MATTEX 2024,
CONFERENCE PROCEEDINGS, v. 1, pp. 3 – 10

LINEAR CODES AND THEIR HULLS*

Stefka Bouyuklieva

ABSTRACT: *The number of linear codes of different types over a finite field with q elements is presented. The numbers of codes with different hulls are compared.*

KEYWORDS: *Linear codes, Self-orthogonal codes, LCD codes*

DOI: https://doi.org/10.46687/IICL3614

ЛИНЕЙНИ КОДОВЕ И ТЕХНИТЕ САМООРТОГОНАЛНИ ПОДКОДОВЕ

Стефка Буюклиева

АБСТРАКТ: *В този доклад се изследва броят на линейните кодове над дадено крайно поле в зависимост от размерността на техните самоортогонални подкодове.*

1 Въведение

Теорията на кодирането е приложна дисциплина, която черпи идеи от алгебрата, геометрията, комбинаториката, теорията на вероятностите и други математически науки. Тя намира директно приложение при предаването и съхранението на информация. Кодовете над различни полета и дори над пръстени са често срещани в съвременната научна литература, при това както в инженерни, така и в чисто математически издания.

От теоретична и от практическа гледна точка особено важно е конструирането на ”оптимални”, или ”най-добри” в някакъв смисъл кодове, както и намирането на ефективни алгоритми за тяхното кодиране и декодиране. Най-изследваният клас от блокови кодове са линейните кодове заради хубавата им алгебрична структура и ефективните алгоритми за кодиране и декодиране. В този клас съществена роля играят самодуалните кодове, за изследването на които голям принос имат колегите от Шуменски университет Васил Йоргов, Никола Зяпков, Радка Русева и Николай Янков. Тези кодове са интересни не само заради богатата си алгебричната структура, но и заради близката връзка с други математически структури като комбинаторни дизайни, решетки, графи, сферични опаковки и т.н.

В този доклад освен самодуални, разглеждаме и други типове линейни кодове. Основната ни идея е да представим последните си разработки, свързани с преброяването на различните кодове от даден тип с дадени параметри над крайно поле с q елемента, където q е степен на просто число.

В следващата секция са представени основните дефиниции, които използваме, и основните резултати, които получаваме. Секция 3 е посветена на Гаусовите биномни коефициенти, които използваме в представените по-нататък формули. В секция 4 показваме резултати, свързани с броя на всички различни кодове от определен тип.

*Supported by Scientific Research Grants РД-08-138/02.02.2024 and РД-08-104/30.01.2024 of Shumen University.

2 Основни резултати

Нека $\mathbb{F}_q$ е крайно поле с q елемента, а $\mathbb{F}_q^n$ е n-мерното векторно пространство над $\mathbb{F}_q$. *Разстояние* (по Хеминг) $d(x,y)$ между два вектора $x=(x_1,x_2,...,x_n)$ и $y=(y_1,y_2,...,y_n)$ от $\mathbb{F}_q^n$ наричаме броя на координатите, в които те се различават, а *тегло* (по Хеминг) $\mathrm{wt}(x)$ на вектора $x=(x_1,x_2,...,x_n)\in\mathbb{F}_q^n$ наричаме броя на ненулевите му координати.

Всяко k-мерно подпространство C на $\mathbb{F}_q^n$ наричаме *линеен код* с дължина n и размерност k над $\mathbb{F}_q$. *Минимално разстояние* $d(C)$ на кода C наричаме най-малкото от разстоянията между две различни кодови думи, а *минимално тегло* - най-малкото от всички ненулеви тегла в кода. Ако минималното разстояние на кода е d, казваме, че C е q-ичен $[n,k,d]$ код или $[n,k,d]_q$ код. За линеен код C минималното разстояние и минималното тегло съвпадат, така че

$$d(C)=\min\{d(x,y)|x,y\in C,\ x\neq y\}=\min\{\mathrm{wt}(x)|x\in C,\ x\neq \mathbf{0}\}.$$

В линейното пространство $\mathbb{F}_q^n$ за фиксиран автоморфизъм σ на полето $\mathbb{F}_q$ задаваме скаларно произведение $(\cdot,\cdot):\mathbb{F}_q^n\times\mathbb{F}_q^n\to\mathbb{F}_q$ с равенството $(u,v)=\sum_{i=1}^{n}u_i\sigma(v_i)$ за $u=(u_1,u_2,\ldots,u_n)$, $v=(v_1,v_2,\ldots,v_n)\in\mathbb{F}_q^n$. Казваме, че два вектора са ортогонални, ако скаларното им произведение е равно на нула. Ортогоналното допълнение $C^\perp=\{v\in\mathbb{F}_q^n|(u,v)=0,\forall u\in C\}$ наричаме *ортогонален код* на кода C, а минималното му разстояние - *дуално разстояние* на C. Много често вместо *ортогонален код* се използва термина *дуален код*, въпреки че подобен термин може да се дефинира и с друго значение. Един линеен код се нарича *самоортогонален*, ако $C\subseteq C^\perp$ и *самодуален*, когато $C=C^\perp$. Всеки самодуален код с дължина n над $\mathbb{F}_q$ има размерност $k=n/2$. Това доказва, че самодуални кодове над поле съществуват само за четни дължини.

Най-често се използват две скаларни произведения. Първото е *стандартното* или *евклидово* скаларно произведение

$$(u,v)=u\cdot v=\sum_{i=1}^{n}u_iv_i$$

Вторият вид е така нареченото *ермитово скаларно произведение*. То се дефинира над поле $\mathbb{F}_q$, в което броят на елементите q е точен квадрат. Тогава

$$(u,v)=\sum_{i=1}^{n}u_i\overline{v_i}=\sum_{i=1}^{n}u_iv_i^{\sqrt{q}}$$

Напоследък усилено се изследват кодове. за които $C\cap C^\perp=\{0\}$, наречени LCD (Linear Complementary Dual) кодове. Характерно за тях е, че цялото векторно пространство $\mathbb{F}_q^n$ е директна сума на кода и неговия дуален (n е дължината на разглежданите кодове). Във връзка с тези кодове беше въведено и понятието самоортогонален подкод (hull) като сечение на кода C и неговия дуален код $C^\perp$:

$$\mathcal{H}(C)=C\cap C^\perp.$$

Да означим с $A_{n,k,\ell}$ броя на всички различни линейни $[n,k]_q$ кодове C, за които $\dim(C\cap C^\perp)=\ell$, $0\leq\ell\leq k$. Основната теорема, която получаваме като резултат от нашите изследвания, се отнася до тези бройки.

Теорема 1. *За дадени естествени числа k и $n\geq 2k$ са в сила следните неравенства:*

(1) $$A_{n,k,0}>A_{n,k,1}>\cdots>A_{n,k,k}.$$

3 Гаусови биномни коефициенти

В тази секция дефинираме Гаусовите биномни коефициенти и представяме някои от основните им свойства [4].

Дефиниция 1. *Нека n и k са неотрицателни цели числа. Гаусовият биномен коефициент $\begin{bmatrix} n \\ k \end{bmatrix}_q$ се дефинира със следната формула*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q-1)},$$

ако $n \geq k$. При $n < k$ коефициентът има стойност 0, а при $k = 0$ стойността му е 1.

Гаусовите биномни коефициенти имат свойства, подобни на свойствата на биномните коефициенти. Тук представяме някои от тях.

$$\begin{aligned}
\begin{bmatrix} n \\ 1 \end{bmatrix}_q &= q^{n-1} + q^{n-2} + \cdots + q + 1 \\
\begin{bmatrix} n \\ k \end{bmatrix}_q &= \begin{bmatrix} n \\ n-k \end{bmatrix}_q \\
\begin{bmatrix} n \\ k \end{bmatrix}_q &= \begin{bmatrix} n \\ m \end{bmatrix}_q \begin{bmatrix} n-m \\ n-k \end{bmatrix}_q \Big/ \begin{bmatrix} k \\ m \end{bmatrix}_q \\
\begin{bmatrix} n \\ k \end{bmatrix}_q &= \frac{q^n-1}{q^{n-k}-1} \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \\
\begin{bmatrix} n \\ k \end{bmatrix}_q &= \frac{q^{n-k+1}-1}{q^k-1} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q \\
\begin{bmatrix} n \\ k \end{bmatrix}_q &= \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q
\end{aligned}$$

Тези коефициенти играят важна роля при преброяването на подпространствата на дадено векторно пространство над крайно поле.

Лема 2. *[3] Броят на k-мерните подпространства на $\mathbb{F}_q^n$ е равен на $\begin{bmatrix} n \\ k \end{bmatrix}_q$.*

Тази лема директно ни дава броя на всички различни линейни $[n,k]_q$ кодове.

Теорема 3. *Броят на различните линейни кодове с дължина n и размерност k над поле с q елемента е равен на $\begin{bmatrix} n \\ k \end{bmatrix}_q$.*

Лема 4. *[3] Ако U е векторно пространство над крайното поле $\mathbb{F}_q$ с размерност n, а V е подпространство на U с размерност $\ell < k$, то броят на k-мерните подпространства на U, съдържащи V, е равен на*

$$\begin{bmatrix} n-\ell \\ k-\ell \end{bmatrix}_q.$$

4 Формули за броя на различни типове кодове

В тази секция представяме формули за броя на различните кодове от даден тип, както и така наречените мас-формули за самоортогоналните кодове, които са много полезни при верификация на класификационни резултати.

Да означим със $\sigma_q(n,k)$ броя на всички различни $[n,k]_q$ самоортогонални кодове. Такива кодове съществуват само при $n \geq 2k$. Формула за този брой е доказана още през шестдесетте години на миналия век от Вера Плес [5].

Теорема 5. *Нека* $m = \lfloor n/2 \rfloor$ *и* $\pi_{n,k} = \prod_{i=1}^{k} \frac{q^{2m-2i+2}-1}{q^i-1}$. *Тогава за всяко естествено число* $k \leq m$ *е в сила*

$$\sigma_q(n,k) = \begin{cases} \pi_{n,k}, & \text{ако } n \text{ е нечетно}, \\ \frac{q^{n-k}-1}{q^n-1}\pi_{n,k}, & \text{ако } n \text{ и } q \text{ са четни}, \\ \frac{q^{m-k}-1}{q^m-1}\pi_{n,k}, & \text{ако } n \equiv 2 \pmod 4 \text{ и } q \equiv 3 \pmod 4, \\ \frac{q^{m-k}+1}{q^m+1}\pi_{n,k}, & \text{ако } (n \equiv 0 \pmod 4) \\ & \text{или } (n \equiv 2 \pmod 4 \text{ и } q \equiv 1 \pmod 4). \end{cases}$$

За кодове над поле с 2 елемента е в сила мас-формула, която може да се използва при класификация на този тип кодове. За да представим формулата, трябва да дефинираме еквивалентност в множеството на всички двоични кодове.

Дефиниция 2. *Два двоични* $[n,k]$ *кода* C_1 *и* C_2 *наричаме еквивалентни, ако съществува пермутация* $\sigma \in S_n$, *такава че* $\sigma(C_1) = C_2$. *Пермутацията* $\sigma \in S_n$ *е автоморфизъм на двоичния код* C, *ако* $\sigma(C) = C$.

Всички автоморфизми на код C образуват група, която бележим с $\mathrm{Aut}(C)$. Тази група се състои от пермутации на координатите на кода и следователно е подгрупа на симетричната група S_n.

Теорема 6. *(mass formula) За* $1 \leq k \leq n/2$ *е в сила формулата*

$$\sigma_2(n,k) = \sum_{C \in \mathcal{B}_2(n,k)} \frac{n!}{|\mathrm{Aut}(C)|},$$

където $\mathcal{B}_2(n,k)$ *е множеството от всички двоични нееквивалентни самоортогонални* $[n,k]$ *кодове.*

Пример 1. Броят на всички двоични кодове с дължина 6 и размерност 3 е $\begin{bmatrix} 6 \\ 3 \end{bmatrix}_2 = 1395$. Точно $\sigma_2(6,3) = \frac{6!}{48} = 15$ от тези кодове са самоортогонални. С точност до еквивалентност обаче съществува единствен самоортогонален $[6,3]$ двоичен код C. Този код има пораждаща матрица

$$gen(C) = \begin{pmatrix} 110000 \\ 001100 \\ 000011 \end{pmatrix}$$

и група от автоморфизми от ред $|\mathrm{Aut}(C)| = 48$.

По-нататък представяме формули за броя на LCD кодовете с дадена дължина и размерност.

За броя $T_2(n,k)$ на всички различни $[n,k]_2$ LCD кодове е изпълнена следната теорема [1].

Теорема 7. *За всяко естествено число $k \leq n-1$ е в сила*

$$T_2(n,k) = \begin{cases} 2^{(nk-k^2+n-1)/2} \begin{bmatrix} n/2-1 \\ (k-1)/2 \end{bmatrix}_4, & \text{ако } n \text{ е четно, а } k \text{ е нечетно число}, \\ 2^{(n-k)(k+1)/2} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_4, & \text{ако } n \text{ и } k \text{ са нечетни}, \\ 2^{k(n-k+1)/2} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_4, & \text{ако } n \text{ е нечетно, а } k \text{ е четно}, \\ 2^{k(n-k)/2} \left(2^{n-k} \begin{bmatrix} n/2-1 \\ k/2-1 \end{bmatrix}_4 + \begin{bmatrix} n/2-1 \\ k/2 \end{bmatrix}_4 \right), & \text{ако } n \text{ и } k \text{ са четни числа}. \end{cases}$$

Пример 2. *Броят на $[6,3]_2$ LCD кодовете е $T_2(6,3) = 2^7.5 = 640$, т.е. много повече от самоортогоналните кодове със същата дължина и размерност. Ако обърнем внимание на еквивалентностите, получаваме следния резултат: Съществуват 8 LCD $[6,3]$ и само един самоортогонален $[6,3]$ нееквивалентни двоични кода!*

В следващата теорема представяме формула за броя на троичните $[n,k]_3$ LCD кодове, означен с $T_3(n,k)$.

Теорема 8. *[1] За всяко естествено число $k \leq n-1$ е в сила*

$$T_3(n,k) = \begin{cases} 3^{(nk-k^2+n-3)/2} \begin{bmatrix} n/2-1 \\ (k-1)/2 \end{bmatrix}_9, & \text{ако } n \equiv 0 \pmod 4 \text{ и } k \text{ е нечетно}, \\ 3^{(nk-k^2+n+1)/2} \begin{bmatrix} n/2-1 \\ (k-1)/2 \end{bmatrix}_9, & \text{ако } n \equiv 2 \pmod 4 \text{ и } k \text{ е нечетно}, \\ 3^{(n-k)(k+1)/2} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_9, & \text{ако } n \text{ и } k \text{ са нечетни}, \\ 3^{k(n-k+1)/2} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_9, & \text{ако } n \text{ е нечетно и } k \text{ е четно}, \\ 3^{k(n-k)/2} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_9, & \text{ако } n \text{ и } k \text{ са четни числа}. \end{cases}$$

Пример 3. *По отношение на троичните кодове с дължина 6 и размерност 3 получаваме следните резултати:*

$$T_3(6,3) = 3^8.10 = 65610, \;\; \sigma_3(6,3) = 0,$$

т.е. има много LCD кодове с тези параметри, но нито един самодуален код. След проверка за еквивалентност получаваме, че съществуват точно 17 троични нееквивалентни LCD $[6,3]$ кода.

Както беше отбелязано в първата секция, с $A_{n,k,\ell}$ е означен броят на всички различни линейни $[n,k]_q$ кодове C, за които $\dim(C \cap C^\perp) = \ell$, $0 \leq \ell \leq k$. Да припомним също, че сечението $C \cap C^\perp$ наричаме самоортогонален подкод на кода C, т.е. $A_{n,k,\ell}$ е броят на всички линейни кодове с дължина n и размерност k над поле с q елемента, които имат самоортогонален подкод с размерност ℓ. Формула за този брой е доказана от Sendrier [6].

Теорема 9. *Нека k и $n \geq 2k$ са естествени числа и $0 \leq \ell \leq k$. Тогава*

$$A_{n,k,\ell} = \sum_{i=\ell}^{k} \begin{bmatrix} n-2i \\ k-i \end{bmatrix} \begin{bmatrix} i \\ \ell \end{bmatrix} (-1)^{i-\ell} q^{\binom{i-\ell}{2}} \sigma_q(n,i). \tag{2}$$

Очевидно $A_{n,k,k} = \sigma_q(n,k)$, а при $q = 2$ и $q = 3$ имаме съответно $A_{n,k,0} = T_2(n,k)$ и $A_{n,k,0} = T_3(n,k)$.

Sendrier в своята статия [6] от 1997 г. е доказал следните две важни теореми.

Теорема 10. *За всяко ℓ, редицата $A_{n,k,\ell}/\begin{bmatrix} n \\ k \end{bmatrix}$ е сходяща при $n \to \infty$ и $k \to \infty$. Ако означим границата с R_ℓ, то*

$$R_\ell = \frac{R_0}{(q-1)(q^2-1)\dots(q^\ell-1)} = \frac{R_{\ell-1}}{q^\ell - 1}, \quad R_0 = \prod_{i=1}^{\infty} \frac{q^i}{q^i+1}. \tag{3}$$

Теорема 11. *Средната размерност на самоортогоналния подкод на линеен код над поле с q елемента е асимптотично равна на*

$$\sum_{\ell \geq 1} \ell R_\ell = \sum_{i \geq 1} \frac{1}{q^i + 1}. \tag{4}$$

Оттук средната стойност на размерността на самоортогоналния подкод на линеен код за по-малките стойности на q е:

$q = 2)$ 0.7645

$q = 3)$ 0.404063

$q = 4)$ 0.2794

$q = 5)$ 0.215062

Във всички представени случаи тази средна размерност е по-малка от единица. Това означава, че много голяма част от линейните $[n,k]_q$ кодове са всъщност LCD кодове.

Резултатите, представени от Sendrier в [6], дават асимптотична оценка на тези бройки (т.е. какво става при $n \to \infty$ и $k \to \infty$). Нашите експерименти показаха, че във всички разглеждани случаи броят на кодове с дължина дължина n и размерност k над дадено поле $\mathbb{F}_q$ намалява при увеличаване на размерността на ортогоналните подкодове. Това ни даде основание да предположим, че такава зависимост е в сила за всички стойности на дължината и размерността, като в последствие доказахме тази хипотеза в Теорема 1. Това е основната теорема в тази статия и както подчертахме, тя се отнася до точните бройки на линейните кодове с фиксирани дължина и размерност над дадено крайно поле. Тук представяме само основните случаи, които разглеждаме в доказателството.

Идеята ни е да докажем, че разликата

$$A_{n,k,l} - A_{n,k,l+1} = \begin{bmatrix} n-2l \\ k-l \end{bmatrix} \sigma_{n,l} + \sum_{i=l+1}^{k} (-1)^{i-l} a_{n,k,l,i}, \tag{5}$$

е положително число. Във формула (5) използваме коефициента

$$a_{n,k,l,i} = \begin{bmatrix} n-2i \\ k-i \end{bmatrix} \begin{bmatrix} i \\ l \end{bmatrix} \frac{q^i - q^{i-l-1} + q^{i-l} - 1}{q^{l+1}-1} q^{\binom{i-l-1}{2}} \sigma_{n,i}.$$

Да припомним, че $\sigma_{n,i}$ е броят на всички самоортогонални кодове с дължина n и размерност i над полето $\mathbb{F}_q$. В процеса доказваме поотделно следните твърдения:

1. Ако $0 \leq l \leq k-1 \leq m-1$, $m = \lfloor n/2 \rfloor$, и $l+1 \leq i \leq k-1$, то $a_{n,k,l,i} > a_{n,k,l,i+1}$.
2. Ако $q \geq 3$ и $0 \leq l \leq k-1$, то $a_{n,k,l,l} > a_{n,k,l,l+1}$.
3. Ако $q = 2$ и $k \leq 2l+1$, то $a_{n,k,l,l} > a_{n,k,l,l+1}$.
4. Ако $q = 2$ и $k > 2l+1$, то $a = a_{n,k,l,l} - a_{n,k,l,l+1} + a_{n,k,l,l+2} - a_{n,k,l,l+3} > 0$.

Пример 4. *При $q = 2$ за кодовете с дължина 6 и размерност 3 получаваме*

$$A_{6,3,0} = 640,\ A_{6,3,1} = 620,\ A_{6,3,2} = 120,\ A_{6,3,3} = 15.$$

Във връзка с разглежданите бройки представяме и две хипотези, по които биха могли да работят и младите колеги алгебристи. Първата хипотеза се отнася до броя на нееквивалентните двоични самодуални кодове. Ако означим с SD_n броя на всички нееквивалентни кодове от този вид с дължина n, то

$$SD_n = \sigma_{n,n/2} \geq \frac{\prod_{i=1}^{n/2-1}(2^i+1)}{n!}$$

Хипотеза 1. *Ако $a_n = SD_n \frac{n!}{\prod_{i=1}^{n/2-1}(2^i+1)}$, то редицата $\{a_n,\ n = 10, 12, 14, \dots\}$ е намаляваща.*

Втората хипотеза се отнася до бройките от нееквиваленти линейни $[n,k]_q$ кодове. Релацията на еквивалентност, която използваме, може да се дефинира по следния начин.

Дефиниция 3. *Казваме, че линейните кодове C_1 и C_2 с дължина n над полето $\mathbb{F}_q$ са еквивалентни ($C_1 \cong C_2$), ако кодовите думи на C_2 могат да бъдат получени от кодовите думи на C_1 след прилагане на крайна последователност от следните трансформации:*

(1) *Пермутация на координатите.*

(2) *Умножаване на елементите в дадена позиция на всички кодови думи с ненулев елемент на полето $\mathbb{F}_q$.*

(3) *Прилагане на автоморфизъм на полето във всички координатни позиции.*

Еквивалентна дефиниция може да се даде и с използването на матрици. Ако C е линеен код с дължина n над полето $\mathbb{F}_q$, а M е квадратна $n \times n$ матрица над същото поле, то

$$CM = \{vM \ :\ v \in C\}.$$

т.е. CM се състои от всички вектори от вида vM, където v обхожда кодовите думи на C. Матрицата M дефинира линейно изображение в пространството $\mathbb{F}_q^n$, откъдето следва, че CM също е линеен код.

Дефиниция 4. *Казваме, че линейните кодове C_1 и C_2 с дължина n над полето $\mathbb{F}_q$ са еквивалентни ($C_1 \cong C_2$), ако $C_2 = C_1 M\gamma$, където $M \in Mon(n,q)$ е мономиална матрица, $\gamma \in Aut(\mathbb{F}_q)$ е автоморфизъм на полето.*

Хипотеза 2. *Неравенствата от Теорема 1 са в сила и за бройките нееквивалентни кодове със дадените дължина и размерност.*

Проблемът с тази хипотеза е, че не са доказани явни формули за броя на нееквивалентните кодове с дадена дължина и размерност. Затова за доказателството трябва да се търсят нови идеи.

5 Заключение

В заключение искам да благодаря на колегите от Факултета по математика и информатика при Шуменски университет "Епископ Константин Преславски" за поканата да представя последните си изследвания в пленарен доклад на конференцията MATTEX. Сътрудничеството ни с алгебричната колегия на факултета в течение на годините доведе до статии в реномирани международни издания, а в личен план за някои колеги до много добра академична кариера. Проф. Васил Йоргов беше мой научен ръководител. Той подпомогна моето развитие като математик, за което съм му много благодарна. Добро сътрудничество през тези години имахме и с проф. Никола Зяпков. Моят бивш докторант Николай Янков е високо ценен професор и доктор на математическите науки. С доц. Радка Русева сме работили по няколко научни проекта, а заедно бяхме и ръководители на докторантурата на Емине Караташ. Благодарение на усърдната работа и професионализма на колегите, получените от нас резултати бяха публикувани в престижни научни издания, като [7, 8, 9, 10, 11, 12, 13] са само част от съвместните статии.

ЛИТЕРАТУРА:

[1] Carlet, C., Mesnager, S., Tang, C., Qi, Y. New Characterization and Parametrization of LCD Codes. IEEE Transactions on Information Theory **65** (2019), 39–49.

[2] Huffman, W.C., Pless, V.S., Fundamentals of Error-Correcting Codes. Cambridge University Press (2003).

[3] MacWilliams, F. J., Sloane, N.J.A., The Theory of Error-Correcting Codes. North-Holland (1977).

[4] Pólya, G., Alexanderson, G., Gaussian binomial coefficients. Elemente der Mathematik **26** (1971), 102–109.

[5] Pless, V., The Number of Isotropic Subspaces in a Finite Geometry. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **39** (1965), 418–421.

[6] Sendrier, N., On the dimension of the hull. SIAM Journal on Discrete Mathematics **10(2)** (1997), 282–93.

[7] Bouyuklieva, S., Yorgov V. Singly-even self-dual codes of length 40. Designs, Codes and Cryptography **9** (1996) 131–141.

[8] Bouyuklieva, S., Russeva, R., Yankov, N. On the structure of binary self-dual codes having an automorphism a square of an odd prime. IEEE Trans. Inform. Theory **51** (2005) 3678–3686.

[9] Bouyuklieva, S., Russeva, R., Yankov, N. Classification of the binary self-dual [42,21,8] codes having an automorphism of order 3. Finite Fields and Their Applications **13**, (2007) 605–615.

[10] Bouyuklieva, S., Yankov, N., Kim, Jon-Lark, Classification of binary self-dual [48,24,10] codes with an automorphism of odd prime order. Finite Fields and Their Applications **18** (2012) 1104–1113.

[11] Bouyuklieva, S., Willems, W., Yankov, N. On the automorphisms of order 15 for a binary self-dual [96,48,20] code, Designs, Codes and Cryptography. **79** (2016) 171–182.

[12] Bouyuklieva, S., Russeva, R., Karatash, E. On some automorphisms of order 3 of the extremal binary codes. Electronic Notes in Discrete Mathematics. **57** (2017) 73–78.

[13] Bouyuklieva, S., Russeva, R., Karatash, E. Binary isodual codes having an automorphism of odd prime order", Mathematics in Computer Science. **14** (2020) 423–429.