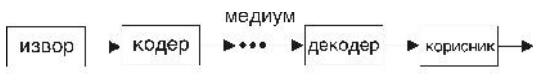
Алекса Малчески, Скопје
Вера Малческа, Германија

ОСНОВНИ ПОИМИ ОД ТЕОРИЈАТА НА КОДИРАЊЕ

1. ВОВЕД

При обработување на податоците, било да станува збор за нивно пренесување, чување или складирање, ние ги преставуваме (кодираме) со зборови од некоја азбука - кодни зборови. Обично, без ограничување на општоста, може да се земе дека и оригиналните зборови се од некоја азбука (може и иста). На цртеж 1 е прикажана шема на систем кај кое ваквото претставување на објектите е неопходно.



цртеж 1

Уредот за кодирање (кодер) оригиналните зборови ги трансформира во нови зборови (со поголема или еднаква должина), т.е. генерира кодни зборови. Уредот за декодирање има задача на корисникот да му проследи податоци кои колку што е можно помалку треба да се разликуваат од изворните податоци. Всушност, пожелно е податоците до корисникот да стигнат непроменети. Меѓутоа, заради несовршеноста на медиумот за пренос, можно е под влијание на шумовите, зборот кој доаѓа на влезот на декодерот да се разликува од зборот на влезот на кодерот.

Основниот проблем на теоријата на кодирање е во тоа да се овозможи, со голема доза на сигурност, препознавање на оригиналниот објект (претставен во кодни зборови), па и во случај кога примениот збор на влезот во декодерот не е едентичен со зборот на излезот од кодерот.

Во зависност од намената на системот, постојат два вида барања за функционирање на декодерот:

i) да ја открие грешката, т.е. да констатира дека примениот збор не е коден збор и информацијата да ја пренесе до корисникот,

ii) во случај кога постои грешка истата да је открие и да се обиде да ја корегира, а потоа да изврши декодирање како воопшто да не постоела грешка.

2. ХЕМИНГОВО РАСТОЈАНИЕ. ГРАНИЦА НА ХЕМИНГ

2.1. Нека $A=\{a_1,a_2,...a_q\}$ е азбука. Во практиката најчесто $q=2$, а како азбука го користиме множеството $B=\{0,1\}$, (бинарен код). Меѓутоа, за $q>2$, постои можност за потребите на теоријата на кодирање да се искористат некои добро изучени математички теории. За таканаречените линеарни кодови се користи добро развиениот апарат на теоријата на конечните полиња, при што $q = p^k$, p е прост број. Ние ќе се ограничиме на разгледување на оние кодови кај кои се користат комбинаторни објекти (латински квадрати, матрици на Адамар и слично). Во множеството од сите зборови над азбуката A се зема едно подмножество чии елементи се *кодни зборови*. Множеството од сите кодни зборови се нарекува *код*. Притоа ќе се ограничиме на таканаречените блокни кодови.

Кодот чии зборови се со иста должина го нарекуваме *блоковски код*.

Ако е A азбука и $C \subseteq A^n$, тогаш C е код над азбуката A. Ако $|A| = q$, тогаш C е $q-$*нарен код*.

Често пати, за кодните зборови говориме како за вектори. Притоа за $i-$та буква a_i на кодниот збор (вектор) $a = a_1 a_2 a_3 ... a_n$ велиме дека е $i-$та координата.

За два $n-$збора (вектори) $x = x_1 x_2 x_3 ... x_n$ и $y = y_1 y_2 y_3 ... y_n$ над азбуката A дефинираме *Хемингово растојание* меѓу нив, во ознака $d(x, y)$, како број на координатите во кои зборовите се разликуваат. Ако во прашање е азбука со две букви $B = \{0,1\}$, тогаш Хеминговото растојание може да се изрази во видот

$$d(x, y) = \sum_{i=1}^{n} | x_i - y_i | .$$

Понатаму, дефинираме *кодно растојание* $d(C)$ на кодот C со: $d(c) = \min\limits_{\substack{x,y \in C \\ x \neq y}} d(x, y)$ т.е. како минимално растојание меѓу различните кодни зборови на кодот C.

За бинарните кодови, *тежината* $\omega(a)$ на кодниот збор a е бројот на единиците во тој збор $\omega(a) = \sum_{i=1}^{n} a_i$.

За кодот ќе велиме дека е *еквидистантен* ако растојанието меѓу било кои два кодни зборови е еднакво. Понатаму, за кодот ќе велиме дека е *урамнотежен* ако сите кодни зборови имаат иста тежина. Ако со B_k^n го означиме множеството од сите зборови од B^n кои имаат тежина k, тогаш сите зборови од урамнотежениот код припаѓаат на множеството B_k^n, за некој $k \in \{0,1,2,...,n\}$. За бројот k велиме дека е *тежина* на овој урамнотежен код.

За кодот велиме дека е $(n, M, d)-$код ако се состои од M зборови со должина n и има кодно растојание d. Ако сакаме само да истакнеме дека кодот има n зборови и кодно растојание d, тогаш велиме дека тоа е $(n, d)-$код.

Множеството од сите $n-$зборови над $q-$азбука A во кое е дефинирано Хемингово растојание е *метрички простор* (A^n, d). Тоа значи дека се исполнети следниве услови за произволни зборови $x, y, z \in A^n$:

1) $d(x, y) = 0$ ако и само ако $x = y$
2) $d(x, y) = d(y, x)$
3) $d(x, y) \leq d(x, z) + d(z, y)$

Во произволен метрички простор (X, d) *сфера* $S(c, r)$ со центар c и радиус r е множеството $S(c, r) = \{x \mid d(c, x) = r\}$, а *затворена топка* $L(c, r)$ со центар c и радиус r е множеството $L(c, r) = \{x \mid d(c, x) \leq r\}$.

2.2. Идејата на декодирање се базира на користење метрика. При изборот на кодот, т.е. множеството на кодни зборови A^n се стремиме кодното растојание, за дадена големина на кодниот број, да биде колку што е можно поголемо. Притоа, под претпоставка дека медиумот не е во целост несовршен, мала е веројатноста за голем број грешки и затоа при декодирањето примениот збор се изедначува со најблискиот коден збор. Ова е таканаречениот принцип на *максимална веројатност на исправување на грешките*. Јасно, кодовите со поголемо кодно растојание имаат поголема можност за корегирање на грешките.

Притоа е пожелно да се избегнат “конфликитите”, т.е. ниту еден збор да не е на еднакво растојание од кодните зборови. “Геометриската” смисла на претходното множество е следнава: кодните зборови ги набљудуваме како центри на дисјунктни затворени топки со еднакви и најголеми можни радиуси. Затоа сите зборови на една топка при декодирањето се идентификуваат со центри на топката.

2.3. Теорема. Сферата со радиус r во множеството $A^n, |A| = q$ содржи $(q-1)^r \binom{n}{r}$ зборови.

Доказ. Бројот на зборови во A^n на растојание r од даден збор $c = c_1 c_2 c_3 \ldots c_n$ е еднаков на $\binom{n}{r}(q-1)^r$. Имено, на $\binom{n}{r}$ начини може да се изберат r букви во зборот c, а за секоја буква постојат $q-1$ можности да се замени со друга буква. ♦

2.4. Теорема. Топка со радиус r во множеството $A^n, |A| = q$ содржи

$$1 + (q-1)\binom{n}{1} + (q-1)^2 \binom{n}{2} + \ldots (q-1)^r \binom{n}{r}$$

зборови.

Доказ. Според теорема 2.3, бројот на зборовите во A^n на растојание k од даден збор $c = c_1 c_2 \ldots c_n$ е еднаков на $\binom{n}{k}(q-1)^k$. Бидејќи $L(c, r)$ е унија од дисјунктни сфери $S(c, k), k = 0, 1, 2, \ldots, r$ со сумирање по k го добиваме тврдењето. ♦

2.5. Теорема (граница на Хеминг). Ако постои код

$$C \subseteq A^n, |A| = q, |c| = M$$

кој исправа t грешки, тогаш важи

$$M[1+(q-1)\binom{n}{1}+(q-1)^2\binom{n}{2}+...+(q-1)^t\binom{n}{t}] \le q^n .$$

Доказ. Ако кодот C исправа t грешки, тоа значи дека сите M топки со радиус t со центри во кодните зборови се дисјунктни. Според теорема 2.4 во секоја од овие топки има

$$1+(q-1)\binom{n}{1}+(q-1)^2\binom{n}{2}+...+(q-1)^t\binom{n}{t}$$

зборови. Сега тврдењето следува од фактот што множеството A^n содржи вкупно q^n зборови. ♦

2.6. За еден код ќе велиме дека открива најмногу k грешки ако за било кој коден збор, при појавување на најмногу k грешки, кодот може да открие дека постои барем една грешка. Ќе велиме дека кодот корегира најмногу k грешки ако за било кој коден збор, при појавување најмногу k грешки, може да ги корегира сите грешки.

2.7. Теорема. Код со кодно растојание d може да открие најмногу $d-1$ грешка.

Доказ. Јасно, овој код не може да открие d грешки. Имено, ако кодот може да открие d грешки, тогаш имаме промена на d букви на зборот x и се добива коден збор y, таков да $d(x, y) = d$. ♦

2.8. Теорема. Код со кодно растојание $d = 2l+1$ може да корегира најмногу l грешки.

Доказ. Да претпоставиме дека при преносот на кодниот збор x се појавила барем една грешка е дека како резултат се добил збор x'. Ако $d(x, x') \le l$, тогаш $d(y, x') > l$ за било кој збор $y \ne x$. Навистина, во спортивно добиваме

$$d(x, y) \le d(x, x') + d(y, x') \le 2l$$

што е противречност. Според тоа, ако се пренесени најмногу l погрешни букви на зборот x, добиениот збор x' може да се исправи и се добива зборот x. Од друга страна, за кодните зборови x и y такви што $d(x, y) = 2l+1$, постои збор z за кој важи $d(x, z) = l+1$ и $d(y, z) = l$. Јасно, ако при преносот на зборот x, заради $l+1$ грешка се добие зборот z, тогаш тој не може да се корегира. ♦

3. ГРАНИЦА НА ПЛОТКИН

3.1. Во овој дел ќе ги разгледаме само бинарните кодови.

Обично претпоставуваме дека не постои координатна позиција во која сите кодни зборови на (n, M, d) – кодот имаат иста буква (во спротивно тоа ќе биде $(n-1, M, d)-$ код). Бидејќи растојанието меѓу кодните зборови не се менува ако во сите зборови на иста позиција се направи замена на буквите (0 со 1 или 1 со 0), секогаш можеме да претпоставиме, ако тоа е потребно, дека кодот содржи збор чии букви се сите нула (нулти вектор). За два $(n, M, d)-$ кода C и D ке велиме дека се *еквивалентни* ако едниот од другиот може да се добие со пермутација на буквите од азбуката и претходно споменатата замена на буквите.

3.2. Теорема. За произволен $(n, M, d)-$ код C, таков што $n < 2d$ важи неравенството

$$M \le 2\left[\frac{d}{2d-n}\right]. \qquad (1)$$

Доказ. Да го разгледаме збирот $\sum_{x\in C}\sum_{y\in C} d(x,y)$. Бидејќи $d(x,y) \ge d$, за $x \ne y$, овој збир не е помал од $M(M-1)d$. Од друга страна, нека A е $M \times n$ матрица, чии редици се кодните зборови на кодот C. Нека $i-$та колона на матрицата A содржи m_i нули и $M - m_i$ единици. Во разгледуваниот збир оваа колона има збир $2m_i(M - m_i)$, па затоа

$$\sum_{x\in C}\sum_{y\in C} d(x,y) = \sum_{i=1}^{n} 2m_i(M - m_i) \qquad (2)$$

Бидејќи $m_i(M - m_i) \le \frac{M^2}{4}$, за парен број M изразот (2) достигнува максимална вредност кога $m_1 = m_2 = ... = m_n = \frac{M}{2}$, па затоа разгледуваниот збир не е поголем од $\frac{nM^2}{2}$. Според тоа, $M(M-1)d \le \frac{nM^2}{2}$ т.е.

$$M \le \frac{2d}{2d-n} \qquad (3)$$

Конечно бидејќи M е парен број, добиваме $M \le 2\left[\frac{d}{2d-n}\right]$.

Ако M е непарен број, разгледуваниот збир не е поголем од $\frac{n(M^2-1)}{2}$ па наместо (3) добиваме $M \le \frac{n}{2d-n} = \frac{2d}{2d-n} - 1$. Оттрука и од неравенството $[2x] = 2[x]+1$ следува

$$M \le \left[\frac{2d}{2d-n}\right] - 1 \le 2\left[\frac{d}{2d-n}\right] + 1 - 1 = 2\left[\frac{d}{2d-n}\right]. \ ♦$$

3.3. Пример. За кодот $(11, 12, 6)$ се достигнува границата (1), т.е. важи

$$M = 2\left[\frac{d}{2d-n}\right]$$

00000000000 11011100010 01101110001 10110111000 01011011100 00101101110 00010110111 10001011011 11000101101 11100010110 01110001011 10111000101. ♦

3.4. Теорема. Со $M(n,d)$ да го означиме најголемиот број M за кој постои $(n, M, d)-$ код. Тогаш

$$M(n, 2r-1) = M(n+1, 2r) .$$

Доказ. Нека C е $(n, M, 2r-1)-$код. Да го прошириме до код со должина $n+1$, на тој начин што секој коден збор ќе му допишеме уште една буква, и тоа буквата 0 ако зборот е со парна должина, а 1 во спротивен случај. Кодот добиен на овој начин има само зборови со парна тежина, па затоа растојанието меѓу било кои два кодни збора е парен број. Бидејќи при проширувањето на кодот растојанието меѓу било кои два збора не се намали, добиен е еден $(n+1, 2r)-$код. Значи, $M(n, 2r-1) \le M(n+1, 2r)$.

Обратно, ако е даден $(n+1, M, 2r)-$код, со изоставување на последната буква во сите зборови, добиваме $(n, M, d)-$код, каде $d \ge 2r-1$, па затоа $M(n, 2r-1) \ge M(n+1, 2r)$. ♦

3.5. Забелешка. Од претходната теорема непосредно следува дека доволно е да се определи $M(n, d)$, за парни вредности на d.

3.6. Теорема. $M(n, d) \le 2M(n-1, d)$.

Доказ. Нека е даден $(n, M, d)-$код. Да ги поделиме кодните зборови на две класи: зборови кои почнуваат со буквата 0 и зборови кои почнуваат на буквата 1. Барен една од овие класи содржи најмалку половина од вкупниот број кодни зборови. Со остранување на првата буква од кодните зборови на оваа класа, добиваме код со должина $n-1$, со кодно растојание барем еден d. Според тоа, $M(n-1, d) \ge \frac{M(n,d)}{2}$. ♦

3.7. Теорема. (граница на Плоткин). Ако d е непарен број и $2d > n$, тогаш

$$M(n, d) \le 2\left[\frac{d}{2d-n}\right] \tag{4}$$

$$M(2d-1, d) \le 2d \tag{5}$$

$$M(2d, d) \le 4d \tag{6}$$

Ако d е непарен број и $2d+1 > n$, тогаш

$$M(n, d) \le 2\left[\frac{d+1}{2d+1-n}\right] \tag{7}$$

$$M(2d+1, d) \le 4d+4 \tag{8}$$

Доказ. Неравенството (4) следува непосредно од теоремата 7.2, додека (5) е специјален случај на (4). Од (5) и теоремата 3.6 имаме

$$M(2d, d) \le 2M(2d-1, d) \le 4d ,$$

т.е. важи (6).

Ако d е непарен број, тогаш од теорема 3.4 добиваме

$$M(n, d) = M(n+1, d+1+ \le 2\left[\frac{d+1}{2d+1-n}\right].$$

Нека е $n = 2d+1$, $d = 2r-1$. Тогаш од (6) и теорема 3.4 имаме

$$M(2d+1,d)=M(2d+2,d+1)=M(4r,2r)\le 8r=4d+4$$

со што е докажана релацијата (8). ♦

4. КОДОВИ НА АДАМАР

4.1. Нека H_n е нормализирана матрица на Адамар од ред n. Ако во таа матрица секоја единица ја замениме со 0, а сите елементи ги помножиме со -1, добиваме бинарна матрица A_n. Бидејќи сите редици на матрицата H_n се ортогонални, секои две редици на матрицата A_n се совпаѓаат на $\frac{n}{2}$ места и се разликуваат на $\frac{n}{2}$ места. Значи, Хеминговото растојание меѓу нив е еднакво на $\frac{n}{2}$.

Од матрицата A_n се добиваат следните кодови на Адамар:

(c1) $(n-1,n,\frac{n}{2})-$код $\mathbb{A}_n$, кој се состои од редиците на матрицата која се добива од матрицата A_n со остранување на првата колона (во таа колона има само нули).

(c2) $(n-1,2n,\frac{n}{2}-1)-$код $\mathbb{B}_n$, кој се состои од сите зборови на кодот $\mathbb{A}$ и нивните комплементи.

(c3) $(n,2n,\frac{n}{2})-$код $\mathbb{C}_n$, кој се состои од редовите на матрицата A_n и нивните комплементи

(c4) Ако од кодните зборови на кодот $\mathbb{A}_n$ кои почнуваат со нула, ја остaниме почетната нула, добиените кодни зборови формираат $(n-2,\frac{n}{2},\frac{n}{2})-$код $\mathbb{A}_n'$.

Кодот $\mathbb{A}_n$ е урамнотежен, бидејќи растојанието меѓу секои негови зборови е еднакво на $\frac{n}{2}$.

4.2. Пример. Кодот $\mathbb{A}_8$ е добиен на опишаниот начин (c1), од матрицата на Адамар од ред 8:

0000000 1010101 0110011 1100110
0001111 1011010 0111100 1101001

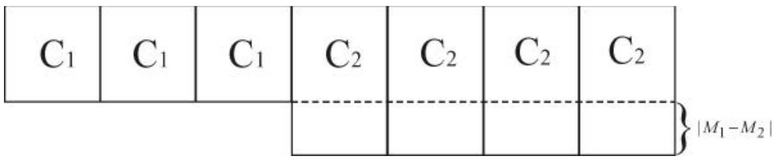
Обиди се да ги составиш кодовите $\mathbb{B}_8$, $\mathbb{C}_8$ и $\mathbb{A}_8'$. ♦

5. ТЕОРЕМА НА ЛЕВЕНШТАЈН

5.1. Во овој дел ќе ја докажеме теоремата на Левенштајн која овозможува да се контруираат кодови кај кои се достигнува границата на Плоткин.

Претходно ќе дадеме уште една конструкција со помош на која од два дадени кодови конструираме нов код.

(c5) Дадени се $(n_1, M_1, d_1)-$код C_1 и $(n_2, M_2, d_2)-$код C_2. Последователно ќе залепиме a копии на кодот C_1, а потоа b копии на кодот C_2. На цртежот долу е преставен случајот $a=3, b=4$.



Ако $M_1 < M_2$ ги отфрламе последните $M_2 - M_1$ редици на кодот C_2, а ако $M_1 > M_2$ ги отфрламе последните $M_1 - M_2$ редици на кодот C_1. На тој начин добиваме $(n, M, d)-$код C, каде $n = an_1 + bn_2$, $M = \min\{M_1, M_2\}$ и $d \geq ad_1 + bd_2$, кој го означуваме со $aC_1 \oplus bC_2$.

5.2. Лема. Нека $2d > n \geq d$, $k = \left[\frac{d}{2d-n}\right]$ и

$$a = d(2k+1-n(k+1);\ b = kn - d(2k-1). \qquad (1)$$

Тогаш a и b се ненегативни цели броеви и

$$n = (2k-1)a + (2k+1)b;\ d = ka + (k+1)b. \qquad (2)$$

Доказ. Бидејќи $k \geq \frac{d}{2d-n} - 1 = \frac{n-d}{2d-n}$ добиваме $(2d-n)k \geq n-d$, односно $d(2k+1) \geq n(k+1)$, па затоа $a = d(2k+1) - n(k+1) \geq 0$.

Слично, од $k \leq \frac{d}{2d-n}$ следува $kn \geq 2dk - d$, па е $b = kn - d(2k-1) \geq 0$. Равенството (2) се докажува со непосредна проверка. ♦

5.3. Теорема (Левенштајн). Ако постојат соодветни матрици на Адамар, тогаш за границата на Плоткин важи равенството. Со други зборови, ако a е парен број, тогаш

$$M(n,d) = 2\left[\frac{d}{2d-n}\right], \text{ ако } 2d > n \geq d, \qquad (3)$$

$$M(2d, d) = 4d \qquad (4)$$

а ако d е непарен број, тогаш

$$M(n,d) = 2\left[\frac{d+1}{2d+1-n}\right], \text{ ако } 2d+1 > n \geq d. \qquad (5)$$

$$M(2d+1, d) = 4d+4. \qquad (6)$$

Доказ. Од теоремата 3.2 и равенствата (3) и (4) непосредно следуваат равенствата (5) и (6), па можеме да претпоставиме дека d е парен број.

Кодот на Адамар C_{2d} е $(2d,4d,d)$ – код од каде што следува (4).

За да го докажеме (3), треба да конструираме (n,M,d) – код каде $M=\left[\frac{d}{2d-n}\right]$, за произволен n и парен d, такви да важи $2d>n\geq d$.

Ако n е парен број, тогаш броевите a и b определени со (1) се парни. Ако n е непарен, а k е парен, тогаш b е парен. Ако n и k се непарни, тогаш a е парен.

Да го разгледаме кодот C , каде

$$C=\frac{a}{2}A'_{4k}\oplus\frac{b}{2}A'_{4k+4}\text{, ако } n \text{ е парен}$$

$$C=aA_{2k}\oplus\frac{b}{2}A'_{4k+4}\text{, ако } n \text{ е непарен, а } k \text{ е парен}$$

$$C=\frac{a}{2}A'_{4k}\oplus bA_{2k+2}\text{, ако } n \text{ и } k \text{ се непарни.}$$

Лесно се гледа дека кодот C во секој случај има должина n, минимално растројание d и содржи $2k=\left[\frac{d}{2d-n}\right]$ кодни зборови. Значи важи (3). ♦

5.4. Забелешка. Лесно се гледа дека за доказот на (4) ни е потребна матрица на Адамар од ред $2d$, а за доказот на (3) доволни се матриците на Адамар од ред $2k$ (ако k е парен), $2k+2$ (ако k е непарен), $4k$ и $4k+4$.

5.5. Пример. Со методот опишан во теоремата на Левенштајн ќе конструираме еден $(27,6,16)$ – код. Во овој случај важи $k=3, a=4, b=1; n$ и k се непарни, па кодот се добива со слепување на две копии на кодот A'_{12} и со една копија на кодот A_8 .

$$H_{12}:\begin{matrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1\\
1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1\\
1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1\\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1\\
1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1\\
1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1\\
1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1\\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1\\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1\\
1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1
\end{matrix}$$

Кодовите A_8 и A'_{12} се добиваат од матриците на Адамар H_8 и H_{12}. ♦

6. ЛАТИНСКИ КВАДРАТИ И КОДОВИ

6.1 Во оваа точка ќе укажеме на примена на латинските квадрати во теоријата на кодирање.

Теорема. Ако постои множеството од квадрати од ред n, при што секои два се ортогонални, тогаш постои $(k+2, n^2, k+1)$ – код над $n-$азбука.

Доказ. Нека

$$L_1 = [a_{ij}^1], L_2 = [a_{ij}^2], \dots, L_k = [a_{ij}^k]$$

се латински квадрати над азбуката $N_n = \{0,1,2,\dots,n-1\}$, таква што се по парови ортогонални. За секој од n^2 различни подредени парови ij формираме $(k+2)-$ збор $ija_{ij}^1 a_{ij}^2 \dots a_{ij}^k$. На овој начин добиваме множество C од n^2 зборови со должина $k+2$ над азбуката $N_n = \{0,1,2,\dots,n-1\}$. Ќе докажеме дека растојанието меѓу било кои два збора од C е поголемо или еднакво на $k+1$.

Да разгледаме два произволни збора од C:

$$i_1 j_1 a_{i_1 j_1}^1 a_{i_1 j_1}^2 \dots a_{i_1 j_1}^k \text{ и } i_2 j_2 a_{i_2 j_2}^1 a_{i_2 j_2}^2 \dots a_{i_2 j_2}^k .$$

Ако $i_1 = i_2, j_1 \neq j_2$, тогаш $a_{i_1 j_1}^s \neq a_{i_2 j_2}^s$, за $1 \leq s \leq k$, бидејќи во секој латински квадрат елементите од иста редица се различни. Значи растојанието меѓу зборовите е $k+1$.

Слично докажуваме и во случај кога $i_1 \neq i_2, j_1 = j_2$.

Нека $i_1 \neq i_2, j_1 \neq j_2$. Ако за некои r и t, $1 \leq r < t \leq k$ важи

$$a_{i_1 j_1}^r = a_{i_2 j_2}^r \text{ и } a_{i_1 j_1}^t = a_{i_2 j_2}^t ,$$

т.е. $(a_{i_1 j_1}^r, a_{i_2 j_2}^t) = (a_{i_2 j_2}^r, a_{i_2 j_2}^t)$, добиваме противречност со ортогоналноста на квадратите L_r и L_t. Значи, во секој случај разгледуваните зборови се поклопуваат најмногу во една позиција. ♦

6.2. Пример. Тргнувајќи од ПСОЛК(5) го добиваме следниов $(6,25,5)-$ код:

00 2340	013024	02 4203	03 0432	041111
10 3401	114130	12 0314	131043	14 222
20 4012	214130	221420	23 2104	24 3333 . ♦
30 0123	311302	32 2031	33 3210	34 4444
401234	412413	42 3142	43 4321	44 0000

7. СОВРШЕНИ КОДОВИ

7.1. Кодот $C \subseteq A^n$ со кодно растојание $2l+1$ е совршен ако множеството топки со радиус r со центри во кодните зборови е разбивање на множеството A^n. Од теоремата 2.4 непосредно го добиваме следното тврдење.

Последица. Ако C е совршен $(n, M, 2l+1)$ – код над азбуката q тогаш

$$M = \frac{q^n}{\sum_{i=0}^{l} (q-1)^i \binom{n}{i}}. \ \blacklozenge$$

7.2. Пример. Тргнувајќи од парот латински квадрати

$$\begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix} \quad \text{и} \quad \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}$$

ги добиваме $(4,9,3)$ – кодот над азбуката $\{0,1,2\}$

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{matrix} \qquad \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 0 & 2 \end{matrix} \qquad \begin{matrix} 0 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 \\ 2 & 2 & 1 & 0 \end{matrix}$$

Деветте топки со центри во кодните зборови се меѓусебно дисјунктни и секоја, согласно теоремата 2.4, содржи 9 зборови. Затоа, со овие топки се покриени сите 81 зборови од $\{0,1,2\}^4$., па кодот е совршен. Јасно, кодот открива две, а корегира една грешка. ♦

Литература

1. **Anderson, J. A.:** *Diskretna matematika sa kombinatorikom*, CET, Beograd, 2005
2. **Ерусалимский, Я. М.:** *Дискретная математика*, Везувская книга, Москва, 2004
3. **Малческа, В.; Малчески, С.:** *Латински квадрати и блок дизајни* I и II, Сигма 82 и 83, Скопје, 2008/09
4. **Плотников, А. Д.:** *Дискретная математика*, Новое знание, Москва, 2005

Статијата прв пат е објавена во списанието СИГМА на Сојузот на математичарите на Македонија