with a given winding number $n \neq 0$, $n \in \mathbb{Z}$, around H .

- **C1.** Consider an undirected graph. Find a shortest closed s -walk with nonzero index using $O(V \log V)$ operations.
- **C2.** Consider a directed graph. Find a shortest closed s -walk with nonzero index using $O(V \log V)$ operations.
- **C3.** Consider an undirected graph. Given index $k < 100$, find a shortest closed s -walk using $O(V \log V)$ operations.
- **C4.** Consider a directed graph. Describe a polynomial algorithm that finds a shortest closed s -walk with given index $k < 100$.
- **C5.** Consider a directed graph. Describe an $O(V \log V)$ algorithm that finds a shortest closed s -walk with given index $k < 100$.

D. Shortest walks around two points

Consider two points H_1 and H_2 . The walks around these points have two winding angles and two indices. Recall we have a source vertex s . In the following problems we want to find closed walks with specified properties.

- **D1.** Consider an undirected graph. Given indices $k < 100$, $n < 100$, find a shortest closed s -walk using $O(V \log V)$ operations.
- **D2.** Consider a directed graph. Given indices $k < 100$, $n < 100$, describe a polynomial algorithm that finds a shortest closed s -walk.
- **D3.** Consider a directed graph. Given indices $k < 100$, $n < 100$, describe an $O(V \log V)$ algorithm that finds a shortest closed s -walk.

E. Shortest walks without source vertex

Now we have no source vertex. So we want to find a shortest closed walk.

A *lattice graph*, *mesh graph*, or *grid graph* is the graph whose vertices correspond to the points in the plane with integer coordinates ($x = 1, \dots, n$; $y = 1, \dots, m$) and two vertices are connected by an edge whenever the corresponding points are at distance 1. In directed graphs case, these two vertices are connected by two edges in both directions. The weights are probably asymmetric.

- **E1.** Is there exist an $O(V^{\frac{3}{2}} \log V)$ -algorithm that searches for a shortest closed walk around H in directed lattice graph?
- **E2.** Try to find an $O(V \log V)$ -algorithm that searches for a shortest closed walk around H in directed lattice graph.
- **E3.** Try to find an $O(V^{\frac{3}{2}} \log V)$ -algorithm that searches for a shortest closed walk around H in directed planar graph.

Shortest enclosing walks with a non-zero winding number in directed weighted planar graphs: a technique for image segmentation

Alexey Malistov

ELVEES-NeoTek, Russia,
alexey@malistov.ru

Abstract. This paper presents an efficient graph-based image segmentation algorithm based on finding the shortest closed directed walks surrounding a given point in the image. Our work is motivated by the Intelligent Scissors algorithm, which finds open contours using the shortest-path algorithm, and the Corridor Scissors algorithm, which is able to find closed contours. Both of these algorithms focus on undirected, non-negatively weighted graphs. We generalize these results to directed planar graphs (not necessary with nonnegative weights), which allows our approach to utilize knowledge of the object's appearance. The running time of our algorithm is approximately the same as that of a standard shortest-path algorithm.

1 Introduction

The shortest-paths algorithms are among the most widely used methods for image segmentation [1]. These methods have many applications in the field of medicine [2], optical character recognition systems [3], etc. The shortest-path segmentation is a so-called graph-based method. All graph-based methods represent the image as a weighted graph $G = (V, E)$, where each vertex $v \in V$ corresponds to a pixel in the image, the edges connect neighboring pixels [4]. Weights of the edges depend on the properties of the pixels, for instance, their intensities.

Mortensen and Barret [1] in 1995 was one of the first to present a new segmentation tool known as *Intelligent Scissors*. Their algorithm finds an optimal path from a start pixel to a goal pixel, where each pixel corresponds to a vertex in the graph G . Intelligent Scissors assign weights to edges according to the image gradient: the greater the image gradient, the lower the weight of the edge.

The shortest path from a start pixel s to the same pixel s is trivial. The shortest closed path surrounding a given point H can be considered as a natural generalization of a shortest-paths problem. The shortest closed paths are used as an image segmentation technique in [5–7]. In [5], a new segmentation tool *Corridor Scissors* is presented. Their tool searches for a shortest closed path inside of the corridor marked by a user. The corridor is considered as a ring-shaped graph. This ring-shaped graph is transformed into a lane-shaped graph

by cutting along the shortest cut-path. In [7], a similar technique is used for image composition.

Previous works on closed paths are only focused on undirected, nonnegatively weighted graphs. In this paper we generalize these results. We give a direct algorithm for the shortest closed walks with the non-zero winding number n around a given point of the plane. Our algorithm applies to directed graphs with no negative-weight cycles. Any corridor can be emulated by removing vertices and edges outside the corridor. This generalization allows the algorithm to utilize knowledge of the objects appearance. Negative weights can be used to point a set of mandatory edges for the required walks. Directed graphs can use different weights for different directions, which makes it possible to find inner and outer contours (see fig. 1).

In fact, if the graph is undirected and the source vertex s is fixed, then no cut-path is needed. In [8], Provan found a simple algorithm for the shortest enclosing walk in undirected graphs. The thing is that the shortest enclosing walk can be easily produced from the shortest-paths tree. To find the shortest-paths tree Provan uses Dijkstra's algorithm [9]. The implementation of Fredman and Tarjan [10] has a running time $O(E + V \log V)$. For the square grid, where $|E| = O(V)$, we obtain $O(V \log V)$. To date, there is an algorithm of the running time $O(V)$ for single-source shortest paths in planar graphs with nonnegative weights [11]. The shortest path in directed planar graphs with negative weights can be found in $O(V \log^2 V)$ time [12].

We recall that directed graphs can be useful to enclose an object if we know a priori color models of the object and background. Object always lies to the left of counterclockwise enclosing contour. Suppose that all pixels have integer coordinates. Let us shift each node in the above graph by $(0.5, 0.5)$. Then each node and each edge will lie between pixels. This approach is used in [2]. Let O be an object segmented by the shortest closed walk p around the point $H \in O$. Whenever the walk p travels counterclockwise around the point H , pixels of the object O lie immediately to the left of p , in the traversal. Suppose e is an edge, e' is e given in reverse direction. Let ℓ be a pixel that lies immediately to the left of e (to the right of e'), r be a pixel that lies immediately to the right of e (to the left of e'). If the closed walk p contains e , then ℓ is inside of the object O . If the closed walk p contains e' , then r is inside of the object O . To distinguish this we must have $w(e) \neq w(e')$ (see fig. 1). Thus, we obtain a directed graph.

2 Shortest Enclosing Walks in Directed Graphs

2.1 Background

Let $G = (V, E)$ be a weighted, directed graph with weight function $w: E \rightarrow \mathbb{R}$. Suppose $s, t \in G$. By $s \rightsquigarrow t$ denote an arbitrary walk from s to t . A closed walk is a walk such that its first and last vertices are the same. The weight $w(p)$ of walk p is the sum of the weights of the edges of p . Sometimes the word *length* is used instead of weight. But we reserve *length* for the number of edges in the

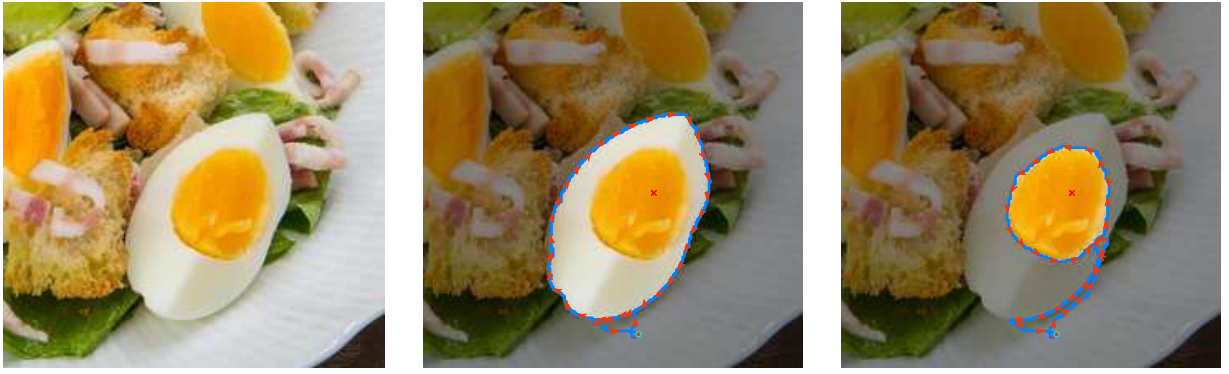


Fig. 1. Shortest enclosing directed walks: left) original image; center) the shortest clockwise walk (winding number = -1); right) the shortest counterclockwise walk (winding number = $+1$). Note that the clockwise walk finds the outer contour of the egg, while the counterclockwise walk find the inner contour (that of the yoke).

walk. In the sequel, only walks of finite length are considered. A shortest walk from vertex s to vertex t is any walk $s \rightsquigarrow t$ with minimal weight. Shortest walks are well defined if and only if the graph G contains no negative-weight cycles. It follows that if the graph is undirected, all weights are non-negative. In the sequel, only graphs without negative-weight cycles are considered. Any shortest walk cannot contain a positive-weight cycle. This cycle can be removed to create a walk with a lower weight. We can also remove 0-weight cycles to create a walk with the same weight. Without loss of generality we can assume that all shortest walks have no cycles. Thus all shortest walks are simple paths. In particular, the shortest path from s to s is the path that contains no edges.

For any vertex s there is a *shortest-paths tree* $T_s = (V_s, E_s)$ such that 1) T_s is a subgraph of G , 2) s is the root of T_s , 3) V_s contains vertices reachable from s , 4) for all $v \in V_s$, the path from root s to v in T_s is the shortest path from s to v in G .

Suppose G has a fixed planar embedding in the plane $P = \mathbb{R}^2$ and this embedding is given by some map $f: V \rightarrow P$. All edges intersect only at endpoints. By (x_v, y_v) we denote the coordinates of vertex v . Suppose that the plane P has a distinguished point H . We will assume that no edge intersects H . In the converse case, remove all those edges. To each pair (u, v) , where $u, v \in V$, assign the directed angle $\theta(u, v) = \angle UHV$ where $U = f(u)$, $V = f(v)$. We have $-2\pi < \theta(u, v) \leq 2\pi$ and $\theta(v, u) = -\theta(u, v)$. Suppose $e \in E$ is an edge of G . By definition, put $\alpha(e) = \theta(u, v)$. A *winding angle* of walk $\alpha(p)$ is the sum of the angles $\alpha(e)$ of the edges of p .

Suppose $s, t \in V$; then it is not hard to prove that for any walk $s \rightsquigarrow t$ there exists a unique $n \in \mathbb{Z}$ such that $\alpha(s \rightsquigarrow t) = \theta(s, t) + 2\pi n$. To do this, one can use the polar coordinate system with the origin at H . In particular, for any closed walk $s \rightsquigarrow s$ we get

$$\alpha(s \rightsquigarrow s) = 2\pi n, \quad n \in \mathbb{Z} . \quad (1)$$

$r(p) = \alpha(p)/2\pi$ is called the *winding number* of walk p . It follows from (1) that the winding number of a closed walk is always integer. If the shortest-paths tree

T_s is fixed, then for all $v \in V_s$ there exists a unique path $q = s \rightsquigarrow v$ in T_s . By $\beta(s, v)$ we denote the winding angle of q .

We recall that the shortest closed walk is a zero-length path. But the shortest closed walk with non-zero winding number is nontrivial. In the sequel, we shall focus on the problem of the shortest closed walk of non-zero winding number. Given a weighted digraph $G = (V, E)$ embedded in the plane P , let H be a point of the plane P , let $s \in V$ be a source vertex. We want to find a shortest closed walk $s \rightsquigarrow s$ with a given winding number $n \neq 0$, $n \in \mathbb{Z}$, around H .

2.2 Undirected Graphs

Let p^{-1} be a walk p given in reverse direction. If G is undirected graph, then we obtain $w(p^{-1}) = w(p)$. It follows that there exist a shortest closed walk of winding number $+n$ if and only if there exists a shortest closed walk of winding number $-n$. Moreover, the weights of these walks are the same. In the next subsection we will show that the shortest closed walk with non-zero winding number has winding number ± 1 (see Theorem 5).

Provan [8] gave the first algorithm for finding nontrivial walks in undirected, nonnegatively weighted graphs with a fixed (not necessarily planar) embedding in the plane. His algorithm finds a shortest closed walk surrounding a given obstacle O in the plane. This shortest walk has non-zero winding number. But we cannot choose an arbitrary winding number n .

Provan considers a plane embedding that is not necessarily planar. For planar graphs, Provan's algorithm gives a closed walk of winding number ± 1 .

2.3 Directed Graphs

For directed graphs, $w(p^{-1})$ is not necessarily equal to $w(p)$. Moreover, the shortest closed walk with winding number $+1$ and the shortest closed walk with winding number -1 may be distinct.

Consider a point $F = (x, y, z) \in \mathbb{R}^3$. By definition, put $x(F) = x$, $y(F) = y$, $z(F) = z$. Fix the source vertex s . Take a vertex $v \in V$. Let \mathcal{H}_v be a set given by

$$\mathcal{H}_v = \{h \in \mathbb{R}^3 \mid x(h) = x_v, y(h) = y_v, z(h) = \theta(s, v) + 2\pi n, n \in \mathbb{Z}\} .$$

For example, since $\theta(s, s) = 0$, it follows that $\mathcal{H}_s = \{(x_s, y_s, 2\pi n) \mid n \in \mathbb{Z}\}$. Put $\mathcal{V} = \bigcup_{v \in V} \mathcal{H}_v$. Let g be the map from \mathcal{V} to V taking $h \in \mathcal{H}_v$ to v . Consider a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where

$$\mathcal{E} = \{(h_1, h_2) \mid h_1, h_2 \in \mathcal{V}, (g(h_1), g(h_2)) \in E, z(v) = z(u) + \theta(g(h_1), g(h_2))\} .$$

For each edge $(h_1, h_2) \in \mathcal{E}$, we have a weight $w(h_1, h_2) = w(g(h_1), g(h_2))$. The graph \mathcal{G} can be embedded in the helicoid (see fig. 2). Consider $S = (x_s, y_s, 0) \in \mathcal{H}_s \subset \mathcal{V}$, where $s \in V$ is the fixed source vertex in G . Clearly, $g(S) = s$. If we take another source vertex s_2 , then we get another graph \mathcal{G}_2 . To simplify the notation we write \mathcal{G} instead of \mathcal{G}_s . In the sequel, s is fixed.

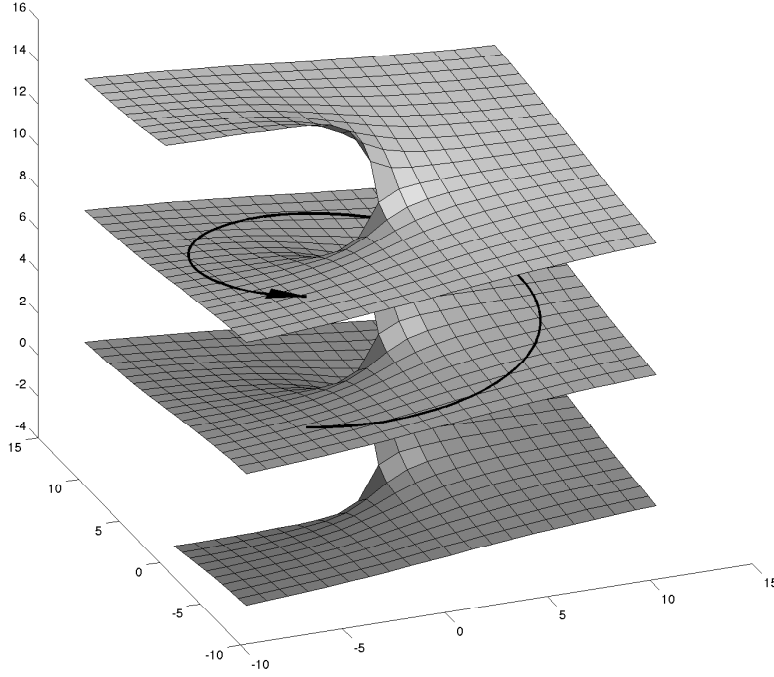


Fig. 2. Helicoid graph.

Lemma 1. *Let W_s be a set of walks from s in the graph G , W_S be a set of walks from S in the graph \mathcal{G} . Then W_s is isomorphic to W_S with respect to weight.*

Proof. Let $p = \langle sv_1 \dots v_\ell \rangle$ be a walk in G . Consider the path $P = \langle SV_1 \dots V_\ell \rangle$ in the graph \mathcal{G} , where $V_i = (x_{v_i}, y_{v_i}, \alpha(sv_1 v_2 \dots v_i))$, $\alpha(sv_1 v_2 \dots v_i)$ is the winding angle of the subwalk $s \rightsquigarrow v_i$. Since $\alpha(sv_1 \dots v_i v_{i+1}) - \alpha(sv_1 \dots v_i) = \theta(v_i, v_{i+1})$, we get $(V_i, V_{i+1}) \in \mathcal{E}$ and $w(V_i, V_{i+1}) = w(v_i, v_{i+1})$. It follows that $w(P) = w(p)$.

Now let $P = \langle SV_1 V_2 \dots V_\ell \rangle$ be a walk in \mathcal{G} . Similarly, consider the walk $p = \langle sv_1 v_2 \dots v_\ell \rangle$, where $v_i = g(V_i)$. The walk p corresponds to P and has the same weight. This completes the proof of Lemma 1. \square

Let I be the isomorphism from Lemma 1, W_s^n be the set of all closed walks in G from s with winding number $n \neq 0$ around H . Then $I(W_s^n)$ is the set of all open walks in \mathcal{G} from $S = (x_s, y_s, 0)$ to $S_n = (x_s, y_s, 2\pi n)$. Thus, the shortest closed walk problem in graph G is equivalent to the shortest path problem in graph \mathcal{G} . No well-known algorithm can be started because the graph \mathcal{G} is infinite. Our aim is to find some subgraph \mathcal{G}' of \mathcal{G} that is finite. Then we can use any well-known shortest-path algorithm.

The first approach is to remove all vertices $h \in \mathcal{V}$ such that $|z(h)| < 4\pi|V|$. This is a good idea because the walks of a length more than $2|V|$ are not very useful. The shortcoming of this method is that the number of vertices in \mathcal{G} is $|\mathcal{V}| = \Theta(|V|^2)$. This method is not optimal. We will show that there is a better way to find a finite subgraph.

2.4 A Finite Subgraph of \mathcal{G}

We recall that $\beta(s, v)$ is the winding angle of the unique path q in the shortest-paths tree T_s . For each vertex $v \in G$ there exists a unique vertex $h \in \mathcal{V}$ such that $h = (x_v, y_v, \beta(s, v))$. Now we shall give the following definitions.

Definition 1. *Suppose $v \in V$. Then the vertex $(x_v, y_v, \beta(s, v)) \in \mathcal{V}$ is called the shortest representative of v in the helicoid graph \mathcal{G} with respect to the source vertex s .*

Since s is fixed, “with respect to the source vertex s ” will be omitted.

Definition 2. *We say that the vertex $h = (x_v, y_v, z) \in \mathcal{V}$ has a tier m and write $\text{tier}(h) = m$ if $z = \beta(s, v) + 2\pi m$, where $v = g(h) \in V$ is the corresponding vertex in G .*

Clearly, all shortest representatives in \mathcal{G} have the tier 0.

Theorem 1 (intermediate value). *For any walk $p = h_1 \rightsquigarrow h_2$ in \mathcal{G} the tier takes any value between $\text{tier}(h_1)$ and $\text{tier}(h_2)$ at some vertex of p .*

Proof. Let (u', v') be an edge of the walk p . Put $u = g(u')$, $v = g(v')$. Then $z(u') = \beta(s, u) + 2\pi \cdot \text{tier } u'$, $z(v') = \beta(s, v) + 2\pi \cdot \text{tier } v'$. We recall that $z(v') - z(u') = \theta(u, v)$. It follows that

$$\begin{aligned} z(v') - z(u') &= \theta(u, v) = \beta(s, v) - \beta(s, u) + 2\pi \cdot (\text{tier } v' - \text{tier } u'), \\ \text{tier } v' - \text{tier } u' &= \frac{\beta(s, u) + \theta(u, v) - \beta(s, v)}{2\pi} = r(s \rightsquigarrow u \rightarrow v \rightsquigarrow s), \end{aligned}$$

where $s \rightsquigarrow u \rightarrow v \rightsquigarrow s$ is the closed curve which contains the shortest path $s \rightsquigarrow u$, the edge $u \rightarrow v$, and the reverse of the shortest path $s \rightsquigarrow v$. This curve has no self-intersections because $s \rightsquigarrow u$ and $s \rightsquigarrow v$ are the paths in the tree T_s . Thus, the winding number $r(s \rightsquigarrow u \rightarrow v \rightsquigarrow s) \in \{0, \pm 1\}$. It follows that either the tiers of the neighboring vertices u' , v' are the same or $\text{tier}(v') - \text{tier}(u') = \pm 1$.

Theorem 2 (tiers). *Suppose $h \in \mathcal{V}$, $\text{tier}(h) \geq 0$. Then there exists a shortest path p from S to h such that for any vertex u of p we have $\text{tier}(u) \geq 0$.*

Proof. For $\text{tier}(h) = 0$, by definition (2), the shortest paths induced by the shortest-paths tree T_s contain only vertices of the tier 0. For $\text{tier}(h) > 0$, assume the converse. Then some shortest path $\langle S \dots u \dots h \rangle$ contains u such that $\text{tier}(u) < 0$. By Theorem 1, there exists a vertex v between u and h such that $\text{tier}(v) = 0$. Replace $\langle S \dots u \dots v \rangle$ with the shortest path $S \rightsquigarrow v$ that contains only vertices with the tier 0. Repeating this operation we obtain the shortest path p from S to h such that for any vertex u of p we have $\text{tier}(u) \geq 0$. This contradiction proves the theorem. \square

Similarly, there exists a shortest path p from the vertex S to a vertex $h \in \mathcal{V}$, $\text{tier}(h) \leq 0$, such that for any vertex u of p we have $\text{tier}(u) \leq 0$.

Corollary 1. *If we want to find a shortest closed walk with the winding number $n > 0$, then any vertex h with $\text{tier}(h) < 0$ can be removed. If we want to find a shortest closed walk with the winding number $n < 0$, then any vertex h with $\text{tier}(h) > 0$ can be removed.*

Consider a vertex $v \in V$ in the input graph and the corresponding set of vertices $\mathcal{H}_v \subset \mathcal{V}$ in the graph \mathcal{G} . We can sort all vertices of \mathcal{H}_v by their shortest distance from S . Evidently, the shortest of the shortest paths from the vertex S to the set \mathcal{H}_v is the path to a vertex $h \in \mathcal{H}_v$ such that $\text{tier}(h) = 0$.

Definition 3. *For $R \geq 0$, we shall say that a vertex $h \in \mathcal{H}_v$ has a rank R and write $\text{rank}(h) = R$ if the shortest distance from S to h is the $(R+1)$ -th minimum of the shortest distances from S to the set \mathcal{H}_v .*

Theorem 3 (ranks). *Suppose $h \in \mathcal{V}$. Then there exists a shortest path p from S to h such that for any vertex u of p it follows that $\text{rank}(u) \leq \text{rank}(h)$.*

Proof. Assume the converse. Then some shortest path $p = \langle S \dots u \dots h \rangle$ contains u such that $\text{rank}(u) > R$, where $R = \text{rank}(h)$. Consider a set $U = \{u_k\}_{k=0}^R$ such that $u_k \in \mathcal{V}$, $\text{rank}(u_k) = k$, and $g(u_k) = g(u)$. We can replace $\langle S \dots u \rangle$ with $S \rightsquigarrow u_k$. Then there exist $R+1$ walks $\langle S \dots u_k \dots \rangle_{k=0}^R$ with a lower weight. All end nodes h_k are distinct because $\forall i \neq j \text{ tier}(h_i) \neq \text{tier}(h_j)$. Since $\forall k \text{ tier}(u_k) \neq \text{tier}(u)$, we get $\forall k \text{ tier}(h_k) \neq \text{tier}(h)$. We have that $w(p)$ is not the $(R+1)$ -th minimum of the shortest distances from S to $\mathcal{H}_{g(h)}$. This contradicts Definition 3. The theorem is proved. \square

Definition 4. *Suppose $\mathcal{H}_v^+ = \{h \in \mathcal{H}_v \mid \text{tier}(h) > 0\}$, $\mathcal{H}_v^- = \{h \in \mathcal{H}_v \mid \text{tier}(h) < 0\}$. We shall say that a vertex $h \in \mathcal{H}_v^+$ has a category $K > 0$ and write $\text{cat}(h) = K$ if the shortest distance from S to h is the K -th minimum of the shortest distances from S to the set \mathcal{H}_v^+ . We shall say that a vertex $h \in \mathcal{H}_v^-$ has a category $K < 0$ if the shortest distance from S to h is the $|K|$ -th minimum of the shortest distances from S to the set \mathcal{H}_v^- . If $\text{tier}(h) = 0$, we put $\text{cat}(h) = 0$.*

Using Theorem 2, Theorem 3 and Definition 4, we get the following theorem.

Theorem 4 (categories). *Suppose $h \in \mathcal{V}$. Then there exists a shortest path p from S to h such that for any vertex u of p it follows that $|\text{cat}(u)| \leq |\text{cat}(h)|$.*

Theorem 5 (Main). $\forall h \in \mathcal{V} \text{ tier}(h) = \text{cat}(h)$.

Proof. The cases $\text{cat}(h) \geq 0$ and $\text{cat}(h) \leq 0$ are equivalent. Without loss of generality it can be assumed that $k = \text{cat}(h) \geq 0$. The proof is by induction over k . For $k = 0$, there is nothing to prove. For $k > 0$, assume the converse. Then there exist $h \in \mathcal{V}$ such that $\text{cat}(h) = k$ and $\text{tier}(h) \neq k$. Let $h_m \in \mathcal{H}_{g(h)}^+$ be a vertex such that $\text{tier}(h_m) = m$. By the inductive assumption, $\forall m < k \text{ cat}(h_m) = \text{tier}(h_m) = m$. If $\text{tier}(h) < k$, then $\text{cat}(h) = \text{cat}(h_{\text{tier}(h)}) = \text{tier}(h)$. Thus, $\text{tier}(h) > k$. Consider the shortest path $p = S \rightsquigarrow h$. Also, consider the first vertex v in p such that $\text{tier}(v) > k$. Clearly, $\text{cat}(v) = k$. If $\text{cat}(v) < k$, then $\text{cat}(v) = \text{tier}(v)$. Let u be

the predecessor of v . By Theorem 4, $\text{cat}(u) \leq \text{cat}(h) = k$. If $\text{cat}(u) < k$, then $\text{tier}(u) = \text{cat}(u) < k$. Thus, $\text{tier}(v) - \text{tier}(u) \geq 2$. This contradicts Theorem 1. It follows that $\text{cat}(u) = \text{tier}(u) = k$ and $\text{tier}(v) = k + 1$. Let u_{k-1} be the vertex such that $\text{cat}(u_{k-1}) = k - 1$ and $g(u_{k-1}) = g(u)$. By the inductive assumption, $\text{tier}(u_{k-1}) = k - 1$. Replace the subpath $S \rightsquigarrow u$ with the shorter path $S \rightsquigarrow u_{k-1}$ ($\text{cat}(u_{k-1}) < \text{cat}(u)$). Then we obtain the shorter path from S to a new vertex v' such that $\text{tier}(v') = k$ and $g(v') = g(v)$. It follows that $\text{cat}(v') = k$ and $\text{cat}(v) \neq k$.

Corollary 2. *If we want to find a shortest closed walk with the winding number n , then any vertex h with $|\text{tier}(h)| > n$ can be removed.*

2.5 An Algorithm For Finding Shortest Enclosing Walks

Corollary 1 and corollary 2 give the following algorithm. Suppose s is the fixed source vertex, n is the winding number.

1. Find the shortest-paths tree T_s .
2. For all $u \in V$ calculate $\beta(s, u)$.
3. Create the finite subgraph $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ of \mathcal{G} such that $h \in \mathcal{V}'$ if and only if $\text{sign}(\text{tier}(h)) = \text{sign}(n)$, $|\text{tier}(h)| \leq n$, or $\text{tier}(h) = 0$.
4. Find the shortest path from $(x_s, y_s, 0)$ to $(x_s, y_s, 2\pi n)$ in \mathcal{G}' .

The running time of our algorithm is $O(nT)$, where T is the running time of the shortest-path algorithm in steps 1 and 4. In particular, for $n = 1$ the running time is $O(T)$.

3 Evaluation

Experimental results are presented in fig. 3. We put the center point H inside the object. Also we put the start point S somewhere outside object and run our algorithm looking for the shortest enclosing walk surrounding the point H . Note that the start point S can be placed far from enclosing object. We use some pictures from The Berkeley Segmentation Dataset [13].

Consider the picture with the bear. Note that the segmentation region is approximately the same for the different start points. Now consider the picture with flowers. We put the center point H inside the left flower. Start point are placed in the background. The shortest clockwise and counterclockwise walks are different. First one helps to find the inner contour inside the left flower. Second one helps to cut flowers.

The special line marked ‘‘Tier cut’’ in the pictures cuts the edges where the tier of the vertices changes. If edge intersects the tier-cut-line, then this edge has vertices with different tiers (see the proof of Theorem 1).

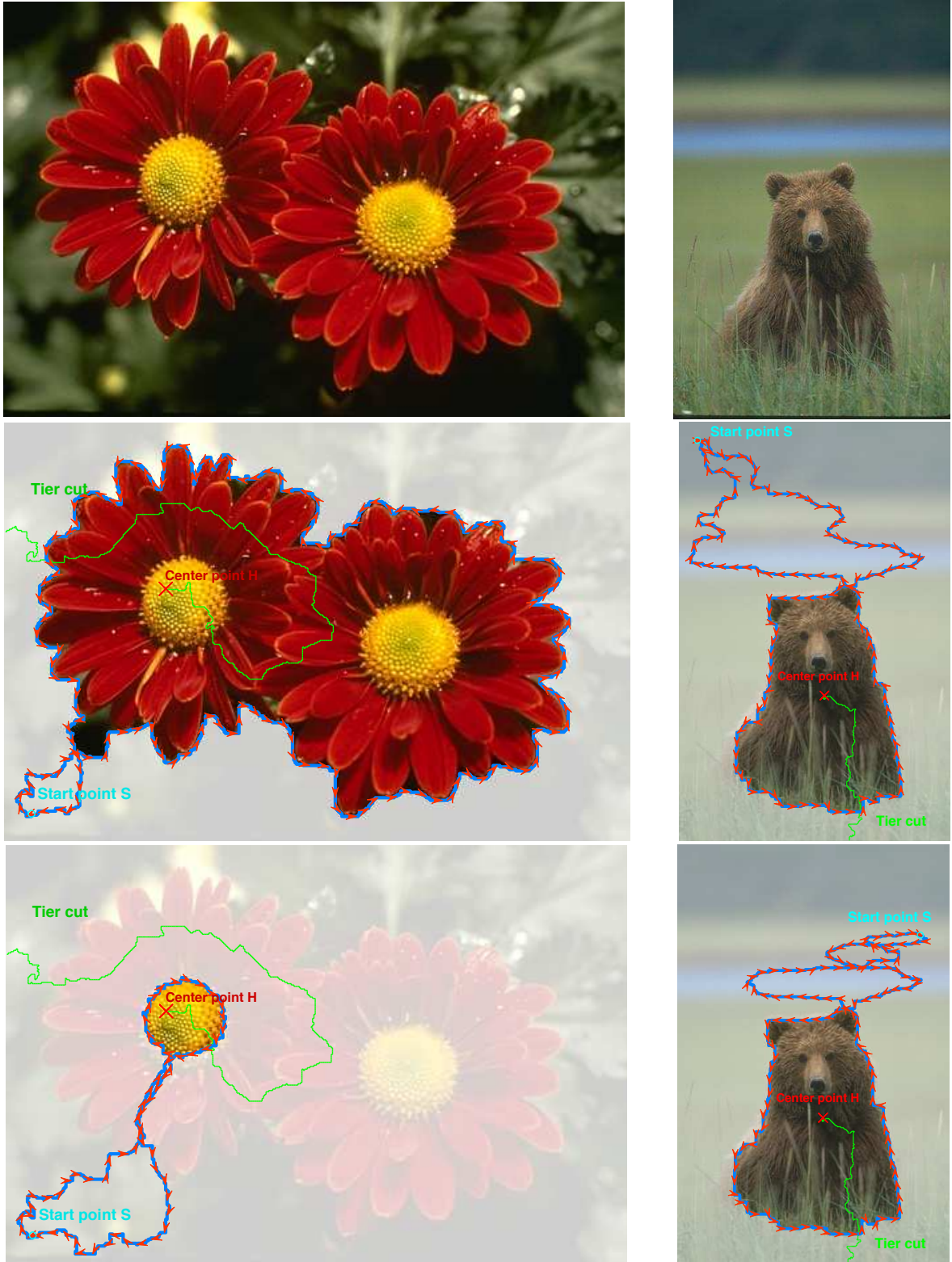


Fig. 3. Experimental results: original image and a segmentation based on the shortest enclosing walk (clockwise and counterclockwise). The center point H is inside the object considered. Note that the start point S is far from enclosing object. “Tier cut” is the line where tier changes (see the proof of Theorem 1). Pictures are from The Berkeley Segmentation Dataset [13].

4 Conclusion and future work

We have presented a new segmentation algorithm which is based on finding a shortest enclosing walk in the directed planar graphs. This walk surrounds a given point of the plane and has a given winding number $n \neq 0$. Our approach generalizes previous works which search for either open simple walks or closed walks in undirected graphs with nonnegative weights. The method runs in $O(nT)$ time, where T is the running time of a regular shortest-path algorithm. For $n = 1$, the running time is $O(T)$.

For future work, we plan to extend our approach to a number of points we want to surround. Also, we want to use an image pyramid representation to assign the weights of the edges according to the information about pixels that does not immediately lie to the left or to the right of closed walks.

References

1. Mortensen, E.N., Barrett, W.A.: Intelligent scissors for image composition. In: Proceedings of the 22nd Annual Conference on Computer Graphics and Interactive Techniques. SIGGRAPH '95, New York, NY, USA, ACM (1995) 191–198
2. Falcao, A., Udupa, J., Miyazawa, F.: An ultra-fast user-steered image segmentation paradigm: live wire on the fly. Medical Imaging, IEEE Transactions on **19** (2000)
3. Tse, J., Jones, C., Curtis, D., Yfantis, E.: An OCR-independent character segmentation using shortest-path in grayscale document images. Sixth International Conference on Machine Learning and Applications (ICMLA 2007) (2007) 142–147
4. Felzenszwalb, P.F., Huttenlocher, D.P.: Efficient graph-based image segmentation. Int. J. Comput. Vision **59** (2004) 167–181
5. Farin, D., Pfeffer, M., de With, P., Effelsberg, W.: Corridor scissors: a semi-automatic segmentation tool employing minimum-cost circular paths. In: Image Processing, 2004. ICIP '04. Intl. Conf. on. Volume 2. (2004) 1177–1180 Vol.2
6. Farin, D., N., P.H.: Shortest circular paths on planar graphs. In: In 27 th Symposium on Information Theory in the Benelux. (2006) 117–124
7. Jia, J., Sun, J., Tang, C.K., Shum, H.Y.: Drag-and-drop pasting. ACM SIGGRAPH (2006) 631
8. Provan, J.S.: Shortest enclosing walks and cycles in embedded graphs. Inf. Process. Lett. **30** (1989) 119–125
9. Dijkstra, E.: A note on two problems in connexion with graphs. Numerische mathematik (1959) 269–271
10. Fredman, M.L., Tarjan, R.E.: Fibonacci heaps and their uses in improved network optimization algorithms. J. ACM **34** (1987) 596–615
11. Klein, P., Rao, S., Rauch, M., Subramanian, S.: Faster shortest-path algorithms for planar graphs. In: Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing. STOC '94, New York, NY, USA, ACM (1994) 27–37
12. Klein, P.N., Mozes, S., Weimann, O.: Shortest paths in directed planar graphs with negative lengths: A linear-space $O(n \log^2 n)$ -time algorithm. ACM Trans. Algorithms **6** (2010) 30:1–30:18
13. Martin, D., Fowlkes, C., Tal, D., Malik, J.: A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics. In: 8th Int'l Conf. Computer Vision. Volume 2. (2001) 416–423

Какого цвета моя шляпа?

Задачу представляют:

Кохась К., Куюмжиян К., Челноков Г.

Следующая задача широко известна, но если вы ее еще не встречали, воспринимайте ее как вызов своему интеллекту. Эта задача будет разобрана после открытия конференции и не влияет на результаты конкурса. Речь идет об объекте, который имеет всего 4 состояния! Итак,

ИНТЕЛЛЕКТУАЛЬНЫЙ ВЫЗОВ: число 4 против миллиардов нейронов вашего мозга!

Вам и мне надевают на голову шляпу. Каждая из шляп может быть черной или белой. Вы видите мою шляпу, я — вашу, но никто из нас не видит при этом своей шляпы. Каждый из нас (не подглядывая, не общаясь и не подавая друг другу никаких сигналов) должен попытаться угадать цвет своей шляпы. Для этого по команде одновременно каждый из нас должен назвать цвет — «черный» или «белый». Если хоть один из нас угадал — мы выиграли. Перед тем как все это произойдет, нам дали возможность посоветоваться. Как нам следует действовать, чтобы в любой ситуации выиграть?

1 Несколько задач о мудрецах

Есть несколько мудрецов и большой запас шляп k различных цветов. С мудрецами проводят следующий ТЕСТ. Ведущий надевает мудрецам шляпы так, что в результате каждый видит шляпы всех остальных мудрецов, но не видит своей шляпы и не знает ее цвета. Мудрецы не общаются. По команде ведущего мудрецы одновременно называют цвет. Считается, что мудрецы успешно прошли тест = «выиграли», если хотя бы один из них угадал.

Перед тестом мудрецам сообщили правила теста и дали возможность устроить СОВЕЩАНИЕ, чтобы они могли договориться о том, как действовать во время теста. Стратегия мудрецов должна быть детерминированной — каждый мудрец должен назвать цвет, исходя только из того, какие цвета он видит у остальных.

- 1.1. Есть n мудрецов и шляпы n цветов. Докажите, что в этой ситуации мудрецы выигрывают.
- 1.2. Пусть имеются шляпы трех цветов и n мудрецов стоят в шеренгу так, что каждый видит лишь соседей (а крайние — одного соседа). Докажите, что в этой ситуации мудрецы проигрывают.
 - a) $n = 3$;
 - b) $n = 4$;
 - c) n — произвольное.
- 1.3. Есть $10k$ мудрецов и шляпы k цветов (опять все видят всех). Докажите, что 10 мудрецов заведомо смогут угадать свой цвет, а вот 11 — вообще говоря, нет.
- 1.4. Есть $4k - 1$ мудрецов, $2k$ черных и $2k$ белых шляп. Ведущий незаметно прячет одну шляпу, а остальные надевает на мудрецов. Какое наибольшее число мудрецов смогут угадать цвет своей шляпы?
- 1.5. Четыре мудреца стоят по кругу возле непрозрачного баобаба, у них шляпы трех цветов. Каждый мудрец видит только двух соседних по кругу мудрецов. Как им действовать, чтобы выиграть?
- 1.6. У трех мудрецов шляпы двух цветов. Пусть теперь мудрецам разрешается пасовать, т. е. сказать «пас», что означает отказ от угадывания. Пусть мудрецы выигрывают, только при условии, что хотя бы один из них угадал правильно, и при этом никто не угадал неправильно. Будем считать, что все расклады шляп равновероятны и что стратегия мудрецов, как и в предыдущих задачах, детерминированная. Теперь уже мудрецы заведомо не могут обеспечить себе стопроцентный выигрыш. Например стратегия «Мудрец А всегда говорит “черный”, остальные всегда говорят “пас»» выигрывает лишь в половине случаев. Оптимальная стратегия — это стратегии, которая для всевозможных раскладов шляп дает наибольшее число выигрышей.
 - a) Предложите стратегию мудрецов, для которой они выигрывают больше чем в 50 % случаев.
 - b) Найдите оптимальную стратегию и докажите, что она оптимальна.

2 Мудрецы на неориентированном графе

Будем рассматривать более общую задачу. Пусть дан неориентированный граф G , в каждой вершине которого находится один мудрец. Мудрецы знакомы друг с другом и расположение мудрецов по вершинам известно всем. В частности, каждый мудрец понимает, в какой вершине находится каждый из его соседей. Мы будем отождествлять вершину графа и мудреца, который в ней находится. Во время теста каждый мудрец видит только шляпы мудрецов, находящиеся в соседних вершинах графа. Остальные правила те же самые — мудрецы должны на совещании выработать стратегию, позволяющую хотя бы одному из них угадать цвет своей шляпы.

При необходимости можно пользоваться следующим формализмом. Пусть цвета шляп пронумерованы числами от 1 до k , пусть $\mathcal{C} = \{1, 2, \dots, k\}$, и пусть у каждой вершины v графа G соседние вершины (пусть d — их количество) упорядочены по возрастанию номеров $u_{n_1}, u_{n_2}, \dots, u_{n_d}$. Стратегия мудреца v — это функция $f_v: \underbrace{\mathcal{C} \times \mathcal{C} \times \dots \times \mathcal{C}}_{d \text{ раз}} \rightarrow \mathcal{C}$. Эти функции выбираются мудрецами на совещании. Действия мудрецов

по угадыванию состоят в том, что каждый мудрец v вычисляет $f_v(c_1, c_2, \dots, c_d)$, где $c_i \in \mathcal{C}$ — цвет шляпы мудреца в вершине u_{n_i} .

Задача 1.1 показывает, что если мудрецы находятся в вершинах графа и могут видеть только соседних мудрецов, то в случае, когда граф имеет k -клик, хотя бы один мудрец сможет угадать свою шляпу. Вопрос становится нетривиальным, если граф не имеет k -клик.

2.1. Докажите, что на четырехвершинном графе «куриная лапа» мудрецы проигрывают ($k \geq 3$).

2.2. Докажите, что на любом дереве мудрецы проигрывают ($k \geq 3$).

Пусть n мудрецов стоят по кругу, $k = 3$. Пусть V — множество из трех элементов (цветов шляп). Пусть $V_i = V$ — множество цветов шляп, которые можно дать i -му мудрецу. Допустим, что мудрецы уже определились со стратегией. Это значит, что i -й мудрец выбрал себе функцию $f_i: V_{i-1} \times V_{i+1} \rightarrow V_i$ (всюду нумерация циклическая). Будем говорить, что последовательность цветов abc , где $a \in V_{i-1}$, $b \in V_i$, $c \in V_{i+1}$, является короткой *опровергающей цепочкой*, если $b \neq f_i(a, c)$. Более длинная цепочка цветов $S = s_1 s_2 \dots s_m$, где $s_1 \in V_\ell$, $s_2 \in V_{\ell+1}$, \dots , $s_m \in V_{\ell+m-1}$, называется опровергающей цепочкой, если каждый ее трехэлементный фрагмент является короткой опровергающей цепочкой. Если выбрана опровергающая цепочка S обозначим $\ell_+(S)$ — число способов продолжить S на один шаг вправо, т. е. число способов выбрать цвет $s_{m+1} \in V_{\ell+m}$, чтобы получилась более длинная опровергающая цепочка. Аналогично обозначим через $\ell_-(S)$ число способов продолжить S на один шаг влево.

2.3. Пусть n мудрецов стоят по кругу, $k = 3$. Докажите, что если нашлась опровергающая цепочка $S = s_1 s_2 \dots s_m$, где $2 \leq m \leq n - 1$, для которой $\ell_-(s_1 s_2) + \ell_+(s_{m-1} s_m) \geq 5$, то стратегия мудрецов не выигрышная.

2.4. Пусть n мудрецов стоят по кругу, $k = 3$. Пусть мудрецы выбрали выигрышную стратегию. Докажите, что для любого мудреца i и любой пары цветов $a \in V_{i-1}$, $b \in V_i$ выполнено равенство $\ell_-(ab) + \ell_+(ab) = 4$.

2.5. Докажите, что при $k = 3$ на графе «цикл из $3n$ звеньев» мудрецы выигрывают.

2.6. Докажите, что при $k = 3$ на графе «цикл из n звеньев» мудрецы проигрывают, если n не делится на 3 и $n \neq 4$.

Следующие задачи показывают, что для выигрыша мудрецов наличие больших клик в графе не является необходимым.

2.7. Докажите, что любого числа цветов k существует двудольный граф, на котором мудрецы выигрывают.

2.8. Пусть G — граф, на котором мудрецы выигрывают, имея шляпы q цветов. Пусть K_r — полный граф на r вершинах (на нем, как мы знаем, мудрецы выигрывают, имея шляпы r цветов). Построим на основе G новый «большой» граф \tilde{G} . Для этого каждую вершину графа G заменим на копию

графа K_r . Если две вершины графа G были соединены ребром, проведем ребра между всеми парами вершин соответствующих копий. Полученный граф и есть граф \tilde{G} .

Докажите, что на графе \tilde{G} мудрецы выигрывают при $k = qr$.

2.9. Если $k = 3m$, то существует граф с $4m$ вершинами и максимальной кликой не более $2m$, на котором мудрецы выигрывают.

3 Мудрецы на ориентированном графе

Теперь будем считать, что мудрецы находятся в вершинах ориентированного графа, мудрец А видит мудреца Б, только если в графе есть ориентированное ребро АВ.

3.1. Докажите, что на графе «ориентированный цикл из n звеньев» мудрецы выигрывают ($k = 2$).

3.2. Мудрецы сидят в вершинах ориентированного графа, каждый видит только соседних, шляпы двух цветов. Пусть c — наибольшее количество вершинно независимых циклов в графе. Докажите, что существуют графы, для которых больше c мудрецов смогут угадать свой цвет ($k = 2$).

3.3. Пусть a — наименьшее число вершин, которое следует удалить из графа, чтобы он стал ациклическим. Докажите, что вообще говоря, не более a мудрецов смогут угадать цвет ($k = 2$).

3.4. Назовем ориентированный граф G *полудвудольным*, если множество его вершин можно разбить на две части L и R так, что между вершинами части L нет ребер, между вершинами части R могут быть ребра, но соответствующий граф — ациклический, а между частями L и R могут быть произвольные ребра.

Пусть k — по прежнему число шляп, s — произвольное натуральное число. Докажите, что если на полудвудольном графе $|L| = k - 2$, $|R| = s$, то мудрецы проигрывают.

Добавление после промежуточного финиша

Вариации предыдущих сюжетов

2.10. Три мудреца А, В, С, все видят друг друга, за исключением того, что мудрец А не видит мудреца В; $k = 3$. Докажите, что мудрецы проигрывают.

2.11. Четыре мудреца стоят по кругу возле непрозрачного баобаба, у них шляпы трех цветов. Каждый мудрец видит только двух соседних по кругу мудрецов, за исключением одного мудреца, который видит лишь одного соседа. Смогут ли мудрецы выиграть?

Пусть n мудрецов стоят по кругу, $k = 3$. Пусть мудрецы выбрали выигрышную стратегию. Будем называть пару цветов ab , где $a \in V_i$, $b \in V_{i+1}$, *левой*, если выполнено равенство $\ell_-(ab) = 1$, *правой*, если выполнено равенство $\ell_-(ab) = 3$, и *инертной*, если выполнено равенство $\ell_-(ab) = 2$.

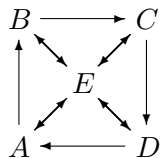
2.12. Докажите, что среди пар ab , где $a \in V_i$, $b \in V_{i+1}$, поровну левых и правых.

2.13. Пусть $n \geq 4$. Докажите, что если ab — правая пара цветов, где $a \in V_i$, $b \in V_{i+1}$, то среди пар цветов c_1a , c_2a , c_3a , где $\{c_1, c_2, c_3\} = V_{i-1}$, ровно одна левая пара цветов, ровно одна правая и ровно одна инертная.

2.14. То же, что в задаче 1.4, но есть $mk - 1$ мудрецов и шляпы k цветов — по m шляп каждого цвета, причем m четно или k нечетно (или и то, и другое одновременно). Одну шляпу незаметно прячут. Докажите, что наибольшее число мудрецов, которые смогут заведомо угадать свой цвет, равно $\frac{1}{2}(mk + m - 2)$.

2.15. Мудрецы стоят в две шеренги: в первой шеренге n мудрецов, а во второй — n^n мудрецов, у них шляпы $(n + 1)$ цветов. Мудрецы видят только тех, кто стоит в другой шеренге. Докажите, что мудрецы могут действовать так, чтобы хотя бы один угадал.

3.5. Какое наибольшее число мудрецов сумеют угадать цвет на следующем графе ($k = 2$)?



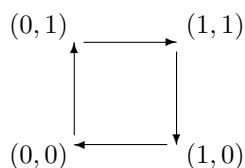
4 Гиперкуб.

Под n -мерным гиперкубом мы понимаем граф, вершины которого занумерованы наборами из n нулей и единиц. Ребрами соединены вершины, номера которых отличаются ровно в одном разряде.

4.1. Докажите алгебраически, что 32 мудреца, стоящие в вершинах пятимерного гиперкуба, выигрывают ($k = 3$).

Пусть количество мудрецов равно n , а $k = 2$, причем цвета шляп мы будем обозначать нулями или единицами. Пусть фиксирована какая-либо стратегия мудрецов. Рассмотрим n -мерный гиперкуб и с его помощью «закодируем» эту стратегию. Это делается следующим образом. Вершины гиперкуба соответствуют наборам из n нулей и единиц, свяжем с i -м мудрецом i -й элемент этого набора. Пусть i -й мудрец (для примера возьмем $n = 5$, $i = 2$) видит цвета шляп других мудрецов, скажем, 1, *, 0, 1, 1 (в качестве второго элемента мы поставили звездочку, которая символизирует, что в нашем примере i -й, т.е. второй мудрец не видит своей шляпы). В гиперкубе есть две вершины с таким набором координат: $(1, 0, 0, 1, 1)$ и $(1, 1, 0, 1, 1)$, причем эти вершины соединены ребром. Стратегия i -го мудреца, собственно, и состоит в том, что он должен «выбрать» одну из этих вершин. Поставим на ребре стрелку, ведущую от невыбранной вершины к выбранной. Расставив подобным образом стрелки на всех ребрах, мы получим наглядную модель стратегии.

Например, стратегия мудрецов из задачи «Интеллектуальный Вызов» описывается следующей ориентацией двумерного гиперкуба:



4.2. Пусть имеется n мудрецов и шляпы красного и синего цвета. Все всех видят. Как мы знаем из задачи 1.3, $\lfloor n/2 \rfloor$ мудрецов смогут угадать свой цвет правильно. Докажите, что существует «сбалансированная по цветам» стратегия угадывания, а именно, стратегия, обладающая свойством: для любой раздачи шляп верно, что если роздано r красных и b синих шляп, то по крайней мере $\lfloor r/2 \rfloor$ мудрецов с красными шляпами угадают цвет и $\lfloor b/2 \rfloor$ мудрецов с синими шляпами угадают цвет.

4.3. Пусть $2n$ мудрецов пользуются оптимальной стратегией, т.е. стратегией, которая дает не менее n правильных догадок. Докажите, что эта стратегия «несмещенная» (в сторону одного из цветов), а именно: для каждого мудреца верно, что если рассмотреть все возможные расклады шляп, то ровно в половине случаев мудрец, угадывая, называет первый цвет и ровно в половине случаев — второй.

Решения

1.1. Пусть цвета — это остатки по модулю n . Каждый мудрец видит все шляпы, кроме своей. Пусть k -й мудрец проверит гипотезу «сумма всех шляп равна k по модулю n ». Тогда ровно один мудрец угадает.

1.2. Утверждение этой задачи — частный случай задачи 2.2.

1.3. [1, Theorem 2]

Для начала приведем стратегию, для которой 10 мудрецов выигрывают. Разделим всех мудрецов на 10 равных групп и воспользуемся задачей 1.1.

Предположим, существует стратегия, гарантирующая 11 правильных угадываний при любой расстановке цветов. Рассмотрим все k^{10k} возможных расстановок. Рассмотрим какие-то k расстановок, отличающихся только цветом первой шляпы. Поскольку стратегия детерминированная, во всех этих расстановках первый мудрец должен называть один и тот же цвет, значит, в этих k случаях он правильно угадает цвет в сумме только один раз. Разбив все начальные ситуации на такие группы по k , заключим, что всего первый мудрец правильно угадывает цвета k^{10k-1} раз. Поскольку для остальных мудрецов верно то же рассуждение, все мудрецы во всех ситуациях в сумме правильно угадают цвет $10k \cdot k^{10k-1}$ раз, что меньше, чем $11 \cdot k^{10k}$.

1.4. [3, пункт 4.2] Для начала докажем, что никакая стратегия не может гарантировать строго больше $3k - 1$ угадавших в любой ситуации.

Рассмотрим произвольного мудреца. Если на нем шляпа того же цвета, что и спрятанная, то он видит $2k$ шляп одного цвета и $2k - 2$ другого, таким образом знает, что его цвет — тот которого меньше.

Если его шляпа не того же цвета, что спрятанная, то назовем такого мудреца *сомневающимся*. Рассуждая аналогично задаче 1.3, докажем, что при любой стратегии любой мудрец угадывает цвет шляпы ровно в половине тех ситуаций, в которых является сомневающимся мудрецом. В самом деле, пусть мудрец номер i является сомневающимся в ситуации A . Построим по ней ситуацию $h_i(A)$: поменяем местами шляпу i -го мудреца и спрятанную. Мудрец i остался сомневающимся и цвета всех шляп, которые он видит, не поменялись, так что он должен назвать тот же цвет. Таким образом можно все ситуации, в которых i является сомневающимся, разбить на пары вида $(A, h_i(A))$, и в каждой паре мудрец угадывает ровно один раз. Таким образом, никакая стратегия не гарантирует больше $2k - 1 + \frac{2k}{2} = 3k - 1$ угадываний.

Построим стратегию, где угадываний будет ровно столько. Выпишем все возможные $\binom{4k}{2k}$ ситуаций, предпишем любому не сомневающемуся угадать свой цвет, далее будем по очереди каждому сомневающемуся в какой-то паре ситуаций $(A, h_i(A))$ сообщать, что он должен в этом случае сказать. Возьмем любую ситуацию A_1 и сомневающегося в ней мудреца i . Предпишем ему назвать цвет его шляпы в A_1 , таким образом в A_1 появился один правильно угадавший сомневающийся, а в $h_i(A)$ появился ошибшийся. Назовем $A_2 = h_i(A)$ и повторим процесс: для A_2 найдем другого сомневающегося j , научим его правильно угадывать в ситуации A_2 и ошибаться в $h_j(A_2)$, и т. д., пока не окажется $A_k = A_1$. В этот момент во всех рассмотренных ситуациях есть поровну сомневающихся, угадавших цвет правильно и неправильно. Если еще не все сомневающиеся во всех ситуациях определились — продолжим процесс.

1.5. Утверждение этой задачи мы взяли в [7]. Приводимое здесь решение М. Иванова, хотя и описывает ту же стратегию игроков, что и в [7], но благодаря изящной алгебраической интерпретации делает ее совершенно прозрачной и мотивированной.

Пусть цвета — это остатки 0, 1, 2 по модулю 3. Тогда нам необходимо найти такие функции $f_A(D, B)$, $f_B(A, C)$, $f_C(B, D)$, $f_D(C, A)$, чтобы для любых значений A, B, C, D хотя бы одна из

функций имела бы значение, совпадающее со значением соответствующей переменной по модулю 3.

Будем искать эти функции в классе линейных функций.

Сначала подберем выражения $A \pm B \pm C + \text{const}$, $A \pm C \pm D + \text{const}$, $A \pm B \pm D + \text{const}$, $B \pm C \pm D + \text{const}$ так, чтобы при любых A, B, C, D хотя бы одно из этих выражений было сравнимо с нулем по модулю 3. Это можно сделать с помощью следующего изящного наблюдения, которое к тому же позволяет обойтись без дополнительных констант. Заметим, что

$$\begin{aligned} (A + B + C)^2 + (A - C + D)^2 + (A - B - D)^2 + (B - C - D)^2 = \\ = 3(A^2 + B^2 + C^2 + D^2) \equiv 0 \pmod{3}. \end{aligned} \quad (1)$$

Если при каких-то A, B, C, D каждое из выражений

$$A + B + C, \quad A - C + D, \quad A - B - D, \quad B - C - D \quad (2)$$

оказалось не равным 0 по модулю 3, то квадраты выражений давали бы остатки 1 по модулю 3, и тогда сумма (1) не могла бы делиться на 3. Значит, для любых целых A, B, C, D хотя бы одно из выражений (2) обращается в 0 по модулю 3.

Положим тогда $f_B = -A - C$, $f_D = C - A$, $f_A = B + D$, $f_C = B - D$. Переводя на язык простых рецептов, мудрец A называет в качестве своей гипотезы сумму $B + D$, мудрец B называет $-A - C$, мудрец C называет $B - D$, мудрец D называет $C - A$.

Замечание. На самом деле, формула (1) — это просто произведение $(A^2 + B^2 + C^2 + D^2)(1^2 + 1^2 + 1^2 + 0^2)$, разложенное по формуле Эйлера

$$\begin{aligned} (A^2 + B^2 + C^2 + D^2)(a^2 + b^2 + c^2 + d^2) = \\ = (Aa + Bb + Cc + Dd)^2 + (Ac - Ca + Db - Bd)^2 + \\ + (Ab - Ba + Cd - Dc)^2 + (Ad - Da + Bc - Cb)^2. \end{aligned}$$

1.6. [2, стр.160] Приведем пример стратегии, выигрывающей в 6 случаях из 8. Пусть мудрец, если видит на двух других шляпы одного цвета, называет другой цвет, а если видит шляпы разных цветов — молчит. Тогда если все три шляпы одного цвета — то в обоих таких случаях все три мудреца ошиблись, если же шляпы не одного цвета, то имеется две шляпы одного и одна другого. Тогда каждый из двоих владельцев шляп цвета большинства промолчит, тот, на ком шляпа другого цвета, правильно назовет ее цвет, итого шесть выигрышных ситуаций.

Докажем, что стратегии лучше быть не может. Пусть стратегия предписывает какому-то мудрецу, видя некоторую пару цветов на двух остальных, назвать цвет. Это соответствует некоторым двум расстановкам шляп (на самом мудреце шляпа может быть первого или второго цвета), так что мудрец делает одно человекоугадывание и одно человеконеугадывание. Суммируя по всем ситуациям и по всем мудрецам, заключаем, что человекоугадываний и человеконеугадываний поровну.

В каждой выигрышной ситуации есть хотя бы одно человекоугадывание и ни одного человеконеугадывания, в каждой проигрышной не больше трех человеконеугадываний (потому что мудрецов всего трое). Значит, соотношение количества выигрышных ситуаций к проигрышным не больше 3 : 1.

Это рассуждение легко обобщается на случай произвольного числа мудрецов. Выше доказано, что выигрышных ситуаций не больше чем $2^n \frac{n}{n+1}$ (здесь и далее число мудрецов обозначено через n). Оценка достигается для n вида $n = 2^k - 1$ при натуральном k . Для удобства будем кодировать каждую из 2^n ситуаций словом длины n из нулей и единиц. Нам потребуется

Утверждение. Для $n = 2^k - 1$ из всех слов из нулей и единиц длины n можно выбрать $2^n \frac{n}{n+1}$ кодовых слов так, что любое слово или выбрано или отличается в одном разряде от выбранного (такая выборка называется *совершенным кодом Хэмминга с кодовым расстоянием 3* или *кодом Хэмминга, исправляющим одну ошибку*). Приведем стратегию, при которой мудрецы выигрывают на всех невыбранных последовательностях и проигрывают на выбранных.

Стратегия: то что видит мудрец есть слово без одного разряда. Если оно является куском кодового слова — то мудрец называет не тот символ, который в этом слове стоит в его разряде. Иначе молчит. Тогда если слово не является кодовым, то оно отличается в одном разряде от кодового, и только мудрец соответствующий этому разряду видит кусок правильного слова, значит назвав неправильный цвет угадывает. Если исходное слово кодовое — то все мудрецы одновременно ошибаются.

2.1. Допустим, что у мудрецов есть выигрышная стратегия. Пусть v — центр лапы, u_1, u_2, u_3 — всячие вершины. Назначим вершине v первый цвет. Пусть мудрецы u_1, u_2, u_3 согласно стратегии называют цвета h_1, h_2, h_3 .

Теперь проведем второй эксперимент: назначим вершине v второй цвет. Пусть мудрецы u_1, u_2, u_3 согласно стратегии называют цвета e_1, e_2, e_3 .

Теперь проведем финальный эксперимент. Для каждого $i = 1, 2, 3$ обозначим через d_i цвет, который не был назван мудрецом u_i в первых двух экспериментах (если есть выбор — берем любой цвет из двух возможных). Для каждого i назначим всячей вершине u_i цвет d_i . Цвета шляп у соседей мудреца v уже заданы, значит, известен его ответ по стратегии. Назначим вершине v тот из цветов — первый или второй, который не совпадает с этим ответом. Мудрецы проиграли.

2.2. Это лемма 8 из [1].

Докажем индукцией по числу вершин следующее утверждение. Пусть T — произвольное дерево, v — его произвольная вершина, c_1, c_2 — два произвольных цвета. Пусть мудрецы уже выбрали себе стратегию Γ . Тогда существует распределение шляп по вершинам, проигрышное для мудрецов, при котором вершина v покрашена в цвет c_1 или c_2 .

База индукции — одна вершина — тривиальна.

Докажем переход. При удалении вершины v дерево распадается на части T_1, T_2, \dots . Обозначим через u_1, u_2, \dots вершины в этих поддеревьях, соседние с v . Аналогично предыдущей задаче проведем два эксперимента: в первом зададим шляпе в вершине v цвет c_1 и переберем всевозможные распределения шляп в деревьях T_i , неудачные для мудрецов, когда они используют в T_i стратегию Γ . Пусть H_i — множество цветов, которые может принимать в этих неудачных раскрасках шляпа u_i . Во втором эксперименте зададим шляпе в вершине v цвет c_2 и построим множество цветов E_i , которые может иметь шляпа u_i во всевозможных неудачных раскрасках.

Заметим, что в обоих экспериментах стратегии мудрецов на каждом дереве T_i отличаются разве лишь функцией, которую использует мудрец u_i . Это значит, что если бы еще и цвет шляпы в вершине u_i был фиксирован, то для каждого расклада шляп на дереве T_i остальные мудрецы в обоих экспериментах давали бы одинаковые ответы.

По индукционному предположению множества H_i и E_i состоят не менее чем из двух элементов каждое, и поэтому пересекаются. Пусть d_i — какой-нибудь цвет из пересечения этих множеств. При каждом i назначим вершине u_i цвет d_i , а для остальных вершин дерева T_i возьмем подходящую неудачную для мудрецов раскраску. Теперь у вершины v заданы цвета всех соседей, следовательно, ответ мудреца v задан однозначно. Назначим шляпе v тот из цветов c_1, c_2 , который не совпадает с этим ответом. Мудрецы проиграли. Индукционный переход доказан.

2.3. [7, Lemma 2c] Можно считать, что $\ell_-(s_1 s_2) = 3$, $\ell_+(s_{m-1} s_m) \geq 2$.

Проверим, что если $\ell_+(s_{m-1} s_m) \geq 2$, то путь можно продолжить вправо, добавив к нему вершину s_{m+1} так, что $s_1 s_2 \dots s_{m+1}$ — это опровергающая цепочка и на ее краю снова выполнено

неравенство $\ell_+(s_m s_{m+1}) \geq 2$.

Действительно, потенциально у нас есть два таких продолжения, скажем $s_m v_1$ и $s_m v_2$. Рассмотрим короткие цепочки $s_m v_1 w$ и $s_m v_2 w$, назовем *перспективной* ту из них (любую из них, если годятся обе), для которой $v_i \neq f_{m+1}(s_m, w)$. Аналогично выберем перспективную цепочку для каждого из двух остальных значений w . Мы наметили три перспективные цепочки, по крайней мере у двух из них совпадают цвета v_i . В качестве s_{m+1} и следует взять цвет v_i .

Итак, мы можем продолжать нашу цепочку сколь угодно далеко вправо. Осталось позаботиться о том, чтобы эта цепочка «заиклилась». Перед заикливанием у нас имеется длинная цепочка $x s_1 s_2 \dots s_{n-1} y$, где для вершины x имеется три варианта выбора, а для вершины y — хотя бы два варианта. Мы без труда выберем $x = y$, для которых $x \neq f_n(s_{n-1} s_1)$.

В результате получилась циклическая опровергающая цепочка. Мудрецы проиграли.

2.4. [7, Lemma 2d]

Если имеется двухэлементная цепочка $s_1 s_2$, для которой $\ell_-(s_1 s_2) + \ell_+(s_1 s_2) > 4$, то по утверждению предыдущей задачи мудрецы проиграли.

С другой стороны, заметим, что для заданного s сумма

$$\ell_+(s s_1) + \ell_+(s s_2) + \ell_+(s s_3) = 6 \quad (3)$$

(где s_1, s_2, s_3 — три различных цвета). Действительно, для каждого цвета w существует ровно два цвета s_i , для которых $s_i \neq f(s, w)$, а так как w можно выбрать тремя способами, получаем 6 вариантов продолжений.

В силу сделанного наблюдения

$$\sum_{s_1, s_2} \ell_+(s_1 s_2) = 18. \quad (4)$$

Таким образом, среднее значение величины $\ell_+(s_1 s_2)$ равно 2. Аналогично среднее значение величины $\ell_-(s_1 s_2)$ равно 2.

Возвращаясь к нашей задаче, заметим, что если для какой-то двухэлементной цепочки $s_1 s_2$ выполнено неравенство $\ell_-(s_1 s_2) + \ell_+(s_1 s_2) < 4$, то обязательно найдется цепочка $s'_1 s'_2$, для которой $\ell_-(s'_1 s'_2) + \ell_+(s'_1 s'_2) > 4$, и мудрецы опять проиграют.

Таким образом, выигрышная стратегия может существовать лишь при условии $\ell_-(s_1 s_2) + \ell_+(s_1 s_2) = 4$ для всех s_1, s_2 .

2.5. [7] Покажем, как может выглядеть стратегия мудрецов на цикле из $N = 3n$ вершин, чтобы для нее не нашлось ни одной опровергающей цепочки.

Из утверждений задач 2.12, 2.13 следует, что для выигрышной стратегии количество правых пар цветов вида ab , где $a \in V_i, b \in V_{i+1}$, одинаково при всех i . (Аналогично одинаково количество левых пар и инертных пар.) Из этих же утверждений вытекает, что любая цепочка, опровергающая выигрышную стратегию, должна состоять из звеньев одинакового типа (то есть в ней все пары цветов соседних шляп правые, либо все левые, либо все инертные), в этом случае всю цепочку будем называть левой, правой или инертной. Действительно, как мы видели в решении задачи 2.13, любая левая пара цветов ab_1 имеет единственное продолжение влево до более длинной цепочки $c_1 ab_1$, и при этом пара $c_1 b$ — опять левая. Аналогично однозначно задано продолжение правой цепочки вправо так, что на краю окажется опять правая цепочка. Таким образом, циклическая цепочка, опровергающая всех мудрецов, должна состоять из звеньев одного типа.

Мы подберем такую стратегию, для которой при всех i имеется три правых пары ab , $a \in V_i, b \in V_{i+1}$, три левых пары и три инертных. В этом случае элементы множеств V_i можно пронумеровать таким способом $V_i = \{v_1^i, v_2^i, v_3^i\}$, что цепочки $v_1^1 v_1^2 v_1^3 \dots, v_2^1 v_2^2 v_2^3 \dots, v_3^1 v_3^2 v_3^3 \dots$ — правые. Мы,

однако, выписали лишь начала этих цепочек, но при попытке построить циклическую цепочку может случиться, что цепочка не заикливаясь с периодом N и при продолжении $v_1^1 v_1^2 v_1^3 \dots v_1^N v_1^{N+1}$ оказывается, что $v_1^{N+1} = v_2^1$ или $v_1^{N+1} = v_3^1$. Обозначим $v_1^{N+1} = v_{\sigma(1)}^1$, $v_2^{N+1} = v_{\sigma(2)}^1$, $v_3^{N+1} = v_{\sigma(3)}^1$, очевидно, σ — это перестановка трехэлементного множества. Именно этого и должны добиваться мудрецы: им нужно придумать такую стратегию, чтобы локальные опровергающие цепочки не могли бы заиклиться в N -элементную цепочку, из-за того что перестановка σ не имеет неподвижных точек. То же должно быть выполнено для левых и для инертных цепочек. Рассмотрим подробнее, как они могут быть устроены в терминах введенной нумерации цветов.

У нас имеется три левых пары ab , $a \in V_i$, $b \in V_{i+1}$, можно считать, что это пары $v_1^i v_3^{i+1}$, $v_2^i v_1^{i+1}$, $v_3^i v_2^{i+1}$. Среди пар ab , $a \in V_{i-1}$, $b \in V_i$ тоже три левых. Заметим, что пара $v_3^{i-1} v_3^i$ правая, поэтому цепочка $v_3^{i-1} v_3^i v_1^{i+1}$ не является короткой опровергающей цепочкой, а тогда $v_3^{i-1} v_2^i v_1^{i+1}$ является опровергающей цепочкой, и это значит, что пара $v_3^{i-1} v_2^i$ есть «опровергающее продолжение» влево для пары $v_2^i v_1^{i+1}$, что означает, что пара $v_3^{i-1} v_2^i$ тоже левая. Рассуждая так же для других наборов индексов, получаем, что при всех i ($i = 1, 2, \dots, N$) множество левых пар ab , $a \in V_i$, $b \in V_{i+1}$ состоит из пар

$$v_1^i v_3^{i+1}, \quad v_2^i v_1^{i+1}, \quad v_3^i v_2^{i+1}.$$

Но тогда левая цепочка, начинающаяся с цвета v_1^1 имеет вид $v_1^1 v_3^2 v_2^3 v_1^4 \dots$ и, таким образом, $(N+1)$ -й элемент этой цепочки (напомним, что N делится на 3) имеет вид $v_{\sigma(1)}^{N+1}$. Значит, левая цепочка тоже не заиклится, если у перестановки σ нет неподвижных точек. Также обстоят дела и с инертными цепочками.

Осталось описать стратегию, которая создаст нам эту прекрасную картину. Пусть все мудрецы пользуются одной и той же стратегией

$$f_i = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 3 & 1 \end{pmatrix}, \quad i = 1, 2, \dots, N$$

где элемент в p -й строке и в q -м столбце — это $f_i(p, q)$ и мы пользуемся соглашением $v_i^{N+1} = v_{\sigma(i)}^1$, где $\sigma : 1 \rightarrow 2 \rightarrow 3 \rightarrow 1$ — циклическая перестановка трехэлементного множества. Иными словами, если $v_1^i = 1$, $v_2^i = 2$, $v_3^i = 3$ при $1 \leq i \leq N$, то $v_1^{N+1} = 2$, $v_2^{N+1} = 3$, $v_3^{N+1} = 1$. Это соглашение обеспечивается свойством $f_i(\sigma(p), \sigma(q)) = \sigma(f_i(p, q))$, которое нетрудно проверить.

Проверку того, что эта стратегия обеспечивает поровну правых, левых и инертных пар цветов, оставляем читателю.

2.6. [7] В решении предыдущей задачи показана роль того, что длина цикла N делится на 3. Оказывается, что опровергающие цепочки имеют 3-периодическую структуру и благодаря этому мудрецы могут не позволить опровергающим цепочкам заиклиться.

В случае, когда N не делится на 3, цепочки обязательно заикливаются. Для случая, когда при всех i имеется три правых пары ab , $a \in V_i$, $b \in V_{i+1}$, три левых и три инертных пары, это нетрудно понять из предыдущего решения.

Но возможны и другие количества правых, левых и инертных пар, для полного решения требуется внимательно изучить структуру цепочек в этих случаях. Читатель, который до сих пор не утратил любопытства в этом вопросе, может обратиться за подробностями к статье [7].

2.7. [1, theorem 7].

Формулировка задачи 3.4 подсказывает нам, что хотя бы в одной из долей должно быть не меньше $k-1$ вершины. Оказывается, эта оценка реализуется.

Пусть левая доля L нашего графа состоит из $n = k-1$ вершины, а правая доля R — из $m = k^{k^n}$ вершин. Пусть C — это множество всевозможных раскрасок доли L в k цветов. Ясно,

что $|C| = k^n$. Тогда $m = k^{|C|}$ и, значит, число m равно количеству отображений из множества C во множество цветов $\{1, 2, \dots, k\}$. Зафиксируем какую-нибудь биекцию между вершинами правой доли и множеством отображений из C во множество цветов $\{1, 2, \dots, k\}$. Пусть мудрецы в правой доле в качестве стратегии используют эту биекцию: у каждого мудреца имеется «свое личное» отображение из C во множество цветов, и когда мудрец видит раскраску левой доли (это элемент из C), он называет в качестве цвета значение этого отображения на этой раскраске.

Нам понадобится следующая лемма.

Лемма. Пусть c_R — это фиксированная раскраска правой доли. Рассмотрим множество C' всех таких раскрасок c_L левой доли, для которых в том случае, когда весь граф покрашен с помощью объединенной раскраски (c_L, c_R) , никто из мудрецов правой части не угадал цвет. Тогда $|C'| < k$.

Доказательство леммы приведено ниже, а сейчас мы определим стратегию для мудрецов из левой доли L . Когда задана раскраска правой доли (и уже задана стратегия мудрецов в правой доле), мы можем построить множество C' из леммы. Оно будет содержать не более $n = k - 1$ элементов. Пусть c_1, c_2, \dots, c_n — список раскрасок левой доли, содержащей все раскраски из C' . Пусть тогда i -й мудрец в левой доле называет цвет $c_i(i)$.

Это выигрышная стратегия для мудрецов. Действительно, если никто из мудрецов правой доли не угадал, то левая доля раскрашена с помощью одной из раскрасок множества C' . Если эта раскраска присутствует в нашем списке как c_j , то j -й мудрец левой доли угадал цвет: он назвал цвет $c_j(j)$!

Осталось доказать лемму. Предположим на секундочку, что множество C' содержит k различных элементов c_1, \dots, c_k . Возьмем любое отображение f из C в $\{1, 2, \dots, k\}$, которое принимает на этих k элементах k различных значений. Пусть $v \in R$ — вершина, соответствующая этому отображению f . Тогда множество цветов $\{f(c_1), f(c_2), \dots, f(c_k)\}$ содержит все k цветов и, следовательно, один из этих цветов $f(c_i)$ совпадает с цветом вершины v . Получается, что при использовании в левой части раскраски c_i кто-то из мудрецов правой части все же угадал цвет правильно, что противоречит определению множества C' . Лемма доказана.

2.8. [4, лемма 1]. Но мы изложим это рассуждение человеческим языком.

На графе G мудрецы выигрывают, имея шляпы q цветов, — будем называть эти цвета теплыми. На графе K_r мудрецы выигрывают, имея шляпы r цветов, — будем называть эти цвета холодными. Покраску вершин графа \tilde{G} в qr цветов можно представлять себе как указание для каждой вершины двух цветов — одного теплого цвета и одного холодного. И тогда при угадывании мудрецы называют тоже два цвета: один теплый и один холодный.

Пусть мудрецы называют холодный цвет, глядя только на своих соседей по копии K_r (и на холодные компоненты цветов их шляп). Тогда ровно один мудрец в каждой копии угадает свой холодный цвет правильно, таких мудрецов назовем удачливыми. Каждый мудрец может с легкостью определить, кто из мудрецов в соседней копии K_r является удачливым. Для определения теплого цвета мудрец должен использовать стратегию на графе G , полагая, что его соседями в смысле графа G являются лишь удачливые мудрецы из соседних копий, и принимая во внимание лишь теплую компоненту цвета шляп этих мудрецов. Тогда по крайней мере один удачливый мудрец правильно угадает свой теплый цвет.

2.9. Это сразу следует из утверждений задач 1.5 и 2.8.

2.10. Подсчетом в стиле решения задачи 1.3 нетрудно убедиться, что в сумме по всем раскладам шляп имеется 3^3 верных угадываний — столько же, сколько и самих раскладов. Таким образом, при применении выигрышной стратегии для каждого расклада шляп ровно один мудрец должен угадать верно.

Для любой стратегии предъявим тогда расклад шляп, на котором угадывают два мудреца. Дадим мудрецу C произвольную шляпу. Потом дадим мудрецу A шляпу того цвета, который он назовет согласно стратегии, увидев, что надето на C . Наконец, дадим мудрецу B шляпу того цвета, который он назовет согласно стратегии, увидев, какие шляпы надеты на A и C .

2.11. Обозначим мудрецов A, B, C, D , и пусть A не видит B . Сначала покажем, что найдутся две трёхэлементные цепочки $a_1d_1c_1$ и $a_1d_1c_2$, в которых A и D не угадывают. Для этого аналогично решению задачи 2.4 рассмотрим все 6 способов раздать цвета A и D так, чтобы A не угадал (его стратегия зависит только от цвета D), и 18 вариантов продолжить эти цепочки в сторону C . Так как D угадывает только в девяти случаях, есть цвет d_1 , который он называет максимум 3 раза, и тогда среди шести цепочек с началом a_1d_1 или a_2d_1 хотя бы три проигрышные для D , и по принципу Дирихле найдутся две трёхэлементных цепочки $a_1d_1c_1$ и $a_1d_1c_2$, в которых A и D не угадывают. Выдадим A цвет a_1 , а D — цвет d_1 .

Теперь изучим стратегию мудреца B . Пусть $f_B(a_1, c_1) = b_1$, $f_B(a_1, c_2) = b_2$. Выдадим ему третий цвет b_3 (любой, если $b_1 = b_2$).

Заметим, что теперь мы знаем всё про соседей мудреца C : у B шляпа цвета b_1 , а у D — цвета d_1 . Но тогда $f_C(b_1, d_1)$ не совпадает с одним из c_1, c_2 . Выдав ему неподходящий цвет, мы заставим всех мудрецов ошибиться.

2.12. [7, лемма 3a] Воспользуемся формулой (4) и аналогичной формулой для ℓ_- :

$$\sum_{a,b} \ell_+(ab) = \sum_{a,b} \ell_-(ab) = 18.$$

Поскольку мы рассматриваем выигрышную стратегию, для любых a, b $\ell_+(ab) + \ell_-(ab) = 4$. Следовательно, каждому слагаемому 1, 2, 3 в первой сумме соответствует слагаемое 3, 2, 1 во второй сумме. Значит, слагаемых 1 и 3 в обеих суммах поровну. Это и требовалось доказать.

2.13. [7, лемма 3d] Пусть $V_{i+1} = \{b, b_1, b_2\}$. Тогда аналогично формуле (3) с учетом равенства $\ell_-(s_1s_2) + \ell_+(s_1s_2) = 4$ имеем

$$\ell_-(ab) + \ell_-(ab_1) + \ell_-(ab_2) = 6.$$

Так как $\ell_-(ab) = 3$, остальные два слагаемых — это 1 и 2, можно считать, что $\ell_-(ab_1) = 1$, и значит, существует короткая опровергающая цепочка, скажем, c_1ab_1 . Тогда $\ell_-(c_1a) = 1$, поскольку в противном случае $\ell_-(c_1a) + \ell_+(ab_1) \geq 5$ и по задаче 2.3 стратегия мудрецов не выигрышная. Применяя аналогичную формулу

$$\ell_-(c_1a) + \ell_-(c_2a) + \ell_-(c_3a) = 6,$$

мы видим, что здесь $\ell_-(c_1a) = 1$, значит, остальные два слагаемых — это 2 и 3, что и требовалось.

2.14. [1, Theorem 16.iii]

2.15. [4] Решение этой задачи требует более сложной конструкции, чем задача 2.7.

3.1. Все мудрецы, кроме одного, называют цвет, противоположный тому, который видят, а последний мудрец — называет тот цвет, который видит.

3.2. [1, пример 6] То, что не менее s мудрецов могут угадать цвет, следует из утверждения предыдущей задачи. Пример графа, для которого число угадывающих мудрецов больше числа независимых циклов, приведен в задаче 3.5.

3.3. [1, лемма 4] Пусть при удалении вершин v_1, v_2, \dots, v_a граф становится ациклическим. Остальные вершины v_{a+1}, \dots, v_n пронумеруем так, чтобы ребра из этих вершин шли только в сторону убывания номеров. Иначе говоря, для последних $n - a$ вершин все выходящие ребра идут влево.

Теперь положим шляпы на первых a мудрецов произвольно. Для каждого следующего мудреца уже заданы цвета шляп у всех, кого он видит, следовательно, ответ, который должен он дать по стратегии, уже известен. Дадим этому мудрецу шляпу так, чтобы он не угадал.

При таком распределении шляп только первые a мудрецов смогут что-нибудь угадать.

3.4. [4, теорема 5] Возьмем произвольную стратегию мудрецов f и докажем, что она проигрышная.

Пусть A — множество цветов шляп, в котором один цвет пропущен, $|A| = k - 1$. Если a — какой-нибудь цвет, обозначим через w_a набор из $k - 2$ цветов (a, a, \dots, a) . Мудрецам из части L мы будем всегда давать набор одинаковых шляп вида w_a , где $a \in A$.

Пусть r_1, r_2, \dots, r_s — вершины R , пронумерованные так, чтобы ребра шли в сторону убывания номеров, для удобства мы можем считать, что каждый мудрец в R видит всех мудрецов с меньшими номерами. Построим набор цветов $Y = \{y_1, \dots, y_s\}$ для мудрецов из части R . Для этого последовательно выберем

$$\begin{aligned} y_1 &\notin \{f_{r_1}(w_a), a \in A\}; \\ y_2 &\notin \{f_{r_2}(w_a, y_1), a \in A\}; \\ &\dots \\ y_s &\notin \{f_{r_s}(w_a, y_1, y_2, \dots, y_{s-1}), a \in A\}. \end{aligned}$$

Поясним этот выбор чуть подробнее на примере y_s . Мудрец в вершине r_s видит всех мудрецов части L (цвета их шляп заданы набором w_a), кроме того, он видит мудрецов части R с меньшими номерами. Значит, определен его ответ $f_{r_s}(w_a, y_1, y_2, \dots, y_{s-1})$ по стратегии. Поскольку цвет a пробегает $(k - 1)$ -элементное множество A , множество, написанное в правой части для выбора y_s , содержит не более $k - 1$ элементов, поэтому цвет y_s действительно можно выбрать.

Итак, мы построили набор цветов Y . Пусть $\ell_1, \ell_2, \dots, \ell_{k-2}$ — вершины L . Выберем цвет $b \in A$, не совпадающий ни с одним из цветов $f_{\ell_1}(Y), \dots, f_{\ell_{k-2}}(Y)$. Тогда для раскраски шляп (w_b, Y) ни один мудрец не угадает цвет правильно.

3.5. [1, Пример 4] Ответ: два мудреца могут угадать свой цвет правильно.

4.1. Выпишем тождество аналогичное (1) и с его помощью назначим линейные функции, задающие ответы мудрецов. Чтобы не выписывать тождество детально (оно очень громоздкое), нам понадобится предварительная работа.

Под N -мерным гиперкубом Q_N мы понимаем граф, содержащий 2^N вершин, которые пронумерованы двоичными N -значными числами, а ребрами соединены вершины, номера которых отличаются лишь в одном двоичном разряде. Приводимые ниже конструкции можно выполнить для любого гиперкуба, но к задаче о мудрецах они применимы лишь при $N \equiv 2 \pmod{3}$.

Лемма. На ребрах гиперкуба Q_N можно так ввести ориентацию, что каждый 4-цикл в Q_N будет содержать 3 ребра, указывающих на одно из направлений обхода цикла, и 1 ребро, указывающее в другом направлении.

Доказательство. Индукция по N . База $N = 2$. 

Индукционный переход. Пусть ориентация на графе Q_N уже задана. Мы можем считать, что граф Q_{n+1} состоит из двух копий графа Q_N — «левой» и «правой» — и из каждой вершины левой копии ведет ребро в соответствующую вершину правой копии. Пусть в левой копии все ребра ориентированы в соответствии с индукционным предположением, а в правой копии введем противоположную ориентацию. Наконец, на ребрах, ведущих из левой копии в правую, зададим направление слева направо. Нетрудно видеть, что эта ориентация удовлетворяет требованиям. \square

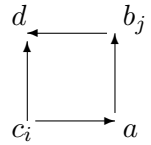
Каждую вершину графа отождествим с какой-нибудь независимой переменной.

Напомним, что в графе Q_N все вершины имеют степень N . Пусть a — произвольная вершина графа; b_1, b_2, \dots — вершины, в которые из a выходит ребро; c_1, c_2, \dots — вершины, из которых в a ведет ребро. Для каждой вершины a графа Q_N рассмотрим выражение f_a , равное квадрату линейной комбинации

$$f_a = (a + b_1 + b_2 + \dots - c_1 - c_2 - \dots)^2. \quad (5)$$

Рассмотрим сумму $\sum f_a$ этих квадратов по всем вершинам графа. Раскроем все скобки. Для каждой вершины a слагаемые вида a^2 будут присутствовать в этой сумме с кратностью $N + 1$, поскольку каждое такое слагаемое появляется при раскрытии скобок $f_a, f_{b_1}, f_{b_2}, \dots, f_{c_1}, f_{c_2}, \dots$ и только в них. Далее, каждому ребру ab соответствует слагаемое $+2ab$, появляющееся при раскрытии скобки в выражении f_a , а также слагаемое $-2ab$, появляющееся при раскрытии скобки в выражении f_b . При раскрытии других скобок такие слагаемые появиться не могут, поэтому все они сокращаются.

Кроме таких слагаемых, при раскрытии скобок f_a появляются слагаемые вида $-2b_j c_i$ — разберемся с ними подробнее. Пусть a имеет номер 00, b_j — номер 01, c_i — номер 10. Рассмотрим также вершину d с номером 11 (ограничимся выписыванием тех битов, где у номеров есть различия). Очевидно, $f_d = (d - b_j - c_i + \dots)^2$, поэтому при раскрытии скобки f_d слагаемое $2b_j c_i$ присутствует со знаком «+». В результате оно сократится. Аналогично рассматриваются другие соответствующие лемме возможные ориентации ребер в цикле.



Итак, $\sum_a f_a = (N + 1) \cdot \sum_a a^2$.

Вернемся к задаче о мудрецах. Пусть $N \equiv 2 \pmod{3}$. В этом случае сумма $\sum_a f_a$ делится на 3. При этом она состоит из 2^N слагаемых. Очевидно, $f_a \equiv 0$ или $1 \pmod{3}$. Поэтому хотя бы одно из слагаемых f_a должно быть нулевым по модулю 3 (а при нечетных N — даже два слагаемых). Для каждой вершины a в обозначениях формулы (5) потребуем, чтобы мудрец, находящийся в этой вершине, в качестве своей гипотезы назвал значение выражения $c_1 + c_2 + \dots - b_1 - b_2 - \dots$. Тогда мудрец, находящийся в вершине a , для которой $f_a \equiv 0 \pmod{3}$, угадает цвет своей шляпы.

4.2. [1, лемма 11] Будем пользоваться гиперкубом для описания стратегий (см. текст перед условием задачи).

Разобьем гиперкуб на слои: к i -му слою отнесем все вершины, у которых сумма координат равна i . Количество (неориентированных) ребер, выходящих из некоторой v вершины к вершинам следующего слоя, будем называть *верхней степенью* этой вершины $\text{udeg } v$, а число ребер, выходящих к вершинам предыдущего слоя, — *нижней степенью* вершины $\text{ddeg } v$.

Рассмотрим ребро между i -м и $(i + 1)$ -м слоями и соответствующего мудреца (=меняющуюся координату), у вершины в $(i + 1)$ -м слое эта координата равна 1, а в i -м слое — 0. Стратегия задает ориентацию на ребре. Если это ребро ориентировано от i -го слоя к $(i + 1)$ -му, то мудрец угадает, когда на нем шляпа цвета 1, и не угадает в противном случае. Если же ребро ориентировано от $(i + 1)$ -го слоя к i -му, то мудрец угадает, когда на нем шляпа цвета 0, и не угадает в противном случае. Нетрудно видеть, что мы заведомо получим сбалансированную стратегию, если для каждой вершины v из i -го слоя, число приходящих в нее ребер из $(i + 1)$ -го слоя будет равно $\lfloor \text{udeg } v / 2 \rfloor$, а число приходящих в нее ребер из $(i - 1)$ -го слоя будет равно $\lfloor \text{ddeg } v / 2 \rfloor$.

Построим сбалансированную стратегию, т. е. введем ориентации на ребрах таким образом, чтобы были выполнены свойства верхних и нижних степеней, упомянутые выше. Идея проста: возьмем произвольное ребро, расположенное между i -м и $(i + 1)$ -м слоями, ориентируем его как-нибудь и будем строить ориентированный путь, добавляя новые ребра так, чтобы путь все время оставался между i -м и $(i + 1)$ -м слоями. Если путь невозможно продолжить (ни вперед, ни назад) и мы ориентировали еще не все ребра, начнем строить следующий путь, и т. д. Когда все ребра будут ориентированы, получится сбалансированная стратегия.

4.3. [1, Предложение 13] Когда количество мудрецов четно, оптимальная стратегия характеризуется тем, что у каждой вершины гиперкуба одинаковы входящая и выходящая степени. В этом случае на гиперкубе можно построить ориентированный Эйлеров путь. Стратегия i -го мудреца — это ориентация ребер, параллельных одному направлению (i -му орту). Половина вершин гиперкуба находится при этом в (левой) грани $x_i = 0$, а другая половина — в правой грани $x_i = 1$. При стрелки, направленные влево, соответствуют случаю, когда мудрец назвал 0, а стрелки, направленные вправо, это когда мудрец назвал 1. Эйлеров путь содержит поровну тех и других стрелок.

ЛИТЕРАТУРА

- [1] *Butler S., Hajiaghayi M., Kleinberg R., Leighton T.* Hat Guessing Games
- [2] *Do N.* Communicating with eyes, hats and light bulbs
- [3] *Fiege U.* You can leave your hat on (if you guess its color).
- [4] *Gadouleau M., Georgiou N.* New constructions and bounds for Winkler’s hat game
<http://arxiv.org/pdf/math/1311.2022v1.pdf>
- [5] *Krzywkowski M.* Hat problem on a graph. Ph.D. dissertation, University of Exeter, 2012.
- [6] *Paterson M., Stinson D.* Yet another hat game // The electronic journal of combinatorics. Vol. 17. 2010. #R86
- [7] *Sztechla W.* The three-colour hat guessing game on the cycle graphs // arXiv:1412.3435v2

What is a color of my hat?

The following problem is well known, but if you miss it before, please, consider it as a challenge. We will discuss this problem after the opening of the conference, it will not affect on results of the competition. The object in the problem has 4 states only!

Intellectual CHALLENGE: the number 4 against milliards of neurons of your brain!

Black or white hats are placed on your and on mine heads. You see my hat, I see your hat, but none of us sees the hat on his own head. Each of us (without any sort of communications) must try to guess the color of his hat. When a signal is given each of us simultaneously says one word only: «black» or «white». We will win if and only if at least one of us has guessed correctly. Before this test we hold a consultation. How should we act in order to win in all possible situations?

1 Several problems about sages

Several sages take part in the following TEST. There are a lot of hats of k different colors. The emcee places hats on the sages' heads. Each sage sees the hats of all other sages and does not see his own hat. The sages do not communicate. When a signal is given they simultaneously name one of colors. The sages win if and only if at least one of them has guessed correctly.

The sages hold a CONSULTATION before the test in order to coordinate their strategy during the test. Repeat that the only form of action is allowed during the test: to say one word just after a signal (independently of other sages). The strategy of sages should be deterministic, i.e. each sage decision is determined uniquely by the hats of other sages.

1.1. There are hats of n colors and n sages. Prove that the sages win.

1.2. There are hats of three colors and n sages are arranged in a line so that each sage can see only his neighbours (the leftmost and rightmost sage see one neighbour). Prove that the sages loose.

a) $n = 3$; b) $n = 4$; c) n is arbitrary.

1.3. There are hats of k colors and $10k$ sages (everybody sees all others). Prove that 10 sages can guess their colors correctly, but in general situation none 11 sages guess their colors correctly.

1.4. There are $4k - 1$ sages, $2k$ black hats and $2k$ white hats. The emcee hides one hat and all other hats place on the sages' heads. What maximal number of sages can guess their color correctly?

1.5. Four sages stand around a non-transparent baobab. The hats are of three colors. A sage sees only his two neighbours. How should they act to win?

1.6. Sages has hats of two colors. It is allowed to say «pass» during guessing, that means that a sage do not make a guess. The sages win if and only if at least one of them has guessed correctly and none of them has guessed incorrectly. We assume that all hats placements have equal probabilities and the sages strategy is deterministic as in previous problems. It is clear that now the sages can not to guarantee 100 % victory. For example a strategy «Sage A always says “black” and all others say “pass”» wins in one half of all possible cases. We call a strategy *optimal* if it wins the most number of all possible cases.

a) Find a strategy that wins in more than 50 % cases.

b) Find an optimal strategy and prove that it is optimal.

2 Sages on a non oriented graph

We will consider the following general problem. Let G be a non oriented graph and let sages live at its vertices: one sage occupies one vertex. All the sages are familiar with each other and all of them know the whole placement

of sages on the vertices of the graph. In particular, each sage understand in what vertex do he and his neighbours live. We will identify a vertex and the sage in it. During the test each sage sees only the hats of sages in the adjacent vertices. Other rules are the same: during the consultation the sages should choose a strategy that allows at least one of them to guess the color of his hat correctly.

We will use the following formalism. Let the colors of hats be numbered from 1 to k and let $\mathcal{C} = \{1, 2, \dots, k\}$. For each vertex v of G order the adjacent vertices by increasing of their numbers (denote by d the number of these vertices): $u_{n_1}, u_{n_2}, \dots, u_{n_d}$. A strategy of the sage v is a function $f_v: \underbrace{\mathcal{C} \times \mathcal{C} \times \dots \times \mathcal{C}}_{d \text{ times}} \rightarrow \mathcal{C}$. The sages choose these functions on the consultation. During the test a sage v calculates $f_v(c_1, c_2, \dots, c_d)$, where $c_i \in \mathcal{C}$ is a color of the sage in the vertex v_{n_i} .

The problem 1.1 shows that if the graph G contains a k -clique, then at least one sage can guess the color of his hat correctly. But if the graph does not contain a k -clique, the question becomes non trivial.

2.1. Let $k \geq 3$. Prove that for 4-vertex graph “chicken feet” the sages loose.

2.2. . Prove that for an arbitrary tree the sages loose ($k \geq 3$).

Now let n sages live at the vertices of a cycle, $k = 3$. Let V be a 3-element set of hats colors. Denote by $V_i = V$ the set of colors of hats that will be placed on the head of the i -th sage. Assume that the sages have chosen a strategy. That means that i -th sage has a function $f_i: V_{i-1} \times V_{i+1} \rightarrow V_i$ (we use cyclical numbering). A sequence of colors abc , where $a \in V_{i-1}$, $b \in V_i$, $c \in V_{i+1}$, is called a short *disproving chain* if $b \neq f_i(a, c)$. A long sequence $S = s_1 s_2 \dots s_m$, where $s_1 \in V_\ell$, $s_2 \in V_{\ell+1}$, \dots , $s_m \in V_{\ell+m-1}$, is called a *disproving chain* if each its 3-element consecutive subsequence is a short disproving chain. For every disproving chain S denote by $\ell_+(S)$ the number of continuations of this sequence by one step to the right, i.e. the number of ways to choose a color $s_{m+1} \in V_{\ell+m}$ that gives us a longer disproving chain. Denote by $\ell_-(S)$ the analogous number of continuations by one step to the left.

2.3. Let n sages live at the vertices of a cycle, $k = 3$. Prove that if there exists a disproving chain $S = s_1 s_2 \dots s_m$, where $2 \leq m \leq n - 1$, for which the inequality $\ell_-(s_1 s_2) + \ell_+(s_{m-1} s_m) \geq 5$ holds then the strategy of sages does not win.

2.4. Let n sages live at the vertices of a cycle, $k = 3$. Let the sages choose a winning strategy. Prove that for each sage i and any pair of colors $a \in V_{i-1}$, $b \in V_i$ the equality $\ell_-(ab) + \ell_+(ab) = 4$ holds.

2.5. Prove that for $k = 3$ the sages win on the graph “a cycle of $3n$ vertices”.

2.6. Prove that for $k = 3$ the sages loose on the graph “a cycle of n vertices”, where n is not divisible by 3 and $n \neq 4$.

The following problems show that the sages can win in graphs without big cliques.

2.7. Prove that for any number of hats k there exists a bipartite graph for which the sages win.

2.8. Let G be a graph for which the sages win when the number of colors equals q . Let K_r be a complete graph on r vertices (we know that the sages win on this graph when the number of colors equals r). Construct a new “big” graph \tilde{G} . For this replace each vertex of the graph G by a copy of graph K_r . If the two vertices were adjacent in G draw the edges between all pairs of vertices in the corresponding copies of K_r . The obtained graph is \tilde{G} .

Prove that the sages win on the graph \tilde{G} when the number of colors equals $k = qr$.

2.9. Prove that for $k = 3m$ there exists a graph with $4m$ vertices and maximal clique of size at most $2m$, for which the sages win.

3 Sages on an oriented graph

Now let the sages live at the vertices of oriented graph; the sage A sees the sage B if and only if the graph contains an oriented edge AB.

3.1. Prove that the sages win on the graph “oriented cycle of n edges” ($k = 2$).

3.2. Denote by c the maximal number of vertex disjoint cycles in a graph. Prove that there exist graphs for which more than c sages can guess the colors correctly ($k = 2$).

3.3. Let a be the minimum number of vertices whose removal makes the graph acyclic. Prove that at most a sages can guess the colors correctly ($k = 2$).

3.4. An oriented graph G is called *semibipartite* if its vertex set can be split onto two parts L and R so that there no edges between vertices of L , and R is acyclic (the edges from L to R and from R to L are not forbidden).

Let the sages have hats of k colors and s be an arbitrary non negative integer. Prove that the sages loose on a semibipartite graph if $|L| = k - 2$, $|R| = s$.

After semifinal

Variations of previous topics

2.10. There are three sages A, B, C, each sees each other, except that the sage A does not see the sage B; $k = 3$. Prove that sages loose.

2.11. Four sages stand around a non-transparent baobab. The hats are of three colors. A sage sees only two his neighbours, except one sage who sees only one his neighbour. Can the sages win?

Let n sages stand at the vertices of a cycle, $k = 3$. Suppose that sages chose a winning strategy. The pair of colors ab , where $a \in V_i$, $b \in V_{i+1}$, will be called a *left* pair, if $\ell_-(ab) = 1$, will be called a *right* pair, if $\ell_-(ab) = 3$, and will be called an *inert* pair, if $\ell_-(ab) = 2$.

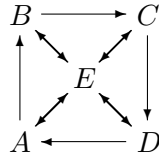
2.12. Prove that the number of left pairs equals the number of right pair among all the pairs ab , such that $a \in V_i$, $b \in V_{i+1}$.

2.13. Let ab be a right pair of colors, $a \in V_i$, $b \in V_{i+1}$. Prove that among the pairs of colors c_1a , c_2a , c_3a , such that $\{c_1, c_2, c_3\} = V_{i-1}$, there is exactly one left pair, exactly one right pair and exactly one inert pair.

2.14. The same setting as in Problem 1.4, but there are $mk - 1$ sages and hats of k colors, m hats of each color, either m is even, or k is odd (possibly both is true). The emcee hides one hat. Prove that the maximal number of sages who can guess their color correctly is $\frac{1}{2}(mk + m - 2)$.

2.15. The sages stand in two lines: n sages in the first line and n^n sages in the second line. They have hats of $(n + 1)$ colors. The sages see only sages standing in the other line. олько тех, кто стоит в другой шеренге. When a signal is given, each of the sages simultaneously names a color. Prove that the sages can act in such a way that at least one guesses.

3.5. What maximal number of sages can guess on the following graph ($k = 2$)?



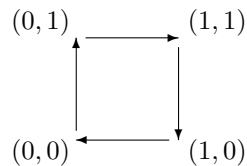
4 Hypercube.

By an n -dimensional hypercube we mean a graph, such that its vertices are numbered by sequences of n zeroes and ones. Two vertices are joined by an edge if and only if their numbers differ only in one digit.

4.1. Prove algebraically that 32 sages, standing in the vertices of a 5-dimensional hypercube, can win ($k = 3$).

Suppose that there are n sages, $k = 2$. Let us denote the colors of hats by one and zero. Let us fix a strategy of the sages. Consider an n -dimensional hypercube and “encode” this strategy with it in the following way. Since the vertices of the hypercube correspond to sequences of n zeros and ones, we relate the i th sage and the i th element of this sequence. Consider the example for $n = 5$, $i = 2$. Suppose that the i th sage sees the colors of hats of the other sages, for instance, 1, *, 0, 1, 1 (the star means that the i th, i.e., the second sage, does not see his own hat color). There are two vertices of the hypercube with such coordinates, namely, (1, 0, 0, 1, 1) and (1, 1, 0, 1, 1), moreover, these vertices are joined by an edge. The strategy of the i th sage is to choose among these two vertices. Let us put an arrow on the corresponding edge, its tail being a non-chosen vertex, its head being a chosen vertex. Putting such arrows on all the edges, we get an illustration of the strategy.

For example, the strategy of sages from the Intellectual CHALLENGE can be described by the following orientation of the 2-dimensional hypercube:



4.2. Suppose that there are n sages, hats can be red or blue. Each sage sees each other. As we know from Problem 1.3, $\lfloor n/2 \rfloor$ sages can guess their color correctly. Suppose that there exists a “balanced with respect to colors” strategy: such that for every distribution of hats, if there are r red and b blue hats, it is true that at least $\lfloor r/2 \rfloor$ sages with red hats guess, and at least $\lfloor b/2 \rfloor$ sages with blue hats guess.

4.3. Suppose that $2n$ sages use the optimal strategy, i.e., the strategy which leads to at least n guesses. Prove that this strategy is “unbiased” (with respect to one of the colors), namely: for every sage it is true, that if we consider all the distributions of hats, he says “red” in exactly half of the cases and “blue” in the other half of the cases according to his strategy.

Solutions

1.1. Let us label colors by residues modulo n . Every sage sees all the hat besides his own one. Let k th sage check the hypothesis “the sum of all the hats equals k modulo n . Then exactly one sage guesses.

1.2. This is a partial case of Problem 2.2.

1.3. [1, Theorem 2]

First we present a strategy for 10. Divide $10k$ sages into 10 groups of k sages each, and use Problem 1.1.

Assume there exists a strategy, that guarantees at least 11 correct guesses in each situation. Consider all k^{10k} ways to arrange colors to hats. Consider the k situations, that differ only in the color of the first hat. Since the strategy is deterministic, in all these situations the first sage will name the same color. Thus in these k situations the first sage will make only one correct guess. Dividing all k^{10k} situations into k^{10k-1} groups of k , we get that the first sage will make just k^{10k-1} correct guesses. The same holds true for every other sage, thus in total there are $10k \cdot k^{10k-1}$ correct guesses, which is not enough to have 11 correct guesses in each of k^{10k} situations.

1.4. [3, 4.2] Consider a sage. If the color of his hat coincides with the color of the hidden one, then he sees $2k$ hats of one color and $2k - 2$ hats of another, thus he is sure that his hat is of minority color.

If his hat and the hidden one have different colors, then call this sage in this situation *a doubting sage*. Arguing analogously to 1.3 we prove that each sage makes a correct guess in exactly half of situations, in which he is a doubting sage. Indeed, let some sage i is doubting in some situation A . Construct the situation $h_i(A)$: take sage’s hat and the hidden one and change there places. The sage i is still doubting, but since we did not change hats of all other sages, he must name the same color in both situations. Thus no strategy can guarantee more then $2k - 1 + \frac{2k}{2} = 3k - 1$ correct guesses.

So, we need to construct a strategy, where exactly half of doubting sages guess correctly in each situation. We do it in the following way.

Make the list of all $\binom{4k}{2k}$ situations and mark all doubting sages in each of them. We will take a pair of sage i and situation A_1 , such that sage i is doubting in situation A_1 , and thus also in situation $h_i(A_1)$. Set our strategy to order the sage i name the color of hat in the situation A_1 whenever he sees what he should see in the situation A_1 . Thus he will make the right guess in A_1 and the wrong one in $h_i(A_1)$. Call $h_i(A_1) = A_2$ find another doubting sage in A_2 and do the same. Thus in A_2 there will be two sages, who’s actions are already determined, and one of them makes the right guess, another one wrong. We continue this process until $A_k = A_1$. At this moment for each situation there are equal amounts of doubting sages, making right and wrong guesses. If not all the doubting sages have their actions determined — continue this process.

1.5. This problem was taken from [7]. We present you the solution after M. Ivanov, which in fact describes the same strategy as in [7], but is more elegant due to its algebraic formulation.

Let us label colors with residues 0, 1, 2 modulo 3. We need to find functions $f_A(D, B)$, $f_B(A, C)$, $f_C(B, D)$, $f_D(C, A)$ such that for any values of A, B, C, D at least one function coincides with the value of the corresponding variable modulo 3.

Let us try to find linear functions satisfying these conditions.

First, find the expressions of the form $A \pm B \pm C + \text{const}$, $A \pm C \pm D + \text{const}$, $A \pm B \pm D + \text{const}$, $B \pm C \pm D + \text{const}$ such that for any A, B, C, D at least one of these expressions is divisible by 3. For this, note that

$$\begin{aligned} (A + B + C)^2 + (A - C + D)^2 + (A - B - D)^2 + (B - C - D)^2 &= \\ &= 3(A^2 + B^2 + C^2 + D^2) \equiv 0 \pmod{3}. \end{aligned} \tag{1}$$

If for some A, B, C, D every expression

$$A + B + C, \quad A - C + D, \quad A - B - D, \quad B - C - D \quad (2)$$

is nonzero modulo 3, then the squares of these expressions have residues 1 modulo 3, and the sum (1) is not divisible by 3. It means that for any integers A, B, C, D , at least one of the expressions (2) is divisible by 3.

Now let $f_B = -A - C$, $f_D = C - A$, $f_A = B + D$, $f_C = B - D$. We can formulate a “recipe” for every sage: sage A says $B + D$, sage B says $-A - C$, sage C says $B - D$, sage D says $C - A$.

Remark. Formula (1) is just the product $(A^2 + B^2 + C^2 + D^2)(1^2 + 1^2 + 1^2 + 0^2)$, rewritten with the help of the Euler formula

$$\begin{aligned} (A^2 + B^2 + C^2 + D^2)(a^2 + b^2 + c^2 + d^2) = \\ = (Aa + Bb + Cc + Dd)^2 + (Ac - Ca + Db - Bd)^2 + \\ + (Ab - Ba + Cd - Dc)^2 + (Ad - Da + Bc - Cb)^2. \end{aligned}$$

1.6. [2, p. 160]

2.1. Suppose that sages have a strategy which wins. Let v be the center of the foot, and let u_1, u_2, u_3 be terminal vertices. Temporarily let v be of the 1st color. Suppose that sages u_1, u_2, u_3 say colors h_1, h_2, h_3 according to their strategies.

Now perform another test: let now v be of the 2nd color. Suppose that sages u_1, u_2, u_3 say colors e_1, e_2, e_3 according to their strategies.

Now perform the final test. For every $i = 1, 2, 3$ we denote by d_i which was not said by the sage u_i in the first two test (if two colors are possible, we choose any one). For every i , we assign the color d_i to the vertex u_i . Since now v knows the colors of all his neighbors, we can predict his answer with respect to his strategy. One of the colors 1 and 2 does not coincide with this answer, so we assign v this color, and sages loose.

2.2. This is Lemma 8 from [1].

Using induction on the number of vertices, we prove the following statement. Let T be any tree, let v be any its vertex, and let c_1, c_2 be two arbitrary colors. Suppose that sages have already chosen a strategy Γ . Then there exists a distribution of hats into vertices, such that sages loose and, moreover, the vertex v has either color c_1 or color c_2 .

Base of induction: if T has only one vertex. This is trivial.

Now we prove the induction step. If we delete the vertex v , the tree T will split into parts T_1, T_2, \dots . Let us denote by u_1, u_2, \dots the vertices in these subgraphs, which were adjacent to v in T . As we did in the solution of the previous problem, we perform two tests. In the first one, we color vertex v in the color c_1 and for every i consider all the distributions of hats in the subtree T_i which are losing for sages if sages use strategy Γ in T_i . Let H_i be the set of colors which u_i can take in these losing distributions. In the second test, let v be of color c_2 and for every i let E_i be the set of colors which u_i can have in all the losing distributions.

Note that in both experiments, the strategies of sages on every tree T_i differ only by the functions of the sage u_i . It means that if we manage to fix the hat color in the vertex u_i , then for every distribution of hats on the tree T_i the other sages would say the same color in both experiments.

By the induction hypothesis, each set H_i and E_i contains at least two elements, hence for every i the intersection of H_i and E_i is nonempty. For each i , choose any color d_i from $H_i \cap E_i$. Now we can construct the losing distribution: each u_i will be of color d_i , every tree T_i will be colored in such a way

that the sages loose, and it remains to color v . Since we know the colors of all its neighbours, we know the answer of v . It does not coincide with one of c_1 and c_2 , so we assign v this color. Now the sages loose.

2.3. [7, Lemma 2c]

Suppose that if $\ell_+(s_{m-1}s_m) \geq 2$, then this chain can be extended to the right by adding a vertex s_{m+1} in such a way that $s_1s_2 \dots s_{m+1}$ is again a disproving chain for which the inequality $\ell_+(s_ms_{m+1}) \geq 2$ is held.

Indeed, potentially we have two (or even three) such extension, denote them by s_mv_1 and s_mv_2 . Consider the short disproving chains s_mv_1w и s_mv_2w , and let us call it *perspective* if $v_i \neq f_{m+1}(s_m, w)$ (we take any of them if both satisfy this condition). In the same way we choose perspective chains for two other values of w . Now we have three perspective chains, and at least two of them have the same color (either v_1 or v_2) of the next vertex. So let s_{m+1} be this value of v_i .

Now without loss of generality let us assume that $\ell_-(s_1s_2) = 3$, $\ell_+(s_{m-1}s_m) \geq 2$. We can unlimitedly extend it to the right. It remains to check that we can loop it. Just before this, we have a long disproving chain $xs_1s_2 \dots s_{n-1}y$, where x has three possibilities and y has at least two possibilities. So there exists $x = y$ such that $x \neq f_n(s_{n-1}s_1)$.

We obtained a cyclic disproving chain, and the sages loose.

2.4. [7, Lemma 2d]

If there exists a two-element disproving chain s_1s_2 such that $\ell_-(s_1s_2) + \ell_+(s_1s_2) > 4$, then the sages loose by the previous problem.

On the other hand, note that for a fixed s , we have

$$\ell_+(ss_1) + \ell_+(ss_2) + \ell_+(ss_3) = 6 \tag{3}$$

(here s_1, s_2, s_3 are three distinct colors). Indeed, if we fix color w , then there exists exactly two colors s_i such that $s_i \neq f(s, w)$. Since there are three possibilities for w , there are six possible continuations.

It means that

$$\sum_{s_1, s_2} \ell_+(s_1s_2) = 18. \tag{4}$$

Hence, the mean value of $\ell_+(s_1s_2)$ is 2. We can similarly show that the mean value of $\ell_-(s_1s_2)$ is 2.

Now let us solve the problem. Note that if for any two-element chain s_1s_2 the inequality $\ell_-(s_1s_2) + \ell_+(s_1s_2) < 4$ is held, then there exists another chain $s'_1s'_2$ such that $\ell_-(s'_1s'_2) + \ell_+(s'_1s'_2) > 4$, and the sages loose.

Hence, the winning strategy can exist only if $\ell_-(s_1s_2) + \ell_+(s_1s_2) = 4$ for any s_1, s_2 .

2.5. [7]

Construct a strategy of sages on the cycle of $N = 3n$ vertices, such that the emcee could not construct a disproving chain.

First, we deduce from Problems 2.12 and 2.13 that for a winning strategy, the number of right pairs of colors ab , where $a \in V_i, b \in V_{i+1}$, is the same for all i . (In the same way the number of left pairs is equal and the number of inert pairs is equal). It would imply that any chain, which disproves a winning strategy, contains links of the same type (i.e., either all the pairs of colors are right, or all the pairs of colors are left, or all the pairs of colors are inert), in this case all the chain will be called right/left/inert. Indeed, as we see in the solution of Problem 2.13, any left pair of colors ab_1 has a unique extension to the left to a more long chain c_1ab_1 , and the pair c_1b is again left. In the same way a right chain can be uniquely extended to the right in such a way that its right link will be again a short right chain. Hence, if there exists a chain disproving all the sages, it contains links of the same type.

Now we find a strategy for the sages such that for all i , there are three right pairs ab , $a \in V_i$, $b \in V_{i+1}$, three left pairs and three inert pairs. So elements of V_i can be enumerated in such a way $V_i = \{v_1^i, v_2^i, v_3^i\}$ that the chains $v_1^1 v_1^2 v_1^3 \dots, v_2^1 v_2^2 v_2^3 \dots, v_3^1 v_3^2 v_3^3 \dots$ are right. We give here the beginnings of these chains, but it can occur that if we loop them, they do not loop with period N , and for the extension $v_1^1 v_1^2 v_1^3 \dots v_1^N v_1^{N+1}$ it turns out that $v_1^{N+1} = v_2^1$ or $v_1^{N+1} = v_3^1$. Denote $v_1^{N+1} = v_{\sigma(1)}^1$, $v_2^{N+1} = v_{\sigma(2)}^1$, $v_3^{N+1} = v_{\sigma(3)}^1$, clearly, σ is a permutation of the three-element set. So the aim of the sages is the following: invent a strategy such that local disproving chains could not loop in an N -element chain because of a permutation σ which has no fixed elements. The same should be true for left chains and for inert chains. Let us examine these chains using the enumerations of colors introduced above.

We have three left pairs ab , $a \in V_i$, $b \in V_{i+1}$, we may assume that these are pairs $v_1^i v_3^{i+1}$, $v_2^i v_1^{i+1}$, $v_3^i v_2^{i+1}$. There are also three left pairs among ab , $a \in V_{i-1}$, $b \in V_i$. Notice that a pair $v_3^{i-1} v_3^i$ is right, hence, the chain $v_3^{i-1} v_3^i v_1^{i+1}$ is not a short disproving chain, consequently, $v_3^{i-1} v_2^i v_1^{i+1}$ is a disproving chain, and this means that the pair $v_3^{i-1} v_2^i$ is a “disproving extension” to the left of the pair $v_2^i v_1^{i+1}$, which means that the pair $v_3^{i-1} v_2^i$ is again left. Using the same reasoning for the other pairs of indices, we obtain that for all i ($i = 1, 2, \dots, N$) the set of left pairs ab , $a \in V_i$, $b \in V_{i+1}$, consists of pairs

$$v_1^i v_3^{i+1}, \quad v_2^i v_1^{i+1}, \quad v_3^i v_2^{i+1}.$$

But then the left chain which begins with the color v_1^1 has the form $v_1^1 v_3^2 v_2^3 v_1^4 \dots$, so its $(N + 1)$ th element (recall that $3 \mid N$) has the form $v_{\sigma(1)}^{N+1}$. Hence, the left chain will not loop if the permutation σ has no fixed elements. The same is true for the inert chains.

It remains to describe the strategy which will provide such a picture. Suppose that all the sages use the same strategy:

$$f_i = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 3 & 1 \end{pmatrix}, \quad i = 1, 2, \dots, N$$

where the element in the p th row and in the q th column is equal to $f_i(p, q)$, and at the end $v_i^{N+1} = v_{\sigma(i)}^1$, where $\sigma : 1 \rightarrow 2 \rightarrow 3 \rightarrow 1$ is an appropriate permutation of the three-element set. In other words, if $v_1^i = 1$, $v_2^i = 2$, $v_3^i = 3$ for $1 \leq i \leq N$, then $v_1^{N+1} = 2$, $v_2^{N+1} = 3$, $v_3^{N+1} = 1$. This is due to the property $f_i(\sigma(p), \sigma(q)) = \sigma(f_i(p, q))$, which can be easily checked.

We leave to the reader the proof of the fact that this strategy has equal number of right, left and inert chains.

2.6. [7]

2.7. [1, Theorem 7]. The statement of Problem 3.4 hints that one or the parts of the graph must contain at least $k - 1$ vertices. It happens that this estimation is exact.

Let G be a complete bipartite graph with $n = k - 1$ vertices on the left side and $m = k^{k^n}$ vertices on the right side. Let C denote the set of all k -colorings of the left side of G . Note that $|C| = k^n$ and $m = k^{|C|}$, hence m is equal to the number of mappings from C to $\{1, 2, \dots, k\}$. Pick a one-to-one correspondence between the vertices on the right side of G and the mappings from C to $\{1, 2, \dots, k\}$, and let each vertex on the right side of G guess its color using the corresponding mapping.

We need the following lemma.

Lemma. Let c_R denote a fixed coloring of the right side of G , and let C' denote the set of all colorings c_L of the left side of G such that the combined coloring (c_L, c_R) causes every vertex on the right side to guess its color incorrectly. Then $|C'| < k$.

Now it's time to define the guessing strategies used by the vertices on the left side of G . Given the coloring of the right side, the set C' defined in the lemma above has at most $n = k - 1$ elements. So let

c_1, c_2, \dots, c_n be a list of colorings which contains every element of C' . For $i = 1, 2, \dots, n$, vertex i on the left guesses that its color is $c_i(i)$. This guessing strategy (combined with the guessing strategy for the vertices on the right side as defined above) guarantees at least one correct answer. This is because the above lemma guarantees that at least one vertex on the right side guesses correctly unless the coloring of the left side belongs to C' . But if the coloring of the left side belongs to C' , then it is equal to c_i for some $i \in \{1, 2, \dots, n\}$, in which case vertex i on the left guesses its color correctly.

It remains to prove the lemma. The proof follows from noting that if C' contains k distinct elements c_1, c_2, \dots, c_k , then there exists a function f from C to $\{1, 2, \dots, k\}$ which assumes k distinct values on the set $\{c_1, \dots, c_k\}$. Let v denote the vertex on the right side of G corresponding to f . Since the set $\{f(c_1), f(c_2), \dots, f(c_k)\}$ contains all k colors, we must have $f(c_i) = cR(v)$ for some i in $1, 2, \dots, k$. Thus, the combined coloring (c_i, c_R) causes vertex v to guess its color correctly, contradicting our assumption that c_i belongs to C' , ending the proof.

2.8. This is Lemma 1 from [4]. We re-write this proof here in a more readable way.

The sages win on the graph G , when they have hats of q colors. Let us call these colors *warm*. The sages win on the graph K_r , when they have hats of r colors. Let us call these colors *cold*. In order to color the graph \tilde{G} into qr colors, we have to assign a warm color and a cold color to each vertex. During the test, the sages will also say two colors: a warm one and a cold one.

To choose a cold color, the sages will look only on the other sages in their copy of K_r (and taking into account only the cold components of their colors). Then for every copy of K_r , exactly one sage will guess his cold color correctly, we call them *lucky*. Every sage can understand which sage is lucky in every adjacent copy of K_r . To guess his warm color, every sage uses his strategy on the graph G , assuming that his neighbors on G have the colors of lucky sages on the K_r s corresponding to vertices of G and taking into account only the warm component of their color. Then at least one lucky sage will guess his color correctly.

2.9. This graph can be obtained from Problems 1.5 and 2.8.

2.10. Let us perform the same computation as we did in Problem 1.3. Let us sum up the number of all guesses in all the distributions of hats. On one hand, there are $3 \cdot 3^2$ guesses. On the other hand, there are 3^3 distributions of hats, so if the strategy of sages is winning, there is exactly one guess in every distribution.

Now fix any strategy and present a distribution of hats where at least two sages guess. Let us assign any color to the sage C . Then give A the hat of color which he says with respect to his strategy for this color of C . произвольную шляпу. Now let B be of the color which he says with respect to his strategy for these colors of A and C .

2.11. Denote the sages by A, B, C, D , and suppose that A does not see B . First of all we show, that there exist two three-element chains $a_1d_1c_1$ and $a_1d_1c_2$ such that A and D do not guess. For this, as we did in the proof of Problem 2.4, consider all the 6 distributions of colors to A and D in such a way that A does not guess (his strategy depends only on the color of D), and 18 possibilities to extend this chain in the direction of C . Since in total D guesses only in 9 situations, there is a color d_1 which he says at most three times. Then among the chains with the beginnings a_1d_1 or a_2d_1 there are at least three losing for D , and by the Pigeonhole Principle there are two three-element chains $a_1d_1c_1$ and $a_1d_1c_2$ such that A and D loose. Give A and D hats of colors a_1 and d_1 , respectively.

Now consider the strategy of B . Let $f_B(a_1, c_1) = b_1$, $f_B(a_1, c_2) = b_2$. Let us give him a hat of the third color b_3 (of any possible color, if $b_1 = b_2$).

Notice that now we know the colors of C 's neighbors: B has color b_1 and D has color d_1 . But $f_C(b_1, d_1)$ does not coincide with one of c_1, c_2 . If we give the sage C the non appropriate color, the sages loose.

2.12. [7, Lemma 3a] We use formula (4) and the analogous formula for ℓ_- :

$$\sum_{a,b} \ell_+(ab) = \sum_{a,b} \ell_-(ab) = 18.$$

Since we consider a winning strategy, for any a, b $\ell_+(ab) + \ell_-(ab) = 4$. Hence, any summand 1, 2, 3 in the first sum corresponds to a summand 3, 2, 1 in the second sum. It means that both sums contain the same number of 1s and 3s.

2.13. [7, Lemma 3d] Let $V_{i+1} = \{b, b_1, b_2\}$. Then, as in Formula (3), and taking into account that $\ell_-(s_1s_2) + \ell_+(s_1s_2) = 4$ we have

$$\ell_-(ab) + \ell_-(ab_1) + \ell_-(ab_2) = 6.$$

Since $\ell_-(ab) = 3$, two other summands are 1 and 2, we may assume that $\ell_-(ab_1) = 1$, it means that there exists a short disproving chain, say, c_1ab_1 . But then $\ell_-(c_1a) = 1$, since in the opposite case $\ell_-(c_1a) + \ell_+(ab_1) \geq 5$ and the strategy is losing by Problem 2.3. We apply the analogous formula

$$\ell_-(c_1a) + \ell_-(c_2a) + \ell_-(c_3a) = 6$$

and see that $\ell_-(c_1a) = 1$, hence, two other summands are 2 and 3. We are done.

2.14. [1, Theorem 16.iii]

2.15. [4]

3.1. All the sages, besides the last one, say the color opposite to the color they see. The last sage says the color he sees.

3.2. [1, Example 6] It follows from Problem 3.1 that at least c sages can guess the color of their hat. In Problem 3.5 you can find the example of the graph for which the number of sages is greater than the number of independent cycles.

3.3. [1, Lemma 4] Suppose that the graph becomes acyclic after deleting vertices v_1, v_2, \dots, v_a . Number the remaining vertices v_{a+1}, \dots, v_n in such a way that the numbers along every edge decrease. In other words, for the last $n - a$ vertices all the edges are directed to the left. Now let us arbitrarily distribute hats among the first a sages. For every next sage, the colors of hats which he sees are already determined, so his answer with respect to his strategy is known. We can give him a hat of another color so that he does not guess.

For this distribution of hats only the first a sages can guess their color.

3.4. This is Theorem 5 from [4]

Take any sages' strategy f and prove that it is losing.

Let A be the set of all but one colors of hats, $|A| = k - 1$. If a is a color, we denote by w_a the collection of $k - 2$ colors (a, a, \dots, a) . The sages from L will always get the same hats of colors w_a , where $a \in A$.

Let us enumerate the vertices of R by r_1, r_2, \dots, r_s in such a way that the numbers along every edge decrease. To simplify the reasoning, we consider only the case when every sage from R sees all the sages with less numbers. Construct the collection of colors $Y = \{y_1, \dots, y_s\}$ for the sages in R . For this, we consequently take

$$\begin{aligned} y_1 &\notin \{f_{r_1}(w_a), a \in A\}; \\ y_2 &\notin \{f_{r_2}(w_a, y_1), a \in A\}; \\ &\dots \\ y_s &\notin \{f_{r_s}(w_a, y_1, y_2, \dots, y_{s-1}), a \in A\}. \end{aligned}$$

Let us explain these formulas for y_s . The sage in the vertex r_s sees all the sages from the part L (their colors are given by the collection w_a), and he sees the sages from part R with smaller numbers. Hence, we know his answer $f_{r_s}(w_a, y_1, y_2 \dots, y_{s-1})$ according to his strategy. The color a takes values in the $(k - 1)$ -element set A ; the set in the right hand of the formula for y_s contains at most $k - 1$ elements, hence, we can choose the appropriate color y_s according to this formula.


Now the set of colors Y is constructed. Let $\ell_1, \ell_2, \dots, \ell_{k-2}$ be the vertices of L . Choose a color $b \in A$ which coincides with none of the colors $f_{\ell_1}(Y), \dots, f_{\ell_{k-2}}(Y)$. Then no sage guesses his color for the distribution (w_b, Y) .

3.5. [1, Example 4]

4.1. Let us present an equality analogous to (1), and with its help construct linear functions, giving the strategies of sages. Since this equality is too long, we will not write it here, so we need some preliminary work.

By an N -dimensional hypercube Q_N we mean a graph, which contains 2^N vertices, enumerated by N -digit numbers in the binary number system, and the edges join numbers differing only in one binary digit. The next constructions can be applied to any hypercube, however they are applicable to the problem about hats only for $N \equiv 2 \pmod{3}$.

Lemma. The edges of the hypercube Q_N can be oriented in such a way that every 4-cycle in Q_N will contain 3 edges pointing to one direction of bypass of this cycle and one edge in the opposite direction.

Proof. Induction on N . Base $N = 2$. 

The step of induction. Suppose that we have already oriented the graph Q_N . We may assume that Q_{n+1} consists of two copies of Q_N , the “left” one and the “right” one, and for every vertex of the left copy there is an edge to the corresponding vertex of the right copy. Suppose that we have already oriented all the edges in the left copy according to the induction hypothesis, and let us orient the right copy in the opposite way. For the edges between the copies, all the arrows will point to the right. It is easy to see that this orientation satisfies the conditions. □

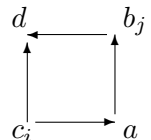
Now let us take independent variables, one for each vertex of Q_N .

Recall that every vertex of Q_N has degree N . Suppose that a is an arbitrary vertex of the graph; b_1, b_2, \dots are vertices such that there are arrows from a to them, c_1, c_2, \dots are vertices such that there are edges from them to a . For any a consider the expression f_a , equal to the square of the linear combination

$$f_a = (a + b_1 + b_2 + \dots - c_1 - c_2 - \dots)^2. \tag{5}$$

Consider the sum $\sum f_a$ of these squares within all the vertices of the graph. Now open all the brackets. For every vertex a , the summands of the form a^2 will appear in this sum with multiplicity $N + 1$, since every such summand appears from the brackets $f_a, f_{b_1}, f_{b_2}, \dots, f_{c_1}, f_{c_2}, \dots$ and only from them. Moreover, every edge ab corresponds to a summand $+2ab$, which appears from the bracket f_a , and a summand $-2ab$, which appears from the bracket f_b . While opening the other brackets, such summands can not appear, so they all vanish.

There is one more type of summands, from the bracket f_a we obtain summands of the form $-2b_jc_i$, let us examine them. Suppose that a has number 00, b_j has number 01, c_i has number 10. Consider also the vertex d with number 11 (we write here only the bytes where the numbers differ). Clearly, $f_d = (d - b_j - c_i + \dots)^2$, so the summand $2b_jc_i$ appears from f_d with the sign “plus”. It will vanish. Another possible orientations of the edges of the cycle can be treated in the same way.



So $\sum_a f_a = (N + 1) \cdot \sum_a a^2$.

Now we come back to our sages. Let $N \equiv 2 \pmod{3}$. Then the sum $\sum_a f_a$ is divisible by 3. It consists of 2^N summands. Clearly, either $f_a \equiv 0$ or $f_a \equiv 1 \pmod{3}$. Hence, at least one of the summands f_a must be zero modulo 3 (for odd N there are at least two such summands). Using the notation of (5), we demand that for every vertex a the sage in this vertex uses the hypothesis $c_1 + c_2 + \dots - b_1 - b_2 - \dots$. Then the sage sitting in a vertex a such that $f_a \equiv 0 \pmod{3}$ will guess the color of his hat.

4.2. [1, Lemma 11] To describe the strategies, we will use the hypercube (see the text before the formulation of the problem).

Let us cut the hypercube into layers: the i th layer will be formed by all the vertices with the sum of coordinates equal to i . The number of non-oriented edges, going from a vertex v to the vertices of the next layer, will be called the *upper degree* $udeg v$ of this vertex, and the number of edges going to the vertices of the previous layer will be called the *lower degree* $ddeg v$ of the vertex.

Consider the edge between the i th and $(i + 1)$ th layers and the corresponding sage (=the coordinate which changes), it equals 1 in the $(i + 1)$ th layer and 0 in the i th layer. The strategy gives the orientation of this edge: if it points from the i th layer to the $(i + 1)$ st layer, then the sage will guess when his hat is of color 1 and will lose in the opposite case. If the edge points from the $(i + 1)$ th layer to the i th, then the sage guesses when his hat is of color 0 and loses in the opposite case. If for every vertex v of the i th layer the number of edges pointing from the $(i + 1)$ th layer to this vertex equals $\lceil udeg v/2 \rceil$, and the number of edges pointing from the $(i - 1)$ st layer to this vertex equals $\lfloor ddeg v/2 \rfloor$, then it is easy to see that we get a balanced strategy.

Construct a balanced strategy, i. e., orient the edges in order to fulfill the properties of upper and lower degrees mentioned above. The idea is clear: we take any edge between the i th and $(i + 1)$ st layers, put any orientation on it and construct an oriented path, adding new edges in such a way that the path remains between the i th and $(i + 1)$ st layers. If it is not possible to extend this path (in both directions) but not all the edges are oriented, we start constructing a new path, etc.. When we orient all the edges, we obtain a balanced strategy.

4.3. [1, Proposition 13] If the number of sages is even, the optimal strategy is a strategy such that for every vertex of the hypercube, the incoming degree and the outgoing degrees are equal. In this case, one can construct an oriented Euler path. Now the strategy of the i th sage is the orientation of edges, parallel to the i th coordinate line. Note that one half of the vertices of the hypercube is in the (left) face $x_i = 0$, and the other half is in the right face $x_i = 1$. The arrows pointing to the left correspond to the case when the sage says 0 and the arrows pointing to the right correspond to the case when the sage says 1. The Euler path contains an equal number of such arrows.

REFERENCES

- [1] Butler S., Hajiaghayi M., Kleinberg R., Leighton T. Hat Guessing Games
- [2] Do N. Communicating with eyes, hats and light bulbs
- [3] Feige U. You can leave your hat on (if you guess its color).
- [4] Gadouleau M., Georgiou N. New constructions and bounds for Winkler's hat game
<http://arxiv.org/pdf/math/1311.2022v1.pdf>
- [5] Krzywkowski M. Hat problem on a graph. Ph.D. dissertation, University of Exeter, 2012.
- [6] Paterson M., Stinson D. Yet another hat game // The electronic journal of combinatorics. Vol. 17. 2010. #R86
- [7] Szczechla W. The three-colour hat guessing game on the cycle graphs // arXiv:1412.3435v2

Yet Another Hat Game

Maura B. Paterson

Department of Economics, Mathematics and Statistics
Birkbeck, University of London
Malet Street, London WC1E 7HX, UK

`m.paterson@bbk.ac.uk`

Douglas R. Stinson*

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo Ontario, N2L 3G1, Canada

`dstinson@uwaterloo.ca`

Submitted: Jan 21, 2010; Accepted: May 26, 2010; Published: Jun 7, 2010

Mathematics Subject Classification: 91A46, 91A12

Abstract

Several different “hat games” have recently received a fair amount of attention. Typically, in a hat game, one or more players are required to correctly guess their hat colour when given some information about other players’ hat colours. Some versions of these games have been motivated by research in complexity theory and have ties to well-known research problems in coding theory, and some variations have led to interesting new research.

In this paper, we review **Ebert’s Hat Game**, which garnered a considerable amount of publicity in the late 90’s and early 00’s, and the **Hats-on-a-line Game**. Then we introduce a new hat game which is a “hybrid” of these two games and provide an optimal strategy for playing the new game. The optimal strategy is quite simple, but the proof involves an interesting combinatorial argument.

1 Introduction

In this introduction, we review two popular hat games and mention some related work. In Section 2, we introduce our new game and give a complete solution for it. In Section 3, we make some brief comments.

*research supported by NSERC discovery grant 203114-06

Table 1: Analysis of Ebert’s hat game for three players

configuration			guesses			outcome
brown	brown	brown	gray	gray	gray	lose
brown	brown	gray	gray			win
brown	gray	brown	gray			win
brown	gray	gray	brown			win
gray	brown	brown	gray			win
gray	brown	gray	brown			win
gray	gray	brown	brown			win
gray	gray	gray	brown	brown	brown	lose

1.1 Ebert’s Hat Game

The following hat game was posed in a 1998 computer science PhD thesis by Todd Ebert [6] (also see [7]). This game garnered a considerable amount of publicity in the late 90’s and early 00’s and was written up in the *New York Times* [10]. There are three players in the game: Alice, Bob, and Charlie. The three players enter a room and a gray or brown hat is placed on each person’s head. The colour of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others.

Each person can see the other players’ hats but not his or her own hat. No communication of any sort is allowed, except for an initial strategy session before the game begins. Once they have had a chance to look at the other hats, the players must simultaneously guess the colour of their own hats, or pass. So each player’s response is one of “gray”, “brown” or “pass”. The group shares a hypothetical \$1,000,000 prize if at least one player guesses correctly and no players guess incorrectly.

It is not hard to devise a strategy that will win 50% of the time. For example, Alice could guess “gray” while Bob and Charlie pass. Is it possible to do better? Clearly, any guess has only a 50% chance of being correct. If more than one player guesses, then the probabilities are reduced: the probability that two guesses are correct is 25%, and the probability that three guesses are correct is 12.5%. Hence, it seems at first glance that it is impossible to win more than 50% of the time.

However, suppose each player uses the following rule: If he observes two hats of the same colour (i.e., gray – gray or brown – brown), then he guesses the opposite colour. Otherwise, when two hats of different colours are observed, he passes. To analyse the probability of winning when using this strategy, we consider all possible distributions of hats. There are $2 \times 2 \times 2 = 8$ cases to consider. In each case, we can figure out if the players win or lose. The probability of winning is equal to the number of winning configurations divided by eight. In the following Table 1, we provide an analysis of all eight cases. Boldface type is used to indicate correct votes.

The group wins in six out of eight cases, so their probability of winning is $6/8 = 3/4 = 75\%$. Observe that each individual guess is correct with a 50% probability. Among

the eight cases, there are six correct guesses and six incorrect guesses. The six correct guesses occurred in six different cases, while the six incorrect guesses were squeezed into two cases. This is why the probability of winning is much higher than 50%, even though each guess has only a 50% chance of being correct!

Here is another way to describe the optimal 3-player strategy:

- specify brown-brown-brown and gray-gray-gray as *bad configurations*.
- If a player’s hat colour could result in a bad configuration, then that player guesses the opposite colour.
- If a player’s hat colour could not result in a bad configuration, then that player passes.

Strategies for more players are based on this idea of specifying certain appropriately chosen bad configurations and then using a similar strategy as in the 3-player game. The bad configurations are obtained using *Hamming codes*, which are perfect single error correcting codes. For every integer $m \geq 2$, there is a Hamming code of length $n = 2^m - 1$ containing $2^{2^m - m - 1} = 2^{n - m}$ codewords.

In a Hamming code, every non-codeword can be changed into exactly one codeword by changing one entry. (This property allows the Hamming code to correct any single error that occurs during transmission.) If the configuration of hats is not a codeword, then there is a unique position i such that changing entry i creates a codeword. Player i will therefore guess correctly and every other player will pass. If the configuration of hats is a codeword, then everyone will guess incorrectly. Thus the group wins if and only if the configuration of hats is not a codeword.

Since there are $2^{n - m}$ codewords and 2^n configurations in total, the success probability is $1 - 2^{-m} = 1 - 1/(n + 1)$. It can be proven fairly easily that this success probability is optimal, and can be attained only when a perfect 1-error correcting code exists. More generally, any strategy for this hat game on an arbitrary number n of players is “equivalent” to a *covering code* of length n , and thus optimal strategies (for any number of players) are known if and only if optimal covering codes are known (see [9] for additional information).

1.2 Hats-on-a-line

Another popular hat game has n players standing in a line. Hats of two colours (gray and brown) are distributed randomly to each player. Each player P_i ($1 \leq i \leq n$) can only see the hats worn by players P_{i+1}, \dots, P_n (i.e., the players “ahead of” P_i in the line). Each player is required to guess their hat colour, and they guess in the order P_1, \dots, P_n . The objective is to maximise the number of correct guesses [3, 2].

Clearly the first player’s guess will be correct with probability 50%, no matter what her strategy is. However, a simple strategy can be devised in which players P_2, \dots, P_n always guess correctly by making use of information gleaned from prior guesses.

As before, suppose that 0 corresponds to gray and 1 corresponds to brown. Let c_i denote the colour of player P_i 's hat, $1 \leq i \leq n$. Here is the strategy:

- P_1 knows the values c_2, \dots, c_n (she can see the hats belonging to P_2, \dots, P_n). P_1 provides as her guess the value

$$g_1 = \sum_{i=2}^n c_i \pmod{2}.$$

- P_2 hears the value g_1 provided by P_1 and P_2 knows the values c_3, \dots, c_n . Therefore P_2 can compute

$$c_2 = g_1 - \sum_{i=3}^n c_i \pmod{2}.$$

P_2 's guess is c_2 , which is correct.

- For any player P_j with $j \geq 2$, P_j hears the values g_1, c_2, \dots, c_{j-1} provided by P_1, \dots, P_{j-1} respectively, and P_j knows the values c_{j+1}, \dots, c_n . Therefore P_j can compute

$$c_j = g_1 - \sum_{i \in \{2, \dots, n\} \setminus \{j\}} c_i \pmod{2}.$$

P_j 's guess is c_j , which is correct.

It is not hard to see that the same strategy can be applied for an arbitrary number of colours, q , where $q > 1$. The colours are named $0, \dots, q-1$ and all computations are performed modulo q . If this is done, then P_1 has probability $1/q$ of guessing correctly, and the remaining $n-1$ players will always guess correctly. Clearly this is optimal.

1.3 Related Work

A few years prior to the introduction of Ebert's Hat Game, in 1994, a similar game was described by Aspnes, Beigel, Furst and Rudich [1]. In their version of the game, players are not allowed to pass, and the objective is for a majority of the players to guess correctly. For the three-player game, it is easy to describe a strategy that will succeed with probability $3/4$, just as in Ebert's game:

- Alice votes the opposite of Bob's hat colour;
- Bob votes the opposite of Charlie's hat colour; and
- Charlie votes the opposite of Alice's hat colour.

This game is analysed in Table 2, where the outcomes for all the possible configurations are listed.

It is also possible to devise a strategy for the majority hats game that uses Hamming codes. We basically follow the presentation from [4]. The idea, which is due to Berlekamp,

Table 2: Analysis of the majority hat game for three players

configuration			guesses			outcome
brown	brown	brown	gray	gray	gray	lose
brown	brown	gray	gray	brown	gray	win
brown	gray	brown	brown	gray	gray	win
brown	gray	gray	brown	brown	gray	win
gray	brown	brown	gray	gray	brown	win
gray	brown	gray	gray	brown	brown	win
gray	gray	brown	brown	gray	brown	win
gray	gray	gray	brown	brown	brown	lose

is to associate a strategy for n players with an orientation of the edges of the n -dimensional cube $\{0, 1\}^n$. Each player's view corresponds in a natural way to an edge of the cube, and that player's guess will be determined by the head of the edge, as specified by the orientation.

If n is a power of 2 minus 1, then there is Hamming code of length n . Direct all the edges of the cube incident with a codeword away from the codeword. The remaining edges form an eulerian graph on the vertices that are not codewords; these edges can be directed according to any eulerian circuit.

The number of correct guesses for a given configuration is equal to the indegree of the corresponding vertex. From this observation, it is not difficult to see that any codeword is a losing configuration for this strategy — in fact, every guess will be incorrect. If the configuration of hats is not a codeword, then there will be $(n + 1)/2$ correct guesses and $(n - 1)/2$ incorrect guesses. So the success probability is $1 - 1/(n + 1)$, as in the Ebert hat game, and this can again be shown to be optimal.

Many other variations of the hat game have been proposed. We complete this section by briefly mentioning some of them.

- Hats could be distributed according to a non-uniform probability distribution ([8]).
- Usually, it is stipulated that each player gets a single guess as to his or her hat colour; however, allowing players to have multiple guesses has also been considered ([1]).
- When sequential responses are used, it may be the case that players can hear all the previous responses (we call this *complete auditory information*), or only some of them, as in [2].
- Some games seek to guarantee that a certain minimum number of correct guesses are made, regardless of the configuration of hats, e.g., in an adversarial setting ([1, 11]).

- In [5], a directed graph, termed a “sight graph”, is used to specify the hats that each player can see. Note that the visual information in Ebert’s game corresponds to a sight graph that is a complete directed graph, while the Hats-on-a-line Game corresponds to the transitive closure of a directed path.

In general, players’ strategies can be deterministic or nondeterministic (randomized). In the situation where hat distribution is done randomly, it suffices to consider only deterministic strategies. However, in an adversarial setting, an optimal strategy may require randomization.

2 A New Hats-on-a-line Game

When the second author gave a talk to high school students about Ebert’s Hat Game, one student asked about sequential voting. It is attractive to consider sequential voting especially in the context of the Hats-on-a-line Game, but in that game the objective is different than in Ebert’s game. A natural “hybrid” game would allow sequential voting, but retain the same objective as in Ebert’s game. So we consider the following new hats-on-a-line game specified as follows:

- hats of $q > 1$ colours are distributed randomly;
- visual information is restricted to the hats-on-a-line scenario;
- sequential voting occurs in the order P_1, \dots, P_n with abstentions allowed; and
- the objective is that at least one player guesses correctly and no player guesses incorrectly.

We’ll call this game the **New Hats-on-a-line Game**.

First, we observe that it is sufficient to consider strategies where exactly one player makes a guess. If the first player to guess is incorrect, then any subsequent guesses are irrelevant because the players have already lost the game. On the other hand, if the first player to guess is correct, then the players will win if all the later players pass.

We consider the simple strategy presented in Table 3, which we term the **Gray Strategy**. The Gray Strategy can be applied for any number of colours (assuming that gray is one of the colours, of course!).

It is easy to analyse the success probability of the Gray Strategy:

Theorem 2.1. *The success probability of the Gray Strategy for the New Hats-on-a-line Game with q hat colours and n players is $1 - ((q - 1)/q)^n$.*

Proof. The probability that P_1 sees no gray hat is $((q - 1)/q)^{n-1}$. In this case, her guess of “gray” is correct with probability $1/q$. If P_1 passes, then there is at least one gray hat among the remaining $n - 1$ players. Let $j = \max\{i : P_i \text{ has a gray hat}\}$. Then players

Table 3: The Gray Strategy

Assume that gray is one of the hat colours. For each player P_i ($1 \leq i \leq n$), when it is player P_i 's turn, if he can see at least one gray hat, he passes; otherwise, he guesses "gray".

P_1, \dots, P_{j-1} will pass and player P_j will correctly guess "gray". So the group wins if player P_1 passes. Overall, the probability of winning is

$$\frac{1}{q} \times \left(\frac{q-1}{q}\right)^{n-1} + 1 \times \left(1 - \left(\frac{q-1}{q}\right)^{n-1}\right) = 1 - \left(\frac{q-1}{q}\right)^n.$$

□

The main purpose of this section is to show that the Gray Strategy is an optimal strategy. (By the term "optimal", we mean that the strategy has the maximum possible probability of success, where the maximum is computed over all possible strategies allowed by the game.) We'll do two simple special cases before proceeding to the general proof. (The proof of the general case is independent of these two proofs, but the proofs of the special cases are still of interest due to their simplicity.)

We first show that the Gray Strategy is optimal if $q = 2$. In this proof and all other proofs in this section, we can restrict our attention without loss of generality to deterministic strategies.

Theorem 2.2. *The maximum success probability for any strategy for the New Hats-on-a-line Game with two hat colours and n players is $1 - 2^{-n}$.*

Proof. The proof is by induction on n . For $n = 1$, the result is trivial, as any guess by P_1 is correct with probability $1/2$. So we can assume $n > 1$.

Suppose there are c configurations of $n - 1$ hats for which player P_1 guesses a colour. We consider two cases:

case 1: $c \geq 1$

There are c cases where P_1 's guess is correct with probability $1/2$. Therefore the probability of an incorrect guess by P_1 is

$$\frac{1}{2} \times \frac{c}{2^{n-1}} \geq \frac{1}{2^n}.$$

case 2: $c = 0$

Since player P_1 always passes, the game reduces to an $(n - 1)$ -player game, in which the probability of winning is at most $1 - 2^{-n+1}$, by induction.

Considering both cases, we see that the probability of winning is at most $\max\{1 - 2^{-n}, 1 - 2^{-n+1}\} = 1 - 2^{-n}$. \square

We observe that the above proof holds even when every player has complete visual information, as the restricted visual information in the hats-on-a-line model is not used in the proof.

We next prove optimality for the two-player game for an arbitrary number of hat colours, as follows.

Theorem 2.3. *The maximum success probability for any strategy for the New Hats-on-a-line Game with q hat colours and two players is*

$$1 - \left(\frac{q-1}{q}\right)^2 = \frac{2q-1}{q^2}.$$

Proof. Suppose that player P_1 guesses her hat colour for r out of the q possible colours for P_2 's hat that she might see. Any guess she makes is correct with probability $1/q$.

We distinguish two cases:

case 1: $r = q$

If $r = q$, then the overall success probability is $1/q$.

case 2: $r < q$

In this case, player P_1 passes with probability $(q-r)/q$. Given that P_1 passes, P_2 knows that his hat is one of $q-r$ equally possible colours, so his guess will be correct with probability $1/(q-r)$. Therefore the overall success probability is

$$\frac{1}{q} \times \frac{r}{q} + \frac{1}{q-r} \times \frac{q-r}{q} = \frac{r}{q^2} + \frac{1}{q}.$$

To maximise this quantity, we take $r = q - 1$. This yields a success probability of $(2q - 1)/q^2$.

Case 2 yields the optimal strategy because $(2q - 1)/q^2 > 1/q$ when $q > 1$. \square

2.1 The Main Theorem

Based on the partial results proven above, it is tempting to conjecture that the maximum success strategy is $1 - ((q-1)/q)^n$, for any integers $n > 1$ and $q > 1$. In fact, we will prove that this is always the case.

The proof is done in two steps. A strategy is defined to be *restricted* if any guess made by any player other than the first player is always correct (furthermore, as already stated, it is not permitted for all players to pass). First, we show that any optimal strategy must be a restricted strategy. Then we prove optimality of the Gray Strategy by considering only restricted strategies.

In all of our proofs, we denote the colour of P_i 's hat by c_i , $1 \leq i \leq n$. The n -tuple (c_1, \dots, c_n) is the *configuration* of hats.

Lemma 2.4. *Any optimal strategy for the New Hats-on-a-line Game is a restricted strategy.*

Proof. Suppose \mathcal{S} is an optimal strategy for the New Hats-on-a-line Game that is not restricted. If player P_1 passes, then the outcome of the game is determined by the $(n-1)$ -tuple (c_2, \dots, c_n) , which is known to P_1 . Since P_1 knows the strategies of all the players, she can determine exactly which $(n-1)$ -tuples will lead to incorrect guesses by a later player. Denote this set of $(n-1)$ -tuples by F . Because \mathcal{S} is not restricted, it follows that $F \neq \emptyset$.

We create a new strategy \mathcal{S}' by modifying \mathcal{S} as follows:

1. If $(c_2, \dots, c_n) \in F$, then P_1 guesses an arbitrary colour (e.g., P_1 could guess “gray”).
2. If $(c_2, \dots, c_n) \notin F$, then proceed as in \mathcal{S} .

It is easy to see that \mathcal{S}' is a restricted strategy. The strategies \mathcal{S} and \mathcal{S}' differ only in what happens for configurations (c_1, \dots, c_n) where $(c_2, \dots, c_n) \in F$. When $(c_2, \dots, c_n) \in F$, \mathcal{S}' will guess correctly with probability $1/q$. On the other hand, \mathcal{S} always results in an incorrect guess when $(c_2, \dots, c_n) \in F$. Because $|F| \geq 1$, the success probability of \mathcal{S}' is greater than the success probability of \mathcal{S} . This contradicts the optimality of \mathcal{S} and the desired result follows. \square

Now we proceed to the second part of the proof.

Lemma 2.5. *The maximum success probability for any restricted strategy for the New Hats-on-a-line Game with q hat colours and n players is $1 - ((q-1)/q)^n$.*

Proof. Suppose an optimal restricted strategy \mathcal{S} is being used. Let A denote the set of $(n-1)$ -tuples (c_2, \dots, c_n) for which P_1 guesses; let B denote the set of $(n-1)$ -tuples for which P_1 passes and P_2 guesses (correctly); and let C denote the set of $(n-1)$ -tuples for which P_1 and P_2 both pass. Clearly every $(n-1)$ -tuple is in exactly one of A , B , or C , so

$$|A| + |B| + |C| = q^{n-1}. \quad (1)$$

Now construct A' (B' , C' , resp.) from A (B , C , resp.) by deleting the first co-ordinate (i.e., the value c_2) from each $(n-1)$ -tuple. A' , B' and C' are treated as multisets. We make some simple observations:

- (i) $B' \cap C' = \emptyset$. This is because P_2 's strategy is determined by the $(n-2)$ -tuple (c_3, \dots, c_n) .
- (ii) For each $(c_3, \dots, c_n) \in B'$, there are precisely $q-1$ occurrences of $(c_3, \dots, c_n) \in A'$. This follows because player P_2 can be guaranteed to guess correctly only when his hat colour is determined uniquely.
- (iii) $A' \cap C' = \emptyset$. This follows from the optimality of the strategy \mathcal{S} . (The existence of an $(n-1)$ -tuple $(c_2, \dots, c_n) \in A$ such that $(c_3, \dots, c_n) \in C'$ contradicts the optimality of \mathcal{S} : P_1 should pass, for this configuration will eventually lead to a correct guess by a later player.)

We now define a restricted strategy \mathcal{S}' for the $(n-1)$ -player game with players P_2, \dots, P_n (here P_2 is the “first” player). The strategy is obtained by modifying \mathcal{S} , as follows:

1. P_2 guesses (arbitrarily) if $(c_3, \dots, c_n) \in A' \cup B'$ and P_2 passes if $(c_3, \dots, c_n) \in C'$.
(This is well-defined in view of the three preceding observations.)
2. P_3, \dots, P_n proceed exactly as in strategy \mathcal{S} .

Since the set of $(n-2)$ -tuples for which P_2 passes is the same in both of strategies \mathcal{S} and \mathcal{S}' , it follows that P_3, \dots, P_n only make correct guesses in \mathcal{S}' , and therefore \mathcal{S}' is restricted.

Let β_n denote the maximum number of $(n-1)$ -tuples for which the first player passes in an optimal restricted strategy. We will prove that

$$\beta_n \leq q^{n-1} - (q-1)^{n-1}. \quad (2)$$

This is true for $n=2$, since $\beta_2 \leq 1$.

Now we proceed by induction on n . We will use a few equations and inequalities. First, from (ii), it is clear that

$$|A| \geq (q-1)|B|. \quad (3)$$

Next, because \mathcal{S}' is a restricted strategy for $n-1$ players, we have

$$|C| \leq q\beta_{n-1}. \quad (4)$$

Finally, from the optimality of \mathcal{S} , it must be the case that

$$|B| + |C| = \beta_n. \quad (5)$$

Applying (1), (3), (4) and (5), we have

$$\begin{aligned} \beta_n &= |B| + |C| \\ &= q^{n-1} - |A| \\ &\leq q^{n-1} - (q-1)|B| \\ &= q^{n-1} - (q-1)(\beta_n - |C|) \\ &\leq q^{n-1} - (q-1)\beta_n + q(q-1)\beta_{n-1}, \end{aligned}$$

from which we obtain

$$\beta_n \leq q^{n-2} + (q-1)\beta_{n-1}.$$

Applying the induction assumption, we see that

$$\beta_n \leq q^{n-2} + (q-1)(q^{n-2} - (q-1)^{n-2}) = q^{n-1} - (q-1)^{n-1},$$

showing that (2) is true.

Finally, using (2), the success probability of \mathcal{S} is computed to be

$$\begin{aligned}
& \Pr[P_1 \text{ passes}] + \frac{1}{q} \times \Pr[P_1 \text{ guesses}] \\
&= \Pr[P_1 \text{ passes}] + \frac{1}{q} \times (1 - \Pr[P_1 \text{ passes}]) \\
&= \frac{1}{q} + \Pr[P_1 \text{ passes}] \times \left(1 - \frac{1}{q}\right) \\
&\leq \frac{1}{q} + \frac{\beta_n}{q^{n-1}} \times \left(1 - \frac{1}{q}\right) \\
&\leq \frac{1}{q} + \left(\frac{q^{n-1} - (q-1)^{n-1}}{q^{n-1}}\right) \times \left(1 - \frac{1}{q}\right) \\
&= 1 - \left(\frac{q-1}{q}\right)^n.
\end{aligned}$$

□

Summarizing, we have proven our main theorem.

Theorem 2.6. *The Gray Strategy for the New Hats-on-a-line Game with q hat colours and n players is optimal.*

Proof. This is an immediate consequence of Theorem 2.1 and Lemmas 2.4 and 2.5. □

3 Comments

It is interesting to compare Ebert's Hat Game, the Hats-on-a-line Game and the New Hats-on-a-line Game. The optimal solutions to Ebert's game are easily shown to be equivalent to covering codes. There are many open problems concerning these combinatorial structures, so the optimal solution to Ebert's game is not known in general. The optimal solution to the Hats-on-a-line Game is a simple arithmetic strategy, and it is obvious that the strategy is optimal. We have introduced the New Hats-on-a-line Game as a hybrid of the two preceding games. The optimal strategy is very simple, but the proof of optimality is rather delicate combinatorial proof by induction. This game does not seem to have any connection to combinatorial structures such as covering codes. The analysis of these three games utilize different techniques. At the present time, there does not appear to be any kind of unified approach that is appropriate for understanding these games and/or other types of hat games.

References

- [1] J. Aspnes, R. Beigel, M. Furst and S. Rudich, *The Expressive Power of Voting Polynomials*, *Combinatorica* **14** (1994), 135–148.
- [2] Sarang Aravamuthan and Sachin Lodha, *Covering Codes for Hats-on-a-line*, *The Electronic Journal of Combinatorics* **13** (2006), #R21.
- [3] Tom Bohman, Oleg Pikhurko, Alan Frieze and Danny Sleator, *Puzzle 15: Hat Problems*, *The Puzzle Toad*. <http://www.cs.cmu.edu/puzzle/puzzle15.html>
- [4] J. P. Buhler, *Hat Tricks*, *Mathematical Intelligencer*, **24(4)** (2002), 44–49.
- [5] S. Butler, M. T. Hajiaghayi, R. D. Kleinberg and T. Leighton, *Hat guessing games*, *SIAM Review* **51** (2009), 399–413.
- [6] Todd Ebert, *Applications of Recursive Operators to Randomness and Complexity*, PhD Thesis, University of California Santa Barbara, 1998.
- [7] T. Ebert and H. Vollmer, *On the Autoreducibility of Random Sequences*, *Proc. 25th International Symposium on Mathematical Foundations of Computer Science*, *Lecture Notes in Computer Science*, **1893** (2000), 333–342.
- [8] W. Guo, S. Kasala, M. Bhaskara Rao and B. Tucker, *The Hat Problem and Some Variations*, in “Advances in Distribution Theory, Order Statistics, and Inference”, Springer, 2006, pp. 459–479.
- [9] Hendrik W. Lenstra and Gadiel Seroussi, *On Hats and Other Covers (extended summary)*. <http://arxiv.org/pdf/cs/0509045>
- [10] Sara Robinson, *Why Mathematicians Now Care About Their Hat Color*, *New York Times*, April 10, 2001. <http://www.nytimes.com/2001/04/10/science/10MATH.html>
- [11] Peter Winkler, *Games People Don’t Play*, in “Puzzlers’ Tribute: A Feast for the Mind”, A. K. Peters, 2002, pp. 301–313.

On a game on graphs

Felix Günther^{*,1}

Irina Mustața^{*,2}

Abstract

We start with the well-known game below: Two players hold a sheet of paper to their forehead on which a positive integer is written. The numbers are consecutive and each player can only see the number of the other one. In each time step, they either say nothing or tell what number they have. Both of them will eventually figure out their number after a certain amount of time. The game is rather cooperative than competitive, and employs the notions of *common knowledge* and *mutual knowledge*. We generalize this game to arbitrary (directed and non-directed) simple graphs and try to establish for which graphs one or both of them will figure out the solution, and how long they do need to find it. We give a complete answer for the case of two players, even if they are both allowed to discuss before the start of the game.

2010 Mathematics Subject Classification: 05C57.

Keywords: game, (directed) graph, common knowledge, mutual knowledge.

1 Introduction

1.1 The original game

We consider a two-player game, also known as a Conway paradox, originally introduced by Conway et al. in [1] and analysed by van Ende-Boas, Groenendijk and Stokhof in [5]. Two players, A and B , get each a sheet of paper on their forehead containing one element of a pair of two consecutive positive integers. They can only see the number on the other player. Now each player tries to figure out which number is on their sheet. The only information they get is that in each time step (which is the same for both, e.g., given by a clock) they are allowed to either say nothing or to say the correct number they have. After some time both of them will eventually figure out their number: as a base case example, if one of them has 1 on their forehead, the other player will know immediately that they have 2, in the next step the other player will know that they have 1. If no one has 1, both of them will know that no one has 1 after the first time step. In the second round a player will know immediately the right answer if the other has 2 and so on. This is formalized in the Theorem on page 5 in [5].

The paradox is that although they might figure out immediately that both numbers are positive without being told so, they cannot figure out the correct solution unless a lower (or upper) bound is given. In each step, they simulate playing a smaller pair of consecutive integers, hence the problem has an essentially finite descent approach, the direction being however bottom-up.

^{*}Berlin Mathematical School, Institut für Mathematik, MA 2-2, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany.

¹Supported by the Deutsche Telekom Stiftung. E-mail: fguenth@math.tu-berlin.de

²Supported by the Berlin Mathematical School. E-mail: mustata@math.tu-berlin.de

Equivalently, we can consider the set of positive integers as a semi-infinite path (a very simple graph structure). If an upper bound is given as well, the path is finite. Now both players are sitting on an edge knowing only the position of the other player and try to figure out their own position. The strategy we described above consists of cutting off leaves (or edges, as in [5], but the term “leaves” is better suiting our purpose).

1.2 Background

One classical formulation of such a problem we find in the book of Fagin, Halpern, Moses and Vardi [2]: A family has n children playing outdoors one day. Some of them (for instance k) have gotten some mud on their foreheads, and whoever does, must clean up before dinner. Everyone can only see the faces of others, and no discussion of whose forehead is muddied happens. At some point the father goes out, looks at them, and says “At least one of you has mud on their forehead.” Nothing happens for the first $k - 1$ time intervals, and during the k th, the muddied children go and wash their faces. The question is, what was the reasoning behind this. After all, the father does not impart new information to any child (assuming $k \geq 2$). However, what he says makes each child aware that the others have the same information.

As for example in [2], we can formalize the above, by stating that these paradoxes play on the notion of mutual vs. common knowledge. While mutual knowledge is limited to one epistemic level (“ A and B know a fact φ ”), common knowledge presumes an ad infinitum iteration of the statement: “ A knows that B knows that A knows... the fact φ ” and the converse. Hence, if in the game from 1.1 no bounds for the pair of numbers are given, it is mutual knowledge if, say, A and B are assigned the pair $(5, 6)$ that the numbers are positive, but, since lacking a base case, no common knowledge can be derived from it. Thus, it is not possible that the players work their way up to a solution.

Introduced by Lewis in [3], and also analysed in [2], common knowledge plays a central role in daily life, as it is necessary for the interaction of a group of agents and for establishing convention. For instance, one such convention is that the red colour of the street light means “stop”. Here, it does not suffice that each driver and pedestrian is aware of this, but that each is aware the other is aware, and so on (that is, it is safe to cross the road as a pedestrian when it is red for vehicles, since any pedestrian assumes any driver is aware of the convention).

Several models exist for this (and epistemological aspects in general), one of them using an extension of modal logic [2, 4], leading to a graph representation based on the concept of possible worlds (from the perspective of any agent, given their current level of information) [2]. For a detailed description we direct the reader to the given literature.

1.3 Organization of the paper

Our purpose is to generalize the game from 1.1 to finite graphs, where the players are given the endpoint labels of an arbitrary edge, with the aim to guess it. There are essentially two variants of this game: Either they are both allowed to speak in each time step, or they talk one after another, the starting player being known. Note that in the base problem above, there is not a big difference between both variants.

In Section 2, we will discuss the case of two players on finite (simple) graphs. First, we show in Section 2.1 that at least one player will figure out the solution for any edge of the graph if and only if the graph is a forest. The result is the same if both players are allowed to discuss before the start of the game, already knowing the graph. Moreover, cutting off leaves is the most effective strategy in

the sense of knowing the solution as quickly as possible. It will follow that cutting off leaves is also the strategy they come up with if they are not allowed to discuss before. If they speak in turns, the strategy is very similar, but slightly differs with respect whose turn is it. Note that if both players can discuss a strategy, it does not matter whether they are allowed to talk at the same time or not. We describe the strategy of cutting off leaves in more detail in the proof of Theorem 2.2.

In Section 2.2 we show that for any tree there exists a strategy such that both players can determine their position. In the case they do not discuss before, we give a criterion which player will answer first, how long the player needs and if the other one also can find out their position. Here it makes a difference whether they talk simultaneously or alternately in each time step.

The ideas we developed in the case of undirected graphs work for directed graphs in a similar way. Only the concept of a path will slightly differ. We state the corresponding results in Section 3.

We close our paper with remarks to some possible future directions in Section 4.

2 Two-player game on simple graphs

Let $G = (V, E)$ be a finite simple graph. The players A and B are placed on nodes $u \neq v \in V$ not knowing on which position in V they are, but knowing that their assigned nodes are adjacent. For simplicity, we identify the players with the vertices they are placed on. Now both try to figure out on which position they are knowing only G and the vertex of the other. Since the connected component of the graph they are placed on is common knowledge, we will assume that G is connected.

2.1 Strategy

In the following, we will simultaneously handle the cases whether they are taking turns in speaking or are making their statements at the same time. For the next lemma, it does not matter whether both players have discussed a strategy before or come up with one independently.

Lemma 2.1. *Suppose both players have a strategy such that they are knowing the right answer when they say so. Let A guess their position after n time steps where B has not said anything before time n . Then, if A had been placed on a different vertex adjacent to B , B would have guessed their position correctly not later than time $n - 1$.*

Proof. Assume the contrary. Then A would have the same information in both situations, namely the position of B and that B had not said anything in the $n - 1$ steps before. Thus, A would guess the same position for both cases, contradicting that they knows the correct answer. \square

The following proposition will describe the graphs where such a game is possible to finish, regardless of the chosen positions:

Theorem 2.2. *All edges of a simple graph G can be guessed correctly by at least one of the players if and only if G is a tree.*

Proof. \Rightarrow : Suppose the contrary. Since G is connected, G contains a cycle. We choose an edge of the cycle and a positioning of the two players on it in such a way, that the time n needed for guessing the edge correctly is minimal. By Lemma 2.1, at least one neighboring edge of the cycle is guessed in at most $n - 1$ steps (assuming the right positioning of players), contradiction.

\Leftarrow : In the following, we consider a tree G . For any $X \subseteq V(G)$ we define $L(X)$ as the set of all leaves of G contained in X .

Suppose first that they talk simultaneously. If both players have not discussed a strategy before, then they can at least cut off all vertices of degree 1 of the graph after both players have said nothing, since one of them would now give the answer immediately if they know the other one to be on a leaf. The strategy corresponding to cutting off all vertices of (current) degree 1 will be called *cutting off leaves*. Thus, all edges of a tree can be guessed with this strategy.

Suppose now they speak alternately, A being the starting player. Since G is a tree and thus bipartite, we take the corresponding decomposition of V into V_A and V_B , such that $A \in V_A$. After A said nothing in the first round, B knows that they are not in $L(V_B)$ and can cut all these leaves off. Both players can then remove $G(L(V_B))$ and update G . If they still do not know where they are, A can now cut off all vertices of $L(V_A)$, followed again by removing $G(L(V_A))$, and so on. Since G is a tree, they cannot get stuck. We call this strategy *cutting off leaves* as well. \square

The following theorem shows that they cannot exclude more vertices in a step, such that cutting off leaves is exactly the strategy they will play if they cannot talk about a strategy before.

Theorem 2.3. *Let $G = (V, E)$ be a tree and suppose both players have a correct strategy. Take any positioning of A and B . Partition V into two independent sets V_A and V_B such that $A \in V_A$. Now we direct any edge to the player who knows the answer first (if they both say the correct answer in the same moment, the edge will be bidirected) and label it by the time in which the player says the correct answer. Here the choice of players on the edge is given by the partition of V into V_A and V_B .*

Then the labels are strictly increasing along directed paths. Moreover, unless G consists of only one edge, there exist either one or two vertices with all incident edges going inward. For all other vertices, there is exactly one incident edge going outward. If there are two vertices with all incident edges going inward, then they are connected by a bidirectional edge. Also, this is the only case an edge with two directions can appear.

In particular, any strategy is a variant of cutting off leaves, and both players come up with cutting off leaves if they do not discuss before.

Proof. That labels are strictly increasing along directed paths follows directly from Lemma 2.1. Of course, in the case they speak alternately, the label corresponding to an edge pointing to the player speaking at odd or even time can only be odd or even, respectively.

The endpoint v of an unextendible directed path is defined as a vertex with all incident edges going inward. By Lemma 2.1, any path from a point $v' \neq v$ to v is directed to v . If no incident edge has two directions, v is the only vertex with this property. If there is such one, the other vertex v^* incident to this edge also has the property of having all incident edges ingoing.

Lemma 2.1 shows that if one edge incident to a vertex is outgoing, all other edges incident to this vertex have to be ingoing and cannot be outgoing. In particular, bidirected edges can only connect vertices with all incident edges going inward. No other adjacent edge can have two directions. It follows that v and v^* are the only vertices with all incident edges being ingoing, and the edge incident to both is the only one with two directions.

We directly see that in time step n only leaves of the graph consisting of edges with labels greater or equal than n are guessed, and the player on the interior endpoint says the correct answer (unless the updated graph consists of only one edge by this point and we cannot speak about the interior). Thus, any strategy is a variant of cutting off leaves, and the latter one is the fastest one among all

strategies. Since both players can at least cut off all leaves of the corresponding set V_A or V_B in their step when they do not discuss before, cutting off leaves is exactly the strategy they come up with if they have not discussed before. \square

Example. Figure 1 and Figure 2 visualize the strategy of cutting of leaves when speaking simultaneously or alternately, respectively, in the notation of Theorem 2.3. White vertices correspond to V_A and black to V_B . Player A starts and talks at odd time, player B at even time.

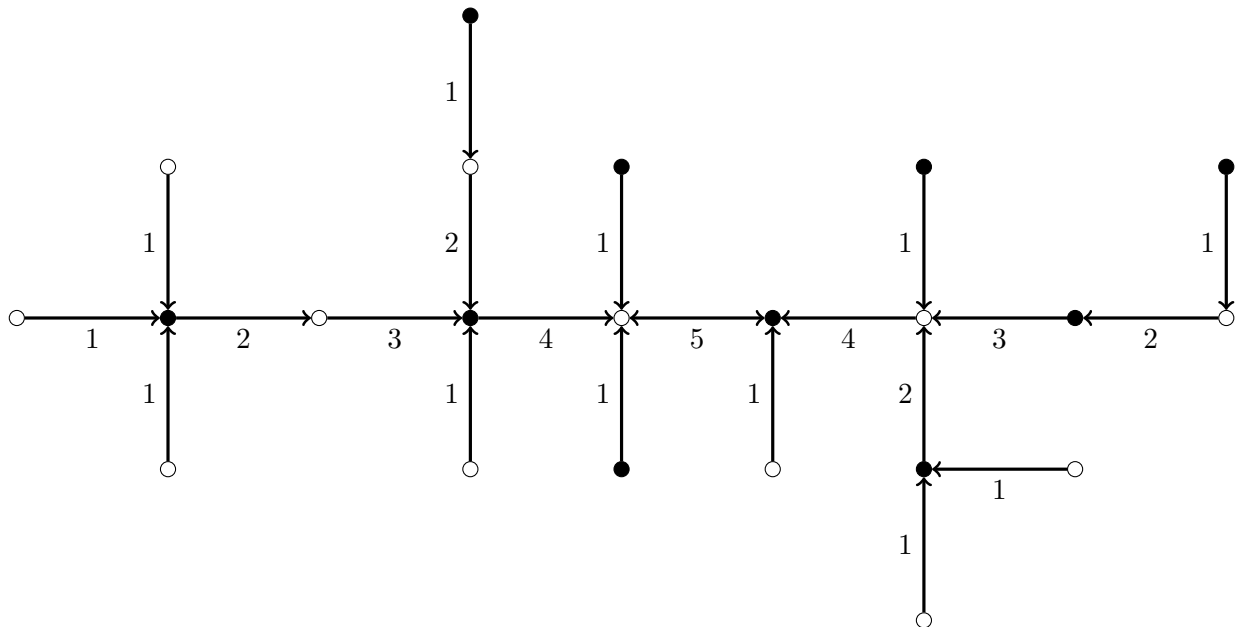


Figure 1: Notation of Theorem 2.3 for cutting off leaves when speaking simultaneously

We can summarize the difference between the cases where the players speak simultaneously or alternately, as follows:

- If the game is played simultaneously: At each time step, G is updated by removing all leaves of G .
- If the game is played alternately: After each odd time step, G is updated by removing all leaves of G that are in V_B , whereas after each even one, all vertices of V_A that are leaves of G get removed.

Remark. Suppose G is a directed tree equipped with a labeling fulfilling the statement of Theorem 2.3, respecting the parity in the case the players speak alternately, meaning that the starting player can only guess their position at odd and the other one at even times. Then this labeling corresponds to a strategy: Player A (B) looks at all edges incident to the position of B (A), and if an edge with label n is pointing away, they indicate at time n the endpoint of this edge unless B (A) has said their position before (we do not specify yet what they will say after the other player has told their position, assuming for the moment the game stops at this point). Note that there is at most one such edge, since at most one edge incident to a vertex is outgoing. Since each edge is directed, at least the player on the vertex where the edge is ingoing will say the answer after some time. The strategy is correct, since by construction, all ingoing edges to the position of B (A) are guessed by B (A) themselves before.

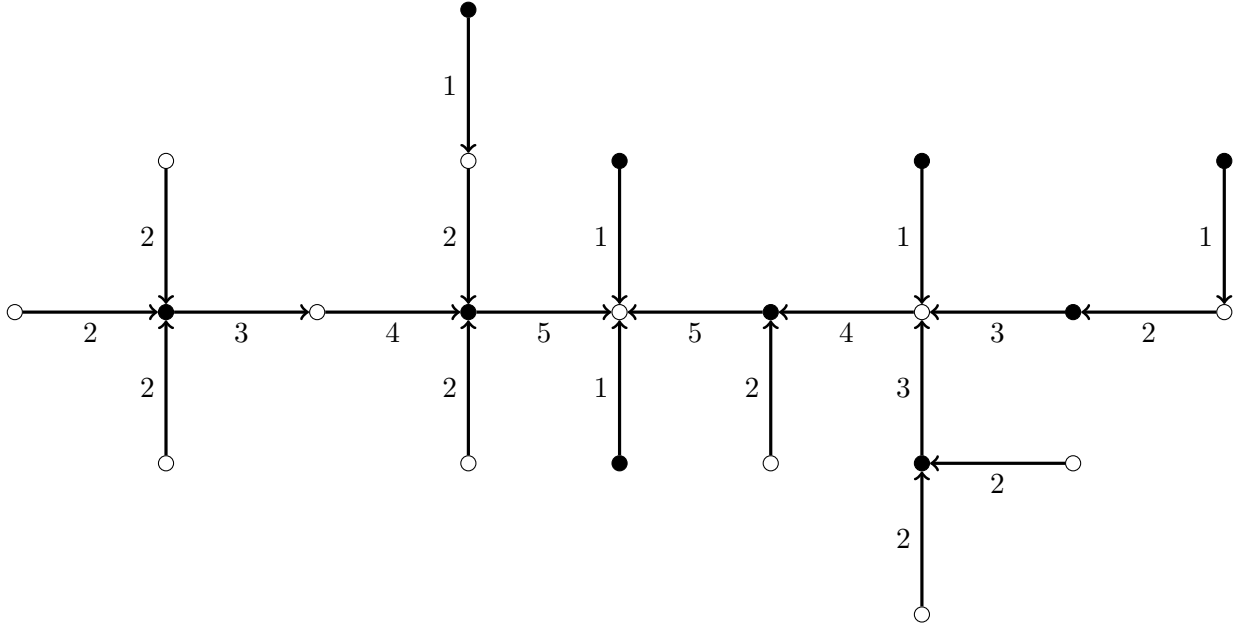


Figure 2: Notation of Theorem 2.3 for cutting off leaves when speaking alternately

Finally, note that if A and B can discuss before, the cases when speaking simultaneously or alternately are essentially equivalent.

Proposition 2.4. *If both players can discuss a strategy before the start of the game, the set of edges of the graph they can find out correctly is the same independent of whether they speak simultaneously or alternately in each time step.*

Proof. Suppose the players have a strategy if they speak simultaneously. They can adapt it to the alternative case as follows: they agree before that player A speaks in each odd and player B in each even time step. Moreover, B ignores the information they just got from the immediately preceding round of A just until after their own turn is over.

Now suppose they have a strategy when they speak alternately. Then in each time step, when one player would remain silent, the same says nothing when they are allowed to talk at the same time. This yields an equivalent strategy for the case of simultaneously speaking. \square

2.2 Who is first?

Proposition 2.5. *For any tree $G = (V, E)$, there is a strategy allowing both players to determine their position.*

Proof. Direct and label G according to Theorem 2.3 and the cutting off leaves strategy. Now multiply all labels by $|E|$. Establish a bijection ϕ between E and the set $\{0, 1, \dots, |E| - 1\}$. Now for each $e \in E$ add $\phi(e)$ to the label of e . In the case they speak alternately, multiply the resulting number by 2. Additionally, subtract 1 if and only if the edge is pointing to the starting player. We obtain a labeling of G fulfilling the statement of Theorem 2.3 with all labels being different. By the remark after Theorem 2.3, the labeling corresponds to a strategy. Since all labels are different, the player who

does not say the answer first can figure out their position correctly by the time the other one needed. Thus, both players can find out their position. \square

Because both players can figure out their position with the right strategy by Proposition 2.5, we now consider the case they do not talk about a strategy before. We will discuss whether both players can get the right answer and how long the first player needs. This also gives an lower bound for the case of general strategies by Theorem 2.3.

Theorem 2.6. *Let $G = (V, E)$ be a tree and assume that both players play without discussing about a strategy before. Let $h_B(A)$ be the height of A in the tree rooted in B and $h_A(B)$ the height of B in the tree rooted in A . Let $h'_B(A) := h_B(A) + 1$ if $h_B(A)$ is odd, and $h'_B(A) := h_B(A)$ otherwise. In the same way, let $h'_A(B) := h_A(B) + 1$ if $h_A(B)$ is even, and $h'_A(B) := h_A(B)$ otherwise.*

- (i) *Suppose they speak simultaneously in each step. If $h_B(A) > h_A(B)$, player A will first know their position at time $h_A(B)$; if $h_B(A) = h_A(B)$, both of them will figure out their position at the same time $h_B(A) = h_A(B)$; if $h_B(A) < h_A(B)$, player B says the answer first at time $h_B(A)$.*

In the case that $h_B(A) > h_A(B)$, B will figure out their position at time $h_A(B) + 1$ as well if and only if there is no node other than B in the tree rooted in A with height $h_A(B)$. The analogous statement is true for the case $h_B(A) < h_A(B)$.

- (ii) *Suppose they speak alternately in each step, A being the starting player. If $h'_B(A) > h'_A(B)$, player A will first know their position at time $h'_A(B)$; if $h'_B(A) < h'_A(B)$, player B says the answer first at time $h'_B(A)$.*

In the case that $h'_B(A) > h'_A(B)$, B will figure out their position at time $h'_A(B) + 1$ as well if and only if there is no node other than B in the tree rooted in A with height $h'_A(B)$ or $h'_A(B) - 1$. The analogous statement is true for the case $h'_B(A) < h'_A(B)$.

Proof. (i) Consider the longest simple path starting in A going through B and the longest simple path starting in B going through A . By Theorem 2.3, the shorter of them will determine the time until one player knows the answer. If both have the same length, both players will know the answer at the same time (the corresponding edge has two directions), otherwise the edge is pointing to the player being on the boundary of the shortest path. The lengths of these paths are given by $h_A(B)$ and $h_B(A)$, respectively.

For the second part of the statement, assume without loss of generality that A knows the answer first at time n . Then B can figure out their position as well if and only if the edge incident to A and B is the only edge incident to A with label $h_A(B)$ (note that any edge going out from A has a label greater than $h_A(B)$ by Lemma 2.1). This is the case if and only if there is no node other than B in the tree rooted in A with height $h_A(B)$.

(ii) In the same way as in (i), the label on the edge connecting A and B is given by the smaller of $h'_B(A)$ and $h'_A(B)$. The possible difference of 1 between h' and h is due to the fact that A can say the answer at odd and B at even times only. The edge is directed to A if $h'_A(B)$ is smaller, otherwise it is directed to B .

Without loss of generality, assume A knows the answer first. As above, B can figure out their position as well if and only if the edge incident to A and B is the only edge incident to A with label $h'_A(B)$. Remembering that A can answer at odd times only, this is only the case if and only if there is no node other than B in the tree rooted in A with height $h'_A(B)$ or $h'_A(B) - 1$. In the first case, the leaf determining the height of B is in V_B , in the second case in V_A . As before, V is partitioned into V_A and V_B such that each edge is incident to points in both sets and $A \in V_A$. \square

3 Two-player game on directed graphs

Let $G = (V, E)$ be a finite directed graph. The players A and B are placed on an edge in E . For simplicity, we identify the players with the vertices they are placed on. Now both try to figure out on which position they are knowing only G , the vertex of the other and the orientation of the edge.

In the following, we are only considering simple directed graphs if we speak about a directed graph. Note that the graphs in Section 2 occur as a special case, when any two adjacent vertices are connected by two edges with different orientation. Since the ideas are very similar, we will often refer to Section 2 for proofs of analogous statements.

Definition. An edge together with a placement of A and B on the endpoints is called *admissible*, if the orientation of the edge agrees with the orientation the players got assigned before.

If the placement is clear (for example, when the position of one player is given or for vertex sets associated to A or B), we will not give the details.

The following analogue of Lemma 2.1 is shown in the same way.

Lemma 3.1. *Suppose both players have a strategy such that they are knowing the right answer when they say so. Assume A guesses their position after n time steps where B has not said anything before time n . Then if A had been placed on a vertex $A' \neq A$ adjacent to B , such that the edge (A', B) is admissible, B would have guessed their position correctly no later than time $n - 1$.*

To transfer the theorems of the previous section to the case of directed graphs, we need a new concept of paths, see for example Figure 3.

Definition. A *zig-zag-path* is a path, where at each interior vertex either both incident edges are ingoing or both are outgoing. If the path is closed, we call it a *zig-zag-cycle*.

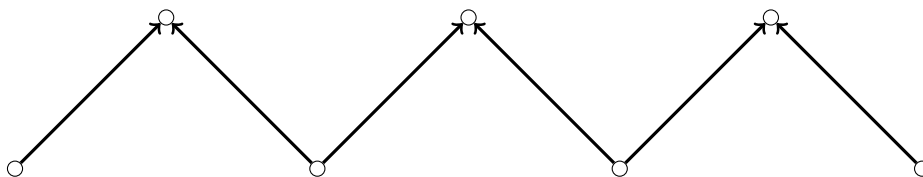


Figure 3: A zig-zag-path

We introduce now vertex sets V_A and V_B .

Definition. $A \in V_A$, whereas any other vertex A' is in V_A if and only if there is a zig-zag-path from A to A' of even length such that the first edge (incident to A) of this path is admissible. V_B is defined in the same way as V_A by replacing A by B . Equivalently, any point of V_B can be reached by an appropriate zig-zag-path of odd length starting in A .

Remark. Note that also for connected G without zig-zag-cycles, there might be vertices being neither in V_A nor in V_B . Moreover, the intersection $V_A \cap V_B$ might be non-empty.

If both players have not discussed a strategy before, they can restrict to the subgraph $G(V_A \cup V_B)$ immediately. Namely, this set can be constructed in the following way: Starting in A , add all adjacent vertices B' with an admissible orientation of the edge AB' (i.e. all B' candidates for B). For each of

them, add all adjacent vertices that are candidates for A . Continue this procedure. This set is known for both A and B as well knowing the position of each other.

This resulting graph G' will be further modified as follows: Note that the only vertices with both indegree and outdegree non-zero are those belonging to both V_A and V_B . Let $v \in V(G')$ with $\text{indeg}(v) \neq 0$ and $\text{outdeg}(v) \neq 0$. This vertex will now be removed and replaced (split) by v_{in} and v_{out} , vertices incident exactly to the ingoing and outgoing edges of v , respectively. Since the procedure strictly decreases the number of vertices with mixed degree, it must be finite.

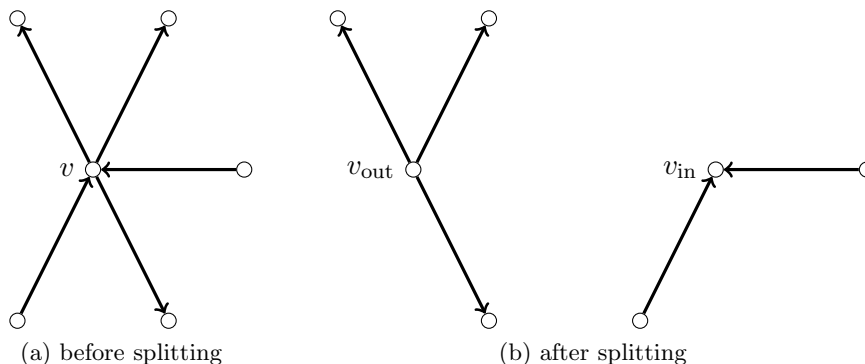


Figure 4: Split vertex v

Remark. The graph G_s obtained after applying the sequence of all possible splits to G' has only zig-zag paths and all edges are admissible.

It is important to notice that G_s contains a zig-zag cycle if and only if G' does. Indeed, suppose G_s has such a cycle. Then, there are two cases:

- No pair of vertices on the cycle stem from the same split vertex. Then, it must also have existed before splitting, since the procedure does not add new edges.
- There exists at least a pair $v_{\text{in}}, v_{\text{out}}$ that stem from the same vertex v before the splitting, assuming without loss of generality that v was the last such split vertex. In this case the cycle already existed before splitting, passing twice through v .

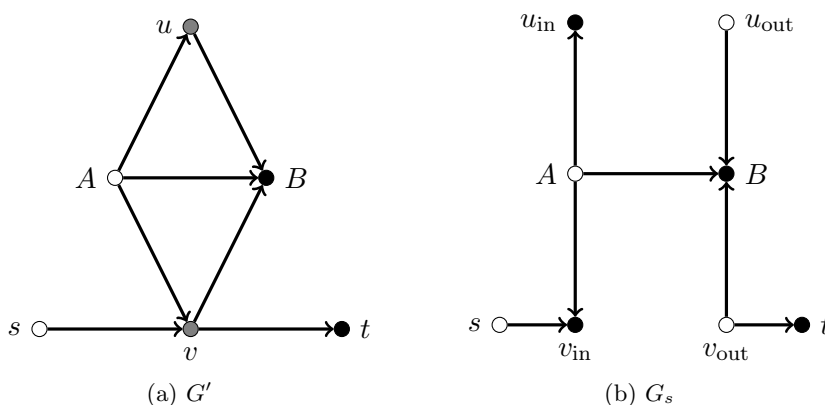


Figure 5: Obtaining the splitgraph

We can now easily reduce the problem to the undirected case and prove, with the exact same argument, the following theorem.

Theorem 3.2. *A directed graph G has all edges guessable under the above conditions if and only if it does not contain zig-zag cycles (i.e. it is a zig-zag forest). All conclusions relating to the number of necessary steps or to who makes the first guess hold. The comparison of the cases of having discussed a strategy before or not concludes along the same lines.*

4 Further directions

One variation, for the two-player case, would be introducing “cycle” as a third allowed answer in addition to saying nothing or the results. This seems to allow further edges to be correctly guessed in a general graph.

On the other hand, one can naturally generalize the problem to a multiplayer game where n players are the vertices of a subgraph H of G with known isomorphism class. The players may or may not know their positions in H , otherwise the rules of the game stay the same. It would be interesting to describe how the game runs in at least a number of particular such cases.

Acknowledgment

We would like to thank Thomas Hixon for numerous fruitful discussions.

References

- [1] J.H. Conway, M.S. Paterson, and U.S.S.R. Moscow. A headache-causing problem. In J.K. Lenstra et al., editor, *Een pak met een korte broek: Papers presented to H.W. Lenstra on the occasion of the publication of his “Euclidische Getallenlichamen”*. Private publication, Amsterdam, 1977.
- [2] R. Fagin, J.Y. Halpern, Y. Moses, and M. Vardi. *Reasoning About Knowledge*. The MIT Press, Cambridge, Massachusetts and London, United Kingdom, 1995.
- [3] D.K. Lewis. *Convention: A Philosophical Study*. Harvard University Press, Cambridge, Massachusetts, 1969.
- [4] J.-J.Ch. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*, volume 41 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, Cambridge, United Kingdom, 1995.
- [5] P. van Emde Boas, J. Groenendijk, and M. Stokhof. The Conway paradox: its solution in an epistemic framework. In *Proceedings of 3rd Amsterdam Montague Symposium*, pages 87–111. Math. Centrum, Amsterdam, 1980. Reprinted by Foris Publications, 1984.

New constructions and bounds for Winkler’s hat game

Maximilien Gadouleau* Nicholas Georgiou†

November 11, 2013

Abstract

Hat problems have recently become a popular topic in combinatorics and discrete mathematics. These have been shown to be strongly related to coding theory, network coding, and auctions. We consider the following version of the hat game, introduced by Winkler and studied by Butler et al. A team is composed of several players; each player is assigned a hat of a given colour; they do not see their own colour, but can see some other hats, according to a directed graph. The team wins if they have a strategy such that, for any possible assignment of colours to their hats, at least one player guesses their own hat colour correctly. In this paper, we discover some new classes of graphs which allow a winning strategy, thus answering some of the open questions in Butler et al. We also derive upper bounds on the maximal number of possible hat colours that allow for a winning strategy for a given graph.

1 Introduction

Hat games are a popular topic in combinatorics. Typically, a hat game involves n players, each wearing a hat that can take a colour from a given set of q colours. No player can see their own hat, but each player can see some subset of the other hats. All players are asked to guess the colour of their own hat at the same time. For an extensive review of different hat games, see [1]. Different variations have been proposed: for instance, the players can be allowed to pass [2], or the players can guess their respective hat’s colour sequentially [3]. The variation in [2] mentioned above has been investigated further (see [1]) for it is strongly connected to coding theory via the concept of covering codes [4]; in particular, some optimal solutions for that variation involve the well-known Hamming codes [5]. In the variation called the “guessing game,” players are not allowed to pass, and must guess simultaneously [6]. The team wins if everyone has guessed their colour correctly; the aim is to maximise the number of hat assignments which are correctly guessed by all players. This version of the hat game has been further studied in [7, 8] due to its relations to graph entropy, to circuit complexity, and to network coding, which is a means to transmit data through a network which allows the intermediate nodes to combine the packets they receive [9].

In this paper, we are interested in the following hat problem, a small variation to Winkler’s hat game presented in [10]. We are given a directed graph D (without loops and repeated arcs, but possibly with bidirectional edges) on n vertices and a finite alphabet $[q] = \{0, \dots, q - 1\}$ ($q \geq 2$). We say that $f = (f_1, \dots, f_n) : [q]^n \rightarrow [q]^n$ is a D -function if every local function $f_v : [q]^n \rightarrow [q]$ only depends on the values in the in-neighbourhood of v in D : $f_v(x) = f_v(x_{N^-(v)})$.

*School of Engineering and Computing Sciences, Durham University, Durham, UK. Email: m.r.gadouleau@durham.ac.uk

†Department of Mathematical Sciences, Durham University, Durham, UK. Email: nicholas.georgiou@durham.ac.uk

We ask whether there is a D -function over $[q]$ such that for any $x = (x_1, \dots, x_n) \in [q]^n$, $f_v(x) = x_v$ for some vertex v . In that case, we say that D is q -solvable and that f solves D .

In terms of the hat game, each vertex in the graph represents a player, an arc from player u to v means that v can see u . The set $[q]$ then represents the possible colours of their hats and $x = (x_1, \dots, x_n) \in [q]^n$ represents a possible hat assignment. Each player v must guess the colour of their hat according to some pre-determined rule which can only depend on the hats that they see: $f_v(x_{N-(x)})$. If one player guesses correctly, i.e., $x_v = f_v(x)$, then the team wins; if all guess incorrectly, the team loses. The question is then to come up with a winning strategy regardless of the hat assignment.

Clearly, if D is q -solvable, then it is also $(q-1)$ -solvable. The clique K_q is q -solvable [10]: if we denote the players as elements in $[q]$, then v guesses that the sum of all hat assignments is equal to v modulo q : $f_v(x) = -\sum_{u \neq v} x_u + v$. More generally, if the players play on K_n , then there is a strategy which guarantees that at least $\lfloor n/q \rfloor$ players guess correctly (simply split K_n into $\lfloor n/q \rfloor$ cliques K_q). The case for K_n and $q = 2$ colours with unequal probabilities was further studied in [11, 12]; its relation to auctions has been revealed in [13] and developed in [14].

Results for other classes of graphs have been found in the literature. Butler et al. proved in [15] that for any q , there exists a q -solvable undirected bipartite graph. Unfortunately, that graph has a doubly exponential number of vertices. In the same paper, they also proved that undirected trees are not 3-solvable.

The main contributions of this paper are as follows. In [15], it is asked whether there exist K_q -free q -solvable undirected graphs with a polynomial number (in q) of vertices. We give an emphatic affirmative answer: for any ϵ , there exist $K_{\epsilon q}$ -free q -solvable graphs with a linear number of vertices; moreover, we present a class of K_ω -free graphs with $\omega = o(q)$ which are q -solvable and have a polynomial number of vertices. We also refine the multiplicative constant for some values of ϵ by considering small undirected graphs or directed graphs. We also prove some non-solvability results for bipartite graphs and for graphs with a large independent set. Another question asked in [15] concerns so-called *edge-critical* graphs, i.e., undirected graphs which are q -solvable but which have no q -solvable proper spanning subgraph. Clearly, the only edge-critical graph for $q = 2$ colours is K_2 ; [15] asks whether there exists an infinite family of edge-critical graphs for any other $q \geq 3$. By studying the solvability of cycles, we are able to show that the cycles whose length are a multiple of six form an infinite family of edge-critical graphs for 3 colours.

The rest of the paper is organised as follows. In Section 2, we prove the existence of bipartite or K_ω -free q -solvable undirected graphs with a relatively small number of vertices. In Section 3, we refine some constructions by extending our consideration to directed graphs. We then derive some non-solvability results in Section 4. Finally, we prove the existence of a class of edge-critical 3-solvable graphs in Section 5.

2 Undirected constructions

In [15], it is proved that for any $q \geq 2$ there exists a q -solvable bipartite graph with a doubly exponential number of vertices ($q^{q^{q-1}} + q - 1$ vertices to be exact). We refine their argument to construct a q -solvable bipartite graph with only an exponential number of vertices.

We say that a set of words S in $[q]^m$ is *distinguishable* if there exists a word $x \in [q]^m$ such that $d_H(x, s) \leq m - 1$ for all $s \in S$, where d_H is the Hamming distance. Alternatively, using the terminology of [16], this is equivalent to S having remoteness at most $m - 1$. The main reason we are interested in distinguishable sets is as follows. If in a graph there is an independent set M of cardinality m , and the vertices in M know that their hat assignment $x \in [q]^m$ is any

possible element of a set $S \subseteq [q]^m$, then there exist guessing functions for the vertices of M achieving at least one correct guess if and only if S is distinguishable.

Theorem 1 (See [15]). *The complete bipartite graph $K_{q-1, (q-1)^{q-1}}$ is q -solvable.*

Proof. Set $m = q - 1$, and label the left vertices of $K_{q-1, (q-1)^{q-1}}$ by v_1, \dots, v_m . Write $[q]_+$ for the set $\{1, \dots, q - 1\}$ (so $[q]_+ \subseteq [q]$) and label the right vertices of $K_{q-1, (q-1)^{q-1}}$ by w_z for $z \in [q]_+^m$. For each $z \in [q]_+^m$ define the guessing function $f_z : [q]^m \rightarrow [q]$ by

$$f_z(x) = \begin{cases} 0 & \text{if } d_H(x, z) = m \\ \min\{i : x_i = z_i\} & \text{if } d_H(x, z) < m \end{cases}$$

It is enough to show that for any hat configuration $(x, y) = (x_1, \dots, x_m, y_{(1, \dots, 1)}, \dots, y_{(q-1, \dots, q-1)})$ if all the vertices w_z guess incorrectly, then the vertices v_i know that the vector x lies in some distinguishable set.

That is, it is enough to show that for all y there exists $a \in [q]^m$ such that

$$\bigcap_{z \in [q]_+^m} f_z^{-1}(y_z)^c \subseteq B_{m-1}(a).$$

(The m components of the vector a , which depends on y , are exactly the guessing functions for the vertices v_1, \dots, v_m .)

We prove by (reverse) induction on i the following:

Claim. *Suppose $(x, y) \in [q]^m \times [q]_+^{[q]_+^m}$ is a configuration of hats guessed incorrectly by every vertex. Then, for every $i = 1, \dots, m$, and every $(z_1, \dots, z_{i-1}) \in [q]_+^{i-1}$ there exists $(z_i, \dots, z_m) \in [q]_+^{m-i+1}$ with $y_{(z_1, \dots, z_m)} \notin \{i, \dots, m\}$.*

Proof of Claim. Let $i = m$, and fix z_1, \dots, z_{m-1} . Consider the variables $y_{(z_1, \dots, z_{m-1}, z)}$ for $z \in [q]_+$; if all are equal to m , then

$$X_m(z) := f_{(z_1, \dots, z_{m-1}, z)}^{-1}(y_{(z_1, \dots, z_{m-1}, z)}) = \{x \in [q]^m : x_i \neq z_i \text{ for all } i < m \text{ and } x_m = z\}.$$

Hence

$$\bigcup_{z \in [q]_+} X_m(z) = \{x \in [q]^m : x_i \neq z_i \text{ for all } i < m \text{ and } x_m \neq 0\}$$

implying that $\bigcap_{z \in [q]_+} X_m(z)^c = B_{m-1}(z_1, \dots, z_{m-1}, 0)$, contradicting the fact that the vertices

v_1, \dots, v_m guess incorrectly. Therefore there exists some $z \in [q]_+$ with $y_{(z_1, \dots, z_{m-1}, z)} \neq m$.

Now, suppose the statement is true for $i > 1$; we show it holds for $i - 1$. Fix z_1, \dots, z_{i-2} ; for each $a \in [q]_+$, by our inductive hypothesis there exist $z_i(a), \dots, z_m(a) \in [q]_+$ with

$$y_{(z_1, \dots, z_{i-2}, a, z_i(a), \dots, z_m(a))} \notin \{i, \dots, m\}.$$

So, it is enough to show that for at least one $a \in [q]_+$ the variable $y_{(z_1, \dots, z_{i-2}, a, z_i(a), \dots, z_m(a))}$ is not equal to $i - 1$. For a contradiction, suppose not, so that all such variables equal $i - 1$. Then,

$$\begin{aligned} X_{i-1}(a) &:= f_{(z_1, \dots, z_{i-2}, a, z_i(a), \dots, z_m(a))}^{-1}(y_{(z_1, \dots, z_{i-2}, a, z_i(a), \dots, z_m(a))}) \\ &= \{x \in [q]^m : x_j \neq z_j \text{ for all } j < i - 1 \text{ and } x_{i-1} = a\}. \end{aligned}$$

Therefore,

$$\bigcup_{a \in [q]_+} X_{i-1}(a) = \{x \in [q]^m : x_j \neq z_j \text{ for all } j < i - 1 \text{ and } x_{i-1} \neq 0\}$$

implying that $\bigcap_{a \in [q]_+} X_{i-1}(a)^c \subseteq B_{m-1}(z_1, \dots, z_{i-2}, 0, \dots, 0)$ contradicting the fact that v_1, \dots, v_m guess incorrectly. \square

Finally, applying the claim for $i = 1$, we find a $z \in [q]_+^m$ where y_z cannot take any value in $\{1, \dots, m\}$. This implies that $y_z = 0$ and $f_z^{-1}(y_z)^c = B_{m-1}(z)$, so that at least one of v_1, \dots, v_m guesses correctly. \square

The *lexicographic product* of a directed graph $D = (V, E)$ and a clique K_r , denoted as (D, r) , is defined as the graph with vertex set $V \times [r]$, where $((u, a), (v, b))$ is an arc if and only if either $(u, v) \in E$ or $u = v$ and $a \neq b$. If D has n vertices and clique number ω , then the graph (D, r) has rn vertices and clique number $r\omega$.

Lemma 1 (The blow-up lemma). *If G is a p -solvable directed graph, then (G, r) is a q -solvable graph, where $q = pr$.*

Proof. Let f be the corresponding guessing function that solves G over p colours. For any vertex (v, a) in (G, r) , we denote the configuration as $(x_{(v,a)}, y_{(v,a)}) \in [p] \times [r]$ and we also denote $X_v = \sum_{a \in [r]} x_{(v,a)}$, $Y_v = \sum_{a \in [r]} y_{(v,a)}$ and write X for the vector $(X_v, v \in G)$. We claim that the (G, r) -function g , defined as follows for each (v, a) , never fails:

$$g_{(v,a)}(x, y) = (f_v(X) - X_v + x_{(v,a)}, -Y_v + y_{(v,a)} - a).$$

Suppose (x, y) is guessed wrong by all vertices. In particular, it is guessed incorrectly by (v, a) , hence either $f_v(X) \neq X_v$ or $Y_v \neq a$. Since this holds for all a , in particular this holds for $a = Y_v$; we conclude that $f_v(X) \neq X_v$. Since this holds for all v , this violates the fact that f is a solution for G . \square

Theorem 2. *For any $\epsilon > 0$, there exists n_ϵ such that the following holds. For any q , there exists a q -solvable undirected graph with at most $n_\epsilon q$ vertices and clique number ϵq .*

Proof. Firstly, let $p = \lceil 1/\epsilon \rceil + 1$ and let q be divisible by p . Let G_p be the p -solvable bipartite graph in Theorem 1 and let g_p denote its size. Then by the blow-up lemma, $(G_p, q/p)$ is a q -solvable graph with $g_p q/p$ vertices and clique number $2q/p$. If q is not divisible by p , consider $q' = p \lceil q/p \rceil \leq q(1 + 1/p)$ and $n_\epsilon = (1 + 1/p)g_p/p$. \square

Theorem 3. *For any ω such that $\omega \geq \frac{q \log \log q}{m \log q}$ holds for large enough q and some $m > 0$, there exists a q -solvable K_ω -free undirected graph with at most q^{2m+1} vertices for q large enough.*

Proof. Let $p = \lfloor \frac{2q}{\omega} \rfloor + 1$. According to Theorem 1, the graph $K_{p-1, (p-1)^{p-1}}$ is p -solvable. Then by the blow-up lemma, there exists a q -solvable graph with $n := \frac{q}{p} ((p-1)^{p-1} + p - 1)$ vertices and clique number $2\frac{q}{p} < \omega$. We have $n \leq q(p-1)^{p-1}$, and hence for q large enough

$$p - 1 \leq \frac{2q}{\omega} \leq 2m \frac{\log q}{\log \log q} \quad \text{and}$$

$$\log n \leq \log q + 2m \frac{\log q}{\log \log q} \{ \log(2m) + \log \log q - \log \log \log q \} \leq (2m + 1) \log q,$$

and hence $n \leq q^{2m+1}$. \square

In general, the constant n_ϵ obtained from Theorem 1 decreases rapidly with ϵ . We refine it below for $\epsilon = 2/3$.

Proposition 1. *The complete bipartite graph $K_{2,2}$ is 3-solvable.*

Proof. Denote the bipartition as $\{v_1, v_2\} \cup \{v_3, v_4\}$. With

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

the guessing function is given by

$$(f_1, f_2) = (x_3, x_4)A, \quad (f_3, f_4) = (x_1, x_2)A^{-1}.$$

Suppose x is guessed wrong by all vertices. The vertices v_3 and v_4 guess wrong, hence we have

$$(x_3, x_4) = (x_1, x_2)A^{-1} + w$$

for some $w = (w_1, w_2) \in S := \{(1, 1), (1, 2), (2, 1), (2, 2)\}$. Similarly, we have

$$(x_1, x_2) = (x_3, x_4)A + u = (x_1, x_2) + wA + u$$

for some $u \in S$. However, it can be shown that for any $(w_1, w_2) \in S$, $wA \notin S$ and hence $wA + u \neq (0, 0)$. We thus obtain the contradiction $(x_1, x_2) \neq (x_1, x_2)$. \square

Corollary 1. *For any q divisible by 3, there exists a q -solvable graph on $4q/3$ vertices with clique number $2q/3$.*

3 Directed constructions

If we allow directed graphs, then we can further refine the constants obtained in Section 2.

Theorem 4. *If q is even, there exists a q -solvable directed graph with $3q/2$ vertices and clique number $q/2$. For any q divisible by 3, there exists a q -solvable directed graph on $4q$ vertices of clique number $q/3$. For any q a multiple of four, there exists a q -solvable directed graph on $10q$ vertices and with clique number $q/4$.*

The main strategy to produce a p -solvable oriented graph is by using a gadget, defined below.

Definition 1. An oriented graph D on n vertices is called a q -gadget if it is not q -solvable, but if there exists a D -function f over $[q]$ such that any configuration x guessed incorrectly by f satisfies an equality of the form $x_1 = \phi(x_2, \dots, x_n)$ for some $\phi : [q]^{n-1} \rightarrow [q]$.

Lemma 2 (The gadget lemma). *If there exists a p -gadget on n vertices, then there exists a p -solvable oriented graph on $n\binom{p}{2} + p$ vertices.*

Proof. Start with a transitive tournament on p vertices with arcs (i, j) for all $i < j$. For any ordered pair (i, j) with $i > j$, add a gadget $D_{i,j}$ and arcs from i to all vertices in $D_{i,j}$ and whence to j . This yields an oriented graph G on $n\binom{p}{2} + p$ vertices; we claim that G is p -solvable.

We denote the vertices of the original tournament as $0, 1, \dots, p-1$ and for each $i > j$, the vertices of the gadget $D_{i,j}$ are $1_{i,j}, \dots, n_{i,j}$.

Let f be the function on the gadget D with corresponding ϕ . The corresponding function g for G is as follows:

$$\begin{aligned} g_j(x) &= - \sum_{k < j} x_k - \sum_{k > j} [\phi(x_{2_{k,j}}, \dots, x_{n_{k,j}}) - x_{1_{k,j}}] + j, \\ g_{1_{i,j}}(x) &= f_1(x_{2_{i,j}}, \dots, x_{n_{i,j}}) - x_i, \\ g_{v_{i,j}}(x) &= f_v(x_{1_{i,j}} + x_i, x_{2_{i,j}}, \dots, x_{n_{i,j}}) \quad v = 2, \dots, n. \end{aligned}$$

Suppose that x is guessed incorrectly by all vertices. First, all vertices in $D_{i,j}$ guess wrong; we then have

$$\begin{aligned} f_1(x_{2_{i,j}}, \dots, x_{n_{i,j}}) &\neq x_{1_{i,j}} + x_i, \\ f_v(x_{1_{i,j}} + x_i, x_{2_{i,j}}, \dots, x_{n_{i,j}}) &\neq x_{v_{i,j}}, \quad v = 2, \dots, n, \end{aligned}$$

hence

$$x_i = \phi(x_{2_{i,j}}, \dots, x_{n_{i,j}}) - x_{1_{i,j}}.$$

for all $i > j$.

Now, j guesses wrong, therefore

$$\sum_{k < j} x_k + \sum_{k > j} [\phi(x_{2_{k,j}}, \dots, x_{n_{k,j}}) - x_{1_{k,j}}] + x_j \neq j,$$

which combined with the above, yields

$$\sum_{k \in [p]} x_k \neq j.$$

Since this holds for all $j \in [p]$, this leads to a contradiction. \square

Proposition 2. *The following graphs are gadgets.*

1. *The graph with a single vertex and no arc is a 2-gadget.*
2. *The directed cycle on three vertices is a 3-gadget.*
3. *The graph D on six vertices in Figure 1 is a 4-gadget.*

Proof. The first graph is trivial. For the directed cycle on vertices 1, 2, 3 and arcs (1, 2), (2, 3), (3, 1), the function f is

$$\begin{aligned} f_1(x) &= x_3 \\ f_2(x) &= x_1 \\ f_3(x) &= x_2. \end{aligned}$$

Therefore, x is not guessed correctly by any vertex if and only if x_1 , x_2 , and x_3 are all distinct. Thus we have $\{x_1, x_2, x_3\} = [3]$ and hence $x_1 + x_2 + x_3 = 0$.

For D , first remark that the transpose of its adjacency matrix (i.e., the matrix A_D where $A_{i,j} = 1$ if and only if (j, i) is an arc in D) is given by

$$A_D = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

For ease of presentation we shall write the hat configuration x as a column vector; we let $f(x) = Mx$, where

$$M = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \\ 1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \end{pmatrix}.$$

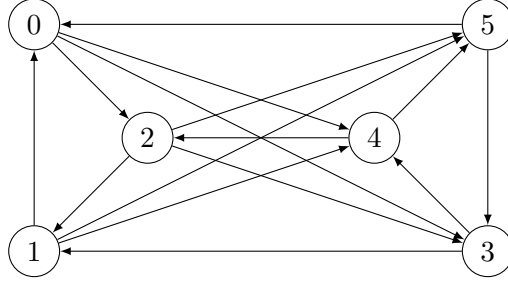


Figure 1: The 4-gadget D in Proposition 2

Then x is guessed wrong by all vertices if and only if Lx is nowhere zero, where

$$L = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 1 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ -1 & 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & 1 & -1 & 0 & 1 \\ 1 & -1 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 1 & -1 \end{pmatrix}.$$

Denoting the rows of L as L_0, \dots, L_5 , we see that $L_3 = L_0 - L_1$, $L_4 = L_1 - L_2$, $L_5 = L_2 - L_0$. Therefore, x is not guessed right if and only if L_0x , L_1x , and L_2x are all distinct and nonzero. Therefore, $\{L_0x, L_1x, L_2x\} = \{1, 2, 3\}$ and x must satisfy

$$2x_0 + 2x_1 + 2x_2 + x_3 + x_4 + x_5 = 2$$

Renaming the vertices such that the fifth vertex becomes first, we obtain the desired equality. \square

However, it is still unknown whether there exist gadgets for more than four colours.

4 Non-solvability results

In Section 2 we showed that a complete bipartite graph with one part of size $q - 1$ was q -solvable. In contrast, in this section we show that any bipartite graph that has a partition with one part of size at most $q - 2$ is not q -solvable. To do this we consider the following non-distinguishable set in $[q]^m$ (in other words, a subset of $[q]^m$ with remoteness m). Set $m = q - 2$, and denote the words $w_a = (a, \dots, a) \in [q]^m$ for all $a \in [q] \setminus \{0\}$, then $W = \{w_a : a \in [q] \setminus \{0\}\}$ is non-distinguishable. Indeed, for any $x \in [q]^m$, let $X = \{b \in [q] : x_i = b \text{ for some } i\}$ denote the set of values taken by the coordinates of x , then $|X| \leq m < |W|$ and hence there exists $a \in ([q] \setminus \{0\}) \setminus X$ and thus $d_H(x, w_a) = m$.

In fact, our proof applies to a larger class of graphs than bipartite graphs, defined as follows.

Definition 2. We say a directed graph D is (m, s) -semibipartite if its vertex set can be partitioned into $V = L \cup R$, where $|L| = m$, $|R| = s$ and $D[L]$ is an independent set and $D[R]$ is acyclic.

Theorem 5. Any (m, s) -semibipartite graph is not $(m + 2)$ -solvable.

Proof. Let $q = m + 2$ and denote the vertices of R as r_1, \dots, r_s . Let $y \in [q]^s$ such that

$$\begin{aligned} y_1 &\notin \{f_{r_1}(w_a) : a \in [q]\} \\ y_2 &\notin \{f_{r_2}(w_a, y_1) : a \in [q]\} \\ &\vdots \\ y_s &\notin \{f_{r_s}(w_a, y_1, \dots, y_{s-1}) : a \in [q]\}; \end{aligned}$$

such y exists for each set on the right hand side has cardinality at most $|W| = q - 1$. Furthermore, let $b \in [q] \setminus \{f_{l_1}(y), \dots, f_{l_m}(y)\}$ (where l_1, \dots, l_m are the vertices of L), then all vertices guess (w_b, y) incorrectly. \square

This theorem is best possible, for Theorem 1 indicates that there are q -solvable bipartite graphs with left part of size $q - 1$.

Corollary 2. *The complete bipartite graph $K_{m,n}$ is not $(m + 2)$ -solvable.*

Corollary 3. *Any graph with a minimum vertex feedback set of cardinality one is q -solvable if and only if $q = 2$.*

Proof. By Theorem 5, such a graph is not 3-solvable. Conversely, it is not acyclic, hence it contains a directed cycle as a subgraph: let us prove that the directed cycle C_n on n vertices is 2-solvable. Let the function be $f_1(x) = x_n$ and $f_i(x) = x_{i-1} + 1$ for $2 \leq i \leq n$, then x is guessed incorrectly by all vertices if and only if $x_1 = x_2 = \dots = x_n = x_1 + 1$, which is clearly impossible. \square

Theorem 6. *Let D be a directed graph on n vertices with an acyclic induced subgraph of size I . If*

$$(n - I) \left(\frac{q}{q - 1} \right)^I < q,$$

then D is not q -solvable.

Proof. We denote the set of vertices inducing an acyclic subgraph of cardinality I as A ; we also denote a guessing function as f . Let $x \in [q]^I$ be the hat assignment on A and $y \in [q]^{n-I}$ be the assignment on the rest of the vertices. For each choice of y , denote by $S_d(y)$ the set of choices for x such that exactly d vertices in A guess correctly for all $0 \leq d \leq I$. It is easy to prove by induction on I that $N_d := |S_d(y)| = \binom{I}{d} (q - 1)^{I-d}$. We shall consider the situation when $x \in S_0(y)$, i.e., when no vertex in A guesses correctly; given y , there are $N_0 = (q - 1)^I$ such assignments.

For any y , let G denote the number of times the vertices in A guess their colours correctly when $x \notin S_0(y)$:

$$G := \sum_{x \in [q]^I} \sum_{i=1}^I \mathbf{1}\{f_{a_i}(x, y) = x_i\} = \sum_{d=1}^I d N_d = I q^{I-1}.$$

The total number of correct guesses, over all assignments (x, y) , is of course equal to $n q^{n-1}$. Therefore, there are at most

$$H := n q^{n-1} - q^{n-I} G = (n - I) q^{n-1}$$

correct guesses over the whole graph for any (x, y) where $x \in S_0(y)$. On average, such an assignment is guessed correctly

$$\frac{H}{q^{n-I} N_0} = \frac{(n - I) q^{I-1}}{(q - 1)^I} < 1$$

times, and hence one hat assignment is never guessed correctly. \square

Corollary 4. *A graph with an acyclic induced subgraph of size I is q -solvable only if it has at least $I + q \left(1 - \frac{1}{q}\right)^I$ vertices in total.*

Corollary 5. *If a graph on n vertices has an acyclic induced subgraph of cardinality at least $n/2$, then it is q -solvable only if $n \geq 2\alpha(q-1)$, where $\alpha \sim 0.5675$ satisfies $\alpha + \log \alpha = 0$.*

Proof. Suppose $n < 2\alpha(q-1)$, and let $i = n/(2q) < \alpha(q-1)/q$, then $\log i + i\frac{q}{q-1} < \log \frac{q-1}{q}$ and hence

$$\begin{aligned} 0 &> \log i + i\frac{q}{q-1} \\ &> \log i + iq \log \left(1 + \frac{1}{q-1}\right) \\ 1 &> i \left(1 + \frac{1}{q-1}\right)^{iq} \\ q &> \frac{n}{2} \left(\frac{q}{q-1}\right)^{\frac{n}{2}}, \end{aligned}$$

which, by Theorem 6, shows that the graph is not q -solvable. □

5 Even cycles

In this section we show that a cycle whose length is a multiple of 6 is 3-solvable. In fact, we can define guessing functions for any even cycle which have the property that at most 3 hat configurations are not guessed correctly by any vertex.

For $n > 1$, let C_{2n} be the cycle of length $2n$ and let $V = \{v_1, v_2, \dots, v_n\}$ and $W = \{w_1, w_2, \dots, w_n\}$ be a partition of the vertices of C_{2n} into independent sets, with v_i adjacent to w_i and w_{i-1} for all $i = 1, \dots, n$ (index arithmetic taken modulo n). Denote the hat colour of v_i by x_i and its guessing function by f_i . Similarly, for w_i , denote its hat colour by y_i and its guessing function by g_i . We define the guessing functions to be

$$f_i(y_{i-1}, y_i) = \begin{cases} y_i - 1 & \text{if } y_i \neq y_{i-1} + 1, \\ y_i + 1 & \text{if } y_i = y_{i-1} + 1, \end{cases} \quad \text{for } i \neq 1; \quad (1)$$

$$f_1(y_n, y_1) = \begin{cases} y_1 - 1 & \text{if } y_1 \neq y_n - 1, \\ y_1 + 1 & \text{if } y_1 = y_n - 1, \end{cases} \quad (2)$$

$$g_i(x_i, x_{i+1}) = \begin{cases} x_i & \text{if } x_i \neq x_{i+1} + 1, \\ x_i - 1 & \text{if } x_i = x_{i+1} + 1, \end{cases} \quad \text{for } i \neq n; \quad (3)$$

$$g_n(x_n, x_1) = \begin{cases} x_n & \text{if } x_n \neq x_1, \\ x_n - 1 & \text{if } x_n = x_1. \end{cases} \quad (4)$$

Graphically, we have

$$\begin{array}{ccc}
 f_i : y_i & \begin{array}{|c|c|c|} \hline 1 & 0 & 1 \\ \hline 2 & 0 & 0 \\ \hline 2 & 2 & 1 \\ \hline \end{array} & \\
 & y_{i-1} & \\
 \\
 g_i : x_{i+1} & \begin{array}{|c|c|c|} \hline 2 & 1 & 2 \\ \hline 0 & 1 & 1 \\ \hline 0 & 0 & 2 \\ \hline \end{array} & \\
 & x_i & \\
 \\
 f_1 : y_1 & \begin{array}{|c|c|c|} \hline 0 & 1 & 1 \\ \hline 0 & 0 & 2 \\ \hline 2 & 1 & 2 \\ \hline \end{array} & \\
 & y_n & \\
 \\
 g_n : x_1 & \begin{array}{|c|c|c|} \hline 0 & 1 & 1 \\ \hline 0 & 0 & 2 \\ \hline 2 & 1 & 2 \\ \hline \end{array} & \\
 & x_n &
 \end{array}$$

the sets $f_i^{-1}(x_i)$ and $g_i^{-1}(y_i)$ forming L-shaped regions of $[3]^n$.

Theorem 7. *The cycle C_{2n} is 3-solvable for $n \equiv 0 \pmod{3}$. Using the guessing functions as defined above, when $n \equiv 1 \pmod{3}$, the only configurations (x, y) that all vertices guess incorrectly are*

$$x = (a, a + 2, a + 1, a, \dots, a), y = (a, a + 2, a + 1, a, \dots, a) \text{ for some } a \in [3],$$

and when $n \equiv 2 \pmod{3}$, the only configurations (x, y) that all vertices guess incorrectly are

$$x = (a + 2, a, a + 1, a + 2, \dots, a), y = (a, a + 1, a + 2, a, \dots, a + 1) \text{ for some } a \in [3].$$

Proof. Suppose $y = (y_1, \dots, y_n) \in [3]^n$ is the configuration of hat colours for the vertices in W and that each vertex in W guesses incorrectly. Then $x \in \bigcap_{i=1}^n g_i^{-1}(y_i)^c$, where

$$\begin{aligned}
 \bigcap_{i=1}^n g_i^{-1}(y_i)^c &= \bigcap_{i < n} \{x : x_i = y_i - 1 \text{ or } x_{i+1} = y_i - 1 \text{ or } (x_i, x_{i+1}) = (y_i + 1, y_i + 1)\} \\
 &\quad \cap \{x : x_n = y_n - 1 \text{ or } x_1 = y_n \text{ or } (x_n, x_1) = (y_n + 1, y_n - 1)\}
 \end{aligned}$$

Suppose further that each vertex in V guesses incorrectly. We claim the following implications are true.

Claim. *If (x, y) is guessed incorrectly by all vertices then the following hold. For all $i \neq 1$,*

- A_i : *if $x_i = y_i - 1$ then $y_i = y_{i-1} + 1$ and $x_{i-1} = y_{i-1} - 1$;*
- B_i : *if $x_i = y_i + 1$ then either*

1. $y_i = y_{i-1}$ and $x_{i-1} = y_{i-1} + 1$, or
2. $y_i \neq y_{i-1} + 1$ and $x_{i-1} = y_{i-1} - 1$;

and for all $i \neq n$,

- C_i : *if $x_i = y_i$ then $y_{i+1} = y_i - 1$ and $x_{i+1} = y_{i+1}$.*

Proof of Claim. Take $i \neq 1$, and suppose $x_i = y_i - 1$. Since v_i guesses incorrectly, we must have $y_i = y_{i-1} + 1$, so that $x_i = y_{i-1}$. But $x \in g_{i-1}^{-1}(y_{i-1})^c$ which implies that $x_{i-1} = y_{i-1} - 1$, establishing A_i .

Now suppose $x_i = y_i + 1$. Since v_i guesses incorrectly, we must have $y_i \neq y_{i-1} + 1$, so that $x_i \neq y_{i-1} - 1$. But $x \in g_{i-1}^{-1}(y_{i-1})^c$ which implies that either $x_{i-1} = y_{i-1} - 1$ or $(x_{i-1}, x_i) = (y_{i-1} + 1, y_{i-1} + 1)$, the latter implying that $y_i = y_{i-1}$, which establishes B_i .

Finally, take $i \neq n$ and suppose $x_i = y_i$. Since $x \in g_i^{-1}(y_i)^c$, we must have $x_{i+1} = y_i - 1$. But v_{i+1} guesses incorrectly which implies that $y_{i+1} = y_i - 1$. To see this, use the fact that the function f_i , for $i \neq 1$, can also be written as

$$f_i(y_{i-1}, y_i) = \begin{cases} y_{i-1} - 1 & \text{if } y_i \neq y_{i-1} - 1, \\ y_{i-1} + 1 & \text{if } y_i = y_{i-1} - 1. \end{cases}$$

Therefore $x_{i+1} = y_{i+1}$, establishing C_i . \square

We use the implications A_i, B_i and C_i as follows. First, suppose $x_n = y_n - 1$. Then using the chain of implications A_n, A_{n-1}, \dots, A_2 we find that $x_i = y_i - 1$ for all i and $y_i = y_{i-1} + 1$ for $i \neq 1$, so $y_n = y_1 + (n-1) \pmod{3}$. Since $x_1 = y_1 - 1$ and v_1 also guesses incorrectly, we must have $y_1 = y_n - 1$, a contradiction unless $n \equiv 2 \pmod{3}$. When $n \equiv 2 \pmod{3}$, we discover that the configurations $x = (a+2, a, a+1, a+2, \dots, a), y = (a, a+1, a+2, a, \dots, a+1)$ for $a \in [3]$ are guessed incorrectly by all vertices.

Now suppose $x_n = y_n + 1$. Since $x \in g_n^{-1}(y_n)^c$ we have that $x_1 \neq y_n + 1$. We consider the chain of implications B_n, B_{n-1}, \dots for as far as possible and note that case 1 of B_i cannot occur for all $i \neq 1$, for then $x_i = y_i + 1$ for all i and $y_i = y_{i-1}$ for $i \neq 1$, contradicting the fact that $x_1 \neq y_n + 1$. This means that for some $k > 1$ case 2 of B_k occurs, so that $x_{k-1} = y_{k-1} - 1$. We then apply the chain of implications $A_{k-1}, A_{k-2}, \dots, A_2$ to find that $x_i = y_i - 1$ for all $i < k$, so in particular $x_1 = y_1 - 1$. Since v_1 guesses incorrectly, we have that $y_1 = y_n - 1$ which contradicts the fact that $x_1 \neq y_n + 1$. Hence for any configuration with $x_n = y_n + 1$ there must be some vertex that guesses correctly.

Finally, suppose $x_n = y_n$. Since $x \in g_n^{-1}(y_n)^c$ we have that $x_1 = y_n$. Since v_1 guesses incorrectly, we must have that $y_1 = y_n$. To see this use the fact that f_1 can be also written as

$$f_1(y_n, y_1) = \begin{cases} y_n & \text{if } y_1 \neq y_n, \\ y_n - 1 & \text{if } y_1 = y_n. \end{cases}$$

Therefore $x_1 = y_1$. We now apply the chain of implications C_1, C_2, \dots, C_{n-1} to find that $x_i = y_i$ for all i , and $y_{i+1} = y_i - 1$ for $i \neq n$. Therefore $y_n = y_1 - (n-1) \pmod{3}$, which is a contradiction unless $n \equiv 1 \pmod{3}$. When $n \equiv 1 \pmod{3}$, we discover that the configurations $x = (a, a+2, a+1, a, \dots, a), y = (a, a+2, a+1, a, \dots, a)$ for $a \in [3]$ are guessed incorrectly by all vertices. \square

Unfortunately, this ‘L-shaped’ construction falls just short of proving 3-solvability when $n \not\equiv 0 \pmod{3}$; indeed, out of the 3^{2n} possible hat configurations, there are only 3 where all vertices guess incorrectly!

In any case, the family of cycles of length a multiple of 6 gives an answer to a question of Butler et al. about edge-critical graphs. A graph G is called *edge-critical for q colours* if G is q -solvable, but $G - e$ is not q -solvable for any edge $e \in G$. For $q = 2$ the only edge-critical graph is the graph of a single edge, and for $q > 2$ there are at least two distinct edge-critical graphs, namely K_q and some subgraph of the bipartite graph $K_{q-1, (q-1)^{q-1}}$ presented earlier. Butler et al. ask whether there are infinitely many graphs which are edge-critical for q colours, for $q > 2$. Since trees are known not to be 3-solvable, the cycles of length a multiple of 6 form such an infinite family for $q = 3$.

Theorem 8. *The family $\{C_{6k} : k \in \mathbb{N}\}$ is an infinite family of edge-critical graphs for 3 colours.*

6 Acknowledgment

This work was produced while the second author was supported by the Engineering and Physical Sciences Research Council [grant number EP/J021784/1].

References

- [1] M. Krzywkowski, “Hat problem on a graph,” Ph.D. dissertation, University of Exeter, 2012.
- [2] T. Ebert, “Applications of recursive operators to randomness and complexity,” Ph.D. dissertation, University of California at Santa Barbara, 1998.
- [3] M. Krzywkowski, “A modified hat problem,” *Commentationes Mathematicae*, vol. 50, pp. 121–126, 2010.
- [4] G. D. Cohen, I. Honkala, S. Litsyn, and A. C. Lobstein, *Covering Codes*. Elsevier, 1997.
- [5] T. Ebert, W. Merkle, and H. Vollmer, “On the autoreducibility of random sequences,” *SIAM Journal on Computing*, vol. 32, pp. 1542–1569, 2003.
- [6] S. Riis, “Information flows, graphs and their guessing numbers,” *The Electronic Journal of Combinatorics*, vol. 14, pp. 1–17, 2007.
- [7] —, “Graph entropy, network coding and guessing games,” November 2007, available at <http://arxiv.org/abs/0711.4175>.
- [8] M. Gadouleau and S. Riis, “Graph-theoretical constructions for graph entropy and network coding based communications,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6703–6717, October 2011.
- [9] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [10] P. Winkler, *Puzzlers’ tribute. A feast for the mind*. Taylor Francis Inc., 2001, ch. Games People Don’t Play.
- [11] U. Feige, “You can leave your hat on (if you guess its color),” *Technical Report, Computer Science and Applied Mathematics, The Weizmann Institute of Science*, vol. MCS04-03, 2004.
- [12] B. Doerr, “Integral approximation,” Ph.D. dissertation, Christian-Albrechts-Universität zu Kiel, 2005.
- [13] G. Aggarwal, A. Fiat, A. V. Goldberg, J. D. Hartline, N. Immorlica, and M. Sudan, “Derandomization of auctions,” *Games and Economic Behavior*, vol. 72, no. 1, pp. 1–11, February 2011.
- [14] O. Ben-Zwi, I. Newman, and G. Wolfvitz, “Hats, auctions and derandomization,” *Random Structures and Algorithms*, to appear 2013.
- [15] S. Butler, M. T. Hajiaghayi, R. D. Kleinberg, and T. Leighton, “Hat guessing games,” *SIAM Journal on Discrete Mathematics*, no. 2, pp. 592–605, 2008.
- [16] P. J. Cameron and M. Gadouleau, “Remoteness of permutation codes,” *European Journal of Combinatorics*, vol. 33, no. 6, pp. 1273–1285, 2012.

The three-colour hat guessing game on the cycle graphs

Witold W. Szczechla *

Abstract

We study a cooperative game in which each member of a team of N players, wearing coloured hats and situated at the vertices of the cycle graph C_N , is guessing their own hat colour merely on the basis of observing the hats worn by their two neighbours without exchanging the information. Each hat can have one of three colours. A predetermined guessing strategy is winning if it guarantees at least one correct individual guess for every assignment of colours. We prove that a winning strategy exists if and only if N is divisible by 3 or $N = 4$.

1 Introduction

N ladies wearing white hats are sitting around the table and discussing a tricky task which is going to be presented to them by the Wizard. They know he will suddenly paint each hat one of three colours (green, orange or purple) in an unpredictable way and then ask each of them to independently guess her own hat colour. The light is so dim that everyone will only see the hat colours of her two neighbours. If at least one of the ladies guesses right, they will all win; if they all guess wrong, they will lose; and they want to be absolutely certain of winning. However, can they devise a winning strategy before they invite the Wizard?

The answer, depending on the number N , is presented in this paper. Problems of this kind have become popular in recent years both as mathematical puzzlers (see [2], [3]) and research subjects. Basic results so far concerned two colours (instead of three), or unrestricted visibility (a complete graph), or probabilistic variants (the expected number of the correct guesses): see [1], [4], [5], [6], [8] and overviews in [7] and [9]. The round-table problem described above has until now remained open for all $N > 5$.

1 Formalism

The team players are seeing each other along the edges of the cyclic graph C_N . Let the set $V_k = \{v_1(k), v_2(k), v_3(k)\}$ represent the three different appearances of the k -th hat, where k is counted modulo N in the positive direction (to the

*Department of Mathematics, Informatics and Mechanics, University of Warsaw, ul.Banacha2, 02-097 Warszawa, Poland. witold@mimuw.edu.pl

right). It will be technically convenient to regard them either as pairwise disjoint ($0 \leq k < N$), or simply as $V_k = \mathbf{Z}_3$. A cyclic notation will also be used:

$$v_i^k = v_j^m = v_i(k) = v_j(m) \quad \text{and} \quad V_k = V_m, \\ \text{where } i, j, k, m \in \mathbf{Z}, \quad i \equiv j \pmod{3}, \quad k \equiv m \pmod{N}.$$

An individual guessing strategy of Player k is represented by a function

$$f_k : V_{k-1} \times V_{k+1} \rightarrow V_k,$$

which may simply be regarded as a function $(i, j) \mapsto r$, where $f_k(v_i^{k-1}, v_j^{k+1}) = v_r^k$. A *composite strategy* is a sequence

$$f = (f_1, \dots, f_N),$$

or equivalently, a function $\mathbf{Z} \ni k \mapsto f_k$, satisfying $f_{k+N} = f_k$.

According to the assumed rules, strategy f is *winning* if and only if there is no sequence (s_1, s_2, \dots, s_N) satisfying

$$s_k \in V_k \quad \text{and} \quad s_k \neq f_k(s_{k-1}, s_{k+1}) \quad \text{for } k = 1, \dots, N, \quad \text{where } s_0 = s_N, \quad s_{N+1} = s_1.$$

If there exists such a sequence, f is a *losing* strategy.

2 Hat games on graphs

In a more general setting an arbitrary ‘visibility’ pattern can be assumed. For a broader exposition, see [7] and [9]. The directed ‘visibility graph’ Γ has N vertices corresponding to the players, and edges $\vec{AB} \in E(\Gamma) = E$ wherever player A is seen by player B . For each vertex $v \in V(\Gamma) = V$ a nonempty set of ‘colours’ V_v is known to all. For each ‘assignment of colours’, i.e., a selector $g : V \rightarrow \bigcup_v V_v$ with $g(v) \in V_v$, each player $u \in V$ tries to guess $g(u)$ by using a function

$$f_u : \prod V_v \rightarrow V_u \quad (\text{product taken over } v\vec{u} \in E).$$

as an individual strategy. The combined, or collective, strategy is the collection $f = \{f_u : u \in V\}$. The game is thus played against an opponent assigning the colours (the Wizard, the Demon, Chance, etc., in a fantasy world). In this paper, the notion of winning or losing refers to the cooperative players. The strategy effectiveness depends only on the numbers of possible colours, i.e., the function h given by $h(v) = |V_v|$. Let $X_h(f, g)$ denote the number of correct guesses. The deterministic minimax approach defines the *value* of this game as

$$\mu(h) = \mu(\Gamma, h) = \max_f \min_g X_h(f, g).$$

This paper concerns the minimal condition $\mu(h) > 0$ where f is a winning strategy if

$$\min_g X_h(f, g) > 0.$$

J.Grytczuk has conjectured that a winning strategy exists provided $|V_v| \leq \deg_-(v)$ for every $v \in V(\Gamma)$. One consequence of our main result is that the weaker condition $|V_v| \leq \deg_-(v) + 1$ is generally not sufficient.

3 Examples with $N < 5$

The game on C_2 In the simplest puzzle (outside our main problem, though) there are just two players and two possible hat colours. In this situation one person should guess that their hats have the same colour and the other person should guess the opposite. If one interpretes the colours as elements $A, B \in \mathbf{Z}_2$, the effect can be written as an alternative:

$$A = B \text{ or } B = A + 1.$$

Next, suppose Player 1 hat can still have two colours, but Player 2 hat can have three colours. Then there are six possible colour assignments. With any strategy, Player 1 guesses right for three assignments, Player 2 for two. Since the number of assignments is $6 > 3 + 2$, they can both be wrong and they have no winning strategy. (In the above cases, the players might as well guess the other person's colour while knowing their own.)

An algebraic strategy for C_3 If $A, B, C \in \mathbf{Z}_3$ represent the appearances of hats, then a winning strategy can be based, for instance, on the alternative:

$$A = -B - C \text{ or } B = -C - A - 1 \text{ or } C = -A - B + 1,$$

clearly valid in \mathbf{Z}_3 .

An algebraic strategy for C_4 Let variables $A, B, C, D \in \mathbf{Z}_3$ represent elements of the sets V_1, V_2, V_3, V_4 , respectively. Then a winning strategy f can be based on the following alternative:

$$\left\{ \begin{array}{l} A = D + B \\ \text{or } B = -A - C \\ \text{or } C = B - D \\ \text{or } D = C - A. \end{array} \right. \quad (1)$$

To verify (1), let us suppose the first and third equalities are false. In \mathbf{Z}_3 this implies

$$\left\{ \begin{array}{l} D + B = A \pm 1 \\ B - D = C \pm 1. \end{array} \right. \quad (2)$$

If the signs above are opposite, we add the equations to get $2B = A + C$, equivalent to the second equation of (1). If the signs are the same, we subtract the equations to get $2D = A - C$, equivalent to the last equation of (1). Thus indeed, strategy f wins.

2 The main result

Let us observe the following (inconvenient, as it turns out) property of the last two examples. For any $b \in V_m$ and $c \in V_{m+1}$ there is exactly one $d \in V_{m+2}$ satisfying $f_{m+1}(b, d) = c$ and exactly one $a \in V_{m-1}$ satisfying $f_m(a, c) = b$. However, winning strategies with this property are *not* possible for $N > 4$ (see Section 4). Our method will thus produce another kind of strategy for some N -gons whenever possible, while demonstrating the losing case for all the rest. The main result of this paper is:

Theorem 1 *In the three-colour hat guessing game on the cycle of length N a winning strategy exists if and only if N is divisible by three or $N = 4$.*

Proof of the main result

An interplay of various relatively simple local and global combinatorial methods will be used.

1 Admissible paths in the enlarged graph

Let us introduce a larger graph $G = G_N$ (which we will also denote $3 * C_N$) whose $3N$ -element set of vertices is $V = V(G) = \bigcup_{k=1}^N V_k$, and $9N$ -element set of edges is

$$E = E(G) = \{\overline{v_i(k-1)v_j(k)} : k = 1, \dots, N; i, j = 1, 2, 3\}.$$

Remark An analogous construction can be applied to any visibility graph Γ and any *height function* $h : V(\Gamma) \rightarrow \mathbf{N} \setminus \{0\}$ (whose values are the numbers of possible colours). The resulting graph, which may be denoted $G = * \Gamma$, has

$$V(G) = \{(i, v) : v \in V(\Gamma), i = 1, \dots, h(v)\}$$

and

$$E(G) = \{(i, v) \vec{v} (j, u) : \vec{v}u \in E(\Gamma)\}.$$

Now let us consider a (composite) strategy f .

Definition 1 Let J be any set of consecutive integers. A path $(s_k)_{k \in J}$ in the graph G will be called *f-admissible* (or simply *admissible*, when f is fixed) if

$$s_k \in V_k \text{ for } k \in J$$

and

$$s_k \neq f_k(s_{k-1}, s_{k+1}) \text{ whenever } k-1, k+1 \in J.$$

□

Thus, a path is admissible if and only if all its 2-edge segments (i.e., sub-paths of length 2) are admissible. It is clear that strategy f is winning if and only if the graph G contains no f -admissible path (of infinite length) which is periodic and has period N , or equivalently, no f -admissible path of length $N + 1$ whose last edge coincides with the first. However, the definition does not directly settle the question of whether any periodic admissible path exists, and if it does, whether it can have period N (or at least less than $9N$).

The set of all the f -admissible paths (of all lengths) will be denoted $\mathcal{A}(f)$. The set of all the edges between V_k and V_{k+1} will be denoted by

$$E_{k,k+1} = V_k \times V_{k+1} = \{\overline{bc} : b \in V_k \text{ and } c \in V_{k+1}\}.$$

Definition 2 Let f be a fixed strategy. For any edge $\overline{bc} \in E_{k,k+1}$, define

$$\ell_+(\overline{bc}) = \#\{d \in V_{k+2} : \overline{bcd} \in \mathcal{A}(f)\},$$

i.e., the number of the immediate admissible continuations of \overline{bc} to the right, and

$$\ell_-(\overline{bc}) = \#\{a \in V_{k-1} : \overline{abc} \in \mathcal{A}(f)\},$$

i.e., the number of the analogous continuations to the left. □

Hence, in general, we have $\ell_+(\overline{bc}), \ell_-(\overline{bc}) \in \{0, 1, 2, 3\}$.

Lemma 2 Consider a fixed strategy f .

- (a) The average value of ℓ_- (resp. ℓ_+) over any three right-adjacent (resp. left-adjacent) edges of G equals 2. That is, for any vertex $b \in V_k$ we have

$$\sum_{a \in V_{k-1}} \ell_-(\overline{ab}) = \sum_{c \in V_{k+1}} \ell_+(\overline{bc}) = 6$$

- (b) If two edges of G have the same left (resp. right) endpoint then one of them has at least two admissible immediate continuations to the right (resp. left). That is, for any vertex $b \in V_k$ and any two distinct vertices $c_i \in V_{k+1}$ ($i = 1, 2$) there is a choice of $i \in \{1, 2\}$ and two distinct vertices $d_1, d_2 \in V_{k+2}$ such that $\overline{bc_i d_j} \in \mathcal{A}(f)$ for $j = 1, 2$; the analogous fact holds for passages to the left.

- (c) If the graph G contains an f -admissible path $\overline{s_1 \dots s_n}$ such that $2 \leq n \leq N-1$ and

$$\ell_-(\overline{s_1 s_2}) + \ell_+(\overline{s_{n-1} s_n}) \geq 5,$$

then f is a losing strategy.

- (d) If f is a winning strategy, then for every edge $\beta \in E(G)$ we have

$$\ell_+(\beta) + \ell_-(\beta) = 4.$$

Proof. (a): Consider ℓ_+ . For any vertex $d \in V_{k+2}$, the set V_{k+1} contains two vertices different from $f_{k+1}(b, d)$, defining two admissible connections of b with each of the three choices of d . (The situation with ℓ_- is symmetric.)

(b): For any $d \in V_{k+2}$ we can choose an $i \in \{1, 2\}$ such that $f_{k+1}(b, d) \neq c_i$. Since d takes three values, two of them must correspond to the same choice of i .

(c): We may assume $\ell_-(\overline{s_1 s_2}) = 3$ and $\ell_+(\overline{s_{n-1} s_n}) \geq 2$, with $s_1 \in V_1$. By (b), the path can be continued to the right until $n = N-1$. Then the paths of the form $\overline{x s_1 s_2 \dots s_{N-1} y}$ are in $\mathcal{A}(f)$ for all three values of $x \in V_0$ and at least two values of $y \in V_N = V_0$. Now it is enough to choose $y \neq f_0(s_{N-1} s_1)$ to make the ends meet, obtaining an N -periodic f -admissible path $\overline{y s_1 s_2 \dots s_{N-1} y s_1 \dots}$. (This argument is partly illustrated in Figure 1.)

(d): Denote $\ell(\gamma) = \ell_+(\gamma) + \ell_-(\gamma)$ for all $\gamma \in E(G)$. If $\ell(\beta) > 4$ for some $\beta \in E(G)$, then f is losing by (c) applied to the single edge β . However, (a) implies that the average value of $\ell(\gamma)$ over $\gamma \in E_{k, k+1}$ equals 4. Hence, if there was an edge $\alpha \in E_{k, k+1}$ with $\ell(\alpha) < 4$, there would also be an edge $\beta \in E_{k, k+1}$ with $\ell(\beta) > 4$, the case already excluded. ■

2 The three categories of edges

Let us assume that strategy f satisfies

$$\ell_+(\gamma) + \ell_-(\gamma) = 4 \quad \text{for all } \gamma \in E(G). \quad (3)$$

Then all the edges $\gamma \in E(G)$ can be divided into three categories:

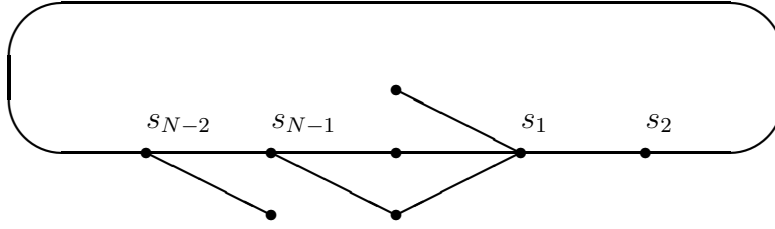


Figure 1: Closing the path of Lemma 2 (c).

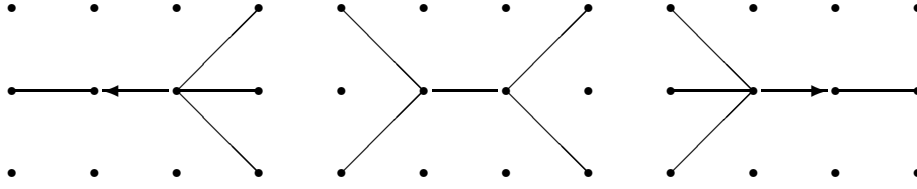


Figure 2: Examples of edges (red, blue, yellow) with their admissible continuations.

- If $\ell_-(\gamma) = 3$ and $\ell_+(\gamma) = 1$, let us paint γ yellow and direct it right.
- If $\ell_-(\gamma) = 1$ and $\ell_+(\gamma) = 3$, let us paint γ red and direct it left.
- If $\ell_-(\gamma) = \ell_+(\gamma) = 2$, let us paint γ blue and leave it undirected.

The three patterns can thus be shown as in Figure 2.

Definition 3 Any strategy f satisfying (3) will be called *balanced* or *colourable*.
□

By Lemma 2(d), every winning strategy is colourable. However, not all balanced strategies will be winning. The sets of all the yellow, red, and blue edges in $E(G)$ (or in $E_{k,k+1}$) will be denoted E^+ , E^- , and E^0 (or $E_{k,k+1}^+$, $E_{k,k+1}^-$, and $E_{k,k+1}^0$), respectively.

Lemma 3 *If strategy f is colourable, then:*

- For each k , there are equal numbers of yellow and red edges in the set $E_{k,k+1}$ (i.e., $|E_{k,k+1}^+| = |E_{k,k+1}^-|$).
- Any three edges of G having a common left or right end-point (i.e., left- or right-adjacent) either have three different colours or all are blue.
- If f is a winning strategy and $N \geq 4$, then every directed edge is admissibly continued in its direction by an edge of the same direction. That is, if $\beta \in E_{k,k+1}$ is yellow, $\gamma \in E_{k+1,k+2}$ and the path $\overline{\beta\gamma}$ is f -admissible, then γ is also yellow. Analogously, if $\beta \in E_{k,k+1}$ is red, $\alpha \in E_{k-1,k}$ and $\overline{\alpha\beta} \in \mathcal{A}(f)$, then α is also red.

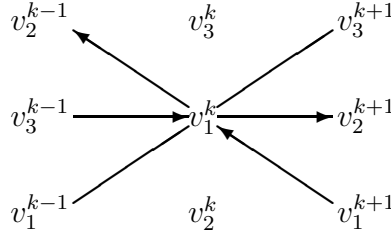


Figure 3: An example of the typical configuration at the head or tail of any directed edge.

- (d) If f is a winning strategy and $N \geq 4$, then every directed edge is a continuation of three edges of three different colours. That is, if $\beta = \overline{bc} \in E_{k,k+1}$ is yellow, then among the three edges \overline{ab} with $a \in V_{k-1}$ one is yellow, one is red, and one is blue. Analogously, if $\beta = \overline{bc}$ is red, then among the edges $\overline{cd} \in E_{k+2}$ one is in E^+ , another in E^- , and the third in E^0 .
- (e) If f is a winning strategy and $N \geq 4$, then any periodic f -admissible path has one colour. Conversely (under the same assumption), any path of a fixed direction (red or yellow) is admissible, and an undirected path (blue) is admissible provided that all its vertices are incident to some directed edges.

Proof. (a): By Lemma 2(a), we have

$$\sum_{\gamma \in E_{k,k+1}} \ell_-(\gamma) = \sum_{\gamma \in E_{k,k+1}} \ell_+(\gamma) = 18.$$

The terms equal to 1 and 3 in the first sum correspond to the terms equal to 3 and 1, respectively, in the second.

(b): This follows from Lemma 2(a)(d), since the number 6 can be expressed as an unordered sum of three terms equal to 1, 2 or 3 in just two ways: $1 + 2 + 3$ and $2 + 2 + 2$.

(c): If β is yellow (i.e., $\ell_-(\beta) = 3$) and γ is not, then $\ell_+(\gamma) \geq 2$. Then Lemma 2(c) applied to the path $\overline{\beta\gamma}$ (where $n = 3 \leq N - 1$) implies that f is a losing strategy, contrary to our assumption.

(d): Let $\beta = \overline{bc} \in E_{k,k+1}$ be yellow. By (b), some edge $\gamma = \overline{bc'} \in E_{k,k+1}$ must be red. Then, by (c), the left continuation of γ into $E_{k-1,k}$ is also red, showing that not all edges $\overline{ab} \in E_{k-1,k}$ are blue. By (b), these edges must be of three colours.

(e): Consider any path containing a yellow (resp. red) edge β . By (c) and the definition of colouring, the edge β has a unique forward (resp. backward) admissible continuation, consisting of edges of the same direction. This proves that every periodic admissible path must have one direction or be undirected. Conversely, any directed path is admissible by (c).

Finally, consider a blue path \overline{abc} (of length 2) with vertex b incident to some directed edge. We may suppose an edge $\overline{bc'}$ is directed. By (b) and (c), there is some left-directed edge $\overline{bc''}$ uniquely continued by another edge $\overline{a'b} \in E^- \not\cong \overline{ab}$. Since $\overline{abc''}$ is not f -admissible and \overline{ab} is blue, both remaining right continuations of \overline{ab} must be f -admissible, including \overline{abc} . ■

Alternative arguments (b) implies (a), since there must be equal numbers (0 or 1) of red and yellow edges left-incident to every vertex of G . Another way of proving (d) is using (c) to continue β to the right with yellow edges until the last one points to the beginning of another, which must be β (the first one), as two yellow edges cannot be (right-)incident, by (b).

3 The characteristic number of a winning strategy

Corollary 4 *Let f be a winning strategy and $N \geq 4$.*

- (a) *Every directed edge $\beta \in E_{k,k+1}$ meets exactly two edges of G having the same direction. Moreover, one of them is an $\alpha \in E_{k-1,k}$ and the other is a $\gamma \in E_{k+1,k+2}$, and the path $\overline{\alpha\beta\gamma}$ is f -admissible.*
- (b) *There exists an integer $\chi(f) \in \{0, 1, 2, 3\}$ such that for all values of k , the set $E_{k,k+1}$ contains exactly $\chi(f)$ yellow edges and the same number of red edges.*

Proof. (a): Consider an edge $\beta \in E_{k,k+1}^+$. By Lemma 3(b), β cannot be co-incident to another element of $E_{k,k+1}^+$. By Lemma 3(d), there is a unique edge $\alpha \in E_{k-1,k}^+$ meeting β . By Lemma 3(c)(b), there is a unique edge $\gamma \in E_{k+1,k+2}^+$ adjacent to β . (Again, the case of E^- is symmetric.)

(b): By (a), the set $E_{k,k+1}^+$ has at most 3 elements (as including no coincidences) and there is a one-to-one correspondence between the elements of $E_{k,k+1}^+$ and $E_{k+1,k+2}^+$ for every k (namely, $\alpha \leftrightarrow \beta \leftrightarrow \gamma$) Now it is enough to use Lemma 3(a) and the fact that the cyclic graph C_N is connected. ■

Definition 4 The number

$$\chi(f) = |E_{k,k+1}^+| = |E_{k,k+1}^-|$$

(as in Corollary 4(b)) will be called the characteristic number of the winning strategy f . □

The case $\chi(f) = 1$ can be excluded outright, since it would imply the existence of an f -admissible N -periodic paths of both directions (red and yellow). Now only three cases remain: $\chi(f) = 0, 2$, and 3.

4 The case $\chi(f) = 0$

Here we additionally suppose that $N \geq 5$ (the cases of $N = 3, 4$ being already settled).

In the case of $\chi(f) = 0$ all the edges of G are blue. That was possible for $N = 3$ and $N = 4$ as shown in Section 3. But supposing $N \geq 5$ we are going to prove that f would in fact be a losing strategy, implying $\chi(f) \neq 0$ for $N > 4$.

Take any edge \overline{ab} of graph G_N . It has, in particular, 32 different f -admissible extensions of length $N + 1$, by $N - 3$ edges to the left and 3 edges to the right, of the form

$$\overline{a_{ij} a_j u_1 \dots u_{N-4} a b b_p b_{pq} b_{pqr}} \quad (4)$$

for $i, j, p, q, r \in \{1, 2\}$, where the choice of vertices $u_1 \dots, u_{N-4}$ is fixed. Observe that, while there are exactly 4 edges of the form $\overline{a_{ij} a_j}$ and $\overline{b_p b_{pq}}$ alike, there may be either 2 or 3 vertices b_{pq} (and a_{ij} alike).

First, suppose vertex b_{pq} assumes three different values. Then there are at least six edges $\overline{b_{pq}b_{pqr}}$, while the number of the edges $\overline{a_{ij}a_j}$ is four, making the path close as $6 + 4 > 9$. Next, suppose there are just two different vertices b_{pq} . We can make index q point to these vertices, so that $b_{0q} = b_{1q}$ for $q = 0, 1$. Since the a_{ij} and b_{pq} are both in a 3-element set V_m , one can now fix i, j, q so that $a_{ij} = b_{0q} = b_{1q}$. Then, one of two paths $\overline{b_p b_{pq} a_j}$ ($p = 0, 1$) must be admissible since $\ell_-(\overline{b_{pq} a_j}) = 2$ and b_p takes 2 values. Thus, the path (4) acquires a closure with no use of vertex b_{pqr} . (But in fact, $a_j = b_{pqr}$ for some r .)

Corollary 5 *For $N > 4$, every winning strategy f has $\chi(f) \neq 0$.*

5 The case $\chi(f) = 3$

By Corollary 4, the yellow edges of graph G are arranged as follows:

$$\begin{array}{cccccccccccc} u_1^0 & \longrightarrow & u_1^1 & \longrightarrow & u_1^2 & \longrightarrow & \cdots & \longrightarrow & u_1^{N-1} & \longrightarrow & u_{\sigma(1)}^0 & \longrightarrow & u_{\sigma(1)}^1 & \longrightarrow & u_{\sigma(1)}^2 & \cdots \\ u_2^0 & \longrightarrow & u_2^1 & \longrightarrow & u_2^2 & \longrightarrow & \cdots & \longrightarrow & u_2^{N-1} & \longrightarrow & u_{\sigma(2)}^0 & \longrightarrow & u_{\sigma(2)}^1 & \longrightarrow & u_{\sigma(2)}^2 & \cdots \\ u_3^0 & \longrightarrow & u_3^1 & \longrightarrow & u_3^2 & \longrightarrow & \cdots & \longrightarrow & u_3^{N-1} & \longrightarrow & u_{\sigma(3)}^0 & \longrightarrow & u_{\sigma(3)}^1 & \longrightarrow & u_{\sigma(3)}^2 & \cdots \end{array}$$

where $\{u_1(k), u_2(k), u_3(k)\} = V_k$ for all k and $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ is a permutation.

(If σ had a fixed point, then a yellow cycle of period N would defeat strategy f . Hence, σ must be a rotation: $\sigma(i) \equiv i \pm 1 \pmod{3}$ for $i = 1, 2, 3$. This observation will be used later to construct winning strategies.)

Now let us locate the other colours. By Corollary 4, the set $E_{1,2}$ contains three disjoint red edges. Thus, we may assume

$$E_{1,2}^- = \left\{ \overline{u_1(1)u_3(2)}, \overline{u_2(1)u_1(2)}, \overline{u_3(1)u_2(2)} \right\}$$

(the other possibility being symmetric: $\overline{u_1u_2}, \overline{u_2u_3}, \overline{u_3u_1}$). Considering the set $E_{0,1}$ (to the left of $E_{1,2}$) we see that $\overline{u_3(0)u_2(1)}$ is red. Indeed, since $\overline{u_3(0)u_3(1)} \in E^+$, we have $\overline{u_3(0)u_3(1)u_1(2)} \notin \mathcal{A}(f)$, so $\overline{u_3(0)u_2(1)u_1(2)} \in \mathcal{A}(f)$, implying that $\overline{u_3(0)u_2(1)}$ must be the left-directed left continuation of $\overline{u_2(1)u_1(2)} \in E^-$ (by Lemma 3(c)). It follows that the edges in $E_{0,1}^-$ have the same arrangement as in $E_{1,2}^-$. Similarly, the sets $E_{k,k+1}^-$ and $E_{k+1,k+2}^-$ have the same arrangement for all $k = 0, \dots, N-2$, so we may assume that

$$E_{k,k+1}^- = \left\{ \overline{u_1^k u_3^{k+1}}, \overline{u_2^k u_1^{k+1}}, \overline{u_3^k u_2^{k+1}} \right\} \quad (k = 0, 1, 2, \dots, N-1).$$

All the remaining edges of G must be blue (by Lemma 3(b)). Here, by Lemma 3(e), the periodic f -admissible paths are precisely the periodic ones of a fixed colour.

Now consider all three one-colour paths of length N , starting at vertex $u_1(0)$ and going to the right (for the red one, this means going back). If N is divisible by 3, they all end at $u_{\sigma(1)}(0)$. But if N is not divisible by 3, they end at three distinct vertices of V_N , one of which must be $v_1(0)$. That makes one of the paths close to defeat the strategy, which is a contradiction. A significant part of the situation for $N = 5$ is illustrated in the diagram.

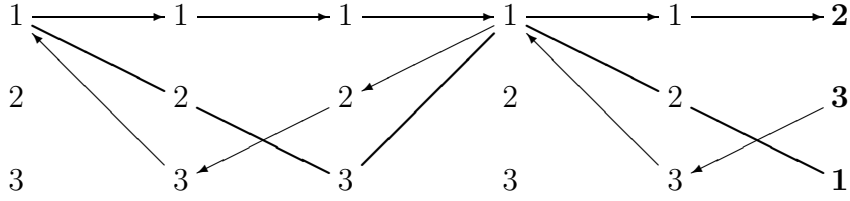


Figure 4: Part of a typical strategy of characteristic 3 on C_5

5.1 Winning for $3|N$

If N is a multiple of 3 and strategy f is colourable in the pattern just considered, then any one-colour path starting at $u_i(0)$ passes through $u_i(N) \neq u_i(0)$ and goes three times around the graph G_N , ending with period $3N \neq N$. Moreover, the considered colour arrangement is always (for every N) given by some colourable strategy, defined in the following way. Let

$$u_i(k + N) = u_{\sigma(i)}(k) \quad \text{for all } k \in \mathbf{Z},$$

where σ is some fixed-point-free permutation, and

$$f_k = \begin{bmatrix} 2 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 3 & 1 \end{bmatrix} \quad (k \in \mathbf{Z}), \quad (5)$$

using the convention: $f_k(i, j)$ in row i , column j . The definition is consistent since f_k is rotation-invariant, i.e.,

$$f_k(\sigma(i), \sigma(j)) = \sigma(f_k(i, j)),$$

which can be checked directly. (In fact, the strategies f_k are uniquely determined by this rotation-invariant colouring, hence they must themselves be σ -invariant).

With this strategy, every directed edge is followed by an edge of the same direction, as in Lemma 3(c). Thus, any admissible periodic path has one colour, as in Lemma 3(e). Since no admissible path has period N , the strategy is winning.

5.2 The solution for $\chi(f) = 3$

Corollary 6 *A winning strategy f with $\chi(f) = 3$ exists if and only if N is divisible by 3. If it exists, f is unique up to isomorphism (induced by permutations of colours at the vertices).*

Remark. The situation for $\chi(f) = 3$ can be visualised on a torus obtained by rotating a triangle which at the same time makes $1/3$ of a full turn in its own plane. This situation can also be viewed using a covering of graph $3 * C_N$ by the graph $3 * C_\infty$, where C_∞ has edges between all pairs of consecutive integers and is the universal covering of C_N .

6 The case $\chi(f) = 2$

Corollary 4 implies the following arrangement of all the yellow edges and some blue edges of graph G :

$$\begin{array}{cccccccccccc} u_1^0 & \longrightarrow & u_1^1 & \longrightarrow & u_1^2 & \longrightarrow & \dots & \longrightarrow & u_1^{N-1} & \longrightarrow & u_{\tau(1)}^0 & \longrightarrow & u_{\tau(1)}^1 & \longrightarrow & u_{\tau(1)}^2 & \dots \\ u_2^0 & \longrightarrow & u_2^1 & \longrightarrow & u_2^2 & \longrightarrow & \dots & \longrightarrow & u_2^{N-1} & \longrightarrow & u_{\tau(2)}^0 & \longrightarrow & u_{\tau(2)}^1 & \longrightarrow & u_{\tau(2)}^2 & \dots \\ u_3^0 & \longrightarrow & u_3^1 & \longrightarrow & u_3^2 & \longrightarrow & \dots & \longrightarrow & u_3^{N-1} & \longrightarrow & u_3^0 & \longrightarrow & u_3^1 & \longrightarrow & u_3^2 & \dots \end{array}$$

where $\{u_1(k), u_2(k), u_3(k)\} = V_k$ for all k and $\tau : \{1, 2\} \rightarrow \{1, 2\}$ is a permutation. If τ were the identity, then two yellow cycles would have period N , contrary to the assumption that f is winning. Thus, τ must be a transposition: $\tau(1) = 2$ and $\tau(2) = 1$.

Let us look for the red and the remaining blue edges. By Lemma 3(b)(d), the red edges are crossing between rows of the yellow ones:

$$E_{k,k+1}^- = \left\{ \overline{u_1(k)u_2(k+1)}, \overline{u_2(k)u_1(k+1)} \right\} \text{ for } k = 0, 1, \dots, N-1$$

and all the remaining edges are blue.

Now if N were an odd number, then the red (left-directed) path (f -admissible by Lemma 3(e)) ending at vertex $u_1(0)$ would begin at vertex $u_{\tau(2)}(N) = u_1(0)$ and have period N , again contrary to the assumption that f is winning. Consequently, N must be an even number.

6.1 The strategy for $\chi(f) = 2$

As in the case of $\chi(f) = 3$, from the obtained colour arrangement one can deduce the form of strategy f . One obtains:

$$f_k = \begin{bmatrix} 3 & 1 & 1 \\ 2 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix} \quad (k \in \mathbf{Z}) \quad (6)$$

with the same convention as before, and the permutation $\sigma = (2, 1, 3)$. Again, this colourable strategy f with single-colour admissibility exists for all even numbers N since f_1 is invariant under the permutation $(2, 1, 3)$.

Since both directed paths have period $2N$, any N -periodic admissible path must be blue by Lemma 3(e). The only admissible blue paths of length 2 are:

$$\overline{u_i^k u_3^{k+1} u_3^{k+2}}, \overline{u_3^k u_3^{k+1} u_i^{k+2}}, \overline{u_3^k u_i^{k+1} u_3^{k+2}}, \text{ where } i \in \{1, 2\}.$$

6.2 The question of winning with $\chi(f) = 2$

Already for $N = 2$ (despite the fact that $\chi(f)$ was not defined for $N < 4$) a losing blue cycle can be observed, namely

$$\overline{\dots v_3^0 v_1^1 v_3^2 v_2^3 v_3^4 v_1^5 \dots},$$

where $v_1^1 = v_2^3$.

Now consider the case $N = 4$. Then any admissible path containing an edge $\overline{v_3^k v_3^{k+1}}$ could not close with period 4. At the same time, any admissible path containing no such edge must have the form $\overline{\dots 31323132 \dots}$, i.e. (up to a shift),

$$\overline{\dots u_3(0)u_1(1)u_3(2)u_2(3)u_3(4)u_1(5)u_3(6)u_2(7), \dots},$$

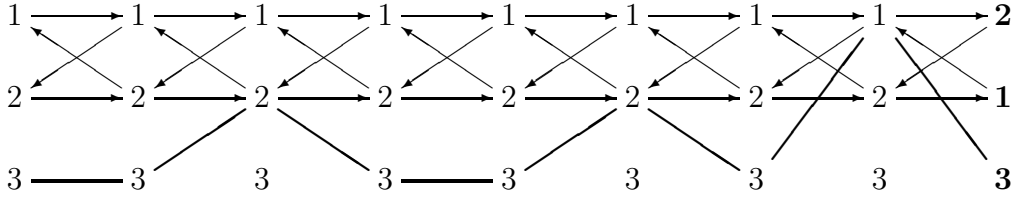


Figure 5: A diagram of the typical strategy of characteristic 2 on C_8 , showing all the directed edges and a critical undirected path.

which has period 8 as $u_1(1) \neq u_1(5)$. This shows that f is a winning strategy for $N = 4$.

If, however, $2|N$ and $N \geq 6$, then there exists the following admissible blue path of period N :

$$\dots \overline{3313(31)(32)(31)(32) \dots (3j) \dots}$$

(where $j \in \{1, 2\}$ and $j \equiv N/2 \pmod{2}$). Consequently, the strategy f is losing for $N > 4$. The situation for $N = 8$ is illustrated in the diagram.

6.3 The solution for $\chi(f) = 2$

Corollary 7 *A winning strategy f with $\chi(f) = 2$ exists only for $N = 4$ (and is unique up to isomorphism).*

Remark. The above situation for $2|N$ can be visualised as a Möbius band with the yellow cycle on the boundary and the red cycle inside, completed with a separate blue cycle which is not admissible. The edges can be drawn on a Klein bottle arising from this construction. As before, this is equivalent to using an appropriate covering of graph $3 * C_N$ by the graph $3 * C_\infty$.

Thus we have proved Theorem 1. ■

3 Corollaries

The number of 3 colours turns out to be effectively maximal for the cycle graphs.

Corollary 8 *The hat game on any cycle C_N ($n > 4$) with the height function h satisfying $h(1) = 4$ and $h(k) = 3$ for $k = 2, \dots, N$ is losing, i.e., $\mu(h) = 0$.*

Proof. If f were a winning strategy for this game, then it would also be winning for any of its 3-colour restrictions. It follows that choosing any $k \in \{1, 2, 3, 4\}$ and changing any values $f_1(i, j) = k$ into any values $f_1(i, j) \neq k$ would result in a winning strategy for the 3-colour game. By Corollary 6, such a strategy is unique up to permutations of colours. Now, f_1 assumes some values, so for instance, we have $f_1(i, j) = 4$ for some pair(s) (i, j) . But the form (5) of the individual strategy shows that f_1 must assume each value three times. Some arbitrary choice of $f(i, j) \neq 4$ could always change that, contrary to the fact that f should remain a winning strategy. ■

If N is *not* divisible by 3, at least a strategy with a high *probability* of winning can be found.

Corollary 9 *In the three-colour game on any cycle C_N ($3 \nmid N$) there exists a strategy for which the probability of winning is $\geq 1 - 3^{-N+1}$.*

Proof. This follows from the fact that the strategy described in Section 5 has at most three admissible N -periodic paths. ■

Acknowledgements. I would like to thank Prof. Jarosław Grytczuk and Sławomir Porębski for acquainting me with the hat problems.

References

- [1] Todd Ebert: *PhD Thesis*. Univ. California St. Barbara, 1998.
- [2] *Why mathematicians now care about their hat color*. The New York Times, page D5, April 10, 2001.
- [3] P.Winkler: *Games people don't play*. In *Puzzler's Tribute*. A.K.Peters, 2001.
- [4] Uriel Feige: *You can leave your hat on (if you guess its color)*. Technical report MCS04-03, *Computer Science and Applied Mathematics*, The Weizmann Institute of Science, page 10pp., 2004.
- [5] Soren Riis: *Information flows, graphs and their guessing number*. The Electronic Journal of Combinatorics **14** (2007), #R44
- [6] Taoyong Wu, Peter Cameron, Soren Riis: *On the guessing number of shift graphs*. J. Discrete Algorithms **7** (2009), 220–226.
- [7] Butler, Mohammad Taghi Hajiaghayi, Robert D. Kleinberg, Tom Leighton: *Hat guessing games*. SIAM J. Discrete Math. **22(2)**, 592–605, 2008.
- [8] Marcin Krzywkowski: *Hat problem on odd cycles*. Houston J Math 37 (2011), 1063–1069.
- [9] Marcin Krzywkowski: *On the hat problem, its variations and their implications*. Annales Universitatis Paedagogicae Cracoviensis Studia Mathematica 9 (2010) 55–67.

You can leave your hat on (if you guess its color)

Uriel Feige
Department of Computer Science and Applied Mathematics
The Weizmann Institute
Rehovot, Israel
uriel.feige@weizmann.ac.il

March 16, 2004

Abstract

We present a methodology for solving a variety of games involving guessing the colors of hats. As an example, consider the following game. Seven players sit in a circle. There are four blue hats and four red hats. Seven hats are placed on the heads of the seven players, and the remaining hat is discarded. Every player can see the colors of the hats of the other six players, but cannot see the color of his own hat, or that of the discarded hat. Then every player needs to guess the color of his own hat. The players may coordinate a strategy before the game begins, but once the hats are placed on their heads, there is no communication of any form between the players, and in particular, no player knows whether another player already produced a guess. Is there a guessing strategy that guarantees (with absolute certainty) that at least five of the players guess correctly?

1 Introduction

In this paper we consider several multiplayer games in which every player needs to guess the color of the hat placed on his/her head, while seeing only the colors of the hats placed on the heads of other players. In all the games that we consider, if all players guess at random, a certain number of guesses are expected to be correct. The problem is to design a deterministic strategy that guarantees that the number of correct guesses is as expected.

We call such a strategy a *perfect* strategy. The trigger to the work reported here was a collection of results of Benjamin Doerr (currently unpublished), concerning variations on a setting described by Peter Winkler [4].

This paper is organized as follows. The abstract presents a puzzle that the reader may try to solve before reading the rest of the paper. In Section 2 we describe several color guessing games. In Section 3 we give some preliminary observations that may help orient the reader towards solutions to our puzzles. In Section 4 we present solutions to two of our color guessing games. In Section 5 we present a general methodology for establishing that a large class of color guessing games have perfect strategies. We show how this methodology applies to the remaining color guessing games of Section 2. In Section 6 we conclude with some additional observations and open questions.

2 The games

In all our puzzles, the number of players is denoted by n . Sometimes, n will need to be of a special form, and then we will use an additional parameter k to indicate this. For example, $n = 2k$ indicates that n is even. Players are allowed to coordinate a strategy before the game begins. The game consists of placing colored hats on the heads of the players, where C denotes the set of allowable colors in the game. For simplicity, these colors are denoted by $c_0, \dots, c_{|C|-1}$. Every player can see the colors of the hat of all other players (and nothing else), and needs to guess the color of his own hat. Players have *names* (and for simplicity, the names will be p_1, \dots, p_n). The colors of their hats will be denoted by h_1, \dots, h_n . The guesses of the players are denoted by g_1, \dots, g_n . Formally, a strategy is a collection of n strategies, one for each player. A strategy $s_i : C^{n-1} \rightarrow C$ for player p_i specifies the “guess” of p_i as a (deterministic) function of the tuple of colors $(h_1, \dots, h_{i-1}, h_{i+1}, \dots, h_n)$.

We may view the actual colors h_1, \dots, h_n of the hats as being assigned by an *adversary* who knows the strategy of the players, and tries to select the combination of colors that causes the strategy to be least successful.

A strategy of the players will be called *perfect* if it meets some conditions (that differ from game to game). In all games, the question is to find a perfect strategy (or show that no such strategy exist).

2.1 The *plain* version

This version appears in [4].

Here $|C| = 2$ and $n = 2k$. A perfect strategy is one that guarantees that at least $k = n/2$ players correctly guess the colors of their hats.

One may also consider the case of having more than two colors for the hats. Then $|C| = c \geq 2$, $n = ck$, and at least $k = n/c$ players need to guess correctly.

2.2 The *discarded hat* version

This is the version that appears in the abstract to this paper.

Here $|C| = 2$ and $n = 4k - 1$. (The version in the abstract corresponds to the choice $k = 2$.) The players are given one more piece of information before the game begins, namely, that the total numbers of hats of color c_0 will be either $2k - 1$ or $2k$ (with the rest of the hats being of color c_1). Equivalently, one may think of there being $2k$ hats of each color, and one hat is discarded (without the players knowing which hat is discarded). In this game, a perfect strategy guarantees that at least $3k - 1$ players guess their color correctly.

2.3 The *everywhere balanced* version

Here $|C| = c \geq 2$ and n is arbitrary. The goal of the players is as follows. Let H_j be the set of the players that have a hat of color c_j . Hence $\sum_{j=0}^{c-1} |H_j| = n$. (A player does not know to which set he belongs, and the players do not know the cardinalities of the sets H_j .) A perfect strategy guarantees that in every such set H_j , the number of players who guess correctly (namely, guess c_j) is between $\lfloor |H_j|/c \rfloor$ and $\lceil |H_j|/c \rceil$.

2.4 The *majority* version

This version was studied by Doerr (private communication).

Here $|C| = 2$, n is arbitrary, and there is an additional parameter m that may depend on n . For H_j as defined above, a perfect strategy guarantees that at least $\max\{|H_0|, |H_1|\} - m$ players guess their color correctly. How small can m be for a perfect strategy to exist?

3 Preliminary observations

For the plain version (with $c = 2$), it is not hard to see that no strategy can guarantee more than $n/2$ correct guesses. Regardless of the strategy of the players, if the adversary assigns the colors of the hats independently at random, each player guesses his color correctly with probability half. By linearity of the expectation, the expected number of players who guess correctly is $n/2$. As expectation is an averaging operator, it follows that there is some assignment of the adversary that causes the number of correct guesses not to exceed $n/2$. (For $c > 2$, the same argument shows that no strategy can guarantee more than n/c correct guesses.)

For the discarded hat version, call the color that appears on $2k$ hats the *majority* color, and the color that appears on $2k - 1$ hats the *minority* color. Every player that has a hat of the minority color sees two more hats of the majority color than the minority color, and hence knows the color of his own hat. This guarantees $2k - 1$ correct guesses. The players that have a hat of the majority color see an equal number of hats of each color. It can be

shown that if the adversary assigns the colors at random, then regardless of the strategy of the players, in expectation k of the players that have a hat of the majority color guess correctly. Hence no strategy can guarantee more than $3k - 1$ correct guesses.

For the everywhere balanced version, again averaging arguments show that no strategy may guarantee more than $|H_j|/c$ correct guesses, and similarly, no strategy can guarantee less than $|H_j|/c$ correct guesses. Hence the range between $\lfloor |H_j|/c \rfloor$ and $\lceil |H_j|/c \rceil$ is the best one can hope for.

For the majority version, let us bound m from below as a function of n . Recall that if the adversary assigns hat colors at random, in expectation $n/2$ players guess their color correctly. On the other hand, the majority color is expected to include $n/2 + \Theta(\sqrt{n})$ hats (as this is the standard deviation of the Binomial distribution). Hence in expectation, the number of correct guesses is $\Omega(\sqrt{n})$ below $\max[|H_0|, |H_1|]$, implying that one needs $m \geq \Omega(\sqrt{n})$.

The reader may find it useful to tackle the plain version and the discarded hat version by first considering the most simple setting of the parameters, namely, that of $k = 1$. For the plain version this gives two players, one of whom needs to guess correctly. For the discarded hat version, this gives three players, two receive hats of the same color and the other receives a hat of a different color, and two players need to guess correctly.

4 Perfect strategies

In this section we present perfect strategies for two of the games of Section 2.

4.1 The plain version

The perfect strategy presented by Winkler for this version is to pair players together (for $1 \leq i \leq k$, the pairs can be p_i and p_{i+k}), and have each pair play the case $n = 2$. That is, player p_i guesses h_{i+k} as the color of his hat, and player p_{i+k} guesses the color not equal to h_i as the color of his hat.

Another perfect strategy for the plain version (that came up in a discussion with Amir Shpilka) is based on a *symmetric* strategy. A strategy is called symmetric if the guess of a player is a function of the number of hats of each color (except his own), disregarding the distribution of hats among the players. Different players may use different symmetric functions.

For $1 \leq i \leq k$, player p_i guesses c_0 if he sees an odd number of hats of color c_0 , and c_1 otherwise. For $k+1 \leq i \leq 2k = n$, player p_i guesses c_0 if he sees an even number of hats of color c_0 , and c_1 otherwise. As the true total number of hats with color c_0 is either even or odd, either the first k players all guess correctly, or the last.

The above solutions generalizes easily to the case $c > 2$. We show the generalization for the symmetric strategy. Think of the color names as the numbers $0, \dots, c-1$. For $0 \leq j \leq c-1$, for $jk+1 \leq i \leq (j+1)k$, player i guesses for his hat the color g_i that leads to equality in $g_i + \sum_{l \neq i} h_l = j$

(modulo c). As there is some j such that $\sum_{l=1}^n h_l = j$ (modulo c), exactly k players guess correctly. (The above strategy in fact appears in a manuscript of Doerr for the case $c = n$.)

4.2 The discarded hat version

Recall that the difficulty in the discarded hat version is to ensure that of those players that have a hat with the majority color (that we call the *majority players*), half would guess correctly. A player can easily tell whether he is a majority player or not (but without knowing which is the majority color), and all minority players guess correctly their colors. Hence we shall only specify the strategy that players use when they are majority players.

Symmetric strategies cannot be perfect in the discarded hat version. All majority players see exactly $2k - 1$ hats of color c_0 and $2k - 1$ hats of color c_1 . Hence there are only two possible symmetric strategies in this case: either guess c_0 , or guess c_1 . If all players have symmetric strategies, then at least $2k$ players have the same symmetric strategy (say, guess c_1). The adversary may assign these $2k$ players hats of color c_0 and all other players hats of color c_1 . In this case, all majority players fail in their guess, and the number of correct guesses is only $2k - 1$.

We now present a perfect nonsymmetric strategy for the discarded hat version. Think of the players as sitting in a circle. Every player that sees $2k - 1$ hats of each color (and hence does not know the color of his own hat), computes which of the two colors occurs more times among the hats of the $(4k - 2)/2 = 2k - 1$ players that follow him in clockwise order. He then guesses the same color for his own hat.

We show now that exactly k of the majority players guess correctly. Assume without loss of generality that there are $2k$ blue hats, and consider only the players having blue hats. Starting with an arbitrary such player, name them from b_1 to b_{2k} in clockwise order. Now for every $1 \leq i \leq k$, exactly one of the two players b_i and b_{k+i} guesses correctly, because either b_{k+i} sits at most $2k - 1$ locations after b_i (and then b_i guesses correctly) or b_i sits at most $2k - 1$ locations after b_{k+i} (and then b_{k+i} guesses correctly). This is an exclusive or that follows from the fact that there are exactly $4k - 1$ players altogether.

5 A general methodology

In Section 4 we presented strategies for the plain version and the discarded hat version of the color guessing game. These solutions were elegant (so the author thinks), and may well be understood by nonmathematicians. However, they were of an ad-hoc nature, and it is difficult to see how to extend them to other color guessing games (such as the everywhere balanced version and the majority version). In this section we present general principles for establishing that certain color guessing games have perfect strategies.

Though we try to keep the presentation at a fairly elementary level, some level of mathematical maturity is needed in order to follow this section. In particular, we only prove the existence of a perfect strategy, but do not actually exhibit one. (Our methodology provides an algorithm for designing a perfect strategy, but the complexity of the algorithm is exponential in n . As bad as this complexity sounds, it is still much better than the time complexity of exhaustive search over all possible strategies, which is doubly exponential in n .)

A common property of all our color guessing games is that it is relatively easy to come up with randomized strategies for the players that achieve the goal of the game *in expectation*. For example, for the plain version, if every player guesses a random color for his hat, in expectation $n/2$ players guess correctly. Our methodology is based on transforming a randomized strategy into a deterministic one. Rather than discuss randomized strategies, we shall deal with what we call *fractional* strategies. In the following we shall use $\bar{h} = (h_1, \dots, h_n) \in C^n$ to denote a vector of n hat-colors, and $\bar{h}_i = (h_1, \dots, h_{i-1}, h_{i+1}, \dots, h_n) \in C^{n-1}$ to denote the subvector of colors seen by player p_i .

Definition 1 A fractional strategy $s_i : (C, C^{n-1}) \rightarrow C$ for player p_i maps to every color $g \in C$ and every tuple of colors $\bar{h}_i \in C^{n-1}$ a value z_{i,g,\bar{h}_i} , where the following two constraints must be satisfied:

1. For every i, g and \bar{h} we have $z_{i,g,\bar{h}_i} \geq 0$.
2. For every i and \bar{h} we have $\sum_{g \in C} z_{i,g,\bar{h}_i} = 1$.

Intuitively, one may view z_{i,g,\bar{h}_i} as the probability that player p_i guesses color g upon seeing colors \bar{h}_i , or as a confidence level that p_i associates with color g upon seeing colors \bar{h}_i . We note that true strategies are special cases of fractional strategies, as they satisfy the additional Boolean constraint that for every i, g, \bar{h} , we have $z_{i,g,\bar{h}_i} \in \{0, 1\}$.

In the color guessing games, for every assignment \bar{h} of hat colors, there is some goal that needs to be met by the strategies of the players (a certain number of correct guesses). We may extend this goal to apply also to fractional strategies. Recall our notation that $H_j(\bar{h})$ denotes the set of players that have a hat of color c_j in \bar{h} . Then for example, for the plain version, we may add the following set of constraints. For every \bar{h} ,

$$\sum_{i \in H_0(\bar{h})} z_{i,0,\bar{h}_i} + \sum_{i \in H_1(\bar{h})} z_{i,1,\bar{h}_i} = n/2.$$

We have seen in Section 4.1 some perfect strategies for the plain version that indeed meet the constraint above. But assume now that we were not clever enough to find perfect strategies for the plain version. We show how our methodology can be used to infer that perfect strategies exist (but without actually exhibiting a strategy).

There is a trivial fractional strategy that satisfies all the constraints, namely, all $z_{i,g,\bar{h}_i} = 1/2$. We shall show that this strategy can be *rounded* to give a true (Boolean) strategy that still satisfies all constraints. The main point that we use in this case is that every *variable* z_{i,g,\bar{h}_i} participates in exactly three constraints:

1. The *nonnegativity* constraint $z_{i,g,\bar{h}_i} \geq 0$.
2. The *strategy* constraint $\sum_{g \in C} z_{i,g,\bar{h}_i} = 1$.
3. The *goal* constraint $\sum_{j \in H_0(\bar{h})} z_{j,0,\bar{h}_j} + \sum_{j \in H_1(\bar{h})} z_{j,1,\bar{h}_j} = n/2$, for \bar{h} that has $h_i = g$ and \bar{h} agrees with \bar{h}_i for all indices $j \neq i$.

Ignoring the nonnegativity constraints, we consider a bipartite graph (that we call the *constraint graph*) with all strategy constraints on one side, and all goal constraints on the other side. Every variable z_{i,g,\bar{h}_i} contributes one edge to the bipartite graph, namely, the edge connecting the two constraints in which z_{i,g,\bar{h}_i} participates. This edge is labeled by the value of z_{i,g,\bar{h}_i} .

We present a rounding procedure that rounds all edge values to 0/1 values, while preserving the sum of edge values incident with every vertex. This gives a true strategy for the game that satisfies the goals of the game. The rounding procedure that we describe has multiple iterations. In every iteration, some edges that previously had fractional values get integer values (either 0 or 1), and are *frozen*. When all edges are frozen, the rounding procedure ends. An invariant preserved by the rounding procedure is that for every vertex, the sum of values that are incident with it does not change.

An iteration of the rounding procedure works as follows. Assume that G contains at least one nonfrozen edge (as otherwise we are done). Observe that the subgraph induced on the nonfrozen edges has minimum degree 2, as otherwise the sum of label values incident with some vertex is noninteger. Hence it must contain a cycle. This cycle must be of even length, because the constraint graph is bipartite. Starting at an arbitrary edge e along the cycle, consider the edges of the cycle as alternating between positive and negative. Add a small value $\delta > 0$ to the values of the labels of all positive edges, and subtract δ from the values of the labels of all negative edges. Note that this does not change the sum of label values incident with any vertex. Now choose δ to be the smallest possible value that makes (at least) one such edge reach a 0/1 value. By this, at least one more edge becomes frozen and the iteration is completed.

Using the approach outlined above, one can show that both the plain version and the discarded hat version have a perfect strategy. But for the everywhere balanced game, and for the majority game, we need to address one technicality. The distinction is that in these latter games, the goal constraints are *inequalities* rather than equalities. For example, in the everywhere balanced game, the goal is to have in every set H_j between $\lfloor |H_j|/c \rfloor$ and $\lceil |H_j|/c \rceil$ correct guesses. A fractional strategy that satisfies the goal

constraints might have the property that in the constraint graph, the sum of values of edges incident with a goal constraint is noninteger. If this happens, it is no longer true that in the rounding procedure the subgraph induced on nonfrozen edges has minimum degree 2. To handle this issue, we add one more vertex r on the strategy constraint side of the bipartite graph, and connect it to every vertex in the goal constraint side. Now if $s(u)$, the sum of values given by the fractional solution to the edges incident with a goal constraint u , is noninteger, then we give to the edge (r, u) the fractional value that rounds $s(u)$ up to the nearest integer. Now the sum of values incident with each goal constraint is integer. For every fractional strategy, it also must hold that the sum of values incident with each strategy constraint is integer. As the values summed up on the left hand side of the bipartite graph must be equal to the values summed up on the right hand side, it follows that also for r the sum of values incident with it is integer. Hence we can round the fractional strategy to an integer strategy. An edge (r, u) ends up with value 0 if $s(u)$ was rounded up, and with value 1 if $s(u)$ was rounded down.

Summarizing, we have the following general theorem.

Theorem 1 *Using the notation of this section, consider an arbitrary color-guessing game with the following properties:*

1. *Every goal constraint addresses one particular \bar{h} and one particular set $I \subset \{1, \dots, n\} \times C$, and has the form $q \leq \sum_{(i,g) \in I} z_{i,g,\bar{h}_i} \leq p$, where q and p are integers (possibly, $q = p$).*
2. *Every variable z_{i,g,\bar{h}_i} appears in at most one goal constraint.*

Then such a game has a perfect strategy iff it has a perfect fractional strategy.

5.1 The everywhere balanced version

The goal constraints of the everywhere balanced game are for every \bar{h} and $j \in \{0, \dots, c-1\}$,

$$\lfloor |H_j|/c \rfloor \leq \sum_{i \in H_j} z_{i,c_j,\bar{h}_i} \leq \lceil |H_j|/c \rceil.$$

The conditions of Theorem 1 are satisfied. Hence we shall only show a perfect fractional strategy for the everywhere balanced game, and then Theorem 1 implies the existence of a perfect strategy (without actually exhibiting one). The fractional strategy is simple: for all i, g, \bar{h} we set $z_{i,g,\bar{h}_i} = 1/c$. It is easy to check that all strategy constraints and all goal constraints are satisfied by this fractional strategy.

5.2 The majority version

Let the two colors be 0 and 1. For a given \bar{h} , recall that H_0 and H_1 denote the set of players with 0-hats and 1-hats respectively. For player p_i , let H_0^i

be the set of players with 0-hats that are seen by p_i (which differs from H_0 when p_i himself has a 0-hat). Consider the following fractional strategy. For a given \bar{h} , if $|H_0^i| \geq n/2 + \sqrt{n}$, then $z_{i,0,\bar{h}_i} = 1$ and $z_{i,1,\bar{h}_i} = 0$. If $|H_0^i| \leq n/2 - \sqrt{n}$, then $z_{i,0,\bar{h}_i} = 0$ and $z_{i,1,\bar{h}_i} = 1$. Else, let b denote $|H_0^i| - n/2$. Then $z_{i,0,\bar{h}_i} = 1/2 + b/2\sqrt{n}$ and $z_{i,1,\bar{h}_i} = 1/2 - b/2\sqrt{n}$.

Clearly, the above fractional strategy satisfies all strategy constraints. We now consider goal constraints. So as to slightly simplify the presentation, for every \bar{h} we strengthen the corresponding goal constraint by breaking it into two separate constraints, one for H_0 and one for H_i . They are:

$$\sum_{i \in H_0} z_{i,0,\bar{h}_i} \geq \min[|H_0|, \left\lfloor |H_0| \left(\frac{1}{2} + \frac{|H_0| - 1 - n/2}{2\sqrt{n}} \right) \right\rfloor]$$

$$\sum_{i \in H_1} z_{i,1,\bar{h}_i} \geq \min[|H_1|, \left\lfloor |H_1| \left(\frac{1}{2} - \frac{|H_0| - n/2}{2\sqrt{n}} \right) \right\rfloor]$$

These constraints are satisfied by the above fractional strategy. Moreover, as goal constraints they satisfy the conditions of Theorem 1. Hence, there is a Boolean strategy satisfying the same goal constraints.

Now, for arbitrary \bar{h} , if $|H_0| > n/2 + \sqrt{n}$ (or $|H_1| \geq n/2 + \sqrt{n}$, respectively) then all H_0 players (H_1 , respectively) guess correctly and the number of correct guesses is $\max[|H_0|, |H_1|]$. If $||H_0| - |H_1|| \leq 2\sqrt{n}$, then sum up the two goal constraints. The number of correct guesses is:

$$\sum_{i \in H_0} z_{i,0,\bar{h}_i} + \sum_{i \in H_1} z_{i,1,\bar{h}_i} \geq \frac{n}{2} + (|H_0| - |H_1|) \frac{|H_0| - n/2}{2\sqrt{n}} - \frac{|H_0|}{2\sqrt{n}} - 2 > \frac{n}{2} - \frac{\sqrt{n}}{2} - 2.$$

As $\max[|H_0|, |H_1|] \leq n/2 + \sqrt{n}$ in these cases, this gives a perfect strategy for the majority game with $m \leq 3\sqrt{n}/2$. (The leading constant in front of \sqrt{n} can be improved with more careful analysis.)

6 Discussion

We presented perfect strategies for various color guessing games. The plain version and the discarded hat version can be appreciated also by nonmathematicians. The everywhere balanced and the majority version are presented so as to illustrate a general approach for solving such problems, via Theorem 1.

In the constraint graph for the discarded hat game, all strategy constraint vertices have degree 2, and all goal constraint vertices have even degree. By shortcutting the degree 2 vertices, we get a bipartite graph of even degree, with H_0 goal constraints on one side and H_1 goal constraints on the other side. This graph is Eulerian. Every Eulerian cycle in this graph gives a perfect strategy, by having red/blue alternate along the edges of the cycle. Moreover, *every* perfect strategy for the discarded hat game can be viewed as a strategy obtained in such a way from an Eulerian cycle. (Think of

the red/blue values as giving right/left orientations to the underlying edge. The resulting directed graph is Eulerian.) Using this characterization of perfect strategies it is not hard to show that every perfect strategy for the discarded hat game must be *unbiased* in the following sense: every majority player guesses *red* on exactly half of the possible hat assignments to the other players, and *blue* on the other half. (Hint: colors necessarily alternate between two successive visits to edges associated with the same player p_i .)

For the majority game, Doerr presents an explicit strategy (one for which the computation performed by every player takes time that is at most polynomial in n), but for $m = O(n^{2/3})$ rather than $m = O(\sqrt{n})$. The author does not know whether the majority game has an explicit strategy when $m = O(\sqrt{n})$.

The puzzles and solutions given in this paper are related to some well studied research areas.

Theorem 1 can be viewed as a special case of the well known fact that linear programs with integer constraints and a totally unimodular constraint matrix always have integer optimal solutions. The connection between total unimodularity and the solution of integer programs was apparently first made in [2], and can be found in any of a number of textbooks.

The puzzles studied here can be cast as questions about *discrepancy*. The approach we used to solve them (by rounding a fractional solution) has been previously used in order to prove other results concerning discrepancy, such as the well known Beck-Fiala theorem [1].

Acknowledgements

I thank Benjamin Doerr for communicating to me his work on games of guessing colors.

This paper is dedicated to Nadav, Ofir and Dror (ages 9, 12 and 15 at the time of the writing) who showed interest in the puzzle posed in the abstract. The color of Nadav's hat is red.

References

- [1] J. Beck and T. Fiala. "Integer-making theorems". *Discrete Applied Mathematics* 3, 1–8, 1981.
- [2] A. Hoffman and J. Kruskal. "Integral boundary points of convex polyhedra". In H. Kuhn and A. Tucker, editors, *Linear inequalities and related systems*, Princeton University Press, 1956.
- [3] R. Newman. "You can leave your hat on". (Recorded by Joe Cocker, Tom Jones, Randy Newman.)
- [4] P. Winkler. "Games people don't play". In D. Wolfe and T. Rogers, editors, *Puzzlers' tribute. A feast for the mind*. A K Peters, 2001.

Hat Guessing Games

Steve Butler^{*} *Mohammad T. Hajiaghayi*[†] *Robert D. Kleinberg*^{†‡§}
Tom Leighton^{†¶}

Abstract

Hat problems have become a popular topic in recreational mathematics. In a typical hat problem, each of n players tries to guess the color of the hat they are wearing by looking at the colors of the hats worn by some of the other players. In this paper we consider several variants of the problem, united by the common theme that the guessing strategies are required to be deterministic and the objective is to maximize the number of correct answers in the worst case. We also summarize what is currently known about the worst-case analysis of deterministic hat-guessing problems with a finite number of players.

Key words: hat game; deterministic strategies; sight graph; Tutte-Berge formula; hypercube

AMS Mathematics Subject Classification: 91A12; 05C20

1 Introduction

Consider the following game. There are n distinguishable players and one adversary. The adversary will place on the heads of the players hats of k different colors, at which point players are allowed to see all hats but their own. No communication is allowed. Each player then makes a private guess as to what hat they are wearing. The goal of the players is to maximize the number of correct guesses.

To help players maximize their correct guesses, the players are allowed to meet before the hats are placed on their heads and to determine a public deterministic strategy (public in that everyone, including the adversary, knows the strategy and deterministic in that the guesses are determined

^{*}Department of Mathematics, University of California, San Diego, La Jolla, CA 92093, U.S.A., Email: sbutler@math.ucsd.edu.

[†]Department of Mathematics and Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, 32 Vassar Street, Cambridge, MA 02139, U.S.A., Emails: {hajiagha,rdk,ftl}@theory.csail.mit.edu.

[‡]Computer Science Division, UC Berkeley, Berkeley, CA 94720; and Department of Computer Science, Cornell University, Ithaca, NY 14853.

[§]Part of this work was supported by a National Science Foundation Mathematical Sciences Postdoctoral Research Fellowship.

[¶]Akamai Technologies, Eight Cambridge Center, Cambridge, MA 02139, U.S.A.

completely by the hat placement). What is the maximum number of correct guesses that can be guaranteed, and what strategy should be implemented to achieve the maximum?

This question has been answered in [3, 9]. Here we will present the answer and consider some variations on the game, showing that they lead to some surprisingly subtle combinatorial and algorithmic problems and theorems. We proceed as follows. In the remainder of the introduction we answer these questions for the game as stated. In Section 2 we consider what happens when players are not able to see everyone, which might be applicable as an abstraction of the problem of guessing information globally in a market or a decentralized computing system, in which each person (or software agent) has only partial/local knowledge. In Section 3 we give a hypercube interpretation of the game which gives insight into the nature of optimal strategies, and we explore a version of the hats game where the adversary has a restricted hat supply.

Hat guessing games have long been a popular source of problems in recreational mathematics, and variations of hat guessing games have recently attracted increasing attention [6], partly because of their connections with coding theory (particularly Hamming codes). As another example, Aggarwal et al. [1] have used hat problems in the design of deterministic auction mechanisms. When constructing truthful auction mechanisms, a mechanism designer must devise a procedure for assigning a price to each bidder based only on the bids of other players (else she may have an incentive to lie about her bid), with the aim of charging many bidders a price which is close to their own bid. Note the formal similarity with hat problems, in which the goal is to devise a procedure for assigning a guess to each player based only on the hat colors of other players, with the aim of assigning to many players a guess which matches their own hat color. By exploiting this similarity between the two problems, Aggarwal et al. used hat-guessing strategies for a variant of the balanced hat problem (discussed below in Section 3.1) to provide a generic procedure for converting a randomized auction into a deterministic auction with approximately the same revenue, in markets with single-parameter bidders and no supply constraints.

Finally it is worth mentioning the fact that we are considering deterministic strategies instead of randomized ones is very important in this paper. The main reason is that these deterministic strategies focus on the worst-case scenarios instead of average or even almost-all scenarios. As a result, for several problems in this paper obtaining a randomized algorithm which guesses a constant fraction of the desired hat colors on average is easy though we cannot even guess one or a constant number of hat colors deterministically (see Sections 2.3 and 2.4).

1.1 A winning approach to the hat guessing game

Example 1. Consider the case where there are 2 players and 2 colors of hats. Then a winning strategy for these players is to have the first player guess what the second player is wearing and the second player guess the color opposite of what the first player is wearing. If they are wearing hats of the same color then the first player guesses correctly. If they are wearing different colors then the second player guesses correctly. In any case there is one correct guess (and one incorrect guess). \square

It is interesting to note that in this example the expected number of correct guesses is 1, the same as if they had guessed randomly. What their strategy has done is to eliminate the variance

involved in the guessing. The other thing to note is that neither player has any idea who guessed correctly, but they do know that collectively one of them did. These two properties will hold in general.

We have the following general result, first proved for 2 colors by Winkler [9] and later generalized to k colors by Feige [3].

Theorem 2. *If there are n players and hats of k different colors then there exists a strategy guaranteeing at least $\lfloor n/k \rfloor$ correct guesses. No strategy can improve on this.*

Proof. We first demonstrate a strategy. Number the players 1 to n and the colors of the hats 1 to k . The i th player will guess as if the sum of all the hats (including their own) is congruent to $i \pmod k$. At least $\lfloor n/k \rfloor$ of the players will be acting correctly and will therefore guess correctly.

To see that this cannot be improved upon we use an averaging argument. If a player sees a particular placement of hats then they are in one of k situations and they will guess correctly in exactly one of these situations. Since there are k^{n-1} ways to place the hats on the remaining players we see that each player will make k^{n-1} correct guesses over all possible placements of hats. Since there are n players and k^n ways to place the hats then on average we have $nk^{n-1}/k^n = n/k$ correct guesses. It follows that the adversary can find some placement of hats with at most $\lfloor n/k \rfloor$ correct guesses. \square

2 Restricting our vision in the game

In the original version of the game every player can see every other player. In an actual implementation of the game with a large group of people this might be difficult to achieve. So we now consider a variation where each player sees some subset of the other players.

To do this we introduce another layer to the game. We consider the “sight graph” where the vertices are the players and we have a directed edge from $a \rightarrow b$ if player a can see player b . As an example, in the original version of the game the graph was the complete graph on n vertices. For a given sight graph G we will let $H(G)$ denote the maximum number of correct guesses that the players can guarantee using an optimal strategy when there are 2 colors of hats.

In this section we will first consider the undirected case, i.e., the case in which every directed edge (u, v) is accompanied by the reverse edge (v, u) . For this case, an exact answer to $H(G)$ is known. In the directed case no exact answer for $H(G)$ is known but simple lower and upper bounds do exist. Finally, we consider the case when there are more than 2 colors of hats, for which little is known.

2.1 The undirected case

When we have an undirected graph the obvious strategy is to have players pair up as best as possible. Then in each pair we can implement the strategy in Example 1. This shows that we can guarantee at least $|M|$ correct guesses where M is a maximum matching of G . The next result shows that this cannot be improved upon.

Theorem 3. *Let G be an undirected graph with M a maximum matching of G . Then $H(G) = |M|$.*

Proof. It remains to show that $H(G) \leq |M|$. To do this we use the Tutte-Berge formula [2, 8], which says that there is a subset U of the vertices such that

$$|M| = \frac{|V| + |U| - o(G - U)}{2},$$

where $o(G - U)$ is the number of connected components of the induced subgraph $G - U$ which have an odd number of vertices. For $j = o(G - U)$ let W_1, \dots, W_j be the connected components of $G - U$ which have an odd number of vertices and Y the union of all the connected components of $G - U$ which have an even number of vertices.

Given any strategy we place hats as follows. First place hats on U arbitrarily. Having fixed the hat placement on U , for each player in W_i their guess is now completely determined by the hat placement on W_i (since the only other players that can be seen are U which has already been placed). Applying the arguments from Theorem 2 there is some placement of hats on each W_i with at most $(|W_i| - 1)/2$ correct guesses. Similarly we can place hats on Y so that there are at most $|Y|/2$ correct guesses. Therefore the total number of correct guesses is bounded above by

$$|U| + \frac{|Y|}{2} + \frac{|W_1| - 1}{2} + \dots + \frac{|W_j| - 1}{2} = \frac{|V| + |U| - j}{2} = |M|. \quad \square$$

2.2 The directed case

For the directed case there is no obvious strategy to adopt, and no sharp bound for $H(G)$ is known. However there exist simple upper and lower bounds as shown in the following.

Lemma 4. *Given a directed graph G let $c(G)$ denote the maximal number of vertex disjoint cycles in G , and $F(G)$ denote the minimum number of vertices whose removal from G makes the graph acyclic. Then $c(G) \leq H(G) \leq F(G)$.*

Proof. The lower bound follows by noting that for every cycle we can guarantee one correct guess. For example, if we have a cycle $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_k \rightarrow a_1$ then by having players a_1, \dots, a_{k-1} guess the opposite color of the next player and a_k guess the color of the hat a_1 has, we guarantee at least one correct guess.

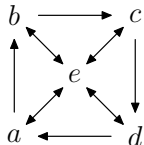
For the upper bound we note we can arrange the vertices in order so that the removal of $v_1, \dots, v_{F(G)}$ leaves the graph acyclic and the remaining vertices $v_{F(G)+1}, \dots, v_n$ are such that if $i > F(G)$ and there is an edge from v_i to v_j then $j < i$. In other words for the last $n - F(G)$ vertices, all outgoing edges point to the left. We place hats on the first $F(G)$ players arbitrarily and then we can place hats on players $F(G) + 1$ to n in turn, choosing each of the last $n - F(G)$ hat colors so as to force the corresponding player to guess incorrectly, given the colors of the preceding players. \square

By a theorem of Reed et al. [4], formerly known as Younger's Conjecture (namely, for every integer $k \geq 0$ there exists an integer $t \geq 0$ such that every digraph G has k vertex disjoint directed cycles, or G can be made acyclic by deleting at most t vertices), this implies a criterion for determining whether a family of directed graphs has unbounded "hat number."

Corollary 5. Let \mathcal{G} be a set of finite directed graphs. The set $\{H(G) : G \in \mathcal{G}\}$ is unbounded if and only if the set $\{F(G) : G \in \mathcal{G}\}$ is unbounded.

Neither bound in Lemma 4 is sharp. For the upper bound, the undirected triangle has $F(G) = 2$ but we know from Theorem 2 that $H(G) = 1$. An example to show the lower bound is not sharp is a little more involved and is given below.

Example 6. Let G consist of a directed four cycle $a \rightarrow b \rightarrow c \rightarrow d \rightarrow a$ with a fifth node e joined to the other four by bi-directed edges. This graph has $c(G) = 1$ and $H(G) = 2$.



To describe a strategy we will let A, B, C, D, E denote the actual colors of hats placed on players a, b, c, d, e respectively, while g_a, g_b, g_c, g_d, g_e denote their guesses. We can describe their strategy in mod 2 arithmetic as follows.

$$g_a = B + E; \quad g_b = C + E; \quad g_c = D + E; \quad g_d = A + E + 1;$$

$$g_e = \begin{cases} 1 & \text{if } (A + B, B + C, C + D, A + D + 1) \text{ has Hamming weight } 1; \\ 0 & \text{if } (A + B, B + C, C + D, A + D + 1) \text{ has Hamming weight } 3. \end{cases}$$

What happens is that the players a, b, c, d will make either 1 or 3 correct guesses depending on what e is wearing. So e guesses as though his/her hat would force 1 correct guess among the other four players. Thus, either e guesses wrong and there are 3 correct guesses among a, b, c, d ; or e guesses correctly and there is 1 correct guess among a, b, c, d for a total of 2 correct guesses. \square

Question. For an undirected graph G how do we calculate $H(G)$? The obvious algorithm for deciding if $H(G) \geq h$ requires nondeterministic exponential time: the algorithm nondeterministically comes up with a guessing strategy for the players, and then spends exponential time verifying that this strategy produces at least h correct answers on every input. We do not know if there is a more efficient algorithm for deciding if $H(G) \geq h$.

We note that in answering this question for directed graphs it suffices to consider graphs G which are strongly connected. In particular, $H(G) = \sum_k H(G_k)$ where G_k are the strongly connected components of G . The proof of this is similar to the argument of the upper bound in Lemma 4. Namely, we can order the strongly connected components so that there is an edge from G_i to G_j only if $i > j$. Then the adversary acts optimally on each of the connected components in turn.

A related question concerns the complexity of optimal guessing strategies. Define a guessing strategy with sight graph G to be *optimal* if it achieves at least $H(G)$ correct answers on every input. We saw in the proof of Theorem 3 that when G is undirected, there is always an optimal guessing strategy in which each player's guess is computed by evaluating a linear function (over the field with two elements) whose inputs are the other players' hat colors together with the constant 1. For directed graphs this is not the case. The sight graph in Example 6 has $H(G) = 2$, but the

reader may verify by a simple case analysis that for every linear guessing strategy, there exists an input on which fewer than 2 players answer correctly.

Question. Is it true that for every directed graph G , there is an optimal guessing strategy in which every player's guess is computed by inserting the other players' hat colors into a Boolean circuit of size polynomial in $|G|$?

Note that an affirmative answer to this question would imply that the problem of deciding if $H(G) \geq h$ belongs to the complexity class Σ_2^P , providing a partial answer to the preceding question.

2.3 More than 2 colors of hats

Considerably less is known when there are more than 2 colors involved in the game. Let $H_k(G)$ denote the maximum number of correct guesses that the players can guarantee using an optimal strategy when there are k colors of hats. From the proof of Theorem 2, we know that $H_k(G) = 1$ when G is an undirected k -clique, and therefore $H_k(G) \geq \ell$ whenever G contains ℓ disjoint undirected k -cliques. However it is possible to avoid k -cliques altogether and still guarantee at least one correct guess, as shown below.

Theorem 7. *For every number k , there exists a bipartite graph G with $H_k(G) > 0$.*

Proof. Let G be a complete bipartite graph with $n = k - 1$ vertices on the left side and $m = k^{k^n}$ vertices on the right side. Let C denote the set of all k -colorings of the left side of G . Note that $|C| = k^n$ and $m = k^{|C|}$, hence m is equal to the number of mappings from C to $\{1, 2, \dots, k\}$. Pick a one-to-one correspondence between the vertices on the right side of G and the mappings from C to $\{1, 2, \dots, k\}$, and let each vertex on the right side of G guess its color using the corresponding mapping.

We will need the following claim.

Claim. Let c_R denote a fixed coloring of the right side of G , and let C' denote the set of all colorings c_L of the left side of G such that the combined coloring (c_L, c_R) causes every vertex on the right side to guess its color incorrectly. Then $|C'| < k$.

Now it's time to define the guessing strategies used by the vertices on the left side of G . Given the coloring of the right side, the set C' defined in the lemma above has at most $n = k - 1$ elements. So let c_1, c_2, \dots, c_n be a list of colorings which contains every element of C' . For $i = 1, 2, \dots, n$, vertex i on the left guesses that its color is $c_i(i)$. This guessing strategy (combined with the guessing strategy for the vertices on the right side as defined above) guarantees at least one correct answer. This is because the above claim guarantees that at least one vertex on the right side guesses correctly unless the coloring of the left side belongs to C' . But if the coloring of the left side belongs to C' , then it is equal to c_i for some i in $1, 2, \dots, n$, in which case vertex i on the left guesses its color correctly.

It remains to prove the claim. The proof follows from noting that if C' contains k distinct elements c_1, c_2, \dots, c_k , then there exists a function f from C to $\{1, 2, \dots, k\}$ which assumes k distinct values on the set $\{c_1, \dots, c_k\}$. Let v denote the vertex on the right side of G corresponding

to f . Since the set $\{f(c_1), f(c_2), \dots, f(c_k)\}$ contains all k colors, we must have $f(c_i) = c_R(v)$ for some i in $1, 2, \dots, k$. Thus, the combined coloring (c_i, c_R) causes vertex v to guess its color correctly, contradicting our assumption that c_i belongs to C' , ending the proof. \square

Question. Is there a bipartite graph G satisfying $H_k(G) > 0$ whose size is polynomial in k ? What if instead of bipartite we consider k -clique-free graphs?

Question. Call an undirected sight graph G “edge-critical for the hats game with k colors” if G has the property that there exists a guessing strategy which guarantees at least one correct answer for the hats game with k colors, but no proper subgraph of G has this property. For $k = 2$, the only edge-critical graph is a 2-clique. For $k > 2$, there are at least two (undirected) edge-critical graphs, namely a k -clique and a subgraph of the complete bipartite $(k - 1)$ -by- (k^{k-1}) graph. For $k > 2$, are there infinitely many graphs which are edge-critical for the hats game with k colors?

We close this section by proving that $H_k(G) = 0$ whenever $k > 2$ and G is an undirected tree. This fact is a consequence of the following more general lemma.

Lemma 8. *Suppose we are given: an undirected tree T ; a guessing strategy Γ for the hat k -coloring problem on T ; a node v in T ; and a pair of colors c_1, c_2 . Then there exists a k -coloring ($k \geq 3$) of T such that every node guesses its color incorrectly; and the color of node v is either c_1 or c_2 .*

Proof. The proof is by induction on the size of T . When $|V(T)| = 1$ the result is trivial. Otherwise deleting v from T partitions the remaining vertices into a collection of disjoint subtrees T_1, T_2, \dots, T_j . For $i = 1, 2, \dots, j$, let $r(T_i)$ denote the unique neighbor of v in T_i . Let $\Gamma_1(T_i)$ (respectively $\Gamma_2(T_i)$) denote the guessing strategy applied in T_i when the color of v is c_1 (respectively c_2). Note that $\Gamma_1(T_i)$ and $\Gamma_2(T_i)$ differ only in the function which $r(T_i)$ uses to guess its color based on the colors of its neighbors in T_i . Let $B_1(T_i)$ denote the set of “bad colorings” for guessing strategy $\Gamma_1(T_i)$, i.e., the colorings which cause every node of T_i to guess its color incorrectly. Let $C_1(T_i)$ denote the set of colors assigned to $r(T_i)$ by colorings in $B_1(T_i)$. Define sets $B_2(T_i), C_2(T_i)$ similarly, but using the guessing strategy $\Gamma_2(T_i)$ in place of $\Gamma_1(T_i)$. The induction hypothesis implies that $C_1(T_i)$ and $C_2(T_i)$ each have at least $k - 1$ elements. (If not, then the complement of one of these sets, say $C_1(T_i)$, contains at least two colors, say c_3, c_4 . Applying the induction hypothesis with tree T_i , guessing strategy $\Gamma_1(T_i)$, node $r(T_i)$, and color pair c_3, c_4 would lead to an element of $B_1(T_i)$ in which the color of $r(T_i)$ is either c_3 or c_4 , contradicting the assumption that c_3, c_4 are both in the complement of $C_1(T_i)$.) Having established that $C_1(T_i)$ and $C_2(T_i)$ each have at least $k - 1$ elements, it follows (from the fact that $k > 2$) that the intersection of $C_1(T_i)$ and $C_2(T_i)$ is non-empty. Choose a color c_i from the intersection of these two sets and assign it to $r(T_i)$. Do this for each i in $\{1, 2, \dots, j\}$. Having assigned a color to each neighbor of v , the guess of node v is now determined. At least one of the colors c_1, c_2 , differs from this guess, so we may assign this color to node v and thereby ensure that it guesses incorrectly. Assume without loss of generality that color c_1 is assigned to v . For each subtree T_i , the set $B_1(T_i)$ contains a coloring which satisfies:

- the color of $r(T_i)$ is c_i ;
- every node guesses its color incorrectly using guessing strategy $\Gamma_1(T_i)$.

We choose one such coloring and use it to assign colors to the nodes of T_i . Doing this for every i in $\{1, 2, \dots, j\}$ yields a coloring of T which satisfies the two properties in the statement of the lemma. \square

Corollary 9. *If G is an undirected tree and $k > 2$ then $H_k(G) = 0$.*

2.4 Generalized guessing graphs

In this section we consider a variation in which players are not necessarily trying to guess their own hat color. Instead there is a set P (“players”) and a set H (“hats”), and two directed graphs G_v (“visibility graph”) and G_g (“guessing graph”). Both graphs have a vertex set which is the union of P and H . Every edge of G_v has its tail in P and its head in H ; we think of edge (u, v) as indicating that person u can see the color of hat v . Every edge of G_g has its tail in H and its head in P ; we think of edge (v, u) as indicating that person u must guess the color of hat v . (Note that the orientation of these edges is from hats to people, the reverse of the orientation convention used in G_v . This orientation convention is adopted because it will be convenient later on.) The hat problem considered in earlier sections corresponds to the case when there is a bijection $\phi : H \rightarrow P$ and the edge set of G_g is $\{(v, \phi(v)) : v \in H\}$.

A “guessing strategy” is a set of functions, one for each edge in G_g . Each such function maps the set of k -colorings of H to the set of colors, and has the property that the value of the function corresponding to edge $e = (v, u)$ depends only on the colors of the elements of H which are adjacent to u in G_v . Given a k -coloring of H and a guessing strategy, we say that edge $e = (v, u)$ of G_g gives a correct answer if its function evaluates to the color which was assigned to v . We define $H_k(G_v, G_g)$ to be the maximum number of correct guesses that the players can guarantee using an optimal strategy when there are k colors of hats.

Theorem 10. *When $k = 2$, $H_k(G_v, G_g) > 0$ if and only if at least one of the following properties holds:*

- a. *There is a vertex of G_g whose outdegree is greater than 1.*
- b. *There is a directed cycle in the union of G_v and G_g .*

Proof. Identify the set of colors with the set $\{0, 1\}$. If property (a) is satisfied and G_g contains edges (v, u) and (v, u') for some v in H and u, u' in P , then assign the constant function 0 to edge (v, u) and the constant function 1 to edge (v, u') . Clearly, on every input, at least one of these edges gives a correct answer.

If property (b) is satisfied, let the vertices of the cycle be

$$v_1 \rightarrow u_1 \rightarrow v_2 \rightarrow u_2 \rightarrow \dots \rightarrow v_n \rightarrow u_n$$

and adopt the following guessing strategy. For $i = 1, 2, \dots, n - 1$, player u_i guesses that the color of v_i is different from the color of v_{i+1} . Player u_n guesses that the color of v_n is the same as the color of v_1 . Observe that this is a legal guessing strategy since each of the edges $(u_1, v_2), (u_2, v_3), \dots, (u_n, v_1)$

belongs to G_v . Also, for any input on which none of u_1, u_2, \dots, u_{n-1} guess correctly, it must be the case that v_1, v_2, \dots, v_n are all assigned the same color. But then (u_n, v_1) guesses correctly.

Finally, suppose neither (a) nor (b) is satisfied; we must prove that for every guessing strategy there exists an input on which every edge guesses incorrectly. We will only sketch this part of the proof. Let G be the union of G_v and G_g , and let G' be the directed graph obtained from G by contracting the edges of G_g . If G' contains a directed cycle, then G must also contain a directed cycle. (In fact, our assumption that property (a) is not satisfied implies that every edge of G' corresponds to a 2-hop path between two elements of P in G .) Since we are assuming G contains no directed cycles, it follows that G' is acyclic. An elementary induction argument, using a topological sort of G' , produces a coloring of H which causes every edge to guess incorrectly. \square

Question. Above we characterize visibility and guessing graphs for which we can guarantee at least one correct answer. It would be nice if we can determine exactly how much more information in the guessing graph we can obtain by adding a particular edge to the visibility graph. More generally, given m , G_v and G_g determine the smallest value j such that there exists a graph G'_v consisting of G_v with j additional edges such that the hat number $H_2(G'_v, G_g)$ is at least m ?

The above question can be loosely considered in the same line as the Aanderaa-Rosenberg Conjecture [7] which asks the minimum number of edges of a graph that should be revealed in order to determine whether the graph has a given monotone property P or not (see also [5]).

3 Using hypercubes to approach the game

One of the interesting connections between hat guessing games and applications lies in interpreting the game in terms of various structure restrictions on hypercubes (the restriction depending on the rule of the particular game). In this section we will consider several questions for which we can use hypercubes to give an answer. One drawback to using hypercubes is that the number of vertices is exponential in the number of players and so many of the constructions are not polynomial in n . Nevertheless insight to the game can be achieved by considering hypercubes (see for example Proposition 13).

Recall that the n -cube has as vertices all 2^n binary words of length n . This has a natural connection with the possible placements of hats. The edges of the n -cube join two vertices which differ in one letter. As an example, in the 4-cube there is an edge between 1011 and 1010; we can represent this in shorthand as 101* where the * indicates an indeterminate bit which is either 0 or 1. The edges of the n -cube represent the decisions which must be made in forming the strategy. So 101* indicates that the fourth player (the *) sees 1, 0, and 1 on the first, second, and third players respectively. In this situation they must either guess 0 or 1. To indicate his/her guess we will “orient” the edge in the direction of the guess. So for instance if the player guesses 0 in this case then we will have 1011 \rightarrow 1010.

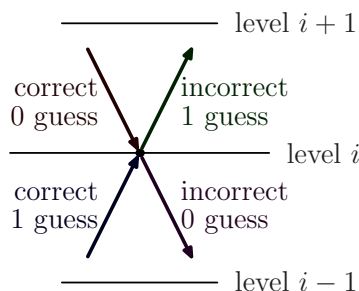
The original version of the game reduces to finding an orientation on the edges of the n -cube to maximize the minimum in-degree.

3.1 Balanced strategies

We now return to the original game. In Theorem 2 we gave one example of how to construct a strategy to guarantee $\lfloor n/k \rfloor$ guesses. This strategy is far from unique, and may not have some desired property. For example, while that strategy is easy to implement the correct guesses are not reflective of the actual hats that are placed on the players. For 2 colors of hats we will show how to construct different strategies and in particular how to construct a balanced strategy.

Lemma 11. *If there are n players and 2 different hat colors, then there exists a strategy which is balanced. That is, if there are b blue hats and r red hats placed on the players ($r + b = n$) then at least $\lfloor b/2 \rfloor$ of the people wearing blue guess correctly and $\lfloor r/2 \rfloor$ of the people wearing red guess correctly.*

We first approach the problem by using hypercubes. To construct a balanced strategy we will group the vertices of the hypercube in i levels, where a vertex is at level i if the word indexing the vertex has Hamming weight i . The up-degree (respectively down-degree) at a vertex in level i will be the number of edges between that vertex and vertices in level $i + 1$ (respectively $i - 1$). If we consider how directing the edges corresponds to guesses we have the following picture.



We now see that the balanced strategy in Lemma 11 would correspond to an orientation on the edges of the hypercube so that at each node the number of directed edges from level $i + 1$ to that node is $\lfloor \text{up-degree}/2 \rfloor$ while the number of directed edges from level $i - 1$ to that node is $\lfloor \text{down-degree}/2 \rfloor$.

Construction of Lemma 11. For n even we start with any edge and orient it arbitrarily and then continue to lengthen the directed path to be as long as possible by continually directing an undirected edge which is incident with the current terminal vertex. The only restriction is that if an edge is between level i and level $i + 1$ then if possible the next edge will also be between level i and level $i + 1$. When the path can no longer be extended, if we have not oriented all the edges, then we pick an unoriented edge and repeat the process.

When n is odd a similar construction works, the only caveat being that we must be careful in selecting our initial edges. Now an initial edge cannot be chosen arbitrarily but must be directed up from a vertex of odd up-degree or down from a vertex of odd down-degree.

It is easy to see that the strategy we construct is balanced, since at each vertex we pair directed in- and out-edges, in such a way that every edge coming in from below (resp. above) is paired, if possible, with an edge going to below (resp. above). \square

Using a different technique based on network flow, it is possible to construct balanced strategies for every k ; see [1] for details.

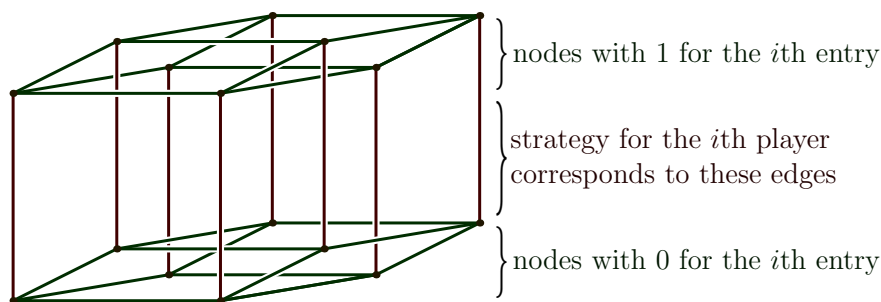
Theorem 12 ([1]). *If there are n players and k different hat colors, then there exists a strategy which is balanced. That is, if a_i of the players are wearing hats of color i ($1 \leq i \leq k$) then at least $\lfloor a_i/k \rfloor$ of the people wearing color i guess correctly for each value of i .*

3.2 Optimal strategies are unbiased

If one constructs many optimal strategies for the 2-color game when n is even, one starts to see a pattern emerge. Namely, each player is as likely to guess one hat color as they are to guess the other. We give a short proof that uses hypercubes.

Proposition 13. *Suppose the set of hat colors is $\{0,1\}$ and there are n players playing an optimal strategy, where n is even. For any fixed player i , looking over all possible hat placements, we have that the number of times that player i guesses 0 is the same as the number of times that player i guesses 1.*

Proof. When n is even an optimal strategy corresponds to an orientation on the edges of the n -cube with the in-degree equal to the out-degree at each vertex. In particular, the strategy corresponds to some Eulerian walk on the n -cube. We now redraw the n -cube as follows.



Then note that the number of edges in the center that point up is the number of times the i th player guesses 1 and the number of edges that point down is the number of times that the i th player guesses 0. Since we have an Eulerian walk the number of up-edges equals the number of down-edges. \square

Proposition 13 can be generalized to games with more than 2 colors.

Proposition 14. *Suppose that n players are playing an optimal strategy of the k -color game, where k is a divisor of n . If the players' hat colors are drawn independently from the uniform distribution on $\{1, 2, \dots, k\}$ then for each player i and each hat color c ,*

$$\Pr(i \text{ guesses } c) = 1/k.$$

Equivalently, in an optimal strategy each player guesses each hat color an equal number of times.

Proof. Let X denote the random variable which counts the number of correct answers provided by the players. Our assumption that the players use an optimal guessing strategy means that $X \geq n/k$ at every point of the sample space. Now let $\mathcal{E}(i, c)$ denote the event that player i is assigned hat color c . We have

$$\mathbb{E}[X \mid \mathcal{E}(i, c)] = \sum_{j=1}^n \Pr(j \text{ guesses correctly} \mid \mathcal{E}(i, c)) \quad (1)$$

$$= \frac{n-1}{k} + \Pr(i \text{ guesses } c \mid \mathcal{E}(i, c)) \quad (2)$$

$$= \frac{n-1}{k} + \Pr(i \text{ guesses } c). \quad (3)$$

Here (1) follows from linearity of expectation, and (2) follows from the fact that, conditional on $\mathcal{E}(i, c)$, every player except i has a hat color which is uniformly distributed and is independent of its own guess. Finally, (3) follows from the fact that player i 's guess is independent of its own hat color.

Recalling now that $X \geq n/k$ at every point of the sample space, we see that

$$\mathbb{E}[X \mid \mathcal{E}(i, s)] \geq n/k,$$

and according to (3) this implies $\Pr(i \text{ guesses } c) \geq 1/k$. Since this inequality applies to every hat color c , it must be the case that $\Pr(i \text{ guesses } c) = 1/k$ for every color c . \square

3.3 The limited hats game

We now consider another variation on the original hats game. The setup is as before, but now the adversary has a limited supply of hats to choose from. We will let $H(n; a_1, a_2, \dots, a_k)$ denote the maximum number of correct guesses that we can guarantee when there are n players and a_1 hats of the first color, a_2 hats of the second color, and so on up through a_k hats of the k th color. We need $a_1 + a_2 + \dots + a_k \geq n$ (to ensure that we have enough hats for the players) and without loss of generality we can assume that $0 < a_i \leq n$ for all i .

Example 15. Suppose that there are 3 players and the adversary has 2 blue hats and 2 red hats. The players can choose to ignore this information and use the same strategy as in Theorem 2 guaranteeing 1 correct guess. However if they modify their strategy then they can guarantee 2 correct guesses. If the players are a, b, c then such a strategy would be for a to guess the opposite of what b is wearing, b to guess the opposite of what c is wearing, and c to guess the opposite of what a is wearing. So $H(3; 2, 2) = 2$. (More generally, it was shown in [3] that $H(4k-1; 2k, 2k) = 3k-1$.) \square

Theorem 16. *We have the following properties:*

$$(i) \ H(n; \underbrace{n, n, \dots, n}_{k \text{ times}}) = \lfloor n/k \rfloor.$$

$$(ii) \ \text{If } a_1 + a_2 + \dots + a_k = n \text{ then } H(n; a_1, a_2, \dots, a_k) = n.$$

(iii) If m is even or k is odd (or both), then $H(mk - 1; \underbrace{m, \dots, m}_{k \text{ times}}) = \frac{mk + m - 2}{2}$.

(iv) $H(n; a_1, a_2, \dots, a_k) = H(n; a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(k)})$ for any permutation σ .

(v) If $b_i \leq a_i$ for all $i = 1, 2, \dots, k$ then $H(n; a_1, a_2, \dots, a_k) \leq H(n; b_1, b_2, \dots, b_k)$.

(vi) $H(n; a_1, a_2, \dots, a_k) \leq \left\lfloor \frac{\sum_{\substack{b_i \leq a_i, 1 \leq i \leq k \\ b_1 + \dots + b_k = n-1}} n \binom{n-1}{b_1, \dots, b_k}}{\sum_{\substack{b_i \leq a_i, 1 \leq i \leq k \\ b_1 + \dots + b_k = n}} \binom{n}{b_1, \dots, b_k}} \right\rfloor$.

Proof. Item (i) is Theorem 2. Item (ii) is obvious because the strategy is to have each player guess the hat they do not see. Item (iv) says we can permute the hat colors. Item (v) follows by noting that the optimal strategy for the $H(n; a_1, a_2, \dots, a_k)$ game is also a (not necessarily optimal) strategy for the $H(n; b_1, b_2, \dots, b_k)$ game.

To prove item (vi) we first give a hyper-hypercube interpretation of the game. The k^n vertices are words of length n from the alphabet $\{0, \dots, k-1\}$ and correspond to the k^n possible placements of hats. The tuples (i.e., edges) represent the decisions which must be made in deciding a strategy. So for example if $n = 5$ and $k = 3$ then one tuple would be $210*1 = \{21001, 21011, 21021\}$ representing the situation when the fourth player (the $*$) sees 2, 1, 0, and 1 on the first, second, third, and fifth players respectively. A strategy corresponds to marking one vertex on each tuple, the marking indicating the guess that the player will make. Note each marking is one correct guess.

We now use an averaging argument similar to that given in Theorem 2.

$$\begin{aligned} H(n; a_1, a_2, \dots, a_k) &\leq \left\lfloor \frac{\# \text{ of correct guesses}}{\# \text{ of possible hat placements}} \right\rfloor \\ &= \left\lfloor \frac{\# \text{ of tuples available for marking}}{\# \text{ of vertices to be marked}} \right\rfloor \\ &= \left\lfloor \frac{\sum_{\substack{b_i \leq a_i, 1 \leq i \leq k \\ b_1 + \dots + b_k = n-1}} n \binom{n-1}{b_1, \dots, b_k}}{\sum_{\substack{b_i \leq a_i, 1 \leq i \leq k \\ b_1 + \dots + b_k = n}} \binom{n}{b_1, \dots, b_k}} \right\rfloor \end{aligned}$$

The numerator is the n possible positions of the $*$ along with the allowable combinations of the remaining $n - 1$ entries. The denominator is the number of ways to place the n hats in allowable combinations.

For item (iii) we have that $H(mk - 1; m, \dots, m) \leq (mk + m - 2)/2$ from (vi). So it suffices to show that we can construct a strategy guaranteeing at least $(mk + m - 2)/2$ correct guesses. There are two types of tuples, those which involve only one markable vertex and those that involve two. The first kind is for players who see a full set of all but one type of hat and so automatically know their hat. The second kind is for players who see a full set of all but two types of hats and so have to make one of two choices.

Every vertex will be associated with $m - 1$ tuples of the first type (one for each hat of the deficient color in the placement), we mark these tuples and put them aside. We now construct a bipartite graph with the remaining edges and tuples as follows: The vertex set is $S \cup T$ where S

is the set of tuples we have not yet marked and T is the set of vertices to be marked, there is an edge between an element in S and an element in T if the corresponding vertex can be marked by the corresponding tuple.

Every element in S has degree 2 and every element in T has degree $mk - m$, which by assumption is even. We now split the elements in T by duplicating each element $(mk - m)/2$ times and then distributing the edges of the original element so that each resulting piece has degree 2. It is easy to now construct a perfect matching between S and T (for example start with any edge and going through a cycle alternatively include/not include the edges). This perfect matching gives a marking on the tuples so that each of the vertices is marked $(mk - m)/2$ times.

In total each vertex was marked $(m - 1) + (mk - m)/2 = (mk + m - 2)/2$ times giving our desired strategy. \square

Question. What is $H(n; a_1, a_2, \dots, a_k)$? Is the upper bound given in Theorem 16 tight? [Note: items (i), (ii) and (iii) in Theorem 16 are examples where the bound is tight.]

As a warmup to the above question, the interested reader might enjoy showing that $H(5; 4, 3) = 3$ (an upper bound of 3 immediately follows from Theorem 16 so it suffices to find a strategy guaranteeing at least 3 correct guesses).

4 Summary and open questions

In this paper we considered hat guessing games in which players wearing hats of various colors use deterministic strategies to guess the color of some hats (usually their own) with the goal of maximizing the number of correct answers in the worst case. In this section we summarize our main results, and we list the open questions which are scattered throughout this paper.

Focusing on hat games with a *sight graph* that specifies the set of hats visible to each player, we defined the *hat number* $H_k(G)$ to be the number of correct answers provided in the worst case by an optimal strategy for players guessing their own hat color, when the sight graph is G and there are k colors of hats. We proved that for two colors and undirected sight graphs, the hat number equals the cardinality of a maximum matching in the sight graph. For a directed graph G and two hat colors, we provided lower and upper bounds on the hat number; these bounds suffice to distinguish graph families with bounded hat number from those with unbounded hat number. For three or more colors, we proved that the hat number of a tree is zero and that there are bipartite graphs with nonzero hat number. When there are two hat colors and there is a *guessing graph* which specifies the set of hat colors which each player must guess, we provided necessary and sufficient conditions for the existence of a strategy which guarantees at least one correct answer.

Turning to questions about the distribution of guesses and of correct guesses, we introduced a hypercube interpretation of the game which permitted us to prove that when there are two colors of hats and players can see all hats except their own, there is a guessing strategy which guarantees that roughly half of the players wearing each type of hat guess correctly. (This result was also proved in [1], which contains a generalization to more than two colors.) We also proved that optimal strategies are unbiased, i.e. when the number of hat colors is a divisor of the number of players, each player guesses each hat color with equal probability when the colors are assigned

independently and uniformly at random. Finally, turning to a version in which the players are given an *a priori* upper bound on the number of hats of each color, we exhibited some bounds on the number of correct answers provided by the optimal strategy in the worst case.

In presenting these results, we also introduced many open questions inspired by them. Here we recapitulate the open questions presented earlier.

Complexity of computing hat numbers and optimal strategies: What is the computational complexity of determining $H_k(G)$, given k and G ? There is a polynomial-time algorithm when $k = 2$ and G is undirected (because a maximum matching can be computed in polynomial time), but for all other cases the best known algorithm requires nondeterministic exponential time. On the other hand, we do not know if the problem is NP-hard.

How much computational power is required to implement an optimal guessing strategy? For $k = 2$, can the optimal guessing strategy for a directed sight graph G always be implemented by players using Boolean circuits of size polynomial in the size of G ?

Graphs with positive hat numbers: Is there a bipartite graph G satisfying $H_k(G) > 0$ whose size is polynomial in k ? What if instead of bipartite we consider k -clique-free graphs? Are there infinitely many graphs G such that $H_k(G) > 0$ but $H_k(G') = 0$ for every proper subgraph $G' \subset G$?

Augmenting sight graphs to improve hat numbers: Given a positive number m and two graphs G_v, G_g (the sight graph and guessing graph of a hat guessing game), determine the smallest value j such that one can add j additional edges to G_v to obtain a graph G'_v satisfying $H_2(G'_v, G_g) \geq m$.

The limited hats game with unrestricted vision: Suppose players can see every hat color except their own, and must guess their own hat color. When there are k hat colors and at most a_i hats in color class i ($1 \leq i \leq k$), compute the maximum number of correct answers that can be guaranteed by a guessing strategy given this limitation on the placement of hats. Is the upper bound in part (vi) of Theorem 16 tight?

5 Acknowledgements

We thank Joe Buhler, Kevin Costello, Harvey Friedman, and Ron Graham for interesting and helpful discussions on this subject.

References

- [1] G. Agarwal, A. Fiat, A. V. Goldberg, J. D. Hartline, N. Immorlica, and M. Sudan. Derandomization of auctions. In *Proceedings of the 37th ACM Symposium on Theory of Computing (STOC)*, pages 619–625, 2005.
- [2] C. Berge. Sur le couplage maximum d'un graphe. *Comptes Rendues Hebdomadaires des Séances de l'Académie des Sciences [Paris]*, 247:258–259, 1958.

- [3] U. Feige. You can leave your hat on (if you guess its color). *Technical Report MCS04-03, Computer Science and Applied Mathematics, The Weizmann Institute of Science*, page 10 pp., 2004.
- [4] B. Reed, N. Robertson, P. Seymour, and R. Thomas. Packing directed circuits. *Combinatorica*, 16(4):535–554, 1996.
- [5] R. L. Rivest and J. Vuillemin. A generalization and proof of the anderaa-rosenberg conjecture. In *STOC '75: Proceedings of seventh annual ACM symposium on Theory of computing*, pages 6–11, New York, NY, USA, 1975. ACM Press.
- [6] S. Robinson. Why mathematicians now care about their hat color. *The New York Times*, page D5, April 10, 2001.
- [7] A. L. Rosenberg. On the time required to recognize properties of graphs: A problem. *SIGACT News*, 5, 1973.
- [8] W. T. Tutte. The factorization of linear graphs. *J. London Math. Society*, 22:107–111, 1947.
- [9] P. Winkler. Games people don't play. In *Puzzlers' Tribute*. A. K. Peters, 2001.

THE THREE-HAT PROBLEM

BRIAN BENSON AND YANG WANG

1. INTRODUCTION

Many classical puzzles involve hats. The general setting for these puzzles is a game in which several players are each given a hat to wear. Associated with each hat is either a color or a number. Every player can see the color or number of everyone else's hat but not his own. The players are then trying to figure out the colors or the numbers on their own hats. The Three-Hat Problem is one of such puzzles.

The Three-Hat Problem. Three players are each given a hat to wear. Written on each hat is a positive integer. Any player can see the other two numbers but not his own. It is known that one of the numbers is the sum of the other two. They take turns to either identify their numbers, or pass if they can't. The following process has taken place:

Player A: Pass.

Player B: Pass.

Player C: Pass.

Player A: My number is 50.

The question is: What are the other numbers?

There is also a more complex version of the above problem, in which the process has gone longer as follows:

Player A: Pass.

Player B: Pass.

Player C: Pass.

Player A: Pass.

Player B: Pass.

Player C: Pass.

Player A: Pass.

Player B: Pass.

Player C: My number is 60.

Again the question is: What are the other numbers?

The most general form of the Three-Hat Problem would have numbers $a, b, a + b$. In this general setting one may ask: (a) Will the players be able to determine their numbers, and (b) how will the process go if so.

As far as we know, both puzzles were proposed by Donald Aucamp in the *MIT Technology Review*, see [4, 5, 6]. Although by no means trivial, the first puzzle is readily within grasp of most enthusiasts who have some familiarity with these type of puzzles. The solution is Player B has 20 and Player C has 30. To see why these two numbers work. Player A on his first turn obviously doesn't know whether his number is 50 or 10. Similarly neither Player B nor Player C can immediately figure out their numbers. However, on his second turn Player A can reason: *If mine is a 10, then Player C would know his number is either 10 or 30. If it is 10 Player B would immediately know his number is 20. But he didn't know. So Player C should know his number is 30. Now since Player C didn't know, my number must be 50.* With this kind of reasoning we can also rule out all other combinations. So [50, 20, 30] is the only solution to the first puzzle. The second In a private communication Aucamp mentioned that he received no solution to the second puzzle from the readers [1]. As it turns out, our study shows that the second puzzle has eight solutions! They are [25, 35, 60], [35, 25, 60], [42, 18, 60], [18, 42, 60], [10, 50, 60], [50, 10, 60], [44, 16, 60], [16, 44, 60].

The Three-Hat Problem is among the more challenging hat puzzles. However, as we shall see, like the Three-Hat Problem many of these hat puzzles can be solved using the same principles and techniques. We list two classical hat puzzles here.

The Two-Hat Problem. Two players are each given to wear a hat with a positive integer written on it. Assume that the two numbers are consecutive integers. Each player can see the other's number but not his own. They take turns to either identify their numbers or pass if they cannot. Will they be able to identify their numbers, and if so what will the process be?

The Color-Hat Problem. Several players are each given either a red or a blue hat to wear. Each player can see all other hats but not his own. They are also told that there is at least one red hat. The game goes by rounds. In each round, every player will either identify the color of his hat or pass, but all players do so *simultaneously*. The game ends when one or more players have correctly identified their colors while no one makes a mistake. What will happen? This puzzle takes on many popular forms, one of which is the *Muddy Face Problem* analyzed in Tanaka and Tsujishita [8].

A very challenging variation of the Color-Hat Problem was due to Todd Ebert [2] and was reported in an article in the New York Times [7]. In this variation, the players are allowed to collaborate as a team and decide on a strategy before the game starts. However, the players have only one chance to identify their colors. They win if at least one player correctly name the color of his hat while no one is wrong. The question is: How well can they do? What is their optimal strategy? This problem has an interesting connection to coding theory.

In fact each of the hat puzzles mentioned here can have a similar *collusion version* that is phrased as a game of strategy. Suppose that we say the players win if at least one player makes a correct identification while no one else is wrong. Then each aforementioned hat puzzle can be viewed as a problem of finding the strategy for the players to win with the least number of go-arounds.

Although this paper is concerned with the Three-Hat Problem, a main additional objective is to show that these type of puzzles can be analyzed easily if we first treat them as games of strategies. Once optimal strategies are found we can often easily show that the non-collusion version and the collusion version for those games are equivalent, and therefore they will end in exactly the same fashion. One of the main advantages of presenting these puzzles as games of strategy is that we can avoid the so-called *super-rationality assumption* (see Hofstadter [3]), namely each player has unlimited mental capacity to process all informations available to them, including long chains of reasonings such as “I know player B knows player C knows I know player C knows ...” Such an assumption can be confusing even to mathematicians without venturing deeply into the realm of set theory and mathematical logic. The Three-Hat Problem is an excellent example to illustrate this point.

2. OPTIMAL STRATEGY FOR THE THREE-HAT PROBLEM

We now discuss a strategy for the collusion version of the Three-Hat Problem. We say a strategy is *viable* if it always leads to a win for the players. (So there is no guessing at any stage.) A viable strategy is *optimal* if it requires the least number of turns (go-arounds) to end the game successfully regardless what the numbers are on the three hats. Of course, not all viable strategies are optimal. In theory it is also possible that an optimal strategy does not exist, in which case a strategy may be the best for some configurations but no strategy is the best for all configurations. For the Three-Hat Problem there does exist an optimal strategy, which we give here. The optimality of the strategy is proved in the next section.

The optimal strategy we describe here is a reduction scheme involving a chain of vectors with positive integer entries. Throughout this paper we assume that the game begins with Player A, followed by Player B next and Player C last. This order remains in all subsequent rounds until the game ends. The numbers a, b, c for Players A, B and C respectively are represented by the vector $[a, b, c]$. Such a vector is called a *three-hat configuration*, or simply just a *configuration*.

Let \mathcal{H} denote the set of all triples $\mathbf{s} = [a, b, c]$ where a, b, c are positive integers such that the largest of which is the sum of the other two. \mathcal{H} represents the set of all possible configurations of the Three-Hat Problem. Define a map $\sigma : \mathcal{H} \rightarrow \mathcal{H}$ as follows: For $\mathbf{s} = [a, b, c] \in \mathcal{H}$, if two of the entries are identical then $\sigma(\mathbf{s}) = \mathbf{s}$; otherwise the largest entry is replaced by the difference of the other two entries. For example, $\sigma([3, 10, 7]) = [3, 4, 7]$, $\sigma([10, 1, 9]) = [8, 1, 9]$, and $\sigma([3, 3, 6]) = [3, 3, 6]$. We shall call $\mathbf{s} \in \mathcal{H}$ a *base configuration* if \mathbf{s} contains two identical entry, or equivalently $\sigma(\mathbf{s}) = \mathbf{s}$. Note that in the base configuration, the player with the largest number can immediately declare that his number is the sum of the other two numbers. (He may choose not to in order to obey his strategy.)

Our strategy for the Three-Hat Problem involves a chain of configurations for each player. For any $\mathbf{s} \in \mathcal{H}$ we obtain a sequence of configurations $\mathbf{s}, \sigma(\mathbf{s}), \dots, \sigma^n(\mathbf{s})$ where $n \geq 0$ is the smallest power such that $\sigma^n(\mathbf{s})$ is a base configuration. For example, for $\mathbf{s} = [3, 10, 7]$ the sequence is

$$[3, 10, 7], [3, 4, 7], [3, 4, 1], [3, 2, 1], [1, 2, 1].$$

We call the sequence in reverse order the *configuration chain* associated with \mathbf{s} . So in the above example $\mathbf{s} = [3, 10, 7]$ the associated configuration chain is

$$[1, 2, 1], [3, 2, 1], [3, 4, 1], [3, 4, 7], [3, 10, 7].$$

Given a configuration, we say that a player has the *cue* if his number is the sum of the other two. For example, for the configuration $[3, 10, 7]$ Player B has the cue.

Chain Reduction Strategy for the Three-Hat Problem. For the Three-Hat Problem with configuration $\mathbf{s} = [a, b, c]$, let $\mathbf{s}_A = [b + c, b, c]$, $\mathbf{s}_B = [a, a + c, c]$ and $\mathbf{s}_C = [a, b, a + b]$. These are the *working configurations* for Players A, B, and C respectively. Each player now writes down the configuration chain associated with his working configuration. It is important to note that the chains differ only at the end. The players with the two smaller numbers have longer chains by one configuration, which may differ for these two players. The rest of the chains are identical.

When the game begins, the players are assigned the first configuration in their respective configuration chain, and proceed with the following reduction scheme:

At each turn, a player looks at what remain on his configuration chain. If it contains only one configuration he declares his number to be the sum of the other two numbers. The game is over. Otherwise he will pass. Each player will now examine his assigned configuration (which is in fact the same for all the players before the game ends). If he sees that the player who has just passed has the cue for this configuration he will cross out the configuration from his chain and assign himself the next configuration in the chain. Otherwise he keeps his assigned configuration and his chain intact. The game continues until a player declares his number. ■

The following two examples will facilitate the understanding of the strategy.

Example 1. The numbers for Players A, B, C are 60, 36, 24, respectively. In this case the working configurations are $\mathbf{s}_A = [60, 36, 24]$, $\mathbf{s}_B = [60, 84, 24]$ and $\mathbf{s}_C = [60, 36, 96]$. The configuration chains are

$$\begin{aligned} \text{Player A : } & [12, 12, 24], [12, 36, 24], [60, 36, 24] \\ \text{Player B : } & [12, 12, 24], [12, 36, 24], [60, 36, 24], [60, 84, 24] \\ \text{Player C : } & [12, 12, 24], [12, 36, 24], [60, 36, 24], [60, 36, 96] \end{aligned}$$

As the start of the game, all players are assigned the configuration $[12, 12, 24]$. Player A will pass, as will Player B and Player C. But Player C has the cue. So after Player C has passed the configuration $[12, 12, 24]$ is crossed out by all players from their chain. The new configuration chains are

Player A : $[12, 36, 24], [60, 36, 24]$
 Player B : $[12, 36, 24], [60, 36, 24], [60, 84, 24]$
 Player C : $[12, 36, 24], [60, 36, 24], [60, 36, 96]$

All three players are now assigned the configuration $[12, 36, 24]$. Player A and Player B will pass again. But since Player B has the cue, after his pass all three players will cross out $[12, 36, 24]$ from their chain and assign themselves the next configuration, which is $[60, 36, 24]$ for everyone. The new configuration chains are

Player A : $[60, 36, 24]$
 Player B : $[60, 36, 24], [60, 84, 24]$
 Player C : $[60, 36, 24], [60, 36, 96]$

It is Player C's turn and he will pass. Now Player A has only one configuration left on his chain, namely $[60, 36, 24]$. So he declares his number to be the sum of the other two numbers, which is 60. The game ends with a win for the players. ■

Example 2. The numbers for Players A, B, C are 3, 10, 7, respectively. In this case the working configurations are $\mathbf{s}_A = [17, 10, 7]$, $\mathbf{s}_B = [3, 10, 7]$ and $\mathbf{s}_C = [3, 10, 13]$. The following shows the configuration chains and the action at each turn. Players with the cue are denoted by a *.

Player A:	Pass	$[1, 2, 1], [3, 2, 1], [3, 4, 1], [3, 4, 7], [3, 10, 7], [17, 10, 7]$
Player B*:	Pass	$[1, 2, 1], [3, 2, 1], [3, 4, 1], [3, 4, 7], [3, 10, 7]$
Player C:	Pass	$[3, 2, 1], [3, 4, 1], [3, 4, 7], [3, 10, 7], [3, 10, 13]$
Player A*:	Pass	$[3, 2, 1], [3, 4, 1], [3, 4, 7], [3, 10, 7], [17, 10, 7]$
Player B*:	Pass	$[3, 4, 1], [3, 4, 7], [3, 10, 7]$
Player C*:	Pass	$[3, 4, 7], [3, 10, 7], [3, 10, 13]$
Player A:	Pass	$[3, 10, 7], [17, 10, 7]$
Player B*:	<i>I have 10</i>	$[3, 10, 7]$.

The game ends successfully for the players. ■

Using this strategy, the player with the sum of the other two numbers will always be the one to declare his number correctly to end the game. This is quite easily shown. Since his chain is a subchain of the other two players, and by the time his chain is down to only one configuration the other players still have two. Moreover, since he holds the cue at that stage

the other players cannot reduce the chain further without waiting for him to act. But when he does act he will declare his number. So he is always the first to identify his number.

3. OPTIMALITY OF THE CHAIN REDUCTION STRATEGY

We will now prove that the above strategy is optimal for the Three-Hat Problem in the sense that no other viable strategy will be able to end the game with fewer turns for all configurations. Before proceeding further we first notice that because $\gcd(a, b) = \gcd(a, c) = \gcd(b, c)$ the players can always divide out the numbers by the greatest common divisor of the two numbers they see. So we may without loss of generality assume that all numbers in the Three-Hat game are pairwise coprime. In the coprime case the only base configurations are $[1, 1, 2]$, $[1, 2, 1]$ and $[2, 1, 1]$.

Proposition 1. *No matter what viable strategy the players use for the Three-Hat Problem, the player whose number is the sum of the other two is always the first player to declare his number.*

Proof. Assume that in the Three-Hat Game a player declared his number on the very first turn of the game. It is easy to see that this can happen only if we have a base configuration and this player has the sum of the other two numbers. No other cases allow the game to end on the very first turn without guessing. For instance, even in the base configuration $[1, 2, 1]$ Player A cannot declare his number on his first turn without guessing, for he can have both 1 or 3.

If the proposition is false then we have a game with configuration $[a, b, c]$ that ends on the n -th turn, $n > 1$, by a player who does not have the sum of the two numbers. Without loss of generality we assume that Player C declares his number to end the game, and he does not have the sum. So $c = |a - b|$. But if so Player C must have concluded on the n -th turn that his number is not $c = a + b$. This is equivalent in saying that had his number been $c = a + b$ the game would have ended earlier, with another player declaring his number. Therefore the strategy the players use allows them to end the three-hat configuration $[a, b, a + b]$ in $k < n$ turns by a player other than Player C. This player does not have the sum of the other two numbers.

We can repeat this reasoning. In the end, we deduce that using their strategy the players can end a non-base configuration game in one turn by a player whose number is not the sum of the other two numbers. This is a contradiction. \blacksquare

Theorem 2. *The Chain Reduction Strategy is the optimal strategy for the Three-Hat Problem.*

Proof. For the Three-Hat Problem with the configuration $[a, b, c]$ let $r([a, b, c])$ denote the number of turns needed to end the game using the Chain Reduction Strategy. We prove that one cannot end the game in fewer turns using any other strategy.

Assume that the players are using another viable strategy such that the game ends in $f([a, b, c])$ turns. Our objective is to show $f([a, b, c]) \geq r([a, b, c])$. Without loss of generality we assume that a, b, c are pairwise coprime. We will prove the optimality of the Chain Reduction Strategy by induction on $\max(a, b, c)$.

For $\max(a, b, c) = 2$ we have the base case. It is clear that the Chain Reduction Strategy is optimal, $f([a, b, c]) \geq r([a, b, c])$. Now assume that $f([a, b, c]) \geq r([a, b, c])$ whenever $\max(a, b, c) < M$. We now prove that $f([a, b, c]) \geq r([a, b, c])$ if $\max(a, b, c) = M$.

We shall examine the case $a = b + c$ and $b > c$, so $a = M$. The other cases are proved in virtually identical fashion so we shall omit them. Note that by Proposition 1 the game will end with Player A declaring his number regardless of the strategy. With this in mind we need only to examine what happens before Player A declares his number. Clearly from his perspective Player A knows he has either $a = b + c$ or $a = b - c$. He is not able to declare his number until he rules out $a = b - c$, regardless of the strategy the players are using. Now since all strategies end with the player with the sum declaring his number, Player A knows that if his number is $a = b - c$ Player B will declare his number first on the n -th turn, where $n = f([b - c, b, c])$. But by the n -th turn Player B will pass because he does not have the sum, and after it the earliest Player A can declare his number is after Player C's pass. Thus

$$f([a, b, c]) \geq 2 + f([b - c, b, c]).$$

Note that here we do not get equality in general because we do not assume the strategy is optimal. By the induction hypothesis, since $\max(b - c, b, c) = b < a = M$ we have $f([b - c, b, c]) \geq r([b - c, b, c])$, and hence $f([a, b, c]) \geq 2 + r([b - c, b, c])$. We argue that

$r([a, b, c]) = 2 + r([b - c, b, c])$. This can be seen easily if we compare the configuration chains for $[b - c, b, c]$ and those for $[a, b, c]$. For all three players the former is a sub-chain of the latter with one less configuration. On the $r([b - c, b, c])$ -th turn Player B will pass, and he has the cue. So $[b - c, b, c]$ is crossed out from everyone's chain, leaving Player A with only one configuration on his chain, namely $[a, b, c]$. After Player C passes Player A is able to declare his number as $a = b + c$ using the Chain Reduction Strategy. Thus $f([a, b, c]) \geq 2 + r([b - c, b, c]) = r([a, b, c])$. This proves the optimality of the Chain Reduction Strategy. ■

One may wonder whether there are indeed non-optimal viable strategies for the Three-Hat Problem. One such strategy is the following: Players will note the larger of the two numbers they see, call these n_A , n_B , and n_C respectively. Unless another player has already declared his number, Player A will pass until his n_A -th turn, when he will declare his number to be the sum of the two other numbers. Players B and C do likewise. This is clearly a viable strategy but by no means an optimal one.

4. EQUIVALENCE OF COLLUSION AND NO-COLLUSION VERSIONS

We now argue that under the super-rationality assumption the no-collusion version of the Three-Hat Problem will end exactly the same way as if the players are colluding using the Chain Reduction Strategy. Specifically, we assert that if there exists an optimal strategy then a super-rational player is able to obtain this result. Clearly, from this perspective, if an optimal strategy exists then the players need not collude. The super-rationality assumption suffices to guarantee that all players will be able to find it and use it with the knowledge that other players will do likewise. Collusion is helpful only when there exists no single optimal strategy. This is the case when for any one strategy there is another strategy that is better for some configurations. If so the players need to collude to decide on one strategy. Note that two strategies for the Three-Hat Problem are considered to be the same if they lead to exactly the same solution for all configurations. In this sense the Chain Reduction Strategy is clearly the unique optimal strategy. By the above argument we have

Theorem 3. *The no-collusion Three-Hat Problem is equivalent to the collusion Three-Hat Problem using the Chain Reduction Strategy.*

By establishing the equivalence of collusion and no-collusion versions we can also solve the other two hat problems easily. For the Two-Hat Problem, the no-collusion version is equivalent to players using the following strategy: Each player will pass until on his n -th turn, when he will declare his number to be $n + 1$, where n is the number written on the other player's hat. The game ends when one player declares his number. For the Color-Hat Problem, the no-collusion version is equivalent to this strategy: Players will each note how many red hats he sees. Say a player sees n red hats. He will then pass in the first n rounds, but declares his hat to be red on the $(n + 1)$ -th round. The game ends when some players declare their numbers. These strategies are easily shown to be optimal by similar arguments for the Three-Hat Problem.

Acknowledgement. The authors would like to thank Ian Fredenburg and Don Aucamp for very helpful discussions. This work was part of the NSF sponsored REU project at Georgia Institute of Technology in the summer of 2006 for the first author. During the completion of this project the second author was serving as a program director at the Division of Mathematical Sciences of the National Science Foundation. The views expressed in this article are those of the authors, and they do not necessarily represent the views of NSF.

REFERENCES

- [1] Donald Aucamp, Private correspondence.
- [2] T. Ebert, *Applications of recursive operators to randomness and complexity*, Ph.D. Thesis, University of California at Santa Barbara, 1998.
- [3] Douglas R. Hofstadter, *Metamagical Themas: Questing for the Essence of Mind and Pattern*, Chapter 30: Dilemmas for Superrational Thinkers, Leading Up to a Luring Lottery, (1985) 739-755, Basic Books, Inc., New York.
- [4] Puzzle Corner, *Technology Review* (2003), October.
- [5] Puzzle Corner, *Technology Review* (2004), March, 31-32.
- [6] Puzzle Corner, *Technology Review* (2006), November - December.
- [7] Sara Robinson, Why Mathematicians Now Care About Their Hat Color, *The New York Times* April 10, 2001, Section F, Column 2, Science Desk, 5.
- [8] Shunichi Tanaka and Toru Tsujishita, Hypersets and dynamics of knowledge, *Hokkaido Mathematical Journal* **24** (1995), 215-230.

P. O. BOX 10000, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GA 30332, USA

E-mail address: `gth858n@mail.gatech.edu`

SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GEORGIA 30332, USA.

E-mail address: `wang@math.gatech.edu`

ТРИ КЛАССА ТРЕУГОЛЬНИКОВ

А.Заславский, О.Заславский, Ф.Ивлев, П.Кожевников, Д.Креков

*Сочинились стихи бредовые
Без какой-либо путной мысли,
Словно ведра воды пудовые
Я принес вам на коромысле.
А.Великий*

1 Определения и вводные задачи

Как известно, вокруг любого треугольника можно описать окружность и в любой треугольник можно вписать окружность. Кроме того, у любого треугольника существуют три внеписанные окружности, каждая из которых касается одной из сторон треугольника и продолжений двух других сторон. Для треугольника ABC обозначаем:

Ω — описанная окружность, O, R — ее центр и радиус;

γ — вписанная окружность, I, r — ее центр и радиус;

$\gamma_a, \gamma_b, \gamma_c$ — внеписанные окружности, I_a, I_b, I_c — их центры, r_a, r_b, r_c — их радиусы.

Основным объектом нашего изучения будут три специальных класса треугольников.

Определение А. *А-треугольником* будем называть треугольник, в котором $OI \parallel BC$.

Определение В. *В-треугольником* будем называть треугольник, в котором окружности γ_b и Ω перпендикулярны.

Определение С. *С-треугольником* будем называть треугольник, удовлетворяющий условию $R = r_c$.

В задачах, помеченных буквой A, B, C , предполагается, что дан соответственно A, B, C -треугольник (иначе треугольник ABC предполагается произвольным). Если в задаче сформулировано утверждение, то его предлагается доказать. Для каждого из доказанных свойств A, B, C -треугольников предлагаем выяснить, эквивалентно ли оно определению A, B, C -треугольников.

Далее для треугольника ABC используем обозначения:

C_0, A_0, B_0 — середины сторон AB, BC и CA соответственно;

AN_a, BN_b, CN_c — высоты;

H'_a, H'_b, H'_c — вторые точки пересечения высот с Ω .

C', A', B' — середины дуг AB, BC, CA окружности Ω , не содержащих вершин треугольника;

C'', A'', B'' — середины дуг ACB, BAC, CBA окружности Ω ;

C_1, A_1, B_1 — точки касания γ со сторонами AB, BC, AC ;

C_c, A_c, B_c — точки касания γ_c со сторонами AB, BC, AC (аналогично для окружностей γ_a и γ_b);

H — ортоцентр, M — точка пересечения медиан, G — точка Жергонна (точка пересечения AA_1, BB_1, CC_1), N — точка Нагеля (точка пересечения AA_a, BB_b, CC_c), F — точка Фейербаха.

1. В любом остроугольном треугольнике сумма расстояний от O до сторон равна $R + r$.
2. а) В любом треугольнике $OI^2 = R^2 - 2Rr$.
В любом треугольнике $OI_c^2 = R^2 + 2Rr_c$.
3. Пусть KA_1 — диаметр окружности γ . Тогда AK проходит через N .

- 1А. Постройте A -треугольник по описанной окружности и точке I .
 - 2А. Точка A' является центром вневписанной окружности для треугольника Δ , образованного прямыми OI, AB и AC .
 - 3А. Точка N лежит на прямой AO .
 - 4А. $\cos \angle B + \cos \angle C = 1$.
 - 5А. $r + r_a = 2R$.
 - 6А. Прямая A_0I пересекает AH в точке Z такой, что $AZ = r$.
 - 7А. $|OA_1| = R - r$.
 - 8А. Докажите, что A_1 лежит на H'_aO .
 - 9А. $\angle AIH = 90^\circ$.
 - 10А. Точка F является лежит на прямой AH .
 - 11А. Центр гомотетии с положительным коэффициентом, переводящей γ в Ω , лежит на высоте, проведённой из вершины A .
 - 12А. $A'C'$ и $A'B'$ — биссектрисы внешних углов треугольника Δ .
- 1В. $r_b = 2R$.
 - 2В. а) $\cos \frac{A}{2} \cos \frac{C}{2} \sin \frac{B}{2} = \frac{1}{2}$.
б) $\cos C + \cos A = \cos B + 1$.
 - 3В. H лежит на прямой A_1C_1 .
 - 4В. Прямая, соединяющая основания высот из A и C , касается γ .
 - 5В. Точка, симметричная I относительно O , лежит на BC .

- 1С. Найдите длину общей хорды окружностей γ_c и Ω (R предполагается известным).
- 2С. Найдите углы равнобедренного C -треугольника
- 3С. а) $\cos \frac{A}{2} \cos \frac{B}{2} \sin \frac{C}{2} = \frac{1}{4}$.
 б) $\cos C = \cos A + \cos B$.
- 4С. Пусть C, A, B — точки касания окружности γ_c со стороной AB и продолжениями сторон BC, AC .
- 5С. а) Докажите, что отрезки IC, I_aA, I_bB и I_cO пересекаются в одной точке.
 б) В каком отношении эта точка делит отрезок I_cO ?
- 6С. $AA_c = BB_c = CC_c$.
- Известно, что прямые, соединяющие вершины любого треугольника с точками касания противоположных сторон и вписанной окружности, пересекаются в одной точке. Эта точка G называется *точкой Жергонна*. Аналогично, если заменить вписанную окружность внеписанной, можно определить три *внешних точки Жергонна* G_a, G_b, G_c .
- 7С. G_c лежит на описанной окружности ABC .
- 8С. O — ортоцентр треугольника $A_cB_cC_c$.

ТРИ КЛАССА ТРЕУГОЛЬНИКОВ

1 Определения и вводные задачи

2 Основные задачи

Будем называть окружность полувписанной для треугольника, если она касается двух его сторон и описанной окружности. Обозначим полувписанную окружность треугольника ABC , касающуюся сторон AB и AC за ω_a .

13А. а) В какой точке касаются ω_a и Ω ?

б) Докажите, что четырёхугольник $H'_a C' AB'$ гармонический.

Рассмотрим окружность с центром в B , касающуюся прямой CH , и окружность с центром в C , касающуюся прямой BH . Обозначим их за Γ_b и Γ_c соответственно.

14А. Докажите, что Γ_b и Γ_c касаются в некоторой точке, лежащей на BC .

Обозначим точку из предыдущей задачи за X .

15А. Докажите, что точки I и X лежат на $H'_a A''$.

16А. Докажите, что прямые IH , BC и $H'_a A'$ пересекаются в одной точке.

Обозначим точку из предыдущей задачи за Y .

17А. Докажите, что Y – центр положительной гомотетии, переводящей Γ_b в Γ_c .

18А. Докажите, что вторые касательные из X к γ и из Y к γ касаются γ в точках её пересечения с высотой, опущенной из вершины A .

19А. Докажите, что HA_0 и $A'X$ пересекаются на окружности Ω .

20А. Докажите, что HA_0 , $H'_a O$ и AA' пересекаются в одной точке.

21А. а) Докажите, что точка из предыдущей задачи является центром ω_a .

б) Пусть R и S – точки пересечения OI с ω_a , а T – центр ω_a . Найдите угол STR .

6В. IH делит AC пополам;

7В. B' лежит на $A_b C_b$.

8В. OI проходит через B_b .

9В. A_a, B_b, C_c, H_b лежат на одной окружности.

Определение. Прямая l называется *полярной* точки P относительно окружности с центром O и радиусом R , если луч OP пересекает l и перпендикулярен ей, а расстояние от O до l равно $\frac{R^2}{OP}$. Треугольник называется *автополярным* относительно окружности, если каждая его сторона является полярной противоположной вершины.

- 9С. Треугольник $A_cB_cC_c$ автополярен относительно Ω .
- 10С. Касательные к окружности Ω в точках A и B пересекаются на прямой A_cB_c .
Пусть AL_a, BL_b — биссектрисы.
- 11С. O лежит на прямой L_aL_b .
- 12С. Пусть прямая L_aL_b пересекает окружность Ω в точках X и Y .
а) Треугольник I_cXY — правильный.
б) Найдите центр этого треугольника.
- 13С. I лежит на H_aH_b .
- 14С. OI проходит через H_c .
- 15С. (A.Golmakani, Iran) Пусть прямые AL_a, BL_b пересекают касательную к Ω , проведенную в точке C , в точках P и Q . Тогда прямая OI делит отрезок PQ пополам.
Известно, что симедианы любого треугольника (прямые, симметричные медианам относительно биссектрис) пересекаются в одной точке, которая называется *точкой Лемуана* L .
- 16С. Прямые OG_c и LI_c параллельны.
- 17С. Поляра G_c относительно вневписанной окружности проходит через L .

3 Дополнительные задачи

- ω_1 и ω_2 содержат центры друг друга и пересекаются в точках P и Q . Касательные из точки C на ω_1 пересекают вторично ω_1 в точках A и B . Докажите, что $AB \parallel PQ$. (или CP и CQ симметричны относительно биссектрисы угла ACB)
- В выпуклом четырехугольнике $ABDC$ $\angle ABD = \angle ACD = 90^\circ$ и $DA = DB + DC$. Докажите, что AD делит периметр треугольника ABC пополам.
- Две окружности радиуса 1 пересекаются в точках X, Y , расстояние между которыми также равно 1. Из точки C одной окружности проведены касательные CA, CB к другой. Прямая CB вторично пересекает первую окружность в точке A' . Найдите расстояние AA' .

Согласно *Теореме Понселе* существует бесконечно много треугольников, имеющих данные описанную и вневписанную окружности. Рассмотрим все такие треугольники ABC .

- 18С. а) Стороны всех соответствующих треугольников $A_cB_cC_c$ касаются одной и той же гиперболы.
б) В какой точке эта гипербола касается прямой A_cB_c ?
в) Найти фокусы гиперболы.
- 19С. а) Доказать, что точки пересечения прямых AB и A_cB_c , AC и A_cC_c , BC и B_cC_c лежат на одной прямой, касающейся гиперболы.
б) В какой точке происходит касание?
- ВС. Прямая OI пересекает одну из сторон треугольника в основании опущенной на эту сторону высоты, а другую в точке ее касания с соответствующей вневписанной окружностью. Найдите угол между этими сторонами.

ТРИ КЛАССА ТРЕУГОЛЬНИКОВ

Решения

1 Определения и вводные задачи

1. Применяя теорему Птолемея к вписанным четырехугольникам OA_0CB_0 , OB_0AC_0 , OC_0BA_0 и складывая полученные равенства, получаем

$$Rp = d_1 \frac{b+c}{2} + d_2 \frac{c+a}{2} + d_3 \frac{a+b}{2},$$

где p — полупериметр треугольника. Так как $\frac{ad_1+bd_2+cd_3}{2} = S_{ABC} = pr$, это равенство равносильно искомому.

Примечание. Эта формула верна и для тупоугольного треугольника, если расстояние до стороны считать ориентированным.

2. а) Заметим, что $R^2 - OI^2 = CI \cdot C'I$. т.к. это модуль степени I относительно Ω . При этом $CI = r / \sin \frac{C}{2}$, а $C'I = AI = BI = 2R \sin \frac{C}{2}$ по теореме о трилистнике. Отсюда, очевидно, следует нужное соотношение.

б) Доказательство полностью аналогично предыдущему, следует рассмотреть степень I_c .

3. Пусть прямая, проходящая через K и параллельная BC , пересекает стороны AB , AC в точках X , Y соответственно. Тогда γ — вневписанная окружность треугольника AXY , гомотетичного ABC . Точки K и A_2 соответствуют друг другу при этой гомотетии, значит, соединяющая их прямая проходит через центр гомотетии A .

1А. Из определения A -треугольника следует, что диаметр, перпендикулярный OI , пересекает описанную окружность в точке A' . По теореме о трилистнике эта точка — центр окружности IBC . Соответственно, построив эту окружность, мы найдем две вершины исходного треугольника. Третья является второй точкой пересечения прямой $A'I$ с описанной окружностью.

2А. Не умаляя общности, $AB \leq AC$. Пусть X — проекция A' на AB , L_a — основание бисектрисы угла A . Заметим, что $\angle OA'I = \angle BA'X$, т.к. $\angle A'BX = \angle A'CA = \sphericalangle ABA' = \sphericalangle AB + \sphericalangle A'C = \angle A'L_aC = \angle A'IO$. Так как $A'B = A'I$, отсюда следует, что A' равноудалена от прямых AB , AC и OI .

3А. Очевидно, следует из предыдущей задачи, если рассмотреть гомотетию, переводящую треугольник Δ в ABC .

4А. Из задачи 1 следует, что сумма расстояний от O до AB и AC равна R , т.к. $OA_0 = r$, что равносильно утверждению задачи, ибо $OC_0 = R \cos \angle C$, $OB_0 = R \cos \angle B$.

- 5А. Аналогично задаче 1, получаем, что в любом треугольнике $r_a - R = d_2 + d_3 - d_1$. Складывая это равенство с равенством задачи 1, получаем, что $r + r_a = BH + CH$. Из предыдущей задачи следует, что в A -треугольнике это равенство равносильно искомому.
- 6А. Это утверждение верно для любого треугольника и следует из подобия треугольников $A_0A'I$ и ZAI . Действительно, так как $A_0A' = R(1 - \cos A) = 2R \sin^2 \frac{A}{2}$, $AZ = A_0A' \cdot AI/A'I = r$.
- 7А. Из предыдущей задачи следует, что $AO \parallel A_0I$. Значит, треугольник $A'A_0I$ подобен равнобедренному треугольнику $A'OA$, т.е. $OA_1 = IA_0 = A_0A' = R - r$. Также это легко следует из задачи 2: действительно, $OA_1^2 = IA_1^2 + IO^2 = r^2 - 2Rr + R^2 = (R - r)^2$. Первое равенство следует из параллельности OI и BC .
- 8А. Так как $AO \parallel A_0I$, прямые OH'_a и A_0I образуют равные углы с высотой AH . Но прямые A_0I и OA_1 также образуют с ней равные углы, поскольку OA_0A_1I — прямоугольник.
- 9А. Так как $\angle IAH = |\frac{B-C}{2}|$, утверждение задачи равносильно равенству $2R \cos A \cos \frac{B-C}{2} = r / \sin \frac{A}{2}$ и $\cos B + \cos C = 1$.
По задаче 6, $AZ = r$, кроме того, $AH = 2OA_0 = 2r$, также $\angle IAZ = \angle IAO = \angle AOI$ в силу параллельности AO и IA_0 . Отсюда, $ZA = ZO = ZI$, из чего утверждение задачи очевидно следует.
- 10А. Из задачи 6А следует, что прямая A_0I делит отрезок AH пополам, т.е. пересекает его в точке Z , лежащей на окружности Эйлера. Кроме того, так как $OA \parallel A_0I$, то $\angle AIZ = \angle OAI = \angle IAZ$ и $IZ = AZ = r$. Значит, Z лежит также на вписанной окружности, т.е. совпадает с F .
- 11А. В любом треугольнике указанный центр гомотетии изогонально сопряжен точке Нагеля. Поэтому искомое утверждение сразу следует из задачи 3А.
- 12А. Очевидно, следует из задачи 2А и того, что $A'C'$ перпендикулярно биссектрисе угла B .
- 1В. Перпендикулярность окружностей означает, что $R^2 + 2Rr_b = OI_b^2 = R^2 + r_b^2$.
- 2В. а) Так как $BA_b = p$, то $R_b = p \operatorname{tg} \frac{B}{2} = R(\sin A + \sin B + \sin C) \operatorname{tg} \frac{B}{2}$. Но $\sin A + \sin B + \sin C = 2 \sin \frac{A+B}{2} \cos \frac{A-B}{2} + 2 \sin \frac{C}{2} \cos \frac{C}{2}$. Поскольку $\frac{A+B}{2} = \frac{\pi}{2} - \frac{C}{2}$, это выражение равно $2 \cos \frac{C}{2} (\cos \frac{A-B}{2} + \cos \frac{A+B}{2}) = 4 \cos \frac{A}{2} \cos \frac{B}{2} \cos \frac{C}{2}$, откуда и получаем искомое равенство.
- б) По предыдущей задаче $1 = 2 \sin \frac{B}{2} \cos \frac{A}{2} \cos \frac{C}{2} = \sin \frac{B}{2} (\cos \frac{A-C}{2} + \sin \frac{B}{2}) = \frac{1}{2} (\sin \frac{B+A-C}{2} + \sin \frac{B+C-A}{2} + 1 - \cos B)$. Так как $\frac{B+A-C}{2} = \frac{\pi}{2} - C$, это равенство равносильно искомому.

- 3В. В следующей задаче доказано, что прямая H_aH_c касается γ , т.е. γ является вневписанной окружностью треугольника BH_aH_c , который подобен исходному с коэффициентом $\cos B$. Значит, $\cos B = r/r_b = (p - b)/p$ и $A_1C_b \perp BC$, $C_1A_b \perp AB$. Тогда по теореме Фалеса прямые AH_a и CH_c пересекают A_1C_1 в одной и той же точке.
- 4В. В силу того, что $H_aH_c = AC \cos B$, условие описанности четырехугольника AH_cH_aC имеет вид $AC + AC \cos B = AC \cos A + AC \cos B$, т.е. совпадает с равенством из задачи 2В.
- 5В. Из равенств $r_b = 2R$ и $r = r_b \cos \beta$ следует, что $OB_0 = r/2$, что, очевидно, влечет искомое утверждение. Заметим также, что точка, симметричная I относительно O , лежит на перпендикулярах, восстановленных их A_2, B_2, C_2 к соответствующим сторонам треугольника. Следовательно, в B -треугольнике эта точка совпадает с B_2 .
- 1С. Пусть $R = r_c = 1$. Тогда по задаче, $2OI_c = \sqrt{3}$. Так как центры окружностей и точки их пересечения образуют ромб, его вторая диагональ равна 1.
- 2С. **Ответ.** $\pi/4, \pi/4, \pi/2$.
Указание. Воспользуйтесь следующей задачей.
- 3С. Решение аналогично задаче 2В.
- 4С.
- 5С. Треугольники II_aI_b и $C_cB_cA_c$ гомотетичны так как их стороны параллельны двум внутренним и одной внешней биссектрисам исходного треугольника. Более того, треугольник ABC для треугольника II_aI_b является ортотреугольником. Значит, радиус описанной окружности треугольника II_aI_b равен $2R$, а ее центр симметричен I_c относительно O . Поэтому центр гомотетии лежит на отрезке I_cO и делит его в отношении $2 : 1$.
- 6С. Непосредственное вычисление показывает, что $\angle OAI_c = \angle AI_cA_c$. Кроме того, $OA = I_cA_c$. Поэтому OAI_cA_c — равнобедренная трапеция и $AA_c = OI_c = R\sqrt{3}$. Аналогично для двух других отрезков.
- 7С. Непосредственно следует из того, что угол между AA_c и BB_c равен $2\angle AI_cB$, ибо эти прямые получаются из прямой II_c отражениями относительно серединных перпендикуляров к AI_c и BI_c соответственно.
- 8С. Непосредственно следует из задачи 5С а также из задачи 6С с помощью рассмотрения получившихся в ней равнобоких трапеций.

ТРИ КЛАССА ТРЕУГОЛЬНИКОВ

1 Определения и вводные задачи

2 Основные задачи

Решения.

13А. а) Ответ. H'_a .

Указание 1. Рассмотрим композицию инверсии с центром A и радиусом $\sqrt{AB \cdot AC}$ и симметрии относительно биссектрисы угла A . Она меняет местами точки B и C , а также прямую BC и описанную окружность треугольника. Поэтому поувписанная окружность переходит во вневписанную и, значит, прямые, соединяющие A с соответствующими точками касания, симметричны относительно биссектрисы. Но в A -треугольнике высота симметрична прямой AA_a .

Указание 2. Точка касания полувписанной и описанной окружностей является центром гомотетии с положительным коэффициентом, переводящей одну из этих окружностей в другую. Рассмотрим также вписанную окружность, воспользуемся теперь результатом задачи 11А и теоремой о центрах трёх гомотетий.

б) Известно, что в любом треугольнике прямая соединяющая точку касания ω_a и Ω с точкой A'' , делит пополам отрезок $B'C'$. Поэтому, так как дуги $B'A''$ и AC' равны, $H'_a A$ является симедианой треугольника $H'_a B'C'$, что равносильно утверждению задачи.

14А. Очевидно следует из того, что сумма радиусов окружностей равна $BC \cos B + BC \cos C = BC$.

15А. Так как $BX : CX = \cos B : \cos C = BH'_a : CH'_a$, то X лежит на биссектрисе $H'_a A''$ треугольника $H'_a BC$, которая в любом треугольнике проходит через I (если заменить H'_a на точку касания полувписанной и описанной окружности).

16А. Прямые IH и $H'_a A'$ являются внешними биссектрисами треугольников HBC и $H'_a BC$, симметричных относительно BC .

17А. Так как HX и $H'Y$ — внутренняя и внешняя биссектрисы угла BHC , точки B , C , X и Y образуют гармоническую четверку. При этом B и C — центры окружностей Γ_b , Γ_c , а X — центр их внутренней гомотетии. Следовательно, Y — центр внешней гомотетии.

18А. Прямая $H'_a A'$ проходит через O и, значит, симметрична $H'_a A$ относительно биссектрисы $H'_a I$ угла $BH'_a C$, т.к. $H'_a A$ — высота треугольника $BH'_a C$. Утверждение задачи следует из того, что X также лежит на этой биссектрисе — точка, симметричная точке касания γ и BC и есть точка из задачи. Доказательство для Y аналогично.

19А. В любом треугольнике прямая HA_0 проходит через точку A_2 , диаметрально противоположную A . Поэтому утверждение задачи равносильно равенству двойных отношений (BCA_0X) и (BCA_2A') , которое проверяется непосредственным вычислением.

Пусть P — вторая точка пересечения $A'X$ и Ω . Тогда $\angle A''PA' = 90^\circ$, значит, прямая $A''P$ проходит через Y . Далее, $\angle A'PA_0 = \angle A'XA_0 = \angle H'_aA' = \angle A'PA_2$, то есть, A_0 лежит на PA_2 .

20А. Рассмотрим треугольники $OA'A_2$ и H'_aIH . Как нам уже известно, $A'O$ пересекает H'_aI в точке A'' . Кроме того, очевидно, H'_aH и A_2O пересекаются в точке A . Стороны HI и A_2A' этих треугольников пересекаются в бесконечно удалённой точке, которая лежит и на $A''A$, ибо все три прямые AA'' , HI и $A'A_2$ перпендикулярны прямой AI . Утверждение задачи теперь непосредственно следует из теоремы Дезарга.

21А. а) Прямые H'_aO и AA' проходят через центр ω_a , поскольку H'_a и A — центры гомотетии ω_a с Ω и γ соответственно.

б) Пусть K — точка пересечения прямых AO и H'_aI . Тогда K и T суть основания биссектрис углов при основании равнобедренного треугольника AOH'_a , откуда легко следует, что $AK = KT = TH'_a$, в частности, TK равен радиусу ω_a . Прямая OI , очевидно, является серединным перпендикуляром к TK , из чего непосредственно следует ответ 120° .

6В. В любом треугольнике прямая B_0I отсекает на высоте BH отрезок, равный r . Но в B -треугольнике $BH = 2R \cos B = r_b \cos B = r$.

7В. Так как I лежит на прямых C_bA_1 и A_bC_1 , четырёхугольник $IA_bI_bC_b$ является ромбом, т.е. середины отрезков A_bC_b и IIC_c совпадают. Но B' — середина IIC_c по теореме о трилистнике.

8В. Доказано в решении задачи 5В.

9В. Из задачи 5В следует, что проекции точки Bb на AB и BC совпадают с C_c и A_a . Следовательно, A_a, B_b, C_c, H_b лежат на окружности с диаметром BB_b .

Определение. Прямая l называется *полярной* точки P относительно окружности с центром O и радиусом R , если луч OP пересекает l и перпендикулярен ей, а расстояние от O до l равно $\frac{R^2}{OP}$. Треугольник называется *автополярным* относительно окружности, если каждая его сторона является полярной противоположной вершины.

9С. Точки A_c, B_c, C_c являются точками пересечения противоположных сторон и диагоналей вписанного в Ω четырёхугольника $ACBG_c$, т.е. вершинами треугольника, автополярного относительно Ω .

10С. Так как прямая AB проходит через полюс C_c прямой A_cB_c , полюс AB лежит на A_cB_c .

- 11С. Так как $\cos C = \cos A + \cos B$, расстояние от O до AB равно сумме расстояний до двух других сторон. Точки L_a, L_b также обладают этим свойством, которое, очевидно, определяет прямую.
- 12С. Известно, что прямая $L_a L_b$ одна и та же для всех треугольников с заданными окружностями Ω и γ_c . Для C -треугольника эта прямая будет диаметром Ω , перпендикулярным OI_c . Очевидно, концы этого диаметра и I_c образуют правильный треугольник, центр которого делит отрезок OI_c в отношении $1 : 2$.
- 13С. Так как треугольники ABC и $H_a H_b C$ подобны с коэффициентом $\cos C$, прямая $H_a H_b$ делит биссектрису угла C в отношении $\cos C : (1 - \cos C)$. Из теоремы о биссектрисе и равенства $\cos C = \cos A + \cos B$ легко получить, что I делит биссектрису в таком же отношении.
- 14С. Биссектриса угла C является также биссектрисой угла OCH_c . Значит, она пересекает отрезок OH_c в точке, делящей его в отношении $R : CH_c$. Поскольку расстояния от точки H_c до сторон BC и AC равны $CH_c \cos B$ и $CH_c \cos A$, получаем, что $\cos C = \cos A + \cos B$ тогда и только тогда, когда эта точка совпадает с I .
- 15С. Так как O лежит на $L_a L_b$, утверждение задачи можно переформулировать следующим образом: прямые IL_a, IL_b, IO и перпендикуляр из I на OC образуют гармоническую четверку. Но из двух предыдущих задач следует, что эти прямые пересекают AB в точках A, B, H_c и точке пересечения AB с $H_a H_b$.
- 16С, 17С. **Указание.** Когда точка C движется по Ω , L движется по гиперболе, касающейся сторон треугольников $A_c B_c C_c$.

THREE CLASSES OF TRIANGLES

A.Zaslavsky, O.Zaslavsky, F.Ivlev, P.Kozhevnikov, D.Krekov

*Сочинились стихи бредовые
Без какой-либо путной мысли,
Словно ведра воды пудовые
Я принес вам на коромысле.
А.Великий*

1 Definitions and introductory problems

Every triangle has an incircle and a circumcircle. In addition to it, every triangle has three excircles, each of them touching one of the sides of the triangle and the extensions of two other sides. For a triangle ABC we denote:

Ω — circumcircle, O , R — its center and radius;

γ — incircle, I , r — its center and radius;

$\gamma_a, \gamma_b, \gamma_c$ — excircles, I_a, I_b, I_c — their centers, r_a, r_b, r_c — their radii.

The main objects that we study are three special kinds of triangles.

Definition A. *A-triangle* is a triangle in which $OI \parallel BC$.

Definition B. *B-triangle* is a triangle in which circles γ_b и Ω are perpendicular.

Definition C. *C-triangle* is a triangle in which $R = r_c$.

In the problems that are marked by the letters A, B, C , we mean that A, B, C -triangle is given (otherwise the triangle ABC is arbitrary). If we formulate some proposition in the problem, you should prove it. For every proved property A, B, C -triangles we offer you to find out, if it is equivalent to the definition of A, B, C -triangles.

For the triangle ABC we use such notations:

C_0, A_0, B_0 — midpoints of AB, BC и CA respectively;

AH_a, BH_b, CH_c — altitudes;

H'_a, H'_b, H'_c — second intersection points of altitudes and Ω .

C', A', B' — middles of the arcs AB, BC, CA of the circle Ω , not containing its vertices;

C'', A'', B'' — middles of the arcs ACB, BAC, CBA of the circle Ω ;

C_1, A_1, B_1 — intersection points of γ and the sides AB, BC, AC respectively;

C_c, A_c, B_c — intersection points of γ_c and the sides AB, BC, AC (similarly for the circles γ_a и γ_b);

H — orthocenter, M — the common point of medians, G — the Gergonne point (the common point of AA_1, BB_1, CC_1), N — The Nagel point (the common point of AA_a, BB_b, CC_c), F — the Feuerbach point.

1. In any acute triangle the sum of distances from O to the sides equals $R + r$.

2. a) In any triangle $OI^2 = R^2 - 2Rr$.

In any triangle $OI_c^2 = R^2 + 2Rr_c$.

3. Let KA_1 — be the diameter of the circle γ . Then AK contains N .

- 1A. Construct A -triangle if its circumcircle and the point I are given.
- 2A. Point A' is the center of excircle of triangle Δ , whose sides are the lines OI , AB and AC .
- 3A. N lies on AO .
- 4A. $\cos \angle B + \cos \angle C = 1$.
- 5A. $r + r_a = 2R$.
- 6A. A_0I intersects AH at the point Z such that $AZ = r$.
- 7A. $|OA_1| = R - r$.
- 8A. A_1 lies on H'_aO .
- 9A. $\angle AIH = 90^\circ$.
- 10A. F lies on AH .
- 11A. The center of homothety with positive ratio taking γ to Ω lies in AH_a .
- 12A. $A'C'$ и $A'B'$ — are external angle bisectors of Δ .
- 1B. $r_b = 2R$.
- 2B. a) $\cos \frac{A}{2} \cos \frac{C}{2} \sin \frac{B}{2} = \frac{1}{2}$.
 б) $\cos C + \cos A = \cos B + 1$.
- 3B. H lies on A_1C_1 .
- 4B. The line that passes through the bases of the altitudes drawn from A и C , is tangent γ .
- 5B. The point symmetric to I with respect to O , lies on BC .
- 1C. Determine the length of the common chord of γ_c и Ω (R is given).
- 2C. Find the angles of isosceles C -triangle
- 3C. a) $\cos \frac{A}{2} \cos \frac{B}{2} \sin \frac{C}{2} = \frac{1}{4}$.
 б) $\cos C = \cos A + \cos B$.
- 4C. Let C_c, A_c, B_c — be the tangent points of γ_c with the side AB and the extensions of the sides BC, AC .
- 5C. a) Prove that the segments IC_c, I_aA_c, I_bB_c и I_cO have a common point.
 б) Determine the ratio in which this point divides the segment I_cO .

6C. $AA_c = BB_c = CC_c$.

It is known that lines joining vertices of a triangle with touching points of the inscribed circle and the opposite side have a common point. This point is called G is called *Gergonne point*. Similarly, if we replace the incircle by the excircle we can define three *external Gergonne points* G_a, G_b, G_c .

7C. G_c lies on the circumcircle of the triangle ABC .

8C. O — is the orthocenter of triangle $A_cB_cC_c$.

ТРИ КЛАССА ТРЕУГОЛЬНИКОВ

1 Определения и вводные задачи

2 Main problems

We will call the circle touching two sides of a triangle and its circumcircle *the semiincircle*. The semiincircle of triangle ABC touching sides AB and AC will be denoted as ω_a .

13A. a) Which is the touching point of ω_a and Ω ?

b) Prove that quadrilateral $H'_a C' AB'$ is harmonic.

Consider the circle with center B touching CH and the circle with center C touching BH . Denote them as Γ_b and Γ_c respectively.

14A. Prove that Γ_b and Γ_c touch at some point lying on BC .

Denote the touching point from the previous problem as X .

15A. Prove that I and X lie on $H'_a A''$.

16A. Prove that lines IH , BC and $H'_a A'$ concur.

Denote the concurrency point from the previous problem as Y .

17A. Prove that Y is the center of positive homothety mapping Γ_b to Γ_c .

18A. Prove that the second tangents to Γ drawn from X and Y touch Γ at its intersection points with the line AH .

19A. Prove that HA_0 and $A'X$ meet at Ω .

20A. Prove that HA_0 , $H'_a O$ and AA' concur.

21A. a) Prove that the concurrency point from the previous problem is the center of ω_a .

b) Let R and S be the common points of OI with ω_a , and T be the center of ω_a . Find angle STR .

6B. IH bisects AC .

7B. B' lies on $A_b C_b$.

8B. OI passes through B_b .

9B. A_a, B_b, C_c, H_b are concyclic.

Definition. Line l is called *the polar* of point P wrt the circle with center O and radius R , if ray OP meets l , is perpendicular to it, and the distance from O to l is equal to $\frac{R^2}{OP}$. A triangle is called *autopolar* wrt the circle, if its sidelines are the polars of opposite vertices.

- 9C. The triangle $A_cB_cC_c$ is autopolar wrt Ω .
- 10C. The intersection point of the lines that are tangent to the circle Ω at the points A and B lies on the line A_cB_c .
Let AL_a, BL_b be the bisectors of angles A and B of triangle ABC .
- 11C. O lies on the line L_aL_b .
- 12C. Let the line L_aL_b intersects the circle Ω at the points X and Y .
a) The triangle I_cXY is equilateral.
b) Determine, which point is the center of this triangle.
- 13C. I lies on the line H_aH_b .
- 14C. The line OI contains H_c .
- 15C. (A.Golmakani, Iran) Let the lines AL_a and BL_b intersect the line, tangent to the circle Ω at point C , at points P and Q respectively. Then the line OI passes through the midpoint of the segment PQ .
It is well known, that in any triangle symmedians (the lines, symmetric to the medians of this triangle with respect to its angle bisectors) have the common point. This point is called *Lemoann point* L .
- 16C. The lines OG_c and LI_c are parallel.
- 17C. The polar of the point G_c with respect to the excircle passes through L .

3 Extra problems

- Each of the circles ω_1 and ω_2 contains the center of the other circle and they intersect each other at points P and Q . The lines, passing through C tangent to ω_1 intersect ω_1 at the second time at the points A and B . Prove that $AB \parallel PQ$. In a convex quadrilateral $ABDC$ $\angle ABD = \angle ACD = 90^\circ$ and $DA = DB + DC$. Prove that AD divides the triangle ABC on two polygons with equal perimeters.
- Two circles of radii 1 intersect each other at points X Y . $XY = 1$. CA and CB are tangent lines to one of these circles from point C lying on the other one of these circles. Line CB meets the first circle for the second time at point A' . Determine the length AA' .

Due to *Poncelet theorem* there exist infinitely many triangles with fixed circumcircle and excircle. Consider all such triangles ABC .

- 18C. a) The sidelines of all correspondent triangles $A_cB_cC_c$ touch some fixed hyperbola.
- b) Which is the touching point of this hyperbola with line A_cB_c ?
- c) Determine the foci of this hyperbola.
- 19C. a) Prove that the common points of lines AB and A_cB_c , AC and A_cC_c , BC and B_cC_c lie on some line touching the hyperbola.
- b) Determine the point of tangency.
- BC. Line OI meets one of sides of a triangle at the base of the correspondent altitude, and the second one at its touching point with the respective excircle. Find the angle between these sides.

Three classes of triangles Solutions

1 Definitions and introductory problems

1. Applying the Ptolemy theorem to cyclic quadrilaterals OA_0CB_0 , OB_0AC_0 , OC_0BA_0 and summing the obtained equalities we have

$$Rp = d_1 \frac{b+c}{2} + d_2 \frac{c+a}{2} + d_3 \frac{a+b}{2},$$

where p is the semiperimeter of the triangle. Since $\frac{ad_1+bd_2+cd_3}{2} = S_{ABC} = pr$, this is equivalent to the desired equality.

Note. If we consider d_1, d_2, d_3 as the oriented distances this formula is also correct for an obtuse-angled triangle.

2. a) Note that $R^2 - OI^2 = CI \cdot C'I$ because this is the absolute value of the degree of I wrt Ω . Also we have that $CI = r/\sin \frac{C}{2}$, and $C'I = AI = BI = 2R \sin \frac{C}{2}$ by the trident theorem. From this we obtain the desired equality.

b) Considering the degree of I_c we obtain the similar proof.

3. Let the line passing through K and parallel to BC meet AB, AC at points X, Y respectively. Then γ is the excircle of triangle AXY homothetic to ABC . Points K and A_2 are correspondent in this homothety, thus these points and the homothety center A are collinear.

1A. Using the definition of A -triangle we obtain that the diameter perpendicular to OI meets the circumcircle at A' . By the trident theorem this point is the circumcircle of triangle IBC . Therefore constructing this circle we find two vertices of the desired triangle. The third vertex is the second common point of $A'I$ and the circumcircle.

2A. We can suppose that $AB \leq AC$. Let X be the projection of A' to AB , and L_a be the base of the bisector from A . Note that $\angle OA'I = \angle BA'X$ because $\angle A'BX = \angle A'CA = \sphericalcap ABA'/2 = \sphericalcap AB + \sphericalcap A'C/2 = \angle A'L_aC = \angle A'IO$. Since $A'B = A'I$ this yields that the distances from A' to AB, AC and OI are equal.

3A. We obtain this from the previous problem considering the homothety mapping Δ to ABC .

4A. By problem 1 the sum of distances from O to AB and AC is equal to R because $OA_0 = r$, this yields the desired assertion because $OC_0 = R \cos \angle C$, $OB_0 = R \cos \angle B$.

- 5A. Similarly to problem 1 we obtain that in an arbitrary triangle $r_a - R = d_2 + d_3 - d_1$. Summing this with the equality of problem 1 we obtain that $r + r_a = BH + CH$. In A -triangle this is equivalent to the desired equality by the previous problem.
- 6A. This assertion is true for an arbitrary triangle and follows from the similarity of triangles $A_0A'I$ and ZAI . In fact since $A_0A' = R(1 - \cos A) = 2R \sin^2 \frac{A}{2}$ we obtain that $AZ = A_0A' \cdot AI/A'I = r$.
- 7A. By the previous problem $AO \parallel A_0I$. Thus triangle $A'A_0I$ is similar to isosceles triangle $A'OA$, i.e. $OA_1 = IA_0 = A_0A' = R - r$. This also follows from problem 2: in fact $OA_1^2 = IA_1^2 + IO^2 = r^2 - 2Rr + R^2 = (R - r)^2$. The first equality is true because $OI \parallel BC$.
- 8A. Since $AO \parallel A_0I$, lines OH'_a and A_0I form equal angles with altitudes AH . But lines A_0I and OA_1 also form equal angles with AH because OA_0A_1I is a rectangle.
- 9A. Since $\angle IAH = |\frac{B-C}{2}|$ the desired assertion is equivalent to $2R \cos A \cos \frac{B-C}{2} = r / \sin \frac{A}{2}$ and to $\cos B + \cos C = 1$.
From problem 6A we have $AZ = r$, also $AH = 2OA_0 = 2r$ and $\angle IAZ = \angle IAO = \angle AOI$ because $AO \parallel IA_0$. From this $ZA = ZO = ZI$, which evidently yields the assertion of the problem.
- 10A. From problem 6A we obtain that line A_0I bisects segment AH , i.e. their common point Z lies on the Euler circle. Also since $OA \parallel A_0I$ we obtain that $\angle AIZ = \angle OAI = \angle IAZ$ and $IZ = AZ = r$. Therefore Z lies also on the incircle, i.e. Z coincide with F .
- 11A. For an arbitrary triangle the considered homothety center is isogonally conjugated to the Nagel point. Hence the desired assertion immediately follows from problem 3A.
- 12A. This evidently follows from problem 2A because $A'C'$ is perpendicular to the bisector of angle B .
- 1B. Since the circles are orthogonal $R^2 + 2Rr_b = OI_b^2 = R^2 + r_b^2$.
- 2B. a) Since $BA_b = p$, we have $R_b = p \operatorname{tg} \frac{B}{2} = R(\sin A + \sin B + \sin C) \operatorname{tg} \frac{B}{2}$. But $\sin A + \sin B + \sin C = 2 \sin \frac{A+B}{2} \cos \frac{A-B}{2} + 2 \sin \frac{C}{2} \cos \frac{C}{2}$. Since $\frac{A+B}{2} = \frac{\pi}{2} - \frac{C}{2}$, this is equal to $2 \cos \frac{C}{2} (\cos \frac{A-B}{2} + \cos \frac{A+B}{2}) = 4 \cos \frac{A}{2} \cos \frac{B}{2} \cos \frac{C}{2}$ which yields the desired equality.
- b) By the previous problem $1 = 2 \sin \frac{B}{2} \cos \frac{A}{2} \cos \frac{C}{2} = \sin \frac{B}{2} (\cos \frac{A-C}{2} + \sin \frac{B}{2}) = \frac{1}{2} (\sin \frac{B+A-C}{2} + \sin \frac{B+C-A}{2} + 1 - \cos B)$. Since $\frac{B+A-C}{2} = \frac{\pi}{2} - C$ this is equivalent to the desired equality.

- 3B. In next problem we prove that line H_aH_c touches γ , i.e. γ is the excircle of triangle BH_aH_c , which is similar to the given triangle with coefficient $\cos B$. Hence $\cos B = r/r_b = (p-b)/p$ and $A_1C_b \perp BC$, $C_1A_b \perp AB$. Then by the Thales theorem lines AH_a and CH_c meet A_1C_1 at the same point.
- 4B. Since $H_aH_c = AC \cos B$ quadrilateral AH_cH_aC is circumscribed if and only if $AC + AC \cos B = AC \cos A + AC \cos B$, which coincide with the equality from problem 2B.
- 5B. Since $r_b = 2R$ and $r = r_b \cos B$ we obtain that $OB_0 = r/2$, which evidently yields the desired assertion. Note also that the reflection of I about O lies on the perpendiculars from A_a , B_b , C_c to the correspondent sidelines. Therefore in B -triangle this point coincide with B_b .
- 1C. Let $R = r_c = 1$. Then by problem 2 $OI_c = \sqrt{3}$. The centers of the circles and their common points form a rhombus, therefore its second diagonal is equal to 1.
- 2C. **Answer.** $\pi/4, \pi/4, \pi/2$.
Hint. Use the next problem.
- 3C. The solution is similar to problem 2B.
- 4C.
- 5C. Triangles II_aI_b and $C_cB_cA_c$ are homothetic because because their sidelines are parallel to two internal and one external bisector of the given triangle. Also triangle ABC is the orthotriangle of triangle II_aI_b . Thus the circumradius of triangle II_aI_b is equal to $2R$, and its circumcenter is the reflection of I_c in O . Hence the homothety center lies on segment I_cO and divide it in ratio 2 : 1.
- 6C. It is easy to see that $\angle OAI_c = \angle AI_cA_c$. Also $OA = I_cA_c$. Thus OAI_cA_c is an isosceles trapezoid and $AA_c = OI_c = R\sqrt{3}$. Similarly two remaining segments have the same length.
- 7C. The angle between AA_c and BB_c is equal to $2\angle AI_cB$ because these lines are symmetric to OI_c wrt the perpendicular bisectors to segments AI_c and BI_c respectively.
- 8C. Immediately follows from problem 5C. Also this can be obtained from problem 6C considering the correspondent isosceles trapezoids.

Three classes of triangles

1 Определения и вводные задачи

2 Main problems

Solutions.

13A. a) **Answer.** H'_a .

Hint 1. For any triangle consider a transformation that is the composition of inversion with center A and radius $\sqrt{AB \cdot AC}$ and symmetry with respect to the bisector of angle A . It maps B to C , and the line BC to Ω . Hence it maps γ_a to ω_a . Thus line through A and touching points of ω_a and Ω is symmetrical to AA_a in AI . But in A -triangle altitude is symmetrical to AA_a in AI .

Hint 2. Touching point of ω_a and Ω is the center of homothety with a positive ratio that maps one of these circles to other. Consider the incircle, and use the result of problem 11A and theorem on three centers of homothety.

b) It is known that in any triangle line connecting tangency point ω_a and Ω with point A'' , bisects segment $B'C''$. Since arcs $B'A''$ and AC'' are equal, H'_aA is a symmedian of triangle $H'_aB'C''$. This is equivalent to the statement of the problem.

14A. Easily follows from the fact that the sum of radii is $BC \cos B + BC \cos C = BC$.

15A. Since $BX : CX = \cos B : \cos C = BH'_a : CH'_a$, we obtain that X lies in the bisector H'_aA'' of triangle H'_aBC . Now the statement follows from the fact: in any triangle the line through A'' and the tangency point of Ω and ω_a passes through I .

16A. Lines IH and H'_aA' are external bisectors of triangles HBC and H'_aBC that are symmetric in BC .

17A. Since HX и HY are internal and external bisector of the angle BHC , the quadruple B, C, X, Y is harmonic. We know that B and C — are centers of circles Γ_b, Γ_c , and X — is the center of their homothety with negative ratio. Hence Y is the center of their homothety with positive ratio.

18A. Line H'_aA_1 passes through O , hence it is symmetric to H'_aA with the respect of the bisector H'_aI of the angle BH'_aC (since H'_aA is the altitude of triangle BH'_aC). The statement of the problem follows from the fact that X also lies in this bisector (a tangent to γ through X passes through the point that is symmetric to A_1 in H'_aI). The proof for Y is analogous.

19A. In any triangle line HA_0 passes through the point A_2 of Ω such that AA_2 is a diameter. Hence the required statement to equality $(BCA_0X) = (BCA_2A')$ that can be obtained by easy calculation.

Let P be the second common point of $A'X$ and Ω . Then $\angle A''PA' = 90^\circ$, thus line $A''P$ passes through Y . Now $\angle A'PA_0 = \angle A'XA_0 = \angle H'_aA' = \angle A'PA_2$, hence A_0 lies in PA_2 .

- 20A. Consider triangles $OA'A_2$ and H'_aIH . We know that $A'O$ meets H'_aI at A'' . Further, it is clear that H'_aH and A_2O meet at A . Sidelines HI and A_2A' meet at the infinite point of $A''A$ since lines AA'' , HI и $A'A_2$ are perpendicular to AI . Now the statement follows from the Desargues theorem.
- 21A. a) Lines H'_aO and AA' pass through the center of ω_a because H'_a and A are homothety centers of ω_a with Ω and γ respectively.
- b) Let K be the common point of AO and H'_aI . Then K and T are the feet of the bisectors in isosceles triangle AOH'_a . From this we obtain that $AK = KT = TH'_a$, hence TK is the radius of ω_a . It is clear that line OI is the perpendicular bisector of TK , therefore the answer is 120° .
- 6B. In any triangle B_0I intersects BH at point Z such that $BZ = r$. In particular, for B -triangle we have $BH = 2R \cos B = r_b \cos B = r$.
- 7B. I lies in lines C_bA_1 and A_bC_1 , hence $IA_bI_bC_b$ is a rhombus, therefore, the midpoint of A_bC_b coincides with the midpoint B' of II_c .
- 8B. Follows from the solution of 5B.
- 9B. From 5B it follows that the projections of Bb to AB and BC are C_c and A_a , respectively. Hence A_a, B_b, C_c, H_b belong to the circle with diameter BB_b .
- 9C. A_c, B_c, C_c are intersection points of the opposite sidelines and diagonals of the quadrilateral $ACBG_c$ inscribed to Ω . Hence A_c, B_c, C_c are the vertices of a triangle autopolar with respect to Ω .
- 10C. AB passes through the pole C_c of the line A_cB_c , therefore the pole of AB lies in A_cB_c .
- 11C. From $\cos C = \cos A + \cos B$ we obtain that the distance from O to AB equals the sum of distances from O to BC and CA . Points L_a, L_b also satisfy this condition. Now it suffices to note that this linear condition defines a line.
- 12C. It is known that the line L_aL_b is fixed for all triangles with fixed circles Ω and γ_c . For C -triangles this line is a diameter of Ω perpendicular to OI_c . The endpoints of this diameter and I_c are the vertices of an equilateral triangle whose center lies in OI_c and divides the segment OI_c with ratio $1 : 2$.
- 13C. Triangles ABC and H_aH_bC similar with ratio $\cos C$, hence H_aH_b intersects the bisector of the angle C with ratio $\cos C : (1 - \cos C)$. From the property of bisectors and equality $\cos C = \cos A + \cos B$ it is easy to prove that I divides the bisector with the same ratio.

- 14C. The bisector of the angle C is the bisector of the angle OCH_c . Hence it intersects the segment OH_c at a point V with $OV : VH_c = R : CH_c$. The distances from H_c to BC and AC equal $CH_c \cos B$ and $CH_c \cos A$, respectively. From this we obtain that the condition $\cos C = \cos A + \cos B$ holds iff $V = I$.
- 15C. Since O lies in $L_a L_b$, one can reformulate the statement of the problem in the following way: IL_a, IL_b, IO , and the perpendicular from I to OC is a harmonic quadruple of lines. From two previous problems it follows that these lines intersect AB at A, B, H_c , and the common point of AB and $H_a H_b$.
- 16C, 17C. **Hint.** When C moves on Ω L moves on the hyperbola touching the sidelines of all triangles $A_c B_c C_c$.

РЕШЕНИЕ УРАВНЕНИЙ С ИСПОЛЬЗОВАНИЕМ ОДНОГО РАДИКАЛА

представляется Д. Ахтямовым,¹ И. Богдановым,²

А. Глебовым,³ А. Зыкиным,⁴ А. Скопенковым⁵ и Е. Стрельцовой⁶

Этот цикл задач посвящен классическим результатам и методам чистой математики, интересным для информатики (теории символьных вычислений). Основные задачи — 3.3.d, 4.2, 5.5.c, 6.7 и 6.17.bc. В отличие от большинства учебников по этой теме, приводимые задачи и решения не используют термина ‘группа Галуа’ (даже термина ‘группа’). Несмотря на отсутствие этих терминов, идеи приводимых доказательств являются *отправными* для теории Галуа [S09] и конструктивной теории Галуа [E].

Мы приглашаем всех школьников, решающих этот цикл задач, *консультироваться* по поводу возникающих вопросов и идей решения.

Школьники, успешно решающие задачи, смогут получить *дополнительные задачи*. Они смогут выступать со своими результатами на конференциях школьников, например, [M].

Школьник (или команда школьников, работающих вместе над циклом задач) получает „звездочку“ за каждое записанное решение, оцененное в + или +.. Жюри будет также награждать дополнительными „звездочками“ за красивые решения, решения сложных задач и за (некоторые) решения, записанные в TeX-е. „Звездочек“ у жюри бесконечно много. Можно сдавать задачи устно, теряя „звездочку“ за каждую попытку.

Решения задач 1.1.ab, 1.2.ab, 1.4.ab, 1.5.a, 2.1.a''f, 2.3.abcd, 3.1.a, 3.2.a, 4.1.a, 5.1.a, 5.2.a, 5.4.ab будут разобраны на представлении, сдавать их можно только до (зато устно и не тратя звездочек).

Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. Если некоторая задача не получается, то читайте дальше — соседние задачи могут оказаться подсказками.

Через \mathbb{Q} обозначается множество всех рациональных чисел; ‘многочлен с рациональными коэффициентами’ коротко называется многочленом. Многочлен называется *неприводимым* над множеством F , если он не раскладывается в произведение многочленов меньшей степени с коэффициентами в F .

Задачи до промежуточного финиша

1 Решение уравнений 3-й и 4-й степени

1.1. (a) Уравнение $ax^3 + bx^2 + cx + d = 0$ ‘сводится’ к уравнению $x^3 + px + q = 0$ заменой переменной.

(b) Уравнение $ax^4 + bx^3 + cx^2 + dx + e = 0$ ‘сводится’ к уравнению $x^4 + px^2 + qx + s = 0$ заменой переменной.

В следующих двух задачах можно пользоваться без доказательства теоремой о промежуточных значениях многочлена: *для многочлена P и чисел $a < b$, если $P(a) > 0$ и $P(b) < 0$, то существует такое $c \in [a, b]$, что $P(c) = 0$.*

1.2. Сколько (вещественных) решений имеет уравнение

(a) $x^3 + 2x + 7 = 0$? (b) $x^3 - 4x - 1 = 0$?

¹Санкт-Петербургский Государственный Университет

²Московский Физико-Технический Институт

³Новосибирский Государственный Университет

⁴Национальный Исследовательский Университет «Высшая школа экономики»

⁵Поддержан грантом фонда Д. Зимина «Династия». Московский Физико-Технический Институт, Независимый Московский Университет; www.mcsme.ru/~skopenko

⁶Московский Государственный Университет

- 1.3.** (а) При каком условии на p, q уравнение $x^3 + px + q = 0$ имеет ровно два решения?
 (б) Выразите эти два решения через p, q .
 (с) Найдите количество (вещественных) решений уравнения $x^3 + px + q = 0$, в зависимости от параметров p, q .

В этом тексте ‘решить уравнение’ означает ‘найти все его вещественные решения’. (Однако рекомендуем найти также все комплексные.)

- 1.4.** (а) Докажите, что $\sqrt[3]{2 + \sqrt{5}} - \sqrt[3]{\sqrt{5} - 2} = 1$.
 (б) Найдите хотя бы одно решение уравнения $x^3 - 3\sqrt[3]{2}x + 3 = 0$.
Указание. Метод дель Ферро. Так как $(b + c)^3 = b^3 + c^3 + 3bc(b + c)$, то число $b + c$ является корнем уравнения $x^3 - 3bcx - (b^3 + c^3) = 0$.
 (с) Решите уравнение $x^3 - 3\sqrt[3]{2}x + 3 = 0$.
 (д)* Решите уравнение $x^3 - 3x - 1 = 0$.

- 1.5.** (а) Разложите на множители выражение $a^3 + b^3 + c^3 - 3abc$.
 (б) Разложите выражение $a^3 + b^3 + c^3 - 3abc$ на линейные множители с комплексными коэффициентами.

1.6. (а) Сформулируйте и докажите теорему, описывающую все вещественные решения уравнения $x^3 + px + q = 0$ в том случае, когда работает метод дель Ферро (см. задачу 1.4). А при каком условии на p, q применим этот метод, если квадратные корни разрешается извлекать только из положительных чисел?

(б) То же для комплексных решений.

1.7. Решите уравнение (а) $(x^2 + 2)^2 = 18(x - 1)^2$.

(б) $x^4 + 4x - 1 = 0$. (с) $x^4 + 2x^2 - 8x - 4 = 0$. (д) $x^4 - 12x^2 - 24x - 14 = 0$.

Указание к 1.7.б. Метод Феррари. Подберите такие α, b, c , что

$$x^4 + 4x - 1 = (x^2 + \alpha)^2 - (bx + c)^2.$$

Для этого найдите хотя бы одно α , для которого квадратный трехчлен $(x^2 + \alpha)^2 - (x^4 + 4x - 1)$ является полным квадратом. Для этого найдите дискриминант этого квадратного трехчлена. Он является кубическим многочленом от α и называется *кубической резольвентой* многочлена $x^4 + 4x - 1$.

2 Представимость с использованием одного радикала

2.1. Представимо ли следующее число в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$?

- (а) $\sqrt{3 + 2\sqrt{2}}$; (а'') $\frac{1}{7 + 5\sqrt{2}}$; (б) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2}$; (с) $\sqrt[3]{7 + 5\sqrt{2}}$; (д) $\cos(2\pi/5)$;
 (е) $\sqrt[3]{2}$; (ф) $\sqrt{2} + \sqrt[3]{2}$; (г) $\cos(2\pi/9)$; (г)* $\cos(2\pi/7)$; (а') $\sqrt{2 + \sqrt{2}}$.

2.2. Число $\cos(2\pi/9)$ является корнем уравнения $8x^3 - 6x + 1 = 0$.

2.3. Пусть $r \in \mathbb{R} \setminus \mathbb{Q}$ и $r^2 \in \mathbb{Q}$.

(а) *Лемма о неприводимости.* Многочлен $x^2 - r^2$ неприводим над \mathbb{Q} .

(б) *Лемма о линейной независимости.* Если $a, b \in \mathbb{Q}$ и $a + br = 0$, то $a = b = 0$.

(с) Если многочлен имеет корень r , то этот многочлен делится на $x^2 - r^2$.

(д) **Теорема о сопряжении.** Если многочлен имеет корень r , то корнем этого многочлена является также число $-r$.

(е) *Следствие.* Если $a, b \in \mathbb{Q}$ и многочлен имеет корень $a + br$, то корнем этого многочлена является также число $a - br$.

(ф) *Следствие.* Если $a, b \in \mathbb{Q}$ и кубический многочлен имеет корень $a + br$, то он имеет рациональный корень.

2.4. Утверждение. Если многочлен степени выше второй неприводим над \mathbb{Q} , то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

2.5. Представимо ли следующее число в виде $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$?

(a) $\sqrt{3}$; (a') $\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}}$; (b) $\cos(2\pi/9)$; (c) $\sqrt[5]{3}$; (d) $\sqrt[3]{3}$.

(e) наименьший положительный корень уравнения $x^3 - 4x + 2 = 0$.

(f)* единственный вещественный корень уравнения $x^3 - 6x - 6 = 0$.

(g)* единственный вещественный корень уравнения $x^3 - 9x - 12 = 0$.

Обозначим

$$\varepsilon_q := \cos \frac{2\pi}{q} + i \sin \frac{2\pi}{q}.$$

2.6. Пусть $r \in \mathbb{R} \setminus \mathbb{Q}$ и $r^3 \in \mathbb{Q}$.

(a) *Лемма о неприводимости.* Многочлен $x^3 - r^3$ неприводим над \mathbb{Q} .

(b) *Лемма о линейной независимости.* Если $a, b, c \in \mathbb{Q}$ и $a + br + cr^2 = 0$, то $a = b = c = 0$.

(c) Если многочлен имеет корень r , то этот многочлен делится на $x^3 - r^3$.

(d) **Теорема о сопряжении.** Если многочлен имеет корень r , то корнями этого многочлена являются также числа $\varepsilon_3 r$ и $\varepsilon_3^2 r$.

(e) *Следствие.* Если $a, b, c \in \mathbb{Q}$ и многочлен имеет корень $x_0 := a + br + cr^2$, то корнем этого многочлена являются также числа

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{и} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2.$$

(a') *Сильная лемма о неприводимости.* Многочлен $x^3 - r^3$ неприводим над

$$\mathbb{Q}[\varepsilon_3] := \{x + y\varepsilon_3 : x, y \in \mathbb{Q}\}.$$

(b') *Сильная лемма о линейной независимости.* Если $k, l, m \in \mathbb{Q}[\varepsilon_3]$ и $k + lr + mr^2 = 0$, то $k = l = m = 0$.

2.7. Пусть $r \in \mathbb{R} \setminus \mathbb{Q}$ и $a, b, c, r^3 \in \mathbb{Q}$.

(a) *Лемма о рациональности.* Число $a + br + cr^2$ является корнем некоторого ненулевого многочлена степени не выше 3.

(b) **Утверждение.** Если многочлен неприводим над \mathbb{Q} и имеет корень вида $a + br + cr^2 \notin \mathbb{Q}$, то степень многочлена равна 3 и он имеет ровно один вещественный корень.

3 Уравнения 3-й степени, разрешимые за один радикал

Сначала у Чебурашки есть число 1. Сложение имеющихся чисел он совершает бесплатно. То же справедливо для вычитания, умножения и деления на ненулевое число. За один юань Чебурашка извлекает корень любой целой положительной степени из положительного числа, уже полученного в процессе вычислений. Других операций он не делает. Зато он вычисляет числа с абсолютной точностью и имеет неограниченную память.

3.1. (a) Помогите Чебурашке получить за 1 юань число $\sqrt[3]{2} + \sqrt[3]{4}$.

(b) Помогите Чебурашке получить за 2 юаня число $\sqrt[3]{2 + \sqrt{3}} + \sqrt[3]{2 - \sqrt{3}}$.

(c) Помогите Чебурашке получить за 1 юань число $\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}}$, не используя деления, но используя бесплатно все рациональные константы.

3.2. (a) Число можно получить за 1 юань, да так, чтобы корень извлекался второй степени, тогда и только тогда, когда оно имеет вид $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ и $b \geq 0$.

(b) Число можно получить за 1 юань, да так, чтобы корень извлекался третьей степени, тогда и только тогда, когда оно имеет вид $a + br + cr^2$, где $r \in \mathbb{R}$ и $a, b, c, r^3 \in \mathbb{Q}$.

(c) **Теорема о калькуляторе.** Число можно получить за 1 юань тогда и только тогда, когда оно равно $A(r)$ для некоторого многочлена A и $r \in \mathbb{R}$, причем $r^n \in \mathbb{Q}$ для некоторого целого $n \geq 1$.

3.3. (a) Придумайте ненулевые рациональные p и q , для которых один из (вещественных) корней уравнения $x^3 + px + q = 0$ Чебурашка сможет получить за 1 юань.

(a') Придумайте рациональные $p \neq 0$ и q , для которых один из (вещественных) корней уравнения $x^3 + px + q = 0$, не имеющего рациональных корней, Чебурашка сможет получить за 1 юань.

(b3) Сможет ли Чебурашка получить хотя бы один корень уравнения $x^3 + 3x + 6 = 0$ за 3 юаня?

(b2) То же за 2 юаня.

(b1)* То же за 1 юань.

(c) Докажите, что если уравнение 3-й степени с рациональными коэффициентами имеет ровно один вещественный корень, то Чебурашка сможет получить этот корень за 2 юаня.

(d)* **Основная задача.** Как по рациональным p, q узнать, сможет ли Чебурашка получить за 1 юань хотя бы один корень уравнения $x^3 + px + q = 0$?

3.4. * (a) Существует ли кубическое уравнение с рациональными коэффициентами, ни один из корней которого Чебурашка не сможет получить за 2 юаня?

(b) То же для 10000 юаней.

Повторим то же на математическом языке. Рассмотрим калькулятор с кнопками

$$1, +, -, \times, : \text{ и } \sqrt[n]{} \text{ для любого } n.$$

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдает ошибку.

Пусть сначала калькулятор *вещественный*, т.е. оперирует с вещественными числами и при извлечении радикала четной степени из отрицательного числа выдает ошибку.

Строгие (и слегка модифицированные) формулировки задач 3.3.cd и 3.4 следующие.

Утверждение о разрешимости в вещественных радикалах. *Если многочлен 3-й степени с рациональными коэффициентами имеет ровно один вещественный корень, то этот корень можно получить на вещественном калькуляторе.*

Более того, это можно сделать так, чтобы извлечение радикала происходило только два раза, один раз второй и один раз третьей степени.

Теорема о неразрешимости в вещественных радикалах. *Существует многочлен 3-й степени с рациональными коэффициентами (например, $x^3 - 3x + 1$), ни один из корней которого невозможно получить на вещественном калькуляторе.*

Более того, если многочлен 3-й степени с рациональными коэффициентами имеет ровно три вещественных корня, то ни один из них невозможно получить на вещественном калькуляторе.

Если же корней ровно два, то они рациональны (ср. с задачей 1.3.ab).

Вопрос. *Корни каких многочленов 3-й степени с рациональными коэффициентами можно получить на вещественном калькуляторе так, чтобы извлечение радикала происходило только один раз? Существует ли алгоритм распознавания принадлежности многочлена такому классу?*

4 Уравнения 4-й степени, разрешимые за один радикал

Назовем многочлен *k-разрешимым*, если хотя бы один его корень можно получить на вещественном калькуляторе за k извлечений корней.

4.1. (a) Любой ли биквадратный многочлен (4-й степени), имеющий вещественный корень, 2-разрешим?

(b)* Как по рациональным p, s узнать, является ли 1-разрешимым многочлен $x^4 + px^2 + s$?

(c)* Любой ли многочлен 4-й степени, имеющий вещественный корень, 4-разрешим?

4.2. Основная задача. (4, 1) Как по рациональным коэффициентам неприводимого над \mathbb{Q} многочлена $x^4 + px^2 + qx + s = 0$ узнать, является ли он 1-разрешимым?

Существует ли алгоритм распознавания 1-разрешимости?

(4, k) (Решение нам неизвестно.) То же для k -разрешимости, $k \geq 2$.

(n) (Решение для $n \geq 4$ нам неизвестно.) Как по рациональным коэффициентам многочлена узнать, является ли он ∞ -разрешимым?

Существует ли алгоритм распознавания ∞ -разрешимости?

(n, k) (Решение нам неизвестно.) Как по рациональным коэффициентам многочлена n -й степени узнать, является ли он k -разрешимым?

Существует ли алгоритм распознавания k -разрешимости?

4.3. (а) Придумайте рациональные p, q и s , для которых $qs \neq 0$, многочлен $x^4 + px^2 + qx + s$ неприводим над \mathbb{Q} и 1-разрешим.

(б) Является ли 1-разрешимым многочлен $x^4 - 6x^2 + 72x - 99$?

4.4. Если $p < 0$ и кубическая резольвента многочлена $x^4 + px^2 + qx + s$ имеет корень $\alpha \in \mathbb{Q}$, для которого $-p > 2\alpha > p$, то этот многочлен 2-разрешим.

4.5. Если неприводимый над \mathbb{Q} многочлен 4-й степени имеет корень, получаемый на вещественном калькуляторе за одно извлечение радикала 4-й степени, то кубическая резольвента этого многочлена имеет рациональный корень.

4.6. Сформулируйте и докажите аналог теорем о сопряжении 2.3.de и 2.6.de для многочленов 4-й степени.

5 Формульная выразимость в вещественных радикалах

Некоторые идеи и конкретные задачи в §5 заимствованы из [CS, L].

В следующей задаче требуется прежде всего придумать формализацию понятия ‘найти’. Такая формализация приводится после условия. Тем самым Вы на простых примерах нащупаете основное определение (выразимости в радикалах). Само решение не должно представлять для Вас больших проблем.

5.1. (а) Всегда ли можно, зная $x + y$ и xy , найти $x - y$? А x ?

Вот простейшая формализация понятия ‘найти’: *существует ли отображение $f: \mathbb{R}^2 \rightarrow \mathbb{R}$, для которого $f(x + y, xy) = x - y$ при любых $x, y \in \mathbb{R}$?*⁷

(б) Всегда ли можно, зная $x + y + z$, $xy + yz + zx$ и xyz , найти $(x - y)(y - z)(z - x)$? (Формализация аналогична пункту (а).)

Основное определение этого раздела — еще одна формализация понятия ‘найти’.

Многочлен $f \in \mathbb{R}[x_1, \dots, x_n]$ с вещественными коэффициентами **выразим в вещественных радикалах через набор многочленов** $a_1, \dots, a_t \in \mathbb{R}[x_1, \dots, x_n]$, если f можно добавить в этот набор цепочкой операций следующего вида:

- добавить в набор многочлен от уже имеющихся;
- если многочлен из набора равен p^k для некоторых $p \in \mathbb{R}[x_1, \dots, x_n]$ и целого $k > 1$, то добавить в набор многочлен p .

⁷Вот другая формализация понятия ‘найти’, который не используется в дальнейшем: *существует ли такое отображение f из \mathbb{R}^2 в множество $2_{fin}^{\mathbb{R}}$ всех конечных подмножеств множества \mathbb{R} , что $f(x + y, xy) \ni x - y$ при любых $x, y \in \mathbb{R}$?* Поясним, почему этот вопрос (и даже его обобщения на несколько переменных) тривиален.

Отображения $f: \mathbb{R}^2 \rightarrow 2_{fin}^{\mathbb{R}}$ (т.е. вещественные конечнозначные функции) можно задавать формулами. Например, формула $f(x) = \pm x$ является сокращением формулы $f(x) = \{x, -x\}$, задающей (не более, чем) двузначное отображение f . (Подумайте, сколько значное отображение задает формула $f(x) = \frac{\pm x}{\pm x}$.) Обозначим через $f(p, q)$ (конечное) множество (вещественных) решений уравнения $t^2 + pt + q = 0$. Тогда формула $x - y = f(x + y, xy) - f(x + y, xy)$ задает искомое отображение (подумайте, как!).

Например, если уже имеются многочлены $x^2 + 2y$ и $x - y^3$, то первой операцией можно добавить многочлен $-5(x^2 + 2y)^2 + 3(x^2 + 2y)(x - y^3)^6$. А если имеется многочлен $x^2 - 2xy + y^2$, то второй операцией можно добавить многочлены $x - y$ и $y - x$.

5.2. Выразим ли в вещественных радикалах через $x + y$ и xy многочлен

(а) $x - y$? (б) x ?

Ответ к задаче 5.2.б показывает, что корень квадратного уравнения выразим в вещественных радикалах через его коэффициенты. Формализация приведена в задаче 6.17.

5.3. (а, б, с) Представьте

$$x^2 + y^2 + z^2, \quad x^2y + y^2z + z^2x + x^2z + z^2y + y^2x, \quad x^3 + y^3 + z^3$$

в виде многочленов от

$$\sigma_1 := x + y + z, \quad \sigma_2 := xy + yz + zx \quad \text{и} \quad \sigma_3 := xyz.$$

(д) Представляется ли $(x^8y + y^8z + z^8x)(x^8z + z^8y + y^8x)$ в виде многочлена от $\sigma_1, \sigma_2, \sigma_3$?

5.4. (а) Мультистепень произведения многочленов от нескольких переменных равна сумме их мультистепеней.

(б) Многочлен f от двух переменных x, y называется *симметрическим*, если многочлены $f(x, y)$ и $f(y, x)$ равны. Докажите, что любой симметрический многочлен от двух переменных x, y является многочленом от $x + y$ и xy .

(с) Многочлен f от трех переменных x, y, z называется *симметрическим*, если многочлены $f(x, y, z)$, $f(y, z, x)$ и $f(z, x, y)$ равны. Докажите, что любой симметрический многочлен от трех переменных x, y, z является многочленом от σ_1, σ_2 и σ_3 .

(д) Сформулируйте и докажите основную теорему о симметрических многочленах для n переменных.

5.5. Выразим ли в вещественных радикалах через $\sigma_1, \sigma_2, \sigma_3$ многочлен

(а) $(x - y)(y - z)(z - x)$? (б) $x^2y + y^2z + z^2x$? (с)* x ?

Указания и решения для представления

1.1. Воспользуйтесь заменой переменной $y := x + \frac{b}{3a}$ в (а) и $y := x + \frac{b}{4a}$ в (б).

1.2. (а) *Ответ:* 1. Так как многочлен нечетной степени, то корень имеется. Ввиду монотонности корень только один.

(б) *Ответ:* 3. Обозначим $f(x) := x^3 - 4x - 1$. Имеем $f(-2) < 0$, $f(-1) > 0$, $f(0) < 0$, $f(3) > 0$. Значит, по теореме о промежуточных значениях многочлена уравнение имеет три вещественных корня.

1.3. (с) *Указание.* Найдите промежутки возрастания и убывания функции $f(x) := x^3 + px + q$. Найдите точки локальных экстремумов и значения в них. Для этого изучите знак выражения $\frac{f(x_1) - f(x_2)}{x_1 - x_2}$ (или, более учено, продифференцируйте функцию f).

1.4. (б) *Ответ:* $x = -1 - \sqrt[3]{2}$.

Ибо $x^3 - 3\sqrt[3]{2}x + 3 = x^3 - 3bcx + (b^3 + c^3)$, где $b = 1$, $c = \sqrt[3]{2}$.

1.5. (а) При $a = -b - c$ многочлен обращается в ноль. Поделите $a^3 - 3abc + (b^3 + c^3)$ на $a + b + c$ 'уголком'.

2.1. (а'') *Ответ:* да. Ибо $\frac{1}{7 + 5\sqrt{2}} = \frac{7 - 5\sqrt{2}}{7^2 - 2 \cdot 5^2} = -7 + 5\sqrt{2}$.

(ф) *Ответ:* нет.

Пусть, напротив, $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$. Это число является корнем многочлена $P(x) := ((x - \sqrt{2})^3 - 2)((x + \sqrt{2})^3 - 2)$ с рациональными коэффициентами. Применим теорему

о сопряжении 2.3.d к $r = \sqrt{b}$ и многочлену $P(a + t)$ (или применим следствие 2.3.e к $r = \sqrt{b}$ и многочлену $P(t)$). Получим, что $P(a - \sqrt{b}) = 0$. По теореме о рациональных корнях у многочлена P нет рациональных корней. Значит, $b \neq 0$ и корни $a \pm \sqrt{b}$ различны. Но у многочлена P только два вещественных корня: $\sqrt{2} + \sqrt[3]{2}$ и $-\sqrt{2} + \sqrt[3]{2}$. Поэтому $a + \sqrt{b} = \sqrt{2} + \sqrt[3]{2}$ и $a - \sqrt{b} = -\sqrt{2} + \sqrt[3]{2}$. Отсюда $\sqrt[3]{2} = a \in \mathbb{Q}$. Противоречие.

2.3. (а) Если многочлен $x^2 - r^2$ приводим над \mathbb{Q} , то он имеет рациональный корень. Противоречие.

(б) Если $b \neq 0$, то $r = -a/b \in \mathbb{Q}$, что невозможно. Поэтому $b = 0$, откуда $a = 0$.

(с) Поделим многочлен с остатком на $x^2 - r^2$. Подставляя $x = r$, получаем по лемме о линейной независимости (б), что остаток нулевой.

(д) По (с) получаем, что если $R^2 = r^2$, то R есть корень многочлена.

3.1. (а) За 1 юань получаем $\sqrt[3]{2}$, после чего $\sqrt[3]{2} + \sqrt[3]{4} = \sqrt[3]{2} + (\sqrt[3]{2})^2$.

3.2. (а) Ясно, что любое число требуемого вида получить можно. Осталось показать, что все получаемые числа имеют этот вид. Достаточно было бы доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания, умножения и деления. Однако это, естественно, не так. Поэтому мы поступим чуть хитрее.

Пусть $r = \sqrt{s}$ — квадратный корень, полученный за юань (тогда $s \in \mathbb{Q}$). Если $r \in \mathbb{Q}$, то утверждение очевидно, ибо все получающиеся числа рациональны. Пусть это не так. Покажем тогда, что все числа, полученные Чебурашкой, имеют вид $a + br$, где $a, b \in \mathbb{Q}$. Для этого достаточно доказать, что сумма, произведение и частное чисел такого вида имеют тот же вид. Это неочевидно лишь для деления, для которого наше утверждение следует из формулы $\frac{1}{a + br} = \frac{a - br}{a^2 - b^2s}$.

4.1. (а) *Ответ:* да. Так как квадрат любого корня биквадратного многочлена является корнем квадратного многочлена, то этот квадрат получается за одно извлечение корня.

5.1. (а) Рассмотрите пары $x = 1, y = 2$ и $x = 2, y = 1$.

5.2. (а) $(x - y)^2 = (x + y)^2 - 4xy$.

5.4. (б) Индукция по мультистепеням многочлена (с лексикографическим порядком). Для симметрического многочлена f мультистепени (k, l) (т.е. со старшим мономом $ax^k y^l$), $k \geq l$, возьмите многочлен $f - a(x + y)^{k-l}(xy)^l$.

6 Задачи к выдаче на промежуточном финише

1. Решение уравнений 3-й и 4-й степени

6.1. * (а) Сформулируйте и докажите теорему, описывающую все вещественные решения уравнения $x^4 + px^2 + qx + s = 0$. Можно использовать корень α кубической резольвенты.

Указание. Используйте метод Феррари (см. задачу 1.7.b). Не забудьте разобрать все случаи!

(б) То же для комплексных решений.

2. Представимость с использованием одного радикала

6.2. Представимо ли следующее число в виде $a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \dots + a_6\sqrt[7]{2^6}$, где $a_0, a_1, a_2, \dots, a_6 \in \mathbb{Q}$?

(а) $\sqrt[3]{3}$; (б) $\cos \frac{2\pi}{21}$; (б') какой-нибудь из корней многочлена $x^7 - 4x + 2$;

(с) $\sqrt[4]{3}$; (д) $\sqrt[7]{3}$.

Указание. Используйте сформулированные ниже леммы.

6.3. Пусть q простое, $r \in \mathbb{R} \setminus \mathbb{Q}$ и $r^q \in \mathbb{Q}$.

(а) *Лемма о неприводимости.* Многочлен $x^q - r^q$ неприводим над \mathbb{Q} .

(b) *Лемма о линейной независимости.* Если A — многочлен степени меньше q и $A(r) = 0$, то $A = 0$.

(c) **Теорема о сопряжении.** Если многочлен имеет корень r , то он имеет также корни $r\varepsilon_q^k$ для каждого $k = 1, 2, 3, \dots, q-1$.

(d) *Лемма о рациональности.* Если A — многочлен, то число $A(r)$ является корнем некоторого ненулевого многочлена степени не выше q .

Обозначим

$$\mathbb{Q}[\varepsilon_q] := \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \dots + a_{q-2}\varepsilon_q^{q-2} \mid a_0, \dots, a_{q-2} \in \mathbb{Q}\}.$$

6.4. Пусть q простое, $r \in \mathbb{C} \setminus \mathbb{Q}[\varepsilon_q]$ и $r^q \in \mathbb{Q}[\varepsilon_q]$.

(a) Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}[\varepsilon_q]$.

(b,c) Докажите аналоги пунктов (b,c) предыдущей задачи для многочлена с коэффициентами в $\mathbb{Q}[\varepsilon_q]$.

6.5. * Пусть q простое, $r \in \mathbb{R} \setminus \mathbb{Q}$ и $r^q \in \mathbb{Q}$.

(a) *Сильная лемма о неприводимости.* Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}[\varepsilon_q]$.

(b) *Сильная лемма о линейной независимости.* Если A — многочлен степени меньше q с коэффициентами в $\mathbb{Q}[\varepsilon_q]$ и $A(r) = 0$, то $A = 0$.

6.6. (a) **Утверждение.** Если многочлен неприводим над \mathbb{Q} и имеет корень $A(r) \notin \mathbb{Q}$ для некоторых многочлена A и $r \in \mathbb{R}$, причем $r^q \in \mathbb{Q}$ для некоторого простого q , то многочлен имеет степень q , и, при $q \neq 2$, не имеет других вещественных корней.

(b) Верен ли аналог п. (a) с заменой условия простоты числа q на условие $r^2, \dots, r^{q-1} \notin \mathbb{Q}$?

3. Уравнения 3-й степени, разрешимые за один радикал

Обозначим

$$D_{pq} := \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2.$$

За доказательство любой ‘логически нетривиальной’ импликации в следующей теореме на Конференции ставится плюс.

6.7. Теорема. Для кубического уравнения $x^3 + px + q = 0$ с рациональными коэффициентами следующие условия равносильны:

(1-разрешимость) хотя бы один его корень можно получить за одно извлечение радикала;

$(a + br + cr^2)$ оно имеет корень вида $a + br + cr^2$, где $r \in \mathbb{R}$ и $a, b, c, r^3 \in \mathbb{Q}$,

$(\sqrt{D_{pq}} \in \mathbb{Q})$ либо оно имеет рациональный корень, либо $D_{pq} \geq 0$ и $\sqrt{D_{pq}} \in \mathbb{Q}$.

6.8. Если y_0, y_1, y_2 — все комплексные корни многочлена $x^3 + px + q$ (с учетом кратности), то

$$-108D_{pq} = (y_0 - y_1)^2(y_1 - y_2)^2(y_0 - y_2)^2.$$

Для $\mu \in \mathbb{C}$ обозначим

$$\mathbb{Q}[\mu] = \{P(\mu) : P \text{ — многочлен с рациональными коэффициентами}\}.$$

Заметим, что это обозначение согласуется с введенным ранее обозначением $\mathbb{Q}[\varepsilon_q]$.

6.9. Если μ — корень ненулевого многочлена, то $1/t \in \mathbb{Q}[\mu]$ для любого ненулевого $t \in \mathbb{Q}[\mu]$.

6.10. (a) Пусть $r \in \mathbb{R} \setminus \mathbb{Q}$, $\alpha \in \mathbb{Q}[r]$ и $r^n \in \mathbb{Q}$ при некотором целом $n > 1$. Тогда существует такое натуральное k , что $\alpha \in \mathbb{Q}[r^k]$ и $r^k \in \mathbb{Q}[\alpha]$ (т.е. что $\mathbb{Q}[r^k] = \mathbb{Q}[\alpha]$).

(b) **Утверждение.** Если многочлен степени n неприводим над \mathbb{Q} и 1-разрешим, то он имеет корень $A(r)$ для некоторых многочлена A и числа $r \in \mathbb{R}$ такого, что $r^n \in \mathbb{Q}$.

Комплексный калькулятор имеет те же кнопки, что и вещественный, но оперирует с комплексными числами и при нажатии кнопки $\sqrt{}$ выдает все значения корня. На комплексном калькуляторе *можно получить число*, если на нем можно получить множество чисел, содержащих заданное число.

Назовем многочлен *комплексно k -разрешимым*, если хотя бы один его корень можно получить на комплексном калькуляторе за k извлечений корней. Основную задачу 4.2 (и другие задачи) интересно решать и для комплексной k -разрешимости. Часто комплексные версии оказываются проще.

- 6.11.** (а) Любой кубический многочлен комплексно 2-разрешим.
 (б) Как по p, q узнать, является ли комплексно 1-разрешимым многочлен $x^3 + px + q$?
 (с) Любой многочлен 4-й степени комплексно 4-разрешим.

4. Уравнения 4-й степени, разрешимые за один радикал

6.12. Теорема о сопряжении. Пусть $a, b, c, d, r^4 \in \mathbb{Q}$, $r^2 \notin \mathbb{Q}$ и число $x_0 := a + br + cr^2 + dr^3$ является корнем некоторого многочлена. Тогда корнями этого многочлена являются также числа

$$x_1 := a + bri - cr^2 - dr^3i, \quad x_2 := a - br + cr^2 - dr^3, \quad x_3 := a - bri - cr^2 + dr^3i.$$

6.13. Пусть многочлен 4-й степени (с нулевым коэффициентом при x^3) имеет комплексные корни y_0, y_1, y_2, y_3 с учетом кратности. Тогда

- (а) $\frac{y_0y_1 + y_2y_3}{2}$ — корень его кубической резольвенты.⁸
 (б) $\frac{y_0y_1 + y_2y_3}{2}, \frac{y_0y_2 + y_1y_3}{2}, \frac{y_0y_3 + y_1y_2}{2}$ — все комплексные корни его кубической резольвенты с учетом кратности.

6.14. Пусть $p, q, s \in \mathbb{Q}$ и $p < 0 < q$.

- (а) Если $q^2 = 2p(4s - p^2)$ и $\sqrt{2q} \in \mathbb{Q}$, то многочлен $x^4 + px^2 + qx + s$ имеет корень, получаемый на вещественном калькуляторе за одно извлечение корня четвертой степени.
 (б) Верно ли обратное?

5. Формульная выразимость в вещественных радикалах

Ответ ‘нет’ к задаче 5.5.с (и задача 6.17.б ниже) показывают, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты*. Подумайте, почему этот результат не противоречит формуле Кардано, выражающей корень кубического уравнения через его коэффициенты (ключ к ответу — выражение дискриминанта через корни из задачи 6.8).

Многочлен f от переменных x_1, x_2, \dots, x_n называется **циклически симметричным**, если многочлены $f(x_1, x_2, \dots, x_n)$ и $f(x_2, x_3, \dots, x_{n-1}, x_n, x_1)$ равны.

6.15. Выразите $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ в радикалах через некоторые циклически симметричные многочлены от x_1, x_2, \dots, x_{10} .

Ответ ‘нет’ к задаче 5.5.с вытекает из следующей задачи.

⁸Напомним, что кубическая резольвента $R_f(\alpha)$ многочлена $f(x) = x^4 + px^2 + qx + s$ — это многочлен от переменной α , являющийся дискриминантом квадратного трехчлена $(x^2 + \alpha)^2 - f(x)$ (относительно переменной x), то есть

$$R_f(\alpha) = q^2 - 4(2\alpha - p)(\alpha^2 - s) = -8\alpha^3 + 4p\alpha^2 + 8s\alpha + (q^2 - 4ps).$$

6.16. Пусть $f, g \in \mathbb{R}[x, y, z]$.

(а) Если для некоторого целого $q > 0$ многочлен f^q циклически симметричен, то f циклически симметричен.

(б) Если $fg = 0$, то $f = 0$ или $g = 0$.

(с) $f^2 + fg + g^2 \neq 0$, если $fg \neq 0$.

6.17. Общее уравнение n -й степени разрешимо в вещественных радикалах, если существуют

- неотрицательные целые числа s, k_1, \dots, k_s и
- многочлены p_0, p_1, \dots, p_s с вещественными коэффициентами и от $n, n+1, \dots, n+s$ переменных, соответственно, такие, что если $a_0, \dots, a_{n-1}, x \in \mathbb{R}$ и

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0,$$

то существуют $f_1, \dots, f_s \in \mathbb{R}$, для которых

$$f_1^{k_1} = p_0(a_0, \dots, a_{n-1}), \quad f_2^{k_2} = p_1(a_0, \dots, a_{n-1}, f_1), \quad \dots$$

$$\dots \quad f_s^{k_s} = p_{s-1}(a_0, \dots, a_{n-1}, f_1, \dots, f_{s-1}), \quad x = p_s(a_0, \dots, a_{n-1}, f_1, \dots, f_s).$$

Обратите внимание, что мы определили свойство числа n (а не конкретного уравнения с заданными коэффициентами, как в *теореме Галуа* [S]).

(а) Общее уравнение 2-й степени разрешимо в вещественных радикалах.

(б)* Общее уравнение 3-й степени не разрешимо в вещественных радикалах

(с)* То же самое для всех $n \geq 3$.

Результат задач 5.5.с и 6.17.б (а также его сравнение с формулой Кардано) показывает, что определение выразимости в вещественных радикалах не совсем удачно формализует идею разрешимости в радикалах. С одной стороны, вместо вещественных чисел разумнее рассматривать комплексные [S']. С другой стороны, вместо работы с многочленами можно работать с числами — это приводит к теореме Галуа [S]. Однако на примере этой не совсем удачной формализации Вы увидите идею доказательства теоремы Руффини, см. [S'].

Указания и решения к выдаче на промежуточном финише

1. Решение уравнений 3-й и 4-й степени

1.3. Ответ. Если $p = q = 0$, то корень один. Иначе при $D_{pq} > 0$ корень один, при $D_{pq} = 0$ корней два, при $D_{pq} < 0$ корней три.

1.4. (с) Ответ: $x = -1 - \sqrt[3]{2}$.

В силу задачи 1.5.а уравнение $x^3 - 3\sqrt[3]{2}x + 3 = 0$ равносильно уравнению

$$(x + b + c)(x^2 + b^2 + c^2 - bc - bx - cx) = 0 \quad \text{с} \quad b = 1 \quad \text{и} \quad c = \sqrt[3]{2}.$$

(д) **Ответ:** $x \in \{2 \cos \frac{\pi}{9}, 2 \cos \frac{7\pi}{9}, 2 \cos \frac{13\pi}{9}\}$.

Заменой $x := 2y$ уравнение $x^3 - 3x - 1 = 0$ сводится к уравнению $4y^3 - 3y = \frac{1}{2}$. Используя тождество $\cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha$, получаем, что числа $\cos \frac{\pi}{9}, \cos \frac{7\pi}{9}, \cos \frac{13\pi}{9}$ являются корнями уравнения $4y^3 - 3y = \frac{1}{2}$.

1.5. (а,б) Ответ:

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca) = (a + b + c)(a + b\varepsilon_3 + c\varepsilon_3^2)(a + b\varepsilon_3^2 + c\varepsilon_3).$$

1.6. (а) Ответ: метод дель Ферро применим, когда $D_{pq} \geq 0$.

Теорема. Пусть $p, q \in \mathbb{R}$. Если $D_{pq} > 0$, то уравнение $x^3 + px + q = 0$ имеет единственный вещественный корень

$$\sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}} - \sqrt[3]{\frac{q}{2} + \sqrt{D_{pq}}}.$$

Если $D_{pq} = 0$, то все вещественные корни уравнения $x^3 + px + q = 0$ — это $-2\sqrt[3]{q/2}$ и $-\sqrt[3]{q/2}$ (они различны при $q \neq 0$).

(b) **Теорема.** Пусть $p, q \in \mathbb{C}$ и $pq \neq 0$. Обозначим через

- $\sqrt{D_{pq}}$ любое из двух значений квадратного корня из D_{pq} ;
- и любое из трех значений кубического корня из $-\frac{q}{2} - \sqrt{D_{pq}}$;
- $v := -\frac{p}{3u}$. (Так как $p \neq 0$, то $(q/2)^2 \neq D_{pq}$, откуда $u^3 = -\frac{q}{2} - \sqrt{D_{pq}} \neq 0$.)

Тогда все корни уравнения $x^3 + px + q = 0$ — числа $u + v$, $u\varepsilon_3 + v\varepsilon_3^2$, $u\varepsilon_3^2 + v\varepsilon_3$ (они не обязательно различны при $q \neq 0$).

1.7. Ответы: (a) $\frac{-3\sqrt{2} \pm \sqrt{10 + 12\sqrt{2}}}{2}$; (b) $\frac{-\sqrt{2} \pm \sqrt{4\sqrt{2} - 2}}{2}$; (c) $\frac{\sqrt{2} \pm \sqrt{8\sqrt{2} - 6}}{2}$;
(d) $\sqrt{2} \pm (\sqrt[4]{2} + \sqrt[4]{8})$.

2. Представимость с использованием одного радикала

2.1. Ответы: (a, a'', b, c, d) да, (a', e, f, g, h) нет.

(a, c) $\sqrt{3 + 2\sqrt{2}} = \sqrt[3]{7 + 5\sqrt{2}} = 1 + \sqrt{2}$.

(a'') Имеем $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$. (Это равенство несложно найти методом неопределенных коэффициентов или при помощи алгоритма Евклида для многочленов $x^3 - 2$ и $x^2 + 5x + 1$, см. решение задачи 3.2.b.) Поэтому

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(b) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(d) $\cos(2\pi/5) = (\sqrt{5} - 1)/4$.

(e) Пусть представимо. Тогда $2 = (\sqrt[3]{2})^3 = (a^3 + 3ab) + (3a^2 + b)\sqrt{b}$. Так как $3a^2 + b \neq 0$, то $\sqrt{b} \in \mathbb{Q}$. Значит, $\sqrt[3]{2} \in \mathbb{Q}$ — противоречие.

Другие способы — аналогично пунктам (f, g) или утверждению 2.4.

(g) Пусть представимо. По задаче 2.2 число $\cos(2\pi/9)$ является корнем уравнения $4x^3 - 3x = -\frac{1}{2}$. По следствию 2.3.f это уравнение имеет рациональный корень. Противоречие.

Другой способ — аналогично утверждению 2.4.

2.2. По формуле косинуса тройного угла $-1/2 = \cos(2\pi/3) = 4\cos^3(2\pi/9) - 3\cos(2\pi/9)$.

2.3. (e) Обозначим через P многочлен из условия и $G(t) := P(a + bt)$. Тогда $G(r) = 0$. Значит, по пункту (d) $G(-r) = 0$.

(f) Следует из пункта (e) и теоремы Виета.

2.4. Пусть, напротив, данный многочлен P имеет корень $x_0 = a \pm \sqrt{b}$. По следствию 2.3.e и аналогично ему корнем многочлена P является также число $x_1 = a \mp \sqrt{b}$. При $b = 0$ утверждение очевидно. Поэтому считаем, что $b \neq 0$. Тогда $x_0 \neq x_1$. Поэтому $P(x)$ делится на $(x - a)^2 - b$. Так как $\deg P > 2$, то P приводим. Противоречие.

2.5. Ответы: (a, b, c, d, e, g) нет, (f) да.

Обозначим $r := \sqrt[3]{2}$.

(a) *Первое решение.* Пусть представимо. Тогда

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Так как многочлен $x^3 - 2$ не имеет рациональных корней, то он неприводим над \mathbb{Q} . Значит, $2ab + 2c^2 = 2ac + b^2 = 0$ (ср. 2.6.b). Поэтому $b^3 = -2abc = 2c^3$. Тогда либо $b = c = 0$, либо $\sqrt[3]{2} = b/c$. Оба случая невозможны.

Второе решение. Пусть представимо. Обозначим $P(x) := x^2 - 3$. По следствию 2.6.e P имеет три корня x_0, x_1, x_2 , введенных в формулировке следствия. Так как ни один из них не рационален, то $b = c = 0$ невозможно. Значит, по сильной лемме о линейной независимости 2.6.b' эти корни различны. Противоречие.

(b) Пусть представимо. Число $\cos(2\pi/9)$ является корнем уравнения $4x^3 - 3x = -\frac{1}{2}$. Два других его вещественных корня есть $\cos(8\pi/9)$ и $\cos(4\pi/9)$.

По следствию 2.6.e многочлен $8x^3 - 6x - 1$ имеет три корня x_0, x_1, x_2 , введенных в формулировке следствия. Так как ни один из них не рационален, то $b = c = 0$ невозможно. Значит, по сильной лемме о линейной независимости 2.6.b' эти корни различны.

Так как $\bar{\varepsilon}_3 = \varepsilon_3^2$, то $\bar{x}_2 = x_1$. Значит, x_2 и x_1 не могут быть вещественными и различными. Противоречие.

(c) Пусть представимо. По задаче 2.7.a, некоторый кубический многочлен имеет корень $a + br + cr^2$. Противоречие с неприводимостью многочлена $x^5 - 3$ над \mathbb{Q} .

2.6. (a) Если многочлен $x^3 - r^3$ приводим над \mathbb{Q} , то он имеет рациональный корень. Противоречие.

(b) Предположим противное. Поделим $x^3 - r^3$ на $a + bx + cx^2$ с остатком. По (a) остаток ненулевой. Оба многочлена $x^3 - r^3$ и $a + bx + cx^2$ имеют корень $x = r$. Значит, остаток имеет корень $x = r$. Значит остаток первой степени и имеет иррациональный корень. Противоречие.

(c) Поделим многочлен с остатком на $x^3 - r^3$. Подставляя $x = r$, получаем по лемме о линейной независимости (b), что остаток нулевой.

(d) По пункту (c) получаем, что если $R^3 = r^3$, то R есть корень многочлена.

(e) Обозначим через P многочлен из условия и $G(t) := P(a + bt + ct^2)$. Тогда $G(r) = 0$. Значит, по пункту (d) $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(a') Если приводим, то один из его корней лежит в $\mathbb{Q}[\varepsilon_3]$. Тогда $r \in \mathbb{Q}[\varepsilon_3] \cap \mathbb{R} = \mathbb{Q}$. Противоречие.

Это утверждение также следует из пункта (b').

(b') Рассмотрите вещественную и мнимую части.

Это утверждение также следует из пункта (a').

2.7. (a) *Первое решение.* Достаточно доказать утверждение для $a = 0$. Для числа $t = br + cr^2$ выполнено $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

(Иными словами, ввиду равенства из решения задачи 1.5.a число $a + br + cr^2$ является корнем многочлена $(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6$.)

Второе решение. Обозначим $x_0 = a + br + cr^2$. Разложим числа x_0^k при $k = 0, 1, 2, 3$ по степеням числа r :

$$x_0^k = a_k + b_k r + c_k r^2.$$

Чтобы решить задачу, достаточно найти числа $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$, не все из которых равны нулю, такие, что $\lambda_0 + \lambda_1 x_0 + \lambda_2 x_0^2 + \lambda_3 x_0^3 = 0$. Для этого достаточно, чтобы эти числа удовлетворяли системе уравнений

$$\begin{cases} \lambda_0 a_0 + \dots + \lambda_3 a_3 = 0 \\ \lambda_0 b_0 + \dots + \lambda_3 b_3 = 0 \\ \lambda_0 c_0 + \dots + \lambda_3 c_3 = 0 \end{cases} .$$

Как известно, однородная (т.е. с нулевыми правыми частями) система линейных уравнений с рациональными коэффициентами, в которой уравнений меньше, чем переменных, всегда имеет нетривиальное рациональное решение. Значит, требуемые числа найдутся.

(То, что полученный многочлен имеет степень ровно 3, получается из задач 2.6.eb'.)

Еще одно решение приведено в качестве первого доказательства леммы о рациональности 6.3.d.

3. Уравнения 3-й степени, разрешимые за один радикал

3.1. (b) Число $\sqrt[3]{2 + \sqrt{3}}$ получается за два юаня. Осталось заметить, что

$$\sqrt[3]{2 - \sqrt{3}} = \frac{1}{\sqrt[3]{2 + \sqrt{3}}} = (\sqrt[3]{2 + \sqrt{3}})^2 \cdot (2 - \sqrt{3}).$$

(Последнее равенство позволяет даже обойтись без деления на иррациональные числа.)

(c) См. решение задачи 2.1.a''.

3.2. (b) Ясно, что любое описанное число можно получить за юань. Для доказательства обратного утверждения, аналогично предыдущему пункту мы показываем, что все числа, полученные Чебурашкой, имеют вид $a + br + cr^2$, где $r = \sqrt[3]{s}$ — кубический корень, на который был потрачен трудовой юань. Сейчас, правда, несколько сложнее показать, что число $\frac{1}{a + br + cr^2}$ имеет требуемый вид (в случае, когда $r = \sqrt[3]{s} \notin \mathbb{Q}$). Покажем же это.

По лемме о неприводимости, многочлен $x^3 - r^3$ неприводим над \mathbb{Q} , а значит, взаимно прост с многочленом $a + bx + cx^2$. Поэтому существуют многочлены g и h , для которых $h(x)(a + bx + cx^2) + g(x)(x^3 - r^3) = 1$. Тогда $h(r) = \frac{1}{a + br + cr^2}$, откуда и следует требуемое.

3.3. (a) Например, годится уравнение $x^3 - 3x + 2 = 0$, корнем которого является число 1.

(a') Например, годится уравнение $x^3 - 6x - 6 = 0$, корнем которого является число $\sqrt[3]{2} + \sqrt[3]{4}$ (из задачи 3.1.b). Это уравнение можно получить, например, аналогично доказательству леммы о рациональности 2.7.a.

(b3, b2) *Ответы:* да.

Методом дель Ферро получаем, что одним из корней уравнения является число

$$\sqrt[3]{-3 + \sqrt{10}} + \sqrt[3]{-3 - \sqrt{10}} = \sqrt[3]{-3 + \sqrt{10}} - \frac{1}{\sqrt[3]{-3 + \sqrt{10}}}.$$

(b1) Отрицательный ответ следует из решения пункта (d), т.е. из теоремы 6.7.

(c) Согласно задаче 1.1.a, можно считать, что уравнение имеет вид $x^3 + px + q = 0$. Если $p = 0$, утверждение очевидно. Иначе, поскольку уравнение имеет ровно один вещественный корень, из решения задачи 1.3 следует, что $D_{pq} > 0$. Значит, число $u = \sqrt[3]{-\frac{q}{2} - \sqrt{D_{pq}}}$ из теоремы в решении задачи 1.6.a получается за два юаня. После этого число $v = \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}} = -\frac{p}{3u}$ получается бесплатно. Значит, и корень исходного уравнения, равный $u + v$ по вышеупомянутой теореме, получается за два юаня.

(d) См. теорему 6.7.

4. Уравнения 4-й степени, разрешимые за один радикал

4.1. (b) Можно выразить корень x_0 многочлена через p и s , а затем приравнять x_0 к $br + cr^2 + dr^3$, где $b, c, d, r^4 \in \mathbb{Q}$, $r \in \mathbb{R}$.

(c) *Гипотеза:* нет. Попробуйте доказать, что уравнение 4-й степени, резольвента которого имеет ровно три вещественных корня (или отрицательный *дискриминант*), не является 10000-разрешимым. Формула для нахождения корня уравнения 4-й степени, резольвента которого имеет не более двух различных вещественных корней (или неотрицательный дискриминант), за четыре извлечения корня, является целью задачи 6.1.a.

- 4.3.** (a) Например, многочлен $x^4 - 12x^2 - 24x - 14$ из задачи 1.7.d имеет корень $\sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$. (Поймите, как построить этот многочлен по его корню!)
 (b) Да, согласно задаче 6.14.a.

5. Формульная выразимость в вещественных радикалах

- 5.1.** (b) Рассмотрите тройки $x = 0, y = 1, z = -1$ и $x = 0, y = -1, z = 1$.

5.2. (b) $x = \frac{x + y + (x - y)}{2}$.

- 5.3.** Ответы: (a) $\sigma_1^2 - 2\sigma_2$; (b) $\sigma_1\sigma_2 - 3\sigma_3$; (c) $\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.
 (d) Используйте 5.4.c.

5.4. (c) Индукция по мультистепени многочлена (с лексикографическим порядком). Для симметрического многочлена f мультистепени (k, ℓ, m) (т.е. со старшим мономом $ax^k y^\ell z^m$), $k \geq 1$, возьмите многочлен $f - a\sigma_1^{k-\ell}\sigma_2^{\ell-m}\sigma_3^m$.

5.5. (a) $(x - y)^2(y - z)^2(z - x)^2$ — симметрический многочлен. Пункт (a) можно также свести к (b).

(b) Обозначим $M = x^2y + y^2z + z^2x$ и $N = y^2x + x^2z + z^2y$. Тогда многочлены $M + N$ и MN симметрические. Значит, они являются многочленами от элементарных симметрических многочленов $\sigma_1, \sigma_2, \sigma_3$. (Конкретное выражение приведено в решении задачи 6.8.) Само же M выражается через $M + N$ и MN по формуле корней квадратного уравнения.

Указания и решения к выдаче на финише

1. Решение уравнений 3-й и 4-й степени

1.6. Доказательство теоремы из п. (a). Обозначим $u := -\sqrt[3]{\frac{q}{2} + \sqrt{D_{pq}}}$ и $v := \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}}$. Имеем $uv = -p/3$ и $u^3 + v^3 = -q$. Значит, по формуле из решения задачи 1.5.a для $a = x$, $b = -u$, $c = -v$ число $u + v$ является корнем многочлена $x^3 + px + q = x^3 - 3uvx - u^3 - v^3$. Так как $2(x^2 + u^2 + v^2 - xu - xv - uv) = (x - u)^2 + (x - v)^2 + (u - v)^2$, то при $D_{pq} > 0$ других корней нет, а при $D_{pq} = 0$ есть еще один корень $u = v = -\sqrt[3]{q/2}$.

Доказательство теоремы из п. (b). Имеем $uv = -p/3$ и $u^3 + v^3 = -q$. Значит, теорема верна по формуле из решения задачи 1.5.b для $a = x$, $b = -u$, $c = -v$.

6.1. Если $q = 0$, то уравнение биквадратное и решается легко. Будем считать, что $q \neq 0$.

(a) **Теорема.** Пусть $p, q, s \in \mathbb{R}$ и $q \neq 0$. Тогда существует $\alpha > p/2$, для которого $q^2 = 4(2\alpha - p)(\alpha^2 - s)$. Для любого такого α обозначим $A := \sqrt{2\alpha - p}$. Тогда все вещественные корни уравнения $x^4 + px^2 + qx + s = 0$ —

$$\begin{cases} \text{нет корней,} & 2\alpha + p > 2|q|/A; \\ x_{\pm} := \left(-A \pm \sqrt{-2\alpha - p + \frac{2q}{A}}\right) / 2, & -2q/A < 2\alpha + p \leq 2q/A; \\ y_{\pm} := \left(A \pm \sqrt{-2\alpha - p - \frac{2q}{A}}\right) / 2, & 2q/A < 2\alpha + p \leq -2q/A; \\ x_{\pm}, y_{\pm}, & 2\alpha + p \leq -2|q|/A. \end{cases}$$

Доказательство. Обозначим $R(x) := 4(2x - p)(x^2 - s) - q^2$. Тогда $R(p/2) = -q^2 < 0$. При достаточно больших x имеем $R(x) > 0$. Значит, по теореме о промежуточных значениях многочлена существует $\alpha > p/2$, для которого $R(\alpha) = 0$.

Так как $p = 2\alpha - A^2$ и α — корень резольвенты, то $s = \alpha^2 - \frac{q^2}{4(2\alpha - p)} = \alpha^2 - \frac{q^2}{4A^2}$. Тогда

$$x^4 + px^2 + qx + s = \left(x^2 - Ax + \alpha + \frac{q}{2A}\right) \left(x^2 + Ax + \alpha - \frac{q}{2A}\right).$$

Теперь, решая 2 квадратных уравнения, получаем требуемые формулы.

(b) **Теорема.** Пусть $p, q, s \in \mathbb{C}$ и $q \neq 0$. Обозначим через α любой корень уравнения $q^2 = 4(2\alpha - p)(\alpha^2 - s)$. Обозначим через A любое из значений квадратного корня из $2\alpha - p$. Тогда все корни уравнения $x^4 + px^2 + qx + s = 0$ —

$$\left(A + \sqrt{-2\alpha - p - \frac{2q}{A}} \right) / 2 \quad \text{и} \quad \left(-A + \sqrt{-2\alpha - p + \frac{2q}{A}} \right) / 2,$$

где \sqrt{y} — многозначная функция, выдающая оба значения корня из y ; поскольку $q^2 = 4A^2(\alpha^2 - s) \neq 0$, то $A \neq 0$.

Доказательство аналогично доказательству теоремы из п. (a).

Замечание. Все комплексные корни этого уравнения — это

$$\pm \sqrt{2\alpha_1 - p} \pm \sqrt{2\alpha_2 - p} \pm \sqrt{2\alpha_3 - p},$$

где $\alpha_1, \alpha_2, \alpha_3$ — все корни кубической резольвенты, число минусов четно, а значения корней выбираются так, что их произведение равно $-q$.

2. Представимость с использованием одного радикала

2.1. (a') Пусть представимо. Корнями многочлена $P(x) := (x^2 - 2)^2 - 2$ являются 4 числа $\pm \sqrt{2 \pm \sqrt{2}}$, где знаки $+$ и $-$ не обязательно согласованы. Несложно проверить, что $P(x)$ не имеет рациональных корней, и что произведение любых двух корней многочлена $P(x)$ иррационально. Значит, $P(x)$ неприводим над \mathbb{Q} . Теперь из утверждения 2.4 получаем противоречие.

(h) (И. Брауде-Золотарев) Из равенства $1 + \varepsilon_7 + \varepsilon_7^2 + \dots + \varepsilon_7^6 = 0$ получаем $\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) = -1/2$. Используя формулы для $\cos 2\alpha$ и $\cos 3\alpha$, получаем, что число $\cos(2\pi/7)$ является корнем уравнения $8t^3 + 4t^2 - 4t - 1 = 0$. Заменим $u = 2t$, получим $u^3 + u^2 - 2u - 1 = 0$. Это уравнение не имеет рациональных корней. Значит, уравнение $8t^3 + 4t^2 - 4t - 1 = 0$ тоже. Значит, по задаче 2.3.f получаем ответ.

2.5. (d) Обозначим $r := \sqrt[3]{2}$. Аналогично (a), (b) получаем, что комплексные корни многочлена $x^3 - 3$ есть числа x_0, x_1, x_2 , введенные в формулировке следствия 2.6.e. Поэтому $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$ для некоторого $s \in \{1, 2\}$. Отсюда по сильной лемме о линейной независимости 2.6.b' $a = 0$ и $bc = 0$. Поэтому либо $\sqrt[3]{3} = br$, либо $\sqrt[3]{3} = cr^2$. Противоречие.

(e) Аналогично (b).

(f) Это уравнение имеет корень $\sqrt[3]{2} + \sqrt[3]{4}$.

(g) Единственный вещественный корень этого уравнения — $\sqrt[3]{3} + \sqrt[3]{9}$. Пусть, напротив, это число выражается в требуемом виде. Тогда по следствию 2.6.e корнями данного уравнения являются числа x_0, x_1, x_2 , введенные в формулировке следствия 2.6.e. По сильной лемме о линейной независимости 2.6.b' эти корни различны. Значит, это все корни данного уравнения. С другой стороны, по теореме из решения задачи 1.6.b все корни данного уравнения —

$$y_0 := \sqrt[3]{3} + \sqrt[3]{9}, \quad y_1 := \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_2 := \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

Поскольку данное уравнение имеет ровно один вещественный корень, то $x_0 = y_0$ и либо $x_1 = y_1, x_2 = y_2$, либо, наоборот, $x_2 = y_1, x_1 = y_2$.

Обозначим $P(x) := \sqrt[3]{3}x + \sqrt[3]{9}x^2$. Обозначим $S(x) := a + brx + cr^2x^2$ и $S(x) := a + brx^2 + cr^2x$ для первого и второго случая, соответственно. Тогда многочлен $P(x) - S(x)$ имеет 3 различных корня $1, \varepsilon_3, \varepsilon_3^2$. Но его степень не выше второй. Поэтому $P = S$. Значит, $\sqrt[3]{3} = br$ или $\sqrt[3]{3} = cr^2$. Противоречие.

2.7. (b) По лемме о рациональности 2.7.a существует многочлен степени не выше 3 с корнем $a + br + cr^2$. Из этого и неприводимости над \mathbb{Q} данного многочлена P получаем, что $\deg P \leq 3$. По следствию 2.6.e многочлен P имеет три корня x_0, x_1, x_2 , введенных в формулировке следствия. Так как P неприводим над \mathbb{Q} , то ни один из корней не рационален, поэтому $b = c = 0$ невозможно. Значит, по сильной лемме о линейной независимости 2.6.b' эти корни различны. Значит, $\deg P = 3$.

Так как $\varepsilon_3^k = \varepsilon_3^{-k}$, то $\overline{x_2} = x_1$. Значит, x_2 и x_1 не могут быть вещественными и различными. Значит, $x_2, x_1 \in \mathbb{C} \setminus \mathbb{R}$. Поэтому P имеет ровно один вещественный корень.

6.2. *Ответы: не представимы.* Обозначим $r := \sqrt[7]{2}$ и $A(x) := a_0 + a_1x + a_2x^2 + \dots + a_6x^6$.

(a) Пусть представимо. Тогда по теореме о сопряжении 6.3.c многочлен $x^2 - 3$ имеет корни $A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \dots, 6$. Так как этот многочлен не имеет рациональных корней, то по сильной лемме о линейной независимости 6.5.b эти корни попарно различны. Противоречие.

(b') Пусть представимо. Данный многочлен P не имеет рациональных корней. Тогда по теореме о сопряжении 6.3.c и сильной лемме о линейной независимости 6.5.b P имеет попарно различные корни $x_k := A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \dots, 6$. Так как $P(0) > 0$, $P(1) < 0$ и $P(2) > 0$, то P имеет вещественный корень x_k , отличный от x_0 . Имеем $\varepsilon_7^k = \varepsilon_7^{-k}$. Поэтому $x_k = \overline{x_k} = x_{7-k}$. Противоречие.

(b) Пусть представимо. Обозначим через P многочлен, для которого $\cos 7x = P(\cos x)$ (докажите, что он существует!). Корнями многочлена $2P(x) + 1$ являются вещественные числа $y_k := \cos \frac{2(3k+1)\pi}{21}$ при $k = 0, \dots, 6$. Одно из них, а именно $y_2 = -1/2$, рационально.

Докажем, что число y_0 иррационально.

(Действительно, иначе $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$ влечет $\varepsilon_{21} = a + i\sqrt{b}$ для некоторых $a, b \in \mathbb{Q}$. Тогда и число $\varepsilon_7 = \varepsilon_{21}^3$ тоже выражается в таком виде. Но ε_7 является корнем неприводимого⁹ многочлена $1 + x + \dots + x^6$, что противоречит аналогу утверждения 2.4 для чисел вида $a + i\sqrt{b}$.)

Итак, наше число y_0 иррационально и является корнем многочлена $\frac{2P(x) + 1}{x - y_2}$ степени 6. Но тогда по теореме о сопряжении 6.3.c и сильной лемме о линейной независимости 6.5.b этот многочлен имеет семь попарно различных корней, что невозможно.

(c) Пусть представимо. Тогда из леммы о рациональности 6.3.d получаем, что существует ненулевой многочлен степени не выше седьмой с корнем $\sqrt[11]{3}$. Противоречие с неприводимостью многочлена $x^{11} - 3$ над \mathbb{Q} .

(d) Пусть представимо. Аналогично (a), (b') получаем, что комплексные корни многочлена $x^7 - 3$ есть $A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \dots, 6$. Поэтому $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ для некоторого $s \in \{1, 2, 3, 4, 5, 6\}$. Отсюда по сильной лемме о линейной независимости 6.5.b получаем $a_k = 0$ для любого $k \neq s$. Поэтому $\sqrt[7]{3} = a_s r^s$. Противоречие.

6.3. (a) Все корни многочлена $x^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$. Пусть он приводим над \mathbb{Q} . Модуль свободного члена одного из унитарных сомножителей разложения рационален и равен произведению модулей некоторых k из этих корней, $0 < k < q$. Значит, $r^k \in \mathbb{Q}$. Так как q простое, то $kx + qy = 1$ для некоторых целых x, y . Тогда $r^{kx} = r(r^q)^{-y}$, откуда $r \in \mathbb{Q}$. Противоречие.

(b) Предположим противное. Рассмотрим многочлен $A(x)$ наименьшей степени, для которого лемма не выполняется. Поделим $x^q - r^q$ на $A(x)$ с остатком $R(x)$. Тогда $\deg R < \deg A$, $R(r) = 0$ и, по пункту (a), $R(x)$ ненулевой. Противоречие с выбором A .

(c) Аналогично задачам 2.3.cd, 2.6.cd и 6.12. Используйте (b).

⁹Неприводимость многочлена $g(x) = 1 + x + \dots + x^6$ можно показать, например, применив признак Эйзенштейна к многочлену $g(x+1)$. Впрочем, здесь достаточно доказать, что у него нет рациональных делителей степени 1 и 2.

(d) *Первое решение.* Произведение

$$(x - A(x_0))(x - A(x_1)) \dots (x - A(x_{q-1}))$$

является симметрическим многочленом от x_0, x_1, \dots, x_{q-1} . Значит, оно является многочленом от x и от элементарных симметрических многочленов от x_0, x_1, \dots, x_{q-1} . Значения этих элементарных симметрических многочленов при $x_k = r\varepsilon_q^k$, $k = 0, 1, \dots, q-1$, равны коэффициентам многочлена $x^q - r^q$, которые рациональны. Поэтому рассмотренное произведение является искомым многочленом.

Второе решение повторяет второе решение леммы о рациональности 2.7.a. Нужно только везде заменить 3 на q (например, во второй строчке $k = 0, 1, 2, \dots, q$).

6.4. (a) Пусть приводим. Свободный член одного из унитарных сомножителей разложения лежит в $\mathbb{Q}[\varepsilon_q]$ и равен $\pm r^k \varepsilon_q^m$ для некоторого m . Поэтому $r^k \in \mathbb{Q}[\varepsilon_q]$. Далее аналогично лемме 6.3.a получаем $r \in \mathbb{Q}[\varepsilon_q]$. Противоречие.

Пункты (b) и (c) выводятся из (a) аналогично соответствующим пунктам задачи 6.3. Используйте результат задачи 6.9.

6.5. (a) Пусть приводим. Аналогично доказательству леммы о неприводимости 6.4.a (над $\mathbb{Q}[\varepsilon_q]$) получаем $r \in \mathbb{Q}[\varepsilon_q]$. Поэтому $r^2, r^3, \dots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

Докажем, что имеется многочлен степени меньше q с корнем r . Это будет противоречить неприводимости многочлена $x^q - r^q$ над \mathbb{Q} .

Разложим число r^k по степеням числа ε_q для $k = 0, 1, \dots, q-1$:

$$r^k = a_{k,0} + a_{k,1}\varepsilon_q + \dots + a_{k,q-2}\varepsilon_q^{q-2}.$$

Достаточно найти числа $\lambda_0, \dots, \lambda_{q-1} \in \mathbb{Q}$, не равные одновременно нулю, для которых

$$\lambda_0 a_{0,m} + \dots + \lambda_{q-1} a_{q-1,m} = 0 \quad \text{при любом } m = 0, 1, \dots, q-2.$$

Как известно, однородная (т.е. с нулевыми правыми частями) система линейных уравнений с рациональными коэффициентами, в которой уравнений меньше, чем переменных, всегда имеет нетривиальное рациональное решение. Значит, требуемые числа найдутся.

(Иными словами, составим таблицу a_{kl} из рациональных чисел размера $q \times (q-1)$. При помощи прибавлений к одной строке другой, умноженной на рациональное число, можно получить таблицу с нулевой строкой.)

(b) Вытекает из (a).

6.6. (a) *Указание.* Аналогично доказательствам утверждений 2.4, 2.7.b и решениям задач 6.2.ab'c. Используйте теорему о сопряжении 6.3.c, лемму о рациональности 6.3.d и сильную лемму о линейной независимости 6.5.b.

Решение. Предположим противное. Обозначим данный многочлен через P . При $q < \deg P$ получаем противоречие с леммой о рациональности 6.3.d. При $q \geq \deg P$ по теореме о сопряжении 6.3.c и сильной лемме о линейной независимости 6.5.b многочлен P имеет попарно различные корни $x_k = A(r\varepsilon_q^k)$ для $k = 0, 1, 2, \dots, q-1$. При $q > \deg P$ получаем противоречие. При $q = \deg P$ из $q \neq 2$ и $\bar{x}_k = x_{q-k} \neq x_k$ получаем единственность вещественного корня.

(b) *Ответ:* нет. Возьмите $q = 6$ и $r = \sqrt[6]{2}$. Тогда $A(r) = r^3$ — корень многочлена $x^2 - 2$.

3. Уравнения 3-й степени, разрешимые за один радикал

3.2. (c) Нетривиально только доказать, что

число $1/d$ представляется в требуемом виде, если $0 \neq d = a_0 + a_1 r + \dots + a_{n-1} r^{n-1}$ и a_0, \dots, a_{n-1}, r^n рациональны.

Рассуждения из пункта (b) не работают напрямую, ибо многочлен $x^n - r^n$ уже не обязательно неприводим над \mathbb{Q} . Их можно модифицировать, заменив этот многочлен на неприводимый, для которого r является корнем.

Приведем также другое доказательство того же утверждения про $1/d$. Воспользуемся результатом, аналогичным 2.7.a: Если $a_0, \dots, a_{n-1}, r^n \in \mathbb{Q}$, то число $d = a_0 + a_1 r + \dots + a_{n-1} r^{n-1}$ является (не обязательно единственным) корнем некоторого многочлена, степень которого не превосходит n .

Пусть d является корнем многочлена $p_k d^k + \dots + p_0$; можно считать, что $p_0 \neq 0$. Тогда

$$\frac{1}{d} = \frac{p_0}{p_0 d} = \frac{-p_1 d - \dots - p_k d^k}{p_0 d} = \frac{-p_1 - \dots - p_k d^{k-1}}{p_0}.$$

3.4. См. [S, п. 1.2 и 5.3].

6.7. ($\sqrt{D_{pq}} \in \mathbb{Q}$) \Rightarrow (1-разрешимость). Обозначим $r := \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}}$. Тогда по формуле Кардано (см. решение задачи 1.6.a) единственный вещественный корень уравнения $x^3 + px + q = 0$ равен

$$r - \frac{p}{3r} = r - \frac{p}{3r^3} \cdot r^2 = r - \frac{p}{3(-\frac{q}{2} + \sqrt{D_{pq}})} \cdot r^2.$$

$(a + br + cr^2) \Rightarrow (\sqrt{D_{pq}} \in \mathbb{Q})$. Если $r \in \mathbb{Q}$ или $b = c = 0$, то уравнение имеет рациональный корень. В противном случае, обозначим $\varepsilon = \varepsilon_3$. По следствию 2.6.e числа x_0, x_1, x_2 , введенные в формулировке следствия, являются корнями нашего уравнения. По сильной лемме о линейной независимости 2.6.b' эти три корня различны. Значит, x_0, x_1, x_2 — все корни уравнения. Тогда по задаче 6.8 имеем

$$\begin{aligned} -108D_{pq} &= (x_2 - x_1)^2(x_1 - x_0)^2(x_0 - x_2)^2 = \\ &= (br(\varepsilon - \varepsilon^2) + cr^2(\varepsilon^2 - \varepsilon))^2 (br(1 - \varepsilon) + cr^2(1 - \varepsilon^2))^2 (br(1 - \varepsilon^2) + cr^2(1 - \varepsilon))^2 = \\ &= \varepsilon^2(1 - \varepsilon)^6 (br - cr^2)^2 (br + cr^2(1 + \varepsilon))^2 (br(1 + \varepsilon) + cr^2)^2. \end{aligned}$$

Поскольку $(1 + \varepsilon)(1 + \varepsilon^2) = (-\varepsilon)(-\varepsilon^2) = 1$ и $(\varepsilon - 1)^3 = 3\varepsilon - 3\varepsilon^2 = 3\sqrt{3}i$, получаем

$$\begin{aligned} -108D_{pq} &= -27\varepsilon^2(1 + \varepsilon)^2 (br - cr^2)^2 (br(1 + \varepsilon^2) + cr^2)^2 (br(1 + \varepsilon) + cr^2)^2 = \\ &= -27(\varepsilon + \varepsilon^2)^2 (br - cr^2)^2 (b^2 r^2 + br \cdot cr^2 + c^2 r^4)^2 = -27((br)^3 - (cr^2)^3)^2, \end{aligned}$$

откуда и следует требуемое.

$(1\text{-разрешимость}) \Rightarrow (a + br + cr^2)$. Если многочлен приводим, то он имеет рациональный корень. Этот корень имеет нужный вид. Иначе импликация получается из утверждения 6.10.b.

6.8. Обозначим

$$M = y_0^2 y_1 + y_1^2 y_2 + y_2^2 y_0 \quad \text{и} \quad N = y_0^2 y_2 + y_1^2 y_0 + y_2^2 y_1.$$

Тогда $(y_0 - y_1)(y_1 - y_2)(y_0 - y_2) = M - N$. Значит,

$$(y_0 - y_1)^2 (y_1 - y_2)^2 (y_0 - y_2)^2 = (M + N)^2 - 4MN = (3q)^2 - 4(p^3 + 9q^2) = -4p^3 - 27q^2 = -108D_{pq}.$$

Здесь второе равенство справедливо, поскольку по теореме Виета $y_0 + y_1 + y_2 = 0$ и

$$M + N = (y_0 + y_1 + y_2)(y_0 y_1 + y_1 y_2 + y_2 y_0) - 3y_0 y_1 y_2 = 0 \cdot p + 3q = 3q,$$

$$\begin{aligned} MN &= (y_0 y_1 + y_1 y_2 + y_2 y_0)^3 + y_0 y_1 y_2 (y_0 + y_1 + y_2)^3 - 6y_0 y_1 y_2 \sum_{i \neq j} y_i^2 y_j - 9y_0^2 y_1^2 y_2^2 = \\ &= p^3 - q \cdot 0^3 + 6q(p \cdot 0 + 3q) - 9q^2 = p^3 + 9q^2. \end{aligned}$$

6.9. Аналогично задаче 3.1.с и теореме о калькуляторе 3.2.с.

6.10. (а) Число r является корнем ненулевого многочлена $x^n - r^n$ с коэффициентами из $\mathbb{Q}[\alpha]$. Из всех таких многочленов выберем многочлен $f(x)$ наименьшей степени k .

Поскольку НОД многочленов $x^n - r^n$ и $f(x)$ также имеет корень r , коэффициенты в $\mathbb{Q}[\alpha]$ и степень, не превосходящую k , то этот НОД равен $f(x)$. Значит, все комплексные корни многочлена $f(x)$ — это числа вида $r\varepsilon_n^m$ для целых m . Тогда, по теореме Виета, модуль свободного члена многочлена $f(x)$ есть r^k . Так как этот свободный член вещественный, то $r^k \in \mathbb{Q}[\alpha]$.

Осталось показать, что $\alpha \in \mathbb{Q}[r^k]$. Так как $\alpha \in \mathbb{Q}[r]$, то

$$\alpha = b_0(r^k) + rb_1(r^k) + \dots + r^{k-1}b_{k-1}(r^k)$$

для некоторых многочленов $b_0, \dots, b_{k-1} \in \mathbb{Q}[x]$. Если не все многочлены b_1, \dots, b_{k-1} нулевые, то r является корнем ненулевого многочлена

$$(b_0(r^k) - \alpha) + xb_1(r^k) + \dots + x^{k-1}b_{k-1}(r^k)$$

степени меньше k и с коэффициентами в $\mathbb{Q}[\alpha]$ (поскольку $\alpha, r^k \in \mathbb{Q}[\alpha]$). Это противоречит выбору многочлена $f(x)$. Значит, $b_1 = \dots = b_{k-1} = 0$, откуда $\alpha = b_0(r^k) \in \mathbb{Q}[r^k]$.

(b) По теореме о калькуляторе 3.2.с данный многочлен имеет корень $y_0 \in \mathbb{Q}[R]$ для некоторого $R \in \mathbb{R}$ такого, что $R^D \in \mathbb{Q}$ при некотором D . Согласно (а), $\mathbb{Q}[y_0] = \mathbb{Q}[R^k]$ при некотором k . Обозначим $r := R^k$. Так как $R^D \in \mathbb{Q}$, то существует наименьшее $d > 0$, для которого $r^d \in \mathbb{Q}$. Тогда $r, r^2, \dots, r^{d-1} \notin \mathbb{Q}$. Значит, многочлен $x^d - r^d$ неприводим над \mathbb{Q} (ибо свободный член любого его нетривиального унитарного делителя имеет иррациональный модуль r^t , $0 < t < d$; это аналогично доказательству задачи 6.3.а).

Наконец, из равенства $\mathbb{Q}[y_0] = \mathbb{Q}[r]$ и соображений размерности (аналогичных приведенным в доказательстве сильной леммы о неприводимости 6.5.а) следует, что неприводимые над \mathbb{Q} многочлены с корнями y_0 и r имеют одинаковые степени. Значит, $n = d$, откуда и следует требуемое.

6.11. (а) Следует из формулы Кардано (точнее, из теоремы в решении задачи 1.6.б) аналогично задаче 3.3.с.

(b) **Гипотеза.** Для многочлена $x^3 + px + q$ с $p, q \in \mathbb{Q}$ каждое из условий теоремы 6.7 эквивалентно комплексной 1-разрешимости.

В этой гипотезе все импликации, кроме следующей, очевидны или доказываются аналогично теореме 6.7.

Гипотеза. Если многочлен $x^3 + px + q$ с $p, q \in \mathbb{Q}$ комплексно 1-разрешим, то он имеет корень $a + br + cr^2$ для некоторых $a, b, c, r^3 \in \mathbb{Q}$, $r \in \mathbb{C}$.

(c) Следует из теоремы в решении задачи 6.1.б.

4. Уравнения 4-й степени, разрешимые за один радикал

4.2. (4, 1) *Ответ:* Неприводимый над \mathbb{Q} многочлен $x^4 + px^2 + qx + s$ 1-разрешим тогда и только тогда, когда

(4) один из его корней имеет вид $a + br + cr^2 + dr^3$ при $a, b, c, d, r^4 \in \mathbb{Q}$ и $r^2 \notin \mathbb{Q}$.

В терминах коэффициентов это условие формулируется так.

(4i) существует $\alpha \in \mathbb{Q}$ такое, что $2\alpha > p$ и $q^2 - 4(p - 2\alpha)(s - \alpha^2) = 0$, и при этом

(4ii) число $\Gamma = 16(\alpha^2 - s)^2 - (\alpha^2 - s)(2\alpha + p)^2$ является квадратом рационального числа.

Ясно, что условия, предъявленные выше, поддаются алгоритмической проверке.

Утверждение о виде (4) корня разрешимого многочлена доказывается в задаче 6.10.б. Доказательство того, что (4) равносильно (4i) и (4ii), приведено в [A, Theorem 2].

4.4. По теореме из решения задачи 6.1, многочлен $x^4 + px^2 + qx + s$ имеет корень $x_+ = \left(A + \sqrt{-\frac{2q}{A} - 2\alpha - p} \right) / 2$, где $A^2 = 2\alpha - p$ и $Aq \leq 0$. По условию, $2\alpha - p > 0$, поэтому

за первое извлечение корня можно получить число A . Также $-\frac{2q}{A} - 2\alpha - p \geq -2\alpha - p > 0$. Значит, x_+ можно получить за два извлечения корня.

4.5. По теореме о калькуляторе 3.2.c, данный корень нашего многочлена $f(x) = x^4 + px^2 + qx + s$ имеет вид $x_0 = a + br + cr^2 + dr^3$, где $a, b, c, d, r^4 \in \mathbb{Q}$. Можно считать, что $r^2 \notin \mathbb{Q}$ (иначе можно заменить r на $\sqrt{|r|}$ или $\sqrt[4]{|r|}$). Тогда по теореме о сопряжении 6.12, корнями многочлена f также являются числа x_1, x_2 и x_3 .

Так как f неприводим, то x_0 иррационально и x_0, x_2 не могут быть различными корнями квадратного трехчлена с рациональными коэффициентами. Значит, $b = d = 0$ невозможно. Тогда $b + dr^2 \neq 0$ согласно 2.3.b. Поэтому вещественные числа x_0 и x_2 различны. Аналогично числа x_1 и x_3 не вещественны и различны. Отсюда ¹⁰ $f(x) = (x - x_0)(x - x_1)(x - x_2)(x - x_3)$.

По задаче 6.13.a, кубическая резольвента многочлена $f(x)$ имеет корень $\alpha = \frac{x_0x_2 + x_1x_3}{2}$. Поскольку $x_0 + x_1 + x_2 + x_3 = 0$, имеем $a = 0$. Тогда

$$\begin{aligned} 2\alpha = x_0x_2 + x_1x_3 &= ((cr^2)^2 - (br + dr^3)^2) + ((cr^2)^2 - (bri - dr^3i)^2) = \\ &= 2c^2r^4 - r^2(b + dr^2)^2 + r^2(b - dr^2)^2 = 2c^2r^4 - 4bdr^4 = r^4(2c^2 - 4bd) \in \mathbb{Q}. \end{aligned}$$

4.6. Аналог пунктов (d) звучит так.

Теорема. Пусть многочлен имеет корень $r \in \mathbb{R}$, причем $r^4 \in \mathbb{Q}$, но $r^2 \notin \mathbb{Q}$. Тогда корнями этого многочлена являются также числа $ir, -r$ и $-ir$. (Заметим, что $i = \varepsilon_4$.)

Лемма о неприводимости. Если $r \in \mathbb{R}$, причем $r^4 \in \mathbb{Q}$, но $r^2 \notin \mathbb{Q}$, то многочлен $x^4 - r^4$ неприводим над \mathbb{Q} .

Доказательство леммы полностью аналогично доказательству 6.3.a, ибо $r, r^2, r^3 \notin \mathbb{Q}$.

Доказательство теоремы полностью аналогично доказательству других теорем о сопряжении.

Аналогом пунктов (e) является задача 6.12.

6.12. Обозначим через P данный многочлен и $G(t) := P(a + bt + ct^2 + dt^3)$. Тогда, как и в следствии 2.6.e, достаточно применить к G теорему из решения задачи 4.6.

6.13. (a) Применяя теорему Виета и учитывая, что $\sum_i y_i = 0$, проверим, что $q^2 = (y_0y_1 + y_2y_3 - p)((y_0y_1 + y_2y_3)^2 - 4s)$. Детали см. в [A, Statement 2].

(b) Аналогично (a), эти три числа являются корнями. Имеем $y_0y_2 + y_1y_3 - y_0y_1 - y_2y_3 = (y_0 - y_3)(y_2 - y_1)$. Поэтому, если y_1, y_2, y_3, y_4 попарно различны, то эти три числа попарно различны. Случай кратных корней также разбирается несложно.

Другое решение пунктов (a, b). Применяя теорему Виета и учитывая, что $\sum_i y_i = 0$, имеем

$$\begin{aligned} & (2\alpha - (y_0y_1 + y_2y_3))(2\alpha - (y_0y_2 + y_1y_3))(2\alpha - (y_0y_3 + y_1y_2)) \\ &= 8\alpha^3 - 4\alpha^2 \sum_{i < j} y_i y_j + 2\alpha \sum_{j < k, i \notin \{j, k\}} y_i^2 y_j y_k - \prod_{0 < j < k, i \notin \{0, j, k\}} (y_i y_j + y_k y_\ell) \\ &= 8\alpha^3 - 4p\alpha^2 + 2\alpha \cdot \left(\sum_i y_i \cdot \sum_{\{|i, j, k\|=3} y_i y_j y_k - 4y_0 y_1 y_2 y_3 \right) - \left(y_0 y_1 y_2 y_3 \sum_i y_i^2 + \sum_{i < j < k} y_i^2 y_j^2 y_k^2 \right) \\ &= 8\alpha^3 - 4p\alpha^2 - 8s\alpha - (q^2 - 4ps) = -R_f(\alpha), \end{aligned}$$

¹⁰ Вот другое обоснование равенства $f(x) = g(x) := (x - x_0)(x - x_1)(x - x_2)(x - x_3)$. Имеем

$$g(x) = (x - x_0)(x - x_2)(x - x_1)(x - x_3) = [(x - a - cr^2)^2 - r^2(b + dr^2)][(x - a + cr^2)^2 + r^2(b - dr^2)] \in \mathbb{Q}[r^4][x] = \mathbb{Q}[x].$$

(Рациональность коэффициентов многочлена g также получается аналогично второму доказательству леммы о рациональности 6.3.d.) Так как $f(x)$ неприводим и имеет общий корень с $g(x)$, причем степени и старшие коэффициенты этих многочленов равны, то $f(x) = g(x)$.

откуда и следует требуемое.

6.14. (а) Так как $q^2 = 2p(4s - p^2)$, то кубическая резольвента $q^2 - 4(2\alpha - p)(\alpha^2 - s)$ имеет корень $\alpha := -p/2$. Так как $p < 0$, то $2\alpha - p = -2p > 0$. Значит, согласно 6.1, наш многочлен имеет корень

$$-\sqrt{2\alpha - p} + \sqrt{\frac{2q}{\sqrt{2\alpha - p}} - 2\alpha - p} = -\sqrt{-2p} + \frac{\sqrt{2q}}{\sqrt[4]{-2p}}.$$

(б) *Ответ:* Неверно. Многочлен $x^4 - 12x^2 - 24x - 14$ из решения задачи 4.3.а имеет корень $\sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$, но число $2 \cdot (-24) = -48$ не является квадратом рационального числа.

Список литературы

- [A] D. Akhtyamov, Solvability of cubic and quartic equations using one radical, <http://arxiv.org/abs/1411.4990>
- [CS] А.Б. Скопенков и Г.Р. Челноков, Почти симметрические многочлены, подборка задач.
- [E] H.M. Edwards, The construction of solvable polynomials, Bull. Amer. Math. Soc. 46 (2009), 397-411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703-704.
- [L] L. Lerner, Galois Theory without abstract algebra, <http://arxiv.org/abs/1108.4593>.
- [M] Московская математическая конференция школьников, <http://www.mccme.ru/mmks/index.htm>.
- [S09] A. Skopenkov, Philosophical and methodical appendix, in: Mathematics as a sequence of problems, Ed. A. Zaslavsky, D. Permyakov, A. Skopenkov, M. Skopenkov, A. Shapovalov, MCCME, Moscow, 2009.
- [S] A. Skopenkov, Some more proofs from the Book: solvability and insolvability of equations in radicals, www.mccme.ru/circles/oim/kroneck.pdf, <http://arxiv.org/abs/0804.4357>
- [S'] A. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem, www.mccme.ru/circles/oim/ruffini.pdf.

SOLVING EQUATIONS USING ONE RADICAL

presented by D. Akhtyamov¹, I. Bogdanov², A. Glebov³,
A. Skopenkov⁴, E. Streltsova⁵, and A. Zykin⁶

This project is devoted to several classical results and methods in pure mathematics which are also interesting from the point of view of computer science (related to symbolic computations). The main problems of the project are 3.3.d, 4.2, 5.5.c, 6.7, and 6.17.bc. The principal difference of this set of problems from standard textbooks in this topic is that we do not use the notion of the Galois group (and even the notion of group). Despite of the lack of these *words*, the *ideas* of the proofs presented below are starting points for the Galois theory [S09] and the *constructive Galois theory* [E].

We suggest to all the students working on the project to *consult* with the jury on any questions on the project, or on ideas of the solutions. Their results may be used as sources of talks on the students' conferences, e.g., [M].

The students who work on the project well enough will get several *extra problems*.

A student (or a group of students) working on this project get a "star" for every solution which has been written down and marked with either '+' or '+.'. The jury may also award extra stars for beautiful solutions, solutions of hard problems, or (some) solutions typeset in \TeX . The jury has infinitely many stars. One may submit a solution in oral form, but he loses a star with each attempt.

We will tell the solutions of 1.1.ab, 1.2.ab, 1.4.ab, 1.5.a, 2.1.a''f, 2.3.abcd, 3.1.a, 3.2.a, 4.1.a, 5.1.a, 5.2.a, and 5.4.ab at the initial presentation; thus you may submit the solutions of these problems only before this presentation (but you may make this in oral form without loss of stars).

If a problem looks just like a statement, a proof of this statement is required in this problem. If you are stuck on a certain problem, we suggest to try looking at the next ones. They may turn out to be helpful.

We denote the set of rational numbers by \mathbb{Q} . A 'polynomial with rational coefficients' is referred to merely as *polynomial*. A polynomial is *irreducible* over a set F , if it cannot be decomposed as a product of polynomials of lower degrees with coefficients in F .

Problems before the Semifinal

1 Solving equations of degree 3 and 4

1.1. (a) Solving an equation $ax^3 + bx^2 + cx + d = 0$ can be reduced by substitution of variable to solving an equation of the form $x^3 + px + q = 0$.

(b) Solving an equation $ax^4 + bx^3 + cx^2 + dx + e = 0$ can be reduced by a substitution of variable to solving an equation of the form $x^4 + px^2 + qx + r = 0$.

In the next two problems, we allow to use without proof the *Intermediate value theorem* for polynomials: *If a polynomial P satisfies $P(a) > 0$ and $P(b) < 0$ for some $a < b$, then there exists a real number $c \in [a, b]$ such that $P(c) = 0$.*

1.2. Find the number of real roots of the equation

(a) $x^3 + 2x + 7 = 0$; (b) $x^3 - 4x - 1 = 0$.

¹Saint-Petersburg State University

²Moscow Institute of Physics and Technology

³Novosibirsk State University

⁴Supported by the D. Zimin's "Dynasty" fund; Moscow Institute of Physics and Technology, Independent Moscow University; www.mccme.ru/~skopenko

⁵Moscow State University

⁶National Research University "Higher School of Economics"

1.3. (a) Which relations on p and q are equivalent to the condition that the equation $x^3 + px + q = 0$ has exactly two roots?

(b) Under these relations, express the roots in terms of p and q .

(c) Find the number of real roots of $x^3 + px + q = 0$ in terms of the values of p and q .

Hereafter, ‘to solve an equation’ always means ‘to find *all* its *real* roots’. However, we recommend also to find all the complex roots as well.

1.4. (a) Prove that $\sqrt[3]{2 + \sqrt{5}} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(b) Find at least one root of the equation $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

Hint: del Ferro’s method. Since $(b + c)^3 = b^3 + c^3 + 3bc(b + c)$, the number $x = b + c$ satisfies the equation $x^3 - 3bcx - (b^3 + c^3) = 0$.

(c) Solve the equation $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

(d)* Solve the equation $x^3 - 3x - 1 = 0$.

1.5. (a) Factor the expression $a^3 + b^3 + c^3 - 3abc$.

(b) Decompose $a^3 + b^3 + c^3 - 3abc$ into a product of linear factors with complex coefficients.

1.6. (a) Formulate and prove a theorem describing all real roots of the equation $x^3 + px + q = 0$ in a case when del Ferro’s method (see problem 1.4) allows to obtain all of them. Under which relations on p and q this method is applicable, if we allow taking square roots only of positive numbers?

(b) The same question for finding all complex roots.

1.7. Solve the equation (a) $(x^2 + 2)^2 = 18(x - 1)^2$;

(b) $x^4 + 4x - 1 = 0$; (c) $x^4 + 2x^2 - 8x - 4 = 0$; (d) $x^4 - 12x^2 - 24x - 14 = 0$.

Hint to 1.7.b: Ferrari’s method. Find numbers α, b, c such that

$$x^4 + 4x - 1 = (x^2 + \alpha)^2 - (bx + c)^2.$$

For this purpose, one may search for a value of α such that the trinomial $(x^2 + \alpha)^2 - (x^4 + 4x - 1)$ is a square of a linear function. To that end, find the discriminant of this trinomial. (This discriminant is a cubic polynomial in α ; it is called the *cubic resolution* of the polynomial $x^4 + 4x - 1 = 0$.)

2 Representability with use of only one radical

2.1. Determine whether the following number can be represented in the form $a + \sqrt{b}$ with $a, b \in \mathbb{Q}$:

(a) $\sqrt{3 + 2\sqrt{2}}$; (a') $\sqrt{2 + \sqrt{2}}$; (a'') $\frac{1}{7 + 5\sqrt{2}}$; (b) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2}$;

(c) $\sqrt[3]{7 + 5\sqrt{2}}$; (d) $\cos(2\pi/5)$; (e) $\sqrt[3]{2}$; (f) $\sqrt{2 + \sqrt[3]{2}}$; (g) $\cos(2\pi/9)$; (h)* $\cos(2\pi/7)$.

2.2. The number $\cos(2\pi/9)$ is a root of the polynomial $8x^3 - 6x + 1$.

2.3. Assume that $r \in \mathbb{R} \setminus \mathbb{Q}$ is chosen so that $r^2 \in \mathbb{Q}$.

(a) *Irreducibility Lemma.* The polynomial $x^2 - r^2$ is irreducible over \mathbb{Q} .

(b) *Linear Independence Lemma.* If $a + br = 0$ with $a, b \in \mathbb{Q}$, then $a = b = 0$.

(c) If r is a root of some polynomial, then this polynomial is divisible by $x^2 - r^2$.

(d) **Conjugation Theorem.** *If r is a root of a polynomial, then $-r$ is also its root.*

(e) *Corollary.* If a polynomial has a root $a + br$ with $a, b \in \mathbb{Q}$, then $a - br$ is also a root of this polynomial.

(f) *Corollary.* If a cubic polynomial has a root of the form $a + br$ with $a, b \in \mathbb{Q}$, then this polynomial has a rational root.

2.4. Proposition. *If a polynomial of degree at least 3 is irreducible over \mathbb{Q} , then none of its roots has the form $a \pm \sqrt{b}$ with $a, b \in \mathbb{Q}$.*

2.5. Determine whether the following number can be represented in the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$:

- (a) $\sqrt{3}$; (a') $\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}}$; (b) $\cos(2\pi/9)$; (c) $\sqrt[5]{3}$; (d) $\sqrt[3]{3}$;
 (e) the least positive root of $x^3 - 4x + 2 = 0$;
 (f)* the unique real root of $x^3 - 6x - 6 = 0$;
 (g)* the unique real root of $x^3 - 9x - 12 = 0$.

Hereafter, we use the notation

$$\varepsilon_q = \cos \frac{2\pi}{q} + i \sin \frac{2\pi}{q}.$$

2.6. Assume that $r \in \mathbb{R} \setminus \mathbb{Q}$ is chosen so that $r^3 \in \mathbb{Q}$.

- (a) *Irreducibility Lemma.* The polynomial $x^3 - r^3$ is irreducible over \mathbb{Q} .
 (b) *Linear Independence Lemma.* If $a + br + cr^2 = 0$ with $a, b, c \in \mathbb{Q}$, then $a = b = c = 0$.
 (c) If r is a root of a polynomial, then this polynomial is divisible by $x^3 - r^3$.
 (d) **Conjugation Theorem.** *If r is a root of a polynomial, then the numbers $\varepsilon_3 r$ and $\varepsilon_3^2 r$ are also its roots.*
 (e) *Corollary.* If a polynomial has a root $x_1 = a + br + cr^2$ with $a, b, c \in \mathbb{Q}$, then the numbers

$$x_2 = a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{and} \quad x_3 = a + b\varepsilon_3^2 r + c\varepsilon_3 r^2$$

are also its roots.

- (a') *Strong Irreducibility Lemma.* The polynomial $x^3 - r^3$ is irreducible over

$$\mathbb{Q}[\varepsilon_3] = \{x + y\varepsilon_3 : x, y \in \mathbb{Q}\}.$$

(b') *Strong Linear Independence Lemma.* If $k, \ell, m \in \mathbb{Q}[\varepsilon_3]$ satisfy $k + \ell r + m r^2 = 0$, then $k = \ell = m = 0$.

2.7. Assume that $r \in \mathbb{R} \setminus \mathbb{Q}$ and $a, b, c, r^3 \in \mathbb{Q}$.

- (a) *Rationality Lemma.* The number $a + br + cr^2$ is a root of some cubic polynomial.
 (b) **Proposition.** *Assume that an irrational number $a + br + cr^2$ is a root of a polynomial which is irreducible over \mathbb{Q} ; then this polynomial is cubic and it has exactly one real root.*

3 Equations of degree 3 solvable using one radical

Initially, Cheburashka gets a number 1. To the numbers he already has got before, he can apply addition, subtraction, multiplication, and division (by a non-zero number) for free. Moreover, for one yuan Cheburashka can extract an arbitrary degree root of a positive number which he already has got during the calculations. All other operations are out of his reach. But he performs the allowed operations with absolute precision, and he has an unbounded memory.

- 3.1.** (a) Help Cheburashka in obtaining $\sqrt[3]{2} + \sqrt[3]{4}$ for 1 yuan.
 (b) Help Cheburashka in obtaining $\sqrt[3]{2} + \sqrt{3} + \sqrt[3]{2 - \sqrt{3}}$ for 2 yuans.
 (c) Help Cheburashka in obtaining $\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}}$ for 1 yuan, if the operation of division is prohibited, but he may use all rational numbers for free.

3.2. (a) A number can be obtained for 1 yuan paid for extracting a square root, if and only if the number has the form $a \pm \sqrt{b}$ with $a, b \in \mathbb{Q}$.

(b) A number can be obtained for 1 yuan paid for extracting a cubic root, if and only if the number has the form $a + br + cr^2$ with $r \in \mathbb{R}$ and $a, b, c, r^3 \in \mathbb{Q}$.

(c) **Calculator Theorem.** *A number can be obtained for 1 yuan, if and only if the number has the form $A(r)$, where A is a polynomial and r is a real number such that $r^n \in \mathbb{Q}$ for some positive integer n .*

3.3. (a) Present some nonzero rational numbers p and q such that Cheburashka can obtain one of the roots of $x^3 + px + q = 0$ for 1 yuan.

(a') Present some nonzero rational numbers p and q such that the polynomial $x^3 + px + q$ has no rational roots, but Cheburashka still can obtain one of its roots for 1 yuan.

(b3) Can Cheburashka obtain at least one root of $x^3 + 3x + 6 = 0$ for 3 yuans?

(b2) ... for 2 yuans?

(b1)* ... for 1 yuan?

(c) If an equation of degree 3 with rational coefficients has exactly one real root, then Cheburashka can obtain this root for 2 yuans.

(d)* **Main problem.** Given rational p and q , determine whether Cheburashka can obtain at least one root of the equation $x^3 + px + q = 0$ for 1 yuan.

3.4. * (a) Does there exist a cubic equation with rational coefficients such that Cheburashka cannot get any of its roots for 2 yuans?

(b) The same question about 10000 yuans.

Let us reformulate the previous problems using mathematically precise language. Consider a calculator with the following buttons:

$$1, +, -, \times, : \text{ and } \sqrt[n]{} \text{ for every } n.$$

The calculator has absolute precision and unlimited memory. It returns an error if division by 0 is carried out.

Assume first that the calculator is *real*, i.e. that it works only with real numbers; so extracting an even degree root of a negative number results in an error.

Here are mathematically rigorous (and slightly modified) statements of the problems 3.3.cd and 3.4.

Proposition on Solvability in real radicals. *If a cubic polynomial with rational coefficients has precisely one real root, this root can be obtained using the real calculator.*

Moreover, this can be done by extracting roots only twice, once of the second and once of the third degree.

Theorem on Insolvability in real radicals. *There exists a cubic polynomial with rational coefficients (e.g. $x^3 - 3x + 1$) such that none of its roots can be obtained using the real calculator.*

Moreover, if a cubic polynomial with rational coefficients has three distinct real roots, then none of these roots can be obtained with the real calculator.

Notice here that if there are exactly two roots, then they are both rational (cf. problem 1.3.ab).

Question. *How can one decide whether the cubic polynomial with rational coefficients has a root which can be obtained on the calculator using the radical sign only once? Is there an algorithm deciding whether a polynomial belongs to the described class?*

4 Equations of degree 4 solvable using one radical

We say that a polynomial is *k-solvable* if one of its roots can be obtained by using the real calculator with extracting at most k roots.

4.1. (a) Assume that a biquadratic polynomial (of degree 4) has a real root. Is this polynomial necessarily 2-solvable?

(b)* Given rational p and s , determine whether the polynomial $x^4 + px^2 + s$ is 1-solvable.

(c)* Is every quartic polynomial having a real root 4-solvable?

4.2. Main problem. (4,1) Given a polynomial $x^4 + px^2 + qx + s = 0$ with rational coefficients, determine whether it is 1-solvable.

Is there an algorithm for deciding 1-solvability?

(4, 2) (*The jury does not know a solution*) The same question for 2-solvability.

(n) (*The jury does not know a solution for any $n \geq 4$*) Given a polynomial of degree n with rational coefficients, determine whether it is ∞ -solvable?

Is there an algorithm for deciding ∞ -solvability?

(n, k) (*The jury does not know a solution*) Given a polynomial of degree n with rational coefficients, determine whether it is k -solvable?

Is there an algorithm for deciding k -solvability?

4.3. (a) Present rational numbers p , q , and s such that $qs \neq 0$ and that the polynomial $x^4 + px^2 + qx + s$ is irreducible over \mathbb{Q} and 1-solvable.

(b) Determine whether the polynomial $x^4 - 6x^2 + 72x - 99$ is 1-solvable.

4.4. Assume that $p < 0$ and that the cubic resolution of the polynomial $x^4 + px^2 + qx + s$ has a root $\alpha \in \mathbb{Q}$ such that $-p > 2\alpha > p$. Prove that this polynomial is 2-solvable (on the real calculator).

4.5. If a degree 4 polynomial irreducible over \mathbb{Q} has a root that can be obtained using real calculator by extracting only one root, and this extraction provides a root of degree 4, then the cubic resolution of the polynomial has a rational root.

4.6. Formulate and prove the analogues of the Conjugation Theorems 2.3.d and 2.6.d for degree 4 polynomials.

5 Formal expressibility in real radicals

The priority goal of the first problem in this section is to formalize the notion of 'to determine'. We give such a formalization after the problem statement. So you have a chance to approach the basic definition starting from simple examples. The solutions themselves should not be difficult for you.

5.1. (a) Given $x + y$ and xy , is it always possible to determine $x - y$? To determine x ?

The primary formalization of the notion 'to determine' in the problem above can be given in the following way: *does there exist a mapping $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ such that $f(x + y, xy) = x - y$ for all $x, y \in \mathbb{R}$?*⁷

(b) Given $x + y + z$, $xy + yz + zx$ and xyz , is it always possible to determine $(x - y)(y - z)(z - x)$? (The formalization is similar to that in (a).)

The basic definition in this text is yet another formalization of the notion 'to determine'.

Definition. A polynomial $f \in \mathbb{R}[x_1, \dots, x_n]$ is **expressible in real radicals via the collection of polynomials** $a_1, \dots, a_t \in \mathbb{R}[x_1, \dots, x_n]$, if one can append f to this collection by a sequence of operations of the following types:

- if several polynomials b_1, \dots, b_k are already in the collection and $F \in \mathbb{R}[t_1, \dots, t_k]$ is an arbitrary polynomial, then it is allowed to append the polynomial $F(b_1, b_2, \dots, b_k)$ to the collection;

- if some polynomial in the collection has the form p^k for some $p \in \mathbb{R}[x_1, \dots, x_n]$ and integer $k > 1$, then one may append p to the collection.

⁷Another formalization of the notion 'to determine' which is not further used is as follows: *does there exist a mapping f from \mathbb{R}^2 to the set $2_{fin}^{\mathbb{R}}$ of all finite subsets of \mathbb{R} such that $f(x + y, xy) \ni x - y$ for all $x, y \in \mathbb{R}$?* Let us show that this question (together with its generalizations to several variables) is trivial.

Mappings $f : \mathbb{R}^2 \rightarrow 2_{fin}^{\mathbb{R}}$ (i.e. real finite-valued functions of \mathbb{R}^2) may be defined by formulae. For example, the formula $f(x) = \pm x$ is a reduction of the formula $f(x) = \{x, -x\}$ which defines the (at most)-2-valued mapping f . (*Exercise:* Establish how-many-valued mapping is defined by the formula $f(x) = \frac{\pm x}{\pm x}$.) Denote by $f(p, q)$ the (finite) set of (real) solutions of the equation $t^2 + pt + q = 0$. Then the formula $x - y = f(x + y, xy) - f(x + y, xy)$ defines the desired mapping (Why?).

For example, if a collection contains $x^2 + 2y$ and $x - y^3$, then one may apply the first operation in order to append the polynomial $-5(x^2 + 2y)^2 + 3(x^2 + 2y)(x - y^3)^6$; moreover, if a collection already contains $x^2 - 2xy + y^2$, then applying the second operation one may append $x - y$ and $y - x$.

5.2. Determine if the following polynomial is expressible in real radicals via $x + y$ and xy :

- (a) $x - y$; (b) x .

The answer to 5.2.b shows that *the root of a quadratic equation is expressible in real radicals via its coefficients*. The formalization of this statement will be given later in problem 6.17.

5.3. (a,b,c) Represent

$$x^2 + y^2 + z^2, \quad x^2y + y^2z + z^2x + x^2z + z^2y + y^2x, \quad x^3 + y^3 + z^3$$

as polynomials in

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + yz + zx \quad \text{and} \quad \sigma_3 = xyz.$$

- (d) Is $(x^8y + y^8z + z^8x)(x^8z + z^8y + y^8x)$ representable as a polynomial in $\sigma_1, \sigma_2, \sigma_3$?

5.4. (a) The multi-degree of the product of polynomials (in several variables) is the sum of their multi-degrees.

(b) We say that a polynomial f in two variables x, y is *symmetric* if the polynomials $f(x, y)$ and $f(y, x)$ are equal. Prove that every symmetric polynomial in two variables x, y is a polynomial in $x + y$ and xy .

(c) We say that a polynomial f in three variables x, y, z is *symmetric* if the polynomials $f(x, y, z)$, $f(y, z, x)$ and $f(y, x, z)$ are equal. Prove that every symmetric polynomial in three variables x, y, z is a polynomial in σ_1, σ_2 and σ_3 .

(d) Formulate and prove the main theorem about symmetric polynomials in n variables.

5.5. Determine whether the following polynomial is expressible in real radicals via $\sigma_1, \sigma_2, \sigma_3$:

- (a) $(x - y)(y - z)(z - x)$; (b) $x^2y + y^2z + z^2x$. (c)* x ?

Hints and Solutions for the initial presentation

1.1. Use the substitution (a) $y = x + \frac{b}{3a}$ and (b) $y = x + \frac{b}{4a}$.

1.2. (a) *Answer:* 1. Since the degree is odd, the polynomial has a real root. Since the polynomial is monotonous, this root is unique.

(b) *Answer:* 3. Let $f(x) = x^3 - 4x - 1$. We have $f(-2) < 0$, $f(-1) > 0$, $f(0) < 0$, $f(3) > 0$. By the Intermediate value theorem, the equation has three real roots.

1.3. (c) *Hint:* Determine the intervals of monotonicity of $f(x) = x^3 + px + q$. Find the points of local extrema and the values of f at these points. For this purpose, explore the sign of $\frac{f(x_1) - f(x_2)}{x_1 - x_2}$ (or, if you are educated enough, take a derivative of f).

1.4. (b) *Answer:* $x = -1 - \sqrt[3]{2}$.

Hint: $x^3 - 3\sqrt[3]{2}x + 3 = x^3 - 3bcx + (b^3 + c^3)$, where $b = 1$, $c = \sqrt[3]{2}$.

1.5. (a) The given polynomial vanishes at $a = -b - c$, which means that it is divisible by $a + b + c = a - (-b - c)$. Now one may divide $a^3 - 3abc + (b^3 + c^3)$ by $a + b + c$ in a usual way.

2.1. (a'') *Answer:* Yes. $\frac{1}{7 + 5\sqrt{2}} = \frac{7 - 5\sqrt{2}}{7^2 - 2 \cdot 5^2} = -7 + 5\sqrt{2}$.

(f) *Answer:* No.

Arguing indirectly, we assume $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$ for some $a, b \in \mathbb{Q}$. This number is a root of the polynomial $P(x) = ((x - \sqrt{2})^3 - 2)((x + \sqrt{2})^3 - 2)$ having rational coefficients. Applying Conjugation Theorem 2.3.d to $r = \sqrt{b}$ and polynomial $P(a + t)$ (or applying Corollary 2.3.e to $r = \sqrt{b}$ and polynomial $P(t)$), we obtain $P(a - \sqrt{b}) = 0$. By the rational roots theorem, the polynomial P has no rational roots. Therefore, $b \neq 0$, so the roots $a \pm \sqrt{b}$ are distinct. However, the polynomial P has only two real roots, namely $\sqrt{2} + \sqrt[3]{2}$ and $-\sqrt{2} + \sqrt[3]{2}$. Thus $a + \sqrt{b} = \sqrt{2} + \sqrt[3]{2}$ and $a - \sqrt{b} = -\sqrt{2} + \sqrt[3]{2}$, whence $\sqrt[3]{2} = a \in \mathbb{Q}$. This is a contradiction.

2.3. (a) If the polynomial $x^2 - r^2$ is reducible over \mathbb{Q} , then it has a linear factor with rational coefficients. Thus it has a rational root, which is impossible since $\pm r \notin \mathbb{Q}$.

(b) If $b \neq 0$, then $r = -a/b \in \mathbb{Q}$ which is impossible. Hence $b = 0$, and thus $a = 0$ as well.

(c) Divide our polynomial by $x^2 - r^2$ with residue; this residue is linear, and it vanishes at $x = r$. By (b), the residue is 0, as required.

(d) Follows from (c), since the polynomial $x^2 - r^2$ has roots $\pm r$.

3.1. (a) For 1 yuan we get $\sqrt[3]{2}$, which allows us to obtain $\sqrt[3]{2} + \sqrt[3]{4} = \sqrt[3]{2} + (\sqrt[3]{2})^2$.

3.2. (a) Clearly, each number of required form can be obtained for 1 yuan. It remains to prove that all such numbers are of this form. Surely, it would suffice to prove that the set of all numbers of the form $a \pm \sqrt{b}$ is closed under arithmetical operations; but this is obviously false. So we act in a bit different way.

Let $r = \sqrt{s}$ be a square root which has been obtained for 1 yuan (so $s \in \mathbb{Q}$). If $r \in \mathbb{Q}$, then the result is trivial since all obtained numbers are rational. Otherwise, we show that all the obtained numbers have the form $a + br$ with $a, b \in \mathbb{Q}$. It suffices to prove that the result of an arithmetical operation applied to two numbers of this form also has the same form. This is trivial for all operations except division, for which the claim holds due to $\frac{1}{a + br} = \frac{a - br}{a^2 - b^2s}$.

4.1. (a) *Answer:* yes. Since the squares of a real root of a biquadratic polynomial is a roots of a quadratic equation, this square may be obtained for one extraction. Thus the root itself can be obtained in two extractions.

5.1. (a) Consider the pairs $(x, y) = (1, 2)$ and $(x, y) = (2, 1)$.

5.2. (a) $(x - y)^2 = (x + y)^2 - 4xy$.

5.4. (b) We use the lexicographical induction on the multi-degree of the polynomial. Given a symmetric polynomial f of multi-degree (α, β) with $\alpha \geq \beta$ (i.e. with the lexicographically leading monomial of the form $kx^\alpha y^\beta$), one may reduce it to the polynomial $f - k(xy)^\beta(x + y)^{\alpha - \beta}$.

6 Additional Problems at the Semifinal

1. Solving equations of degree 3 and 4

6.1. * (a) Formulate and prove the theorem describing all real roots of the equation $x^4 + px^2 + qx + s = 0$. In the formulation and proof, you may use a root α of the cubic resolution of this equation.

Hint. Use Ferrari's method (see problem 1.7.ab). Do not forget to treat all possible cases!

(b) The same for all complex roots of this equation.

2. Representability with use of only one radical

6.2. Determine whether the following number can be represented in the form $a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \dots + a_6\sqrt[7]{2^6}$ with $a_0, a_1, a_2, \dots, a_6 \in \mathbb{Q}$:

(a) $\sqrt[3]{3}$; (b) $\cos(2\pi/21)$; (b') any of the roots of the equation $x^7 - 4x + 2$;

(c) $\sqrt[11]{3}$; (d) $\sqrt[7]{3}$.

Hint: Apply lemmas formulated below.

6.3. Let q be a prime number, and let $r \in \mathbb{R} \setminus \mathbb{Q}$ be a number such that $r^q \in \mathbb{Q}$.

(a) *Irreducibility Lemma.* The polynomial $x^q - r^q$ is irreducible over \mathbb{Q} .

(b) *Linear Independence Lemma.* If r is a root of a polynomial A whose degree is less than q , then $A = 0$.

(c) **Conjugation Theorem.** *If r is a root of a polynomial, then all the numbers of the form $r\varepsilon_q^k$, $k = 1, 2, 3, \dots, q-1$, are also roots of this polynomial.*

(d) *Rationality Lemma.* If A is a polynomial, then the number $A(r)$ is a root of some nonzero polynomial of degree at most q .

In the sequel, we use the notation

$$\mathbb{Q}[\varepsilon_q] = \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \dots + a_{q-2}\varepsilon_q^{q-2} \mid a_0, \dots, a_{q-2} \in \mathbb{Q}\}.$$

6.4. Let q be a prime number, and let $r \in \mathbb{C} \setminus \mathbb{Q}[\varepsilon_q]$ be a number such that $r^q \in \mathbb{Q}[\varepsilon_q]$.

(a) Prove that the polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}[\varepsilon_q]$.

(b,c) Prove the analogues of the parts (b,c) of the previous problem for the polynomials with coefficients in $\mathbb{Q}[\varepsilon_q]$.

6.5. * Let q be a prime number, and let $r \in \mathbb{R} \setminus \mathbb{Q}$ be a number such that $r^q \in \mathbb{Q}$.

(a) *Strong Irreducibility Lemma.* The polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}[\varepsilon_q]$.

(b) *Strong Linear Independence Lemma.* If A is a polynomial of degree less than q with coefficients in $\mathbb{Q}[\varepsilon_q]$ and $A(r) = 0$, then $A = 0$.

6.6. (a) **Proposition.** *Assume that a polynomial (of degree greater than 1) is irreducible over \mathbb{Q} and has a root of the form $A(r)$, where A is a polynomial and r is a real number such that $r^q \in \mathbb{Q}$ for some prime q . Then this polynomial has degree q ; moreover, if $q \neq 2$, it has no other real root.*

(b) Does the statement still hold if we replace the primality condition for q by the condition $r^2, \dots, r^{q-1} \notin \mathbb{Q}$?

3. Equations of degree 3 solvable using one radical

Set

$$D_{pq} = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2.$$

We regard every implication in the next problem as a separate problem for which you may submit solution.

6.7. Theorem. For a cubic equation $x^3 + px + q = 0$ with rational coefficients, the following conditions are equivalent:

(1-solvability) at least one of its roots can be obtained on the real calculator with extracting at most one root;

($a + br + cr^2$) this equation has a root of the form $a + br + cr^2$, where $r \in \mathbb{R}$ and $a, b, c, r^3 \in \mathbb{Q}$; ($\sqrt{D_{pq}} \in \mathbb{Q}$) either it has a rational root, or $D_{pq} \geq 0$ and $\sqrt{D_{pq}} \in \mathbb{Q}$.

6.8. If y_0, y_1, y_2 are the three complex roots (with multiplicity) of the polynomial $x^3 + px + q$, then

$$-108D_{pq} = (y_0 - y_1)^2(y_1 - y_2)^2(y_0 - y_2)^2.$$

Assume that $\mu \in \mathbb{C}$. We introduce the following notation:

$$\mathbb{Q}[\mu] = \{P(\mu) \mid P \text{ is a polynomial with rational coefficients}\}.$$

Notice that this notation agrees with the particular case introduced above.

6.9. Assume that μ is a root of some nonzero polynomial. Prove that $1/t \in \mathbb{Q}[\mu]$ for every nonzero $t \in \mathbb{Q}[\mu]$.

6.10. (a) Assume that $r \in \mathbb{R} \setminus \mathbb{Q}$ and $r^n \in \mathbb{Q}$ for some integer $n > 1$. Take any $\alpha \in \mathbb{Q}[r]$. Then there exists a positive integer k such that $\alpha \in \mathbb{Q}[r^k]$ and $r^k \in \mathbb{Q}[\alpha]$ (in other words, $\mathbb{Q}[r^k] = \mathbb{Q}[\alpha]$).

(b) **Proposition.** Assume that a polynomial of degree n is irreducible over \mathbb{Q} ; moreover, assume that this polynomial is 1-solvable. Then this polynomial has a root of the form $A(r)$, where A is a polynomial, and a number $r \in \mathbb{R}$ satisfies $r^n \in \mathbb{Q}$.

The *complex calculator* has the same buttons as the real one, but it operates with complex numbers, giving all the complex values of the root when the button ‘ $\sqrt{}$ ’ is pressed. We say that a number can be obtained using the complex calculator, if the calculator can be used to get a set of numbers containing the given one.

We say that a polynomial is *k-solvable in the complex sense* if one of its roots can be obtained on the complex calculator using only k root extractions. The main problem 4.2 (as well as other problems in this section) remains interesting if we replace the real k -solvability by the complex one. The complex versions of these problems may turn out to be easier than the real ones.

6.11. (a) Every cubic polynomial is 2-solvable in the complex sense.

(b) Given rational p and q , decide whether the polynomial $x^3 + px + q$ is 2-solvable in the complex sense.

(c) Every polynomial of degree 4 is 4-solvable in the complex sense.

4. Equations of degree 4 solvable using one radical

6.12. Conjugation Theorem. Let $a, b, c, d, r^4 \in \mathbb{Q}$ and $r^2 \notin \mathbb{Q}$. Assume that the number $x_0 = a + br + cr^2 + dr^3$ is a root of some polynomial. Then the numbers

$$x_1 = a + bri - cr^2 - dr^3i, \quad x_2 = a - br + cr^2 - dr^3, \quad x_3 = a - bri - cr^2 + dr^3i$$

are also its roots.

6.13. Let a polynomial of degree 4 (with zero coefficient of x^3) have complex roots y_0, y_1, y_2 , and y_3 (regarding multiplicity). Then

(a) the number $\frac{y_0y_1 + y_2y_3}{2}$ is a root of the cubic resolution⁸ of our polynomial;

⁸Recall that the cubic resolution $R_f(\alpha)$ of a polynomial $f(x) = x^4 + px^2 + qx + s$ is a polynomial in α defined as the discriminant of the quadratic polynomial $(x^2 + \alpha)^2 - f(x)$ with respect to x , i.e.,

$$R_f(\alpha) = q^2 - 4(2\alpha - p)(\alpha^2 - s) = -8\alpha^3 + 4p\alpha^2 + 8s\alpha + (q^2 - 4ps).$$

(b) the numbers $\frac{y_0y_1 + y_2y_3}{2}$, $\frac{y_0y_2 + y_1y_3}{2}$, $\frac{y_0y_3 + y_1y_2}{2}$ are all the complex roots of the cubic resolution (regarding multiplicity).

6.14. Assume that $p, q, s \in \mathbb{Q}$ and $p < 0 < q$.

(a) If $q^2 = 2p(4s - p^2)$ and $\sqrt{2q} \in \mathbb{Q}$, then the polynomial $x^4 + px^2 + qx + s$ has a root which can be obtained using the real calculator extracting only one root which is the root of degree four.

(b) Is the converse true?

5. Formal expressibility in real radicals

The negative answer to 5.5.c (and to problem 6.17.b below) show that *a root of a cubic equation is not expressible in real radicals via its coefficients*. Try to realize why this result does not contradict the Cardano Formula which expresses the root of a cubic equation via its coefficients (the clue to the answer is in the expression for discriminant in terms of roots, see problem 6.8).

Definition. The polynomial f in variables x_1, x_2, \dots, x_n is *cyclically symmetric* if the polynomials $f(x_1, x_2, \dots, x_n)$ and $f(x_2, x_3, \dots, x_{n-1}, x_n, x_1)$ are equal.

6.15. Express $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ in radicals via cyclically symmetric polynomials in x_1, x_2, \dots, x_{10} .

The negative answer to 5.5.c can be derived from the following problem.

6.16. Let $f, g \in \mathbb{R}[x, y, z]$.

(a) If the polynomial f^q is cyclically symmetric for some positive integer q , then f itself is cyclically symmetric.

(b) If $fg = 0$, then $f = 0$ or $g = 0$.

(c) If $fg \neq 0$, then $f^2 + fg + g^2 \neq 0$.

6.17. We say that *the generic polynomial equation of degree n is solvable in real radicals* if there exist

- non-negative integers s, k_1, \dots, k_s and
- polynomials p_0, p_1, \dots, p_s with real coefficients and in $n, n+1, \dots, n+s$ variables, respectively,

such that if $a_0, \dots, a_{n-1}, x \in \mathbb{R}$ and

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0,$$

then there are $f_1, \dots, f_s \in \mathbb{R}$ for which

$$f_1^{k_1} = p_0(a_0, \dots, a_{n-1}), \quad f_2^{k_2} = p_1(a_0, \dots, a_{n-1}, f_1), \quad \dots$$

$$\dots \quad f_s^{k_s} = p_{s-1}(a_0, \dots, a_{n-1}, f_1, \dots, f_{s-1}), \quad x = p_s(a_0, \dots, a_{n-1}, f_1, \dots, f_s).$$

Note that we have defined a property of *the number n* rather than of a specific equation with given coefficients like in the *Galois Theorem* [S].

(a) The generic polynomial equation of degree 2 is solvable in real radicals.

(b)* The generic polynomial equation of degree 3 is not solvable in real radicals.

(c)* The similar result for each $n \geq 3$.

The results of problems 5.5.c and 6.17.b (and the comparison of them with the Cardano Formula) show that the definition of expressibility in real radicals given above is not a perfect formalization of the concept of solvability in radicals. On one hand, it is more reasonable to consider complex numbers instead of reals — this idea is realized in Section 7. On the other hand, we can work with numbers rather than with polynomials — this leads to the Galois Theorem [S]. However, investigating this imperfect formalization, one may see the main idea of the proof of Ruffini's theorem, see [S'].

Hints and Solutions distributed at the Semifinal

1. Solving equations of degree 3 and 4

1.3. (c) *Answer:* If $p = q = 0$, then there is one root. Otherwise, if $D_{pq} > 0$, then there is one root, if $D_{pq} = 0$, there are two roots, and if $D_{pq} < 0$, there are three roots.

1.4. (c) *Answer:* $x = -1 - \sqrt[3]{2}$.

Hint: By the result of 1.5.a, the equation $x^3 - 3\sqrt[3]{2}x + 3 = 0$ is equivalent to the equation

$$(x + b + c)(x^2 + b^2 + c^2 - bc - bx - cx) = 0, \quad \text{where } b = 1 \quad \text{and} \quad c = \sqrt[3]{2}.$$

(d) *Answer:* $2 \cos \frac{\pi}{9}$, $2 \cos \frac{7\pi}{9}$, and $2 \cos \frac{13\pi}{9}$.

Substituting $x = 2y$ we transform the equation $x^3 - 3x - 1 = 0$ to $4y^3 - 3y = \frac{1}{2}$. Using the identity $\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$ we get that all the numbers $\cos \frac{\pi}{9}$, $\cos \frac{7\pi}{9}$, and $\cos \frac{13\pi}{9}$ are roots of $4y^3 - 3y = \frac{1}{2}$.

1.5. (a,b) *Answer:*

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2 + b^2 + c^2 - ab - bc - ca) = (a+b+c)(a + b\varepsilon_3 + c\varepsilon_3^2)(a + b\varepsilon_3^2 + c\varepsilon_3).$$

1.6. (a) *Answer:* Del Ferro's method is applicable, if $D_{pq} \geq 0$.

Theorem. Let $p, q \in \mathbb{R}$.

If $D_{pq} \geq 0$, then the equation $x^3 + px + q = 0$ has a unique real root

$$\sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}} - \sqrt[3]{\frac{q}{2} + \sqrt{D_{pq}}}.$$

If $D_{pq} = 0$, then all real roots of the equation are $-2\sqrt[3]{q/2}$ and $-\sqrt[3]{q/2}$ (they are distinct, provided that $q \neq 0$).

(b) **Theorem.** Let $p, q \in \mathbb{C}$ and $pq \neq 0$. Let

- $\sqrt{D_{pq}}$ be any of the two values of a square root of D_{pq} ;
- u be any of the three values of a cubic root of $-\frac{q}{2} - \sqrt{D_{pq}}$;
- $v = -\frac{p}{3u}$. (Since $p \neq 0$, we have $(q/2)^2 \neq D_{pq}$, whence $u^3 = -\frac{q}{2} - \sqrt{D_{pq}} \neq 0$.)

Then the three roots of the equation $x^3 + px + q = 0$ are $u + v$, $u\varepsilon_3 + v\varepsilon_3^2$, and $u\varepsilon_3^2 + v\varepsilon_3$. (They are not necessarily distinct, even if $q \neq 0$.)

1.7. *Answers:*

(a) $\frac{-3\sqrt{2} \pm \sqrt{10 + 12\sqrt{2}}}{2}$; (b) $\frac{-\sqrt{2} \pm \sqrt{4\sqrt{2} - 2}}{2}$; (c) $\frac{\sqrt{2} \pm \sqrt{8\sqrt{2} - 6}}{2}$;
 (d) $\sqrt{2} \pm (\sqrt[4]{2} + \sqrt[4]{8})$.

2. Representability with use of only one radical

2.1. Answers: (a,a'',b,c,d) — yes; (a',e,f,g,h) — no.

(a,c) $\sqrt{3 + 2\sqrt{2}} = \sqrt[3]{7 + 5\sqrt{2}} = 1 + \sqrt{2}$.

(a'') Notice that $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$. (This equality can be found easily by the method of undetermined coefficients. Another way of obtaining it is the Euclid algorithm used to find the linear representation of the g.c.d. of $x^3 - 2$ and $x^2 + 5x + 1$, see solution of 3.2.b; that problem claims in fact that such coefficients can be found always.) Therefore,

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(b) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(d) $\cos(2\pi/5) = (\sqrt{5} - 1)/4$.

(e) Assume that it is possible. Then we get $2 = (\sqrt[3]{2})^3 = (a^3 + 3ab) + (3a^2 + b)\sqrt{b}$. Since $3a^2 + b \neq 0$, we have $\sqrt{b} \in \mathbb{Q}$. Thus $\sqrt[3]{2} \in \mathbb{Q}$, which is a contradiction.

Another proofs may be obtained similarly to those of (f,g) or of Proposition 2.4.

(g) Assume that it is possible. By 2.2, our number $\cos(2\pi/9)$ is a root of $4x^3 - 3x = -\frac{1}{2}$. Now by Corollary 2.3.f this equation has a rational root, which is wrong.

Another proof is similar to that of Proposition 2.4.

2.2. By the triple angle formula for cosine we have $-1/2 = \cos(2\pi/3) = 4\cos^3(2\pi/9) - 3\cos(2\pi/9)$.

2.3. (e) Let P be a given polynomial, and set $G(t) = P(a + bt)$. Then $G(r) = 0$. By (d), we get $G(-r) = 0$.

(f) Follows from (e) combined with the Vieta theorem.

2.4. Arguing indirectly, suppose that the given polynomial $P(x)$ has a root $x_0 = a \pm \sqrt{b}$. By corollary 2.3.e and analogously to it, the number $x_1 = a \mp \sqrt{b}$ is also a root of P . If $b = 0$, then the statement is obvious; so we assume that $b \neq 0$. This implies $x_0 \neq x_1$. Therefore, P is divisible by $(x - a)^2 - b$. Since the degree of P is greater than 2, it is reducible. This is a contradiction.

2.5. *Answer:* (a,b,c,d,e,g) no; (f) yes.

Set $r = \sqrt[3]{2}$.

(a) *First solution.* Assume that it is possible. Then

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Since the polynomial $x^3 - 2$ has no rational roots, it is irreducible over \mathbb{Q} . Thus, $2ab + 2c^2 = 2ac + b^2 = 0$ (cf. 2.6.b). So we have $b^3 = -2abc = 2c^3$. It follows that either $b = c = 0$ or $\sqrt[3]{2} = b/c$. Both cases are impossible.

Second solution. Assume that it is possible. Set $P(x) = x^2 - 3$. Then P has three roots x_1, x_2 , and x_3 defined in Corollary 2.6.e. Since none of them is rational, the equality $b = c = 0$ does not hold. So, by Strong Linear Independence Lemma 2.6.b', all three roots are distinct. This is a contradiction.

(b) Assume that it is possible. The number $\cos(2\pi/9)$ is a root of the equation $4x^3 - 3x = -\frac{1}{2}$. Its other two real roots are $\cos(8\pi/9)$ and $\cos(4\pi/9)$.

On the other hand, the polynomial $8x^3 - 6x - 1$ has three roots x_1, x_2, x_3 defined in Corollary 2.6.e. Since none of them is rational, the equality $b = c = 0$ is impossible. By Strong Linear Independence Lemma 2.6.b', all three roots are distinct.

Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_3$. Thus, x_2 and x_3 can not be both real and distinct. This is a contradiction.

(c) Assume the contrary. According to Rationality Lemma 2.7.a, there exists a cubic polynomial whose root is $a + br + cr^2$. But the polynomial $x^5 - 3$ is irreducible over \mathbb{Q} . This is a contradiction.

2.6. (a) Suppose that $x^3 - r^3$ is reducible. Then it has a rational root. This is a contradiction.

(b) Assume the contrary. Divide $x^3 - r^3$ by $a + bx + cx^2$ with residue. Due to (a), the residue is nonzero. Both polynomials $x^3 - r^3$ and $a + bx + cx^2$ have a root $x = r$. Hence the residue has the same root $x = r$. This implies that the residue is linear and has an irrational root, which is impossible.

(c) Divide our polynomial by $x^3 - r^3$ with residue. Substituting $x = r$ and applying Linear Independence Lemma (b), we get that the residue is zero.

(d) By (c), if $R^3 = r^3$, then R is a root of our polynomial.

(e) Let P be the given polynomial, and set $G(t) = P(a + bt + ct^2)$. Then $G(r) = 0$. By (d) we get $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(a') If our polynomial is reducible, it must have a root in $\mathbb{Q}[\varepsilon_3]$. Therefore, $r \in \mathbb{Q}[\varepsilon_3] \cap \mathbb{R} = \mathbb{Q}$, which is a contradiction.

This part can also be derived from (b').

(b') Consider the real and imaginary parts separately.

This part can also be derived from (a').

2.7. (a) *First solution.* Due to the substitution $x = y + a$, it suffices to prove the claim for the vase when $a = 0$. Now notice that the number $t = br + cr^2$ satisfies $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

(In other words, by the equality from the solution of 1.5.a, the number $a + br + cr^2$ is a root of the polynomial $(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6$.)

Second solution. Set $x_0 = a + br + cr^2$. Expand the numbers x_0^k with $k = 0, 1, 2, 3$ as polynomials in r :

$$x_0^k = a_k + b_k r + c_k r^2.$$

In order to solve the problem, it suffices to find numbers $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$, not all zeroes, such that $\lambda_0 + \lambda_1 \alpha + \lambda_2 \alpha^2 + \lambda_3 \alpha^3 = 0$. This condition will be satisfied if these numbers satisfy the system of equations

$$\lambda_0 a_0 + \cdots + \lambda_3 a_3 = 0, \quad \lambda_0 b_0 + \cdots + \lambda_3 b_3 = 0, \quad \lambda_0 c_0 + \cdots + \lambda_3 c_3 = 0.$$

It is known that a homogeneous (i.e. with zero right hand parts) system of linear equations with rational coefficients has a nontrivial rational solution, provided that the number of equations is less than the number of variables. This yields the required result.

The obtained polynomial has degree 3 and is irreducible; this follows from problem 2.6.eb'.

Remark. Yet another proof is shown in the first solution of (more general) Rationality Lemma 6.3.d.

3. Equations of degree 3 solvable using one radical

3.1. (b) Clearly, Cheburashka can obtain $\sqrt[3]{2 + \sqrt{3}}$ for 2 yuans. It remains to notice that

$$\sqrt[3]{2 - \sqrt{3}} = \frac{1}{\sqrt[3]{2 + \sqrt{3}}} = (\sqrt[3]{2 + \sqrt{3}})^2 \cdot (2 - \sqrt{3}).$$

(The last equality shows that one may avoid division by an irrational number in this case.)

(c) See the solution of 2.1.a''.

3.2. (b) Clearly, each described number can be obtained for 1 yuan. To prove the converse, as before, we show that all the obtained numbers have the form $a + br + cr^2$, where $r = \sqrt[3]{s}$ is a cubic root obtained for 1 yuan. The only nontrivial step is, however, a bit harder now: we need to prove that a number $\frac{1}{a + br + cr^2}$ has the required form (in case $r = \sqrt[3]{s} \notin \mathbb{Q}$).

By the Irreducibility Lemma, the polynomial $x^3 - r^3$ is irreducible over \mathbb{Q} , so it is coprime with $a + bx + cx^2$. Therefore, there exist polynomials g and h such that $h(x)(a + bx + cx^2) + g(x)(x^3 - r^3) = 1$. Then $h(r) = \frac{1}{a + br + cr^2}$, which yields the result.

3.3. (a) As an example one may take the equation $x^3 - 3x + 2 = 0$ with root 1.

(a') An example is provided by the equation $x^3 - 6x - 6 = 0$ with a root $\sqrt[3]{2} + \sqrt[3]{4}$ (cf. problem 3.1.b). One may find this equation as in the proof of Rationality Lemma 2.7.a.

(b3, b2) *Answer:* Yes.

By del Ferro's method we get that one of the roots of our equation is

$$\sqrt[3]{-3 + \sqrt{10}} + \sqrt[3]{-3 - \sqrt{10}} = \sqrt[3]{-3 + \sqrt{10}} - \frac{1}{\sqrt[3]{-3 + \sqrt{10}}}.$$

(b1) A negative answer follows from the solution of (d), i.e., from Theorem 6.7.

(c) By 1.1.a we may assume that the equation has the form $x^3 + px + q = 0$. If $p = 0$, the statement is trivial. Otherwise, since the equation has only one real root, we obtain that $D_{pq} > 0$ due to the solution of 1.3. Therefore, the number $u = \sqrt[3]{-\frac{q}{2} - \sqrt{D_{pq}}}$ appearing in the theorem in solution of 1.6.a can be obtained for 1 yuan. After that, the number $v = \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}} = -\frac{p}{3b}$ is obtained for free. By the same theorem, a root $u+v$ of the initial equation also can be obtained for 2 yuans.

(d) See Theorem 6.7.

4. Equations of degree 4 solvable using one radical

4.1. (b) *Hint*: One may express the root x_0 of the polynomial in terms of p and s , and then equalize this expression for x_0 to $br + cr^2 + dr^3$, where $b, c, d, r^4 \in \mathbb{Q}$, $r \in \mathbb{R}$.

(c) *Conjecture*: no.

Try to prove the following statement: Assume that a degree 4 polynomial has a cubic resolution with three real roots (in other words, this resolution has a negative *discriminant*); then this polynomial is not 10000-solvable. On the other hand, the formula presenting a root of a degree four polynomial whose the cubic resolution does not have three distinct real roots (or it has nonnegative discriminant) using four root extractions is the aim of problem 6.1.a.

4.3. (a) For example, the polynomial $x^4 - 12x^2 - 24x - 14$ from problem 1.7.d has a root $\sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$. (How can one *find* this polynomial, given its root?)

(b) *Answer*: yes, due to problem 6.14.a.

5. Formal expressibility in real radicals

5.1. (b) Consider the triples $(x, y, z) = (0, 1, -1)$ and $(x, y, z) = (0, -1, 1)$.

5.2. (b) $x = \frac{(x+y) + (x-y)}{2}$.

5.3. *Answer*: (a) $\sigma_1^2 - 2\sigma_2$; (b) $\sigma_1\sigma_2 - 3\sigma_3$; (c) $\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

(d) Apply 5.4.c.

5.4. (c) Again, we use the lexicographical induction on the multi-degree of the polynomial. Given a symmetric polynomial of multi-degree (k, ℓ, m) with $k \geq \ell \geq m$ and $k \geq 1$ (i.e., the lexicographically leading monomial of the polynomial has the form $ax^k y^\ell z^m$), one may reduce it to the polynomial $f - a\sigma_1^{k-\ell}\sigma_2^{\ell-m}\sigma_3^m$.

5.5. (a) Notice that the polynomial $(x-y)^2(y-z)^2(z-x)^2$ is symmetric. One may also reduce this problem to the next one.

(b) Set $M = x^2y + y^2z + z^2x$ and $N = y^2x + x^2z + z^2y$. Then $M+N$ and MN are symmetric polynomials. Therefore, they are polynomials in elementary symmetric functions $\sigma_1, \sigma_2, \sigma_3$. (We present the explicit expressions in the solution of 6.8.) Finally, M itself now can be expressed via $M+N$ and MN by the formula providing the roots of a quadratic equation.

Hints and Solutions distributed at the Final

1. Solving equations of degree 3 and 4

1.6. *Proof of the theorem formulated in (a).* Set $u = -\sqrt[3]{\frac{q}{2} + \sqrt{D_{pq}}}$ and $v = \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}}$. We have $uv = -p/3$ and $u^3 + v^3 = -q$. By the formula from the solution of 1.5.a applied to $a = x$, $b = -u$, and $c = -v$, the number $u+v$ is a root of the polynomial $x^3 + px + q = x^3 - 3uvx - u^3 - v^3$. Since $2(x^2 + u^2 + v^2 - xu - xv - uv) = (x-u)^2 + (x-v)^2 + (u-v)^2$, in the case $D_{pq} > 0$ we have no other roots, and if $D_{pq} = 0$, then there is an additional (multiple) root $u = v = -\sqrt[3]{q/2}$.

Proof of the theorem formulated in (b). We have $uv = -p/3$ and $u^3 + v^3 = -q$. So it suffices to apply the formula from the solution of 1.5.b to $a = x$, $b = -u$, and $c = -v$.

6.1. If $q = 0$, then the equation is biquadratic, so it is easy to solve it. Henceforth we assume that $q \neq 0$.

(a) **Theorem.** *Suppose that $p, q, s \in \mathbb{R}$ and $q \neq 0$. Then there exists $\alpha > p/2$ such that $q^2 = 4(2\alpha - p)(\alpha^2 - s)$. For each such value of α define $A = \sqrt{2\alpha - p}$. Then all the real roots of the equation $x^4 + px^2 + qx + s = 0$ are:*

$$\begin{cases} \text{no roots,} & \text{if } 2\alpha + p > 2|q|/A; \\ x_{\pm} = \left(-A \pm \sqrt{-2\alpha - p + \frac{2q}{A}}\right)/2, & \text{if } -2q/A < 2\alpha + p \leq 2q/A; \\ y_{\pm} = \left(A \pm \sqrt{-2\alpha - p - \frac{2q}{A}}\right)/2, & \text{if } 2q/A < 2\alpha + p \leq -2q/A; \\ x_{\pm}, y_{\pm}, & \text{if } 2\alpha + p \leq -2|q|/A \end{cases}$$

Proof. Set $R(x) = 4(2x - p)(x^2 - s) - q^2$. Note that $R(p/2) = -q^2 < 0$. On the other hand, for large enough values of x we have $R(x) > 0$. By the Intermediate value theorem, there exists $\alpha > p/2$ such that $R(\alpha) = 0$.

Since $p = 2\alpha - A^2$ and α is a root of the resolution, we get $s = \alpha^2 - \frac{q^2}{4(2\alpha - p)} = \alpha^2 - \frac{q^2}{4A^2}$. Therefore,

$$x^4 + px^2 + qx + s = \left(x^2 - Ax + \alpha + \frac{q}{2A}\right) \left(x^2 + Ax + \alpha - \frac{q}{2A}\right).$$

Solving two quadratic equations, we obtain the required formulas.

(b) **Theorem.** *Suppose $p, q, s \in \mathbb{C}$ and $q \neq 0$. Denote by α any of the roots of the equation $q^2 = 4(2\alpha - p)(\alpha^2 - s)$, and let A be any of two values of square root of $2\alpha - p$. Then all the roots of the equation $x^4 + px^2 + qx + s = 0$ are*

$$\left(A + \sqrt{-2\alpha - p - \frac{2q}{A}}\right)/2 \quad \text{and} \quad \left(-A + \sqrt{-2\alpha - p + \frac{2q}{A}}\right)/2,$$

where \sqrt{y} is a multi-valued function providing both values of the root of y . Notice that, since $q^2 = 4A^2(\alpha^2 - s) \neq 0$, we have $A \neq 0$.

The proof is similar to the proof of the theorem in part (a).

Remark. One may also express all complex roots of the equation as

$$x = (\pm\sqrt{2\alpha_1 - p} \pm \sqrt{2\alpha_2 - p} \pm \sqrt{2\alpha_3 - p}),$$

where α_1, α_2 , and α_3 are the three roots of the cubic resolution, the number of 'minuses' in the formula is even, and the values of the roots are chosen so that their product equals $-q$.

2. Representability with use of only one radical

2.1. (a') Assume that this number is representable. The roots of the polynomial $P(x) = (x^2 - 2)^2 - 2$ are four numbers of the form $\pm\sqrt{2 \pm \sqrt{2}}$, where the choices of signs can be made independently. One can easily check that this polynomial has no rational roots, and moreover, that the product of any two its roots is also irrational. This means that the polynomial $P(x)$ has no non-constant factors of degree at most 2, thus $P(x)$ is irreducible. This contradicts Proposition 2.4.

(h) (I. Braude-Zolotarev) The equality $1 + \varepsilon_7 + \varepsilon_7^2 + \cdots + \varepsilon_7^6 = 0$ implies that $\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) = -1/2$. Applying the formulas $\cos 2\alpha = 2\cos^2 \alpha - 1$ and $\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$ we find that $\cos(2\pi/7)$ is a root of the equation $8t^3 + 4t^2 - 4t - 1 = 0$. Substituting $u = 2t$ we get $u^3 + u^2 - 2u - 1 = 0$. Since the last equation has no rational roots, the same holds for $8t^3 + 4t^2 - 4t - 1 = 0$. Now the negative answer to the question follows from 2.3.f.

2.5. As in the previous parts, we set $r = \sqrt[3]{2}$.

(d) Similarly to (a) and (b), the complex roots of the polynomial $x^3 - 3$ have the form x_1, x_2, x_3 (see Corollary 2.6.e). Thus, $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$ for some $s \in \{1, 2\}$. By Strong Linear Independence Lemma 2.6.b', we have $a = 0$ and $bc = 0$. This implies that either $\sqrt[3]{3} = br$ or $\sqrt[3]{3} = cr^2$, which is a contradiction.

(e) Similar to (b).

(f) This equation has a root $\sqrt[3]{2} + \sqrt[3]{4}$.

(g) The unique real root of this equation is $\sqrt[3]{3} + \sqrt[3]{9}$. Assume that this number is representable in the required form. Then all the numbers x_1, x_2 , and x_3 introduced in Corollary 2.6.e are roots of the given equation. By the Strong Linear Independence Lemma 2.6.b' these roots are distinct, so they are all roots of the equation.

On the other hand, by the theorem formulated in the solution of 1.6.b, all roots of the equation are

$$y_1 = \sqrt[3]{3} + \sqrt[3]{9}, \quad y_2 = \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_3 = \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

Since the equation has exactly one real root, we have $x_0 = y_0$; then we get either $x_1 = y_1$, $x_2 = y_2$, or $x_2 = y_1$, $x_1 = y_2$.

Denote $P(x) = \sqrt[3]{3}x + \sqrt[3]{9}x^2$. Set also $S(x) = a + brx + cr^2x^2$ for the former case above, and $S(x) = a + brx^2 + cr^2x$ for the latter case. Then the polynomial $P(x) - S(x)$ has three distinct roots 1, ε_3 , and ε_3^2 . But the degree of this polynomial is at most 2; thus $P = S$ and, in particular, either $\sqrt[3]{3} = br$ or $\sqrt[3]{3} = cr^2$. Both cases are impossible.

2.7. (b) By Rationality Lemma 2.7.a, there exists a cubic polynomial having $a + br + cr^2$ as a root. Since the given polynomial P is irreducible over \mathbb{Q} and has the same root, we conclude that $\deg P \leq 3$.

On the other hand, P has three roots x_1, x_2, x_3 defined in Corollary 2.6.e. Since P is irreducible, none of its roots is rational. So, the equality $b = c = 0$ cannot hold. By Strong Linear Independence Lemma 2.6.b', all the roots of P are distinct. Hence $\deg P = 3$.

Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_3$. This implies that x_2 and x_3 cannot be simultaneously real and distinct. So, $x_2, x_3 \in \mathbb{C} \setminus \mathbb{R}$. It follows that P has a unique real root.

6.2. Answers: no (in all parts).

We use the following notation: $r = \sqrt[7]{2}$ and $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_6x^6$.

(a) Assume that it is possible. By the Conjugation Theorem 6.3.c, the polynomial $x^2 - 3$ has roots $A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \dots, 6$. Since this polynomial has no rational roots, Strong Linear Independence Lemma 6.5.b yields that these roots are distinct. This is a contradiction.

(b') Assume that it is possible. The given polynomial P has no rational roots by Eisenstein's criterion. Therefore, Conjugation Theorem 6.3.c and Strong Linear Independence Lemma 6.5.b

imply that P has distinct roots $x_k := A(r\varepsilon_7^k)$ with $k = 0, 1, 2, \dots, 6$. Since $P(0) > 0$, $P(1) < 0$, and $P(2) > 0$, the polynomial P has a real root x_k distinct from x_0 .

Notice now that $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Therefore, $x_k = \overline{x_k} = x_{7-k}$, which is a contradiction.

(b) Assume that it is possible. Let P be a polynomial such that $\cos 7x = p(\cos x)$ (prove that it exists!). The roots of the polynomial $2P(x) + 1$ are real numbers $y_k = \cos \frac{2(3k+1)\pi}{21}$ with $k = 0, \dots, 6$. One of them, namely $y_2 = -1/2$, is rational.

On the other hand, we claim that y_0 is irrational. (Otherwise we would have $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$, whence $\varepsilon_{21} = a + i\sqrt{b}$ for some $a, b \in \mathbb{Q}$. Then the number $\varepsilon_7 = \varepsilon_{21}^3$ would also have this form. But the number ε_7 is a root of the irreducible⁹ polynomial $1 + x + \dots + x^6$, which contradicts the analogue of Proposition 2.4 for the numbers of the form $a + i\sqrt{b}$.)

Thus, the number y_0 is an irrational root of the polynomial $\frac{2P(x) + 1}{x - y_2}$ which has degree 6. However, Conjugation Theorem 6.3.c combined with Strong Linear Independence Lemma 6.5.b show that this polynomial has seven distinct roots, which is absurd.

(c) Assume that the number has the required form. Then the Rationality Lemma 6.3.d yields that there exists a nonzero polynomial of degree at most 7 having $\sqrt[11]{3}$ as a root. This contradicts the rational irreducibility of the polynomial $x^{11} - 3$.

(d) Assume that the number has the required form. Similarly to (a) and (b') we obtain that the complex roots of the polynomial $x^7 - 3$ have the form $A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \dots, 6$. Therefore, $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ for some $s \in \{1, 2, 3, 4, 5, 6\}$. Now, by Strong Linear Independence Lemma 6.5.b we obtain that $a_k = 0$ for all $k \neq s$. Therefore, $\sqrt[7]{3} = a_s r^s$, which is a contradiction.

6.3. (a) The roots of the polynomial $x^q - r^q$ are precisely $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$. Assume that $x^q - r^q$ is reducible over \mathbb{Q} . Then the absolute value of a constant term of one of its irreducible factors is rational and equals to the product of absolute values of k of these roots, $0 < k < q$. Therefore, $r^k \in \mathbb{Q}$. Since q is prime, we get $kx + qy = 1$ for some integers x, y . Thus $r^{kx} = r^{(r^q)^{-y}}$, which implies $r \in \mathbb{Q}$. This is a contradiction.

(b) Arguing indirectly, take a polynomial $A(x)$ violating the lemma statement of the minimal possible degree. Let $R(x)$ be the remainder of $x^q - r^q$ divided by $A(x)$. Then we have $\deg R < \deg A$, $R(r) = 0$, and $R(x) \neq 0$ by (a). This contradicts the choice of A .

(c) The solution is similar to that of 2.3.cd, 2.6.cd, and 6.12, with the use of (b).

(d) *First solution.* The product

$$\Pi = (x - A(x_0))(x - A(x_1)) \dots (x - A(x_{q-1}))$$

is a symmetric polynomial in x_0, x_1, \dots, x_{q-1} . This means that Π can be expressed as a polynomial in x and the elementary symmetric polynomials in x_0, x_1, \dots, x_{q-1} . The values of these elementary symmetric polynomials at $x_k = r\varepsilon_q^k$ ($k = 0, 1, \dots, q-1$) are the coefficients of the polynomial $x^q - r^q$, thus they are rational. So Π is the required polynomial.

Second solution. One may also argue exactly as in the second proof of Rationality Lemma 2.7.a, with 3 being replaced by q (e.g., the range ' $k = 0, 1, 2, 3$ ' in the first line of the proof should be replaced by ' $k = 0, 1, \dots, q$ ').

6.4. (a) Assume that our polynomial is reducible, and consider any its nontrivial unitary factor. As in proof of Lemma 6.3.a, the constant term of this factor has the form $\pm r^k \varepsilon_q^m$ and lies in $\mathbb{Q}[\varepsilon_q]$; therefore, $r^k \in \mathbb{Q}[\varepsilon_q]$. Now, again as in proof of Lemma 6.3.a, we obtain that $r \in \mathbb{Q}[\varepsilon_q]$. This is a contradiction.

(b,c) The proofs are similar to those of 6.3.bc; one may need to implement problem 6.9.

⁹The irreducibility of the polynomial $g(x) = 1 + x + \dots + x^6$ may be proved, e.g., by applying Eisenstein's criterion to the polynomial $g(x+1)$. On the other hand, in our situation it suffices to prove that g has no divisors with rational coefficients of degree 1 and 2.

6.5. (a) Suppose that the polynomial is reducible. Similarly to the proof of Irreducibility Lemma 6.4.a (over $\mathbb{Q}[\varepsilon_q]$), we establish that $r \in \mathbb{Q}[\varepsilon_q]$. Thus $r^2, r^3, \dots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

We claim that in this case r is a root of some polynomial of degree at most $q-1$; this clearly contradicts 6.3.a.

For the proof, we argue similarly to the second solution of 2.7.a. Expand the numbers r^k with $k = 0, 1, \dots, q-1$ as polynomials in ε_q :

$$r^k = a_{k,0} + a_{k,1}\varepsilon_q + \dots + a_{k,q-2}\varepsilon_q^{q-2}.$$

Now it suffices to find numbers $\lambda_0, \lambda_1, \dots, \lambda_{q-1} \in \mathbb{Q}$, not all zeroes, such that all the equations

$$\lambda_0 a_{0,m} + \dots + \lambda_{q-1} a_{q-1,m} = 0 \quad \text{for } m = 0, 1, \dots, q-2$$

are satisfied. This is true by the theorem used in the aforementioned solution of 2.7.a.

(b) Follows from (a).

6.6. (a) *Hint:* Similar to the proofs of Propositions 2.4, 2.7.b and to the solutions of 6.2.ab'c. Apply Conjugation Theorem 6.3.c, Rationality Lemma 6.3.d, and Strong Linear Independence Lemma 6.5.b arriving at a contradiction.

Solution: Assume the contrary; let P be the given polynomial. The case $q < \deg P$ contradicts Rationality Lemma 6.3.d; so $q \geq \deg P$. Now, by Conjugation Theorem 6.3.c and Strong Linear Independence Lemma 6.5.b, the polynomial P has pairwise distinct roots $x_k = A(r\varepsilon_q^k)$ for $k = 0, 1, 2, \dots, q-1$. This is impossible unless $q = \deg P$; this proves the first assertion. Finally, if $q \neq 2$, then the relations $\overline{x_k} = x_{q-k} \neq x_k$ for $k = 1, 2, \dots, q-1$ yield the uniqueness of the real root.

(b) *Answer:* No. Set $r = \sqrt[6]{2}$; then the number $A(r)$, where $A(x) = x^3$, is a root of $x^2 - 2$.

3. Equations of degree 3 solvable using one radical

3.2. (c) Similarly to the previous parts, the only nontrivial claim is the following one:

Let $0 \neq d = a_0 + a_1 r + \dots + a_{n-1} r^{n-1}$, where a_0, \dots, a_{n-1}, r^n are rational; then the number $1/d$ is representable in a required form.

The arguments from part (b) do not apply directly, since the polynomial $x^n - r^n$ may be reducible over \mathbb{Q} . In order to make them work, it suffices to replace this polynomial by its irreducible factor having r as a root.

We present also a different proof of the claim. We implement the following result similar to Rationality Lemma 2.7.a: *If $a_0, \dots, a_{n-1}, r^n \in \mathbb{Q}$, then the number $d = a_0 + a_1 r + \dots + a_{n-1} r^{n-1}$ is a (not necessarily unique) root of some polynomial whose degree does not exceed n .*

Suppose that d is a root of a polynomial $p_k d^k + \dots + p_0$; we may assume that $p_0 \neq 0$. Then

$$\frac{1}{d} = \frac{p_0}{p_0 d} = \frac{-p_1 d - \dots - p_k d^k}{p_0 d} = \frac{-p_1 - \dots - p_k d^{k-1}}{p_0}.$$

3.4. See [S, §§1.2 and 5.3].

6.7. $(\sqrt{D_{pq}} \in \mathbb{Q}) \Rightarrow (1\text{-solvability})$. Set $r = \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}}$. By Cardano's formula (see the solution of problem 1.6), the unique real root of the equation $x^3 + px + q = 0$ equals

$$r - \frac{p}{3r} = r - \frac{p}{3r^3} \cdot r^2 = r - \frac{p}{3(-\frac{q}{2} + \sqrt{D_{pq}})} \cdot r^2.$$

$(a + br + cr^2) \Rightarrow (\sqrt{D_{pq}} \in \mathbb{Q})$. If $r \in \mathbb{Q}$ or $b = c = 0$, then the equation has a rational root. In the remaining case, denote $\varepsilon = \varepsilon_3$. Each of the numbers x_1, x_2 , and x_3 defined in

Corollary 2.6.e is a root of our equation. By Strong Linear Independence Lemma 2.6.b', these three roots are distinct. Therefore, x_1 , x_2 , and x_3 are all the roots of our equation. Now, by 6.8 we have

$$\begin{aligned} -108D_{pq} &= (x_2 - x_3)^2(x_1 - x_3)^2(x_1 - x_2)^2 \\ &= (br(\varepsilon - \varepsilon^2) + cr^2(\varepsilon^2 - \varepsilon))^2 (br(1 - \varepsilon) + cr^2(1 - \varepsilon^2))^2 (br(1 - \varepsilon^2) + cr^2(1 - \varepsilon))^2 \\ &= \varepsilon^2(1 - \varepsilon)^6 (br - cr^2)^2 (br + cr^2(1 + \varepsilon))^2 (br(1 + \varepsilon) + cr^2)^2. \end{aligned}$$

Since $(1 + \varepsilon)(1 + \varepsilon^2) = (-\varepsilon)(-\varepsilon^2) = 1$ and $(\varepsilon - 1)^3 = 3\varepsilon - 3\varepsilon^2 = 3\sqrt{3}i$, we obtain

$$\begin{aligned} -108D_{pq} &= -27\varepsilon^2(1 + \varepsilon)^2 (br - cr^2)^2 (br(1 + \varepsilon^2) + cr^2)^2 (br(1 + \varepsilon) + cr^2)^2 \\ &= -27(\varepsilon + \varepsilon^2)^2 (br - cr^2)^2 (b^2r^2 + br \cdot cr^2 + c^2r^4)^2 = -27((br)^3 - (cr^2)^3)^2. \end{aligned}$$

This yields the required result.

(1-solvability) $\Rightarrow (a + br + cr^2)$. If the given polynomial is reducible, then it has a rational root which has the required form. Otherwise the result follows directly from Proposition 6.10.b.

6.8. Set

$$M = y_0^2 y_1 + y_1^2 y_2 + y_2^2 y_0 \quad \text{and} \quad N = y_0^2 y_2 + y_1^2 y_0 + y_2^2 y_1.$$

Then $(y_0 - y_1)(y_1 - y_2)(y_0 - y_2) = M - N$. Therefore,

$$(y_0 - y_1)^2 (y_1 - y_2)^2 (y_0 - y_2)^2 = (M + N)^2 - 4MN = (3q)^2 - 4(p^3 + 9q^2) = -4p^3 - 27q^2 = -108D_{pq};$$

the second equality above follows from the relations $y_0 + y_1 + y_2 = 0$ (due to the Vieta theorem) combined with

$$\begin{aligned} M + N &= (y_0 + y_1 + y_2)(y_0 y_1 + y_1 y_2 + y_2 y_0) - 3y_0 y_1 y_2 = 0 \cdot p + 3q = 3q, \\ MN &= (y_0 y_1 + y_1 y_2 + y_2 y_0)^3 + y_0 y_1 y_2 (y_0 + y_1 + y_2)^3 - 6y_0 y_1 y_2 \sum_{i \neq j} y_i^2 y_j - 9y_0^2 y_1^2 y_2^2 = \\ &= p^3 - q \cdot 0^3 + 6q(p \cdot 0 + 3q) - 9q^2 = p^3 + 9q^2. \end{aligned}$$

6.9. Similarly to the proof of Calculator theorem 3.2.c.

6.10. (a) The number r is a root of some nonzero polynomial with coefficients in $\mathbb{Q}[\alpha]$ (e.g., $x^n - r^n$). Choose such polynomial $f(x)$ of the minimal possible degree k .

Consider the g.c.d. of $x^n - r^n$ and f ; it also has r as a root, its coefficients lie in $\mathbb{Q}[\alpha]$, and its degree does not exceed k ; this means that this g.c.d. is f itself. So all the complex roots of f have the form $r\varepsilon_n^m$. Then, by the Vieta theorem, the absolute value of the constant term of f equals r^k for some $k \leq n - 1$. Since this constant term is real, we obtain that $r^k \in \mathbb{Q}[\alpha]$.

Now it remains to prove that $\alpha \in \mathbb{Q}[r^k]$. Since $\alpha \in \mathbb{Q}[r]$, we have

$$\alpha = b_0(r^k) + r b_1(r^k) + \dots + r^{k-1} b_{k-1}(r^k)$$

for some polynomials $b_0, \dots, b_{k-1} \in \mathbb{Q}[x]$. If not all polynomials b_1, \dots, b_{k-1} are zeroes, then r is a root of a nonzero polynomial

$$(b_0(r^k) - \alpha) + x b_1(r^k) + \dots + x^{k-1} b_{k-1}(r^k)$$

whose degree is k , and whose coefficients lie in $\mathbb{Q}[\alpha]$ (since $\alpha, r^k \in \mathbb{Q}[\alpha]$). This contradicts the choice of $f(x)$. Thus we arrive at $b_1 = \dots = b_{k-1} = 0$, whence $\alpha = b_0(r^k) \in \mathbb{Q}[r^k]$.

(b) By Calculator Theorem 3.2.c, the given polynomial has a root $y_0 \in \mathbb{Q}[R]$ for some $R \in \mathbb{R}$ and some positive integer D satisfying $R^D \in \mathbb{Q}$. By (a), we have $\mathbb{Q}[y_0] = \mathbb{Q}[R^k]$ for some k .

Denote $r = R^k$. Since $R^D \in \mathbb{Q}$, one may choose the minimal positive integer d such that $r^d \in \mathbb{Q}$; then $r, r^2, \dots, r^{d-1} \notin \mathbb{Q}$. Therefore, the polynomial $x^d - r^d$ is irreducible over \mathbb{Q} (since the constant term of any its nontrivial unitary factor has an irrational absolute value r^t , $0 < t < d$; cf. 6.3.a).

Finally, the equality $\mathbb{Q}[y_0] = \mathbb{Q}[r]$, combined with the dimension argument similar to that in the solution of Strong Irreducibility Lemma 6.5.a, yield that any two irreducible (over \mathbb{Q}) polynomials, one with root y_0 and the other with root r , have equal degrees. This shows that $n = d$, as required.

6.11. (a) Follows from the Cardano formula (or, more exactly, from the theorem in the solution of problem 1.6.b) in a way similar to that in 3.3.c.

(b) **Conjecture.** For a polynomial $p(x) = x^3 + px + q$ with $p, q \in \mathbb{Q}$, each of the conditions in Theorem 6.7 is equivalent to the complex 1-solvability of p .

In this conjecture, one may prove almost all implications in a way similar to the proof of Theorem 6.7. The remaining implication is the following one.

Conjecture. If a polynomial $x^3 + px + q$ with $p, q \in \mathbb{Q}$ is 1-solvable in the complex sense, then it has a root of the form $a + br + cr^2$, where $a, b, c, r^3 \in \mathbb{Q}$ and $r \in \mathbb{C}$.

(c) Follows from the theorem in the solution of 6.1.b.

4. Equations of degree 4 solvable using one radical

4.2. (4,1) *Answer:* An irreducible over \mathbb{Q} polynomial of the form $x^4 + px^2 + qx + s$ is 1-solvable if and only if

(4) one of its roots has the form $a + br + cr^2 + dr^3$, where $a, b, c, d, r^4 \in \mathbb{Q}$ but $r^2 \notin \mathbb{Q}$.

This condition is equivalent to the following one, formulated by means of the coefficients:

(4i) there exists $\alpha \in \mathbb{Q}$ such that $2\alpha > p$ and $q^2 - 4(p - 2\alpha)(s - \alpha^2) = 0$, and moreover
(4ii) the number $\Gamma = 16(\alpha^2 - s)^2 - (\alpha^2 - s)(2\alpha + p)^2$ is a square of a rational number.

Clearly, the conditions (4i) and (4ii) are algorithmically decidable.

The statement (4) on the form of a root of a 1-solvable polynomial is proved in 6.10.b. The proof that (4) is equivalent to (4i) together with (4ii) is proved in [A, Theorem 2].

4.4. By the theorem from the solution of 6.1, the polynomial $x^4 + px^2 + qx + s$ has a root $x_+ = \left(A + \sqrt{-\frac{2q}{A} - 2\alpha - p} \right) / 2$, where $A^2 = 2\alpha - p$ and $Aq \leq 0$. By the problem condition, we have $2\alpha - p > 0$, so the number A can be obtained using one extraction of a square root. Moreover, we have $-\frac{2q}{A} - 2\alpha - p \geq -2\alpha - p > 0$. Therefore, the number x_+ can be obtained using two root extractions.

4.5. By the Calculator theorem 3.2.c, the given root x_0 of our polynomial $f(x) = x^4 + px^2 + qx + s$ has the form $x_0 = a + br + cr^2 + dr^3$, where $a, b, c, d, r^4 \in \mathbb{Q}$. We may assume that $r^2 \notin \mathbb{Q}$ (otherwise we may replace r by either $\sqrt{|r|}$ or $\sqrt[4]{|r|}$). Then, applying Conjugation theorem 6.12, we obtain that the numbers x_1, x_2 , and x_3 (defined in the cited theorem) are also roots of our polynomial.

Since f is irreducible, the number x_0 is irrational, and moreover the numbers x_0 and x_2 cannot appear to be the two roots of a quadratic trinomial with rational coefficients. This excludes the case $b = d = 0$. Therefore, $b + dr^2 \neq 0$ due to 2.3.b. Hence the real numbers x_0 and x_2 are distinct. Similarly, the numbers x_1 and x_3 are non-real and distinct. Thus¹⁰
 $f(x) = (x - x_0)(x - x_1)(x - x_2)(x - x_3)$.

¹⁰Here is another proof of the fact that $f(x)$ coincides with $g(x) = (x - x_0)(x - x_1)(x - x_2)(x - x_3)$. We have $g(x) = [(x - a - cr^2)^2 - r^2(b + dr^2)][(x - a + cr^2)^2 + r^2(b - dr^2)] \in \mathbb{Q}[r^4][x] = \mathbb{Q}[x]$. (One may also prove that g has rational coefficients similarly to the second proof of Rationality Lemma 6.3.d.) Now, $f(x)$ is irreducible and has a common root x_0 with $g(x)$, and these two polynomials have the same degrees and leading terms; thus $f(x) = g(x)$.

By problem 6.13, the cubic resolution of $f(x)$ has a root $\alpha = \frac{x_0x_2 + x_1x_3}{2}$. Since $x_0 + x_1 + x_2 + x_3 = 0$, we have $a = 0$. Therefore,

$$\begin{aligned} 2\alpha &= x_0x_2 + x_1x_3 = ((cr^2)^2 - (br + dr^3)^2) + ((cr^2)^2 - (bri - dr^3i)^2) \\ &= 2c^2r^4 - r^2(b + dr^2)^2 + r^2(b - dr^2)^2 = 2c^2r^4 - 4bdr^4 = r^4(2c^2 - 4bd) \in \mathbb{Q}. \end{aligned}$$

4.6. An analogue of parts (d) looks as follows.

Theorem. *Assume that a polynomial has a root $r \in \mathbb{R}$ such that $r^4 \in \mathbb{Q}$ but $r^2 \notin \mathbb{Q}$. Then the numbers ir , $-r$ and $-ir$ are also roots of this polynomial. (Notice here that $i = \varepsilon_4$.)*

Irreducibility Lemma. Assume that $r \in \mathbb{R}$, $r^4 \in \mathbb{Q}$, but $r^2 \notin \mathbb{Q}$. Then the polynomial $x^4 - r^4$ is irreducible over \mathbb{Q} .

The proof of the lemma is similar to the proof of 6.3.a, since $r, r^2, r^3 \notin \mathbb{Q}$. The proof of the theorem follows the lines of proofs of other Conjugation Theorems.

Problem 6.12 serves as an analogue of parts (e).

6.12. Let $P(x)$ be the given polynomial. Then, as in Corollary 2.6.e, it suffices to apply the theorem from the solution of 4.6 to the polynomial $P(a + bx + cx^2 + dx^3)$.

6.13. (a) Applying the Vieta theorem and taking into account that $\sum_i x_i = 0$, one may check that $q^2 = (y_0y_1 + y_2y_3 - p)((y_0y_1 + y_2y_3)^2 - 4s)$. See details in [A, Statement 2].

(b) Similarly to (a), the three given numbers are roots of the cubic resolution. Moreover, we have $y_0y_2 + y_1y_3 - y_0y_1 - y_2y_3 = (y_0 - y_3)(y_2 - y_1)$. Thus, if the roots y_1, y_2, y_3 , and y_4 are distinct, the obtained roots of the cubic resolution are also distinct, and thus the resolution has no other roots. The case when our polynomial has a multiple root can also be treated easily.

Alternative solution to both (a) and (b). Applying the Vieta theorem and taking into account that $\sum_i x_i = 0$, we get

$$\begin{aligned} & (2\alpha - (y_0y_1 + y_2y_3))(2\alpha - (y_0y_2 + y_1y_3))(2\alpha - (y_0y_3 + y_1y_2)) \\ &= 8\alpha^3 - 4\alpha^2 \sum_{i < j} y_i y_j + 2\alpha \sum_{j < k, i \notin \{j, k\}} y_i^2 y_j y_k - \prod_{0 < j < k, i \notin \{0, j, k\}} (y_i y_j + y_k y_\ell) \\ &= 8\alpha^3 - 4p\alpha^2 + 2\alpha \cdot \left(\sum_i y_i \cdot \sum_{|\{i, j, k\}|=3} y_i y_j y_k - 4y_0 y_1 y_2 y_3 \right) - \left(y_0 y_1 y_2 y_3 \sum_i y_i^2 + \sum_{i < j < k} y_i^2 y_j^2 y_k^2 \right) \\ &= 8\alpha^3 - 4p\alpha^2 - 8s\alpha - (q^2 - 4ps) = -R_f(\alpha), \end{aligned}$$

which yields the desired result.

6.14. (a) Since $q^2 = 2p(4s - p^2)$, the cubic resolution $q^2 - 4(2\alpha - p)(\alpha^2 - s)$ has a root $\alpha = -p/2$. Since $p < 0$, we have $2\alpha - p = -2p > 0$. Therefore, by 6.1, our polynomial has a root

$$-\sqrt{2\alpha - p} + \sqrt{\frac{2q}{\sqrt{2\alpha - p}} - 2\alpha - p} = -\sqrt{-2p} + \frac{\sqrt{2q}}{\sqrt[4]{-2p}}.$$

(b) *Answer:* no. For example, the polynomial $x^4 - 12x^2 - 24x - 14$ from the solution of 4.3.a has a root $\sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$, but the number $2 \cdot (-24) = -48$ is not a square of a rational number.

5. Formal expressibility in real radicals

5.4. (d) Theorem. *Every symmetric polynomial can be expressed as a polynomial in elementary symmetric polynomials.*

Proof. We prove the assertion by lexicographical induction on the multi-degree of a given polynomial $f(x_1, x_2, \dots, x_n)$. The base case $f = 0$ is evident.

To prove the induction step, let $u = ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n}$ be the (lexicographically) leading monomial of the polynomial f .

Suppose that $k_i < k_{i+1}$ for some i . Along with u , the polynomial f must contain a monomial $ax_1^{k_1} \dots x_i^{k_{i+1}}x_{i+1}^{k_i} \dots x_n^{k_n}$, whose multi-degree is greater than that of u , which is impossible. So $k_1 \geq k_2 \geq \dots \geq k_n$.

According to (a), the leading monomial of the polynomial $g = a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3} \dots \sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}$ is u . Therefore, the multi-degree of the polynomial $f - g$ is less than the multi-degree of f . Application of the induction hypothesis to $f - g$ finishes the proof. \square

6.15. Set $M = x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ and $N = x_2x_4 + x_4x_6 + x_6x_8 + x_8x_{10} + x_{10}x_2$. Now one may proceed as in 5.5.b.

6.16. (a) Denote $g(x, y, z) := f(y, z, x)$. Since f^q is cyclically symmetric, we have $f^q = g^q$. If q is odd, we obtain $f = g$, so f is cyclically symmetric. Otherwise, if q is even, then $f = \pm g$, which yields either $f = g$ (and thus the result holds) or $f = -g$. In the latter case we have

$$f(x, y, z) = -f(y, z, x) = f(z, x, y) = -f(x, y, z).$$

Thus $f = 0$, and f is cyclically symmetric again..

(b) Use the result of 5.4.a.

$$(c) f^2 + fg + g^2 = \left(\frac{f+g}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}g\right)^2 = (f + \varepsilon_3g)(f + \varepsilon_3^2g).$$

6.17. (a) Take

$$s = 1, \quad k_1 = 2, \quad p_0(y_0, y_1) = y_1^2 - 4y_0, \quad p_1(y_0, y_1, z_1) = \frac{z_1 - y_1}{2} \quad \text{and} \quad f_1 = 2x + a_1.$$

Check that $f_1^2 = p_0(a_0, a_1)$ and $x = p_1(a_0, a_1, f_1)$.

References

- [A] D. Akhtyamov, Solvability of cubic and quartic equations using one radical, <http://arxiv.org/abs/1411.4990>
- [CS] A.B. Skopenkov and G.R. Chelnokov, Almost symmetric polynomials, a collection of problems.
- [E] H.M. Edwards, The construction of solvable polynomials, Bull. Amer. Math. Soc. 46 (2009), 397–411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703–704.
- [Le] L. Lerner, Galois Theory without abstract algebra, <http://arxiv.org/abs/1108.4593>.
- [M] Moscow mathematical students' conference, <http://www.mccme.ru/mmks/index.htm>.
- [S09] A. Skopenkov, Philosophical and methodical appendix, in: Mathematics as a sequence of problems, Ed. A. Zaslavsky, D. Permyakov, A. Skopenkov, M. Skopenkov, A. Shapovalov, MCCME, Moscow, 2009.
- [S] A. Skopenkov, Some more proofs from the Book: solvability and insolvability of equations in radicals, www.mccme.ru/circles/oim/kroneck.pdf.
- [S'] A. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem, www.mccme.ru/circles/oim/ruffini.pdf.