С О Ф И Й С К И   У Н И В Е Р С И Т Е Т
„СВ.   К Л И М Е Н Т   О Х Р И Д С К И“

Ф А К У Л Т Е Т   П О   М А Т Е М А Т И К А   И   И Н Ф О Р М А Т И К А

Любомир Юриев Борисов

Оценки на радиуса на покритие и други параметри на кодове на Мелас и обобщения

ДИПЛОМНА РАБОТА

за придобиване на образователно-квалификационната степен „магистър“

към магистърски програми
„Дискретни и алгебрични структури“ и „Алгебра, геометрия и топология“

Научен ръководител
гл. ас. д-р Асен Божилов

СОФИЯ, 2015

Увод

В тази дипломна работа основно се разглеждат кодовете на Мелас и естествени техни обобщения. Кодовете на Мелас са въведени за първи път от Мелас в [9].

Дипломната работа се състои от 4 глави.

В първа глава се въвеждат основните понятия в теория на кодирането, които се използват по-нататък. Също така се разглеждат уравнения над крайни полета. Отделени са случаите, когато характеристиката е 2 и различна от 2.

Във втора глава се разглеждат кодове на Мелас над крайно поле с характеристика различна от 2. Код на Мелас наричаме цикличен код, на който пораждащият полином е произведение на минималните полиноми на примитивен елемент на разширение на полето и неговия обратен. В параграф 2 се доказва, че радиусът на покритие на код на Мелас не надвишава 3, когато основното поле има поне 5 елемента, а разширението му има поне 13 елемента (Теорема 2.1). Това прецизира резултат, получен от Великова, Божилов в [6]. Аналогичен резултат е доказан и когато основното поле е с 3 елемента, а разширението му е от степен поне 3 (Теорема 2.2). Когато разширението на полето съвпада с основното поле и има поне 5 елемента, е доказано, че радиусът на покритие е точно 2 (Теорема 2.3). В третия параграф се доказва, че минималното разстояние на код на Мелас е точно 2 (Теорема 3.2).

В трета глава се разглежда обобщение на кода на Мелас, когато пораждащият полином е произведение от минималните полиноми на примитивен елемент на разширение на основното поле и квадратът му. Доказано е, че минималното разстояние на такъв код е 3 (Теорема 3). В Теорема 7 и Твърдения 5 и 6 е намерен точният радиус на покритие на такъв код.

В четвъртата глава се разглежда двоичният код на Мелас. Определено е точното минимално кодово разстояние на такъв код в зависимост от четността на степента на разширението.

Съдържание

ГЛАВА I

Предварителни сведения

1. Основни понятия от теория на кодирането

В този параграф по-голямата част от твърденията и дефинициите са взети от [4] и [5].

Нека $\mathbb{F}_q$ е поле с $q = p^k$ елемента и проста характеристика p. Наредените n-торки $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ с елементи от $\mathbb{F}_q$ се наричат думи с дължина n в азбуката $\mathbb{F}_q$.

Определение Под q-ичен *код с дължина n* разбираме непразно множество от думи $C \subset \mathbb{F}_q^n$ с дължина n в азбуката $\mathbb{F}_q$.

Определение *Разстояние на Хеминг* между $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$ е броят на различните компоненти,

$$\mathrm{d}(a, b) = |\{1 \leq i \leq n \mid a_i \neq b_i\}|.$$

Непосредствено се проверява, че разстоянието на Хеминг е метрика, тоест са изпълнени:

1) $\mathrm{d}(a, b) \geq 0$, като $\mathrm{d}(a, b) = 0$ точно когато $a = b$

2) $\mathrm{d}(a, b) = \mathrm{d}(b, a)$

3) Неравенство на триъгълника $\mathrm{d}(a, c) \leq \mathrm{d}(a, b) + \mathrm{d}(b, c)$

Определение *Тегло на Хеминг* $\mathrm{wt}(a)$ на дума a с дължина n е броят на ненулевите координати на a.

Определение *Минималното разстояние* $\mathrm{d}(C)$ на q-ичен код C е минимално разстояние между различни думи от C,

$$\mathrm{d}(C) = \min\{\mathrm{d}(x, y) \mid x, y \in C, x \neq y\}.$$

Определение Разстоянието от дума $x \in \mathbb{F}_q^n$ до кода $C \subset \mathbb{F}_q^n$ е най-късото разстояние между x и кодов вектор,

$$\mathrm{d}(x, C) = \min\{d(x, a) \mid a \in C\}.$$

Една дума е кодова точно когато е на разстояние 0 от кода.

Определение Ако при предаване на кодова дума c е получена дума $y \in \mathbb{F}_q^n \setminus C$, търсим първо c измежду кодовите думи, които са на разстояние 1 от y. Ако не съществува такава кодова дума, търсим c измежду кодовите думи, които са на разстояние 2 от y и така нататък. Този начин за декодиране се нарича *метод на максималното правдоподобие*.

При предаването на информация, вероятността да са станали по-малък брой грешки е по-голяма, отколкото вероятността да са възникнали по-голям брой грешни символи. Затова декодирането се извършва по метода на максималното правдоподобие, тоест получената дума се декодира до думата, която е на най-малко разстояние от нея, когато тя е единствена.

Нека $\left[\dfrac{d-1}{2}\right]$ е най-голямото цяло число, ненадминаващо $\dfrac{d-1}{2}$. Ако при предаване на думите на код C с минимално разстояние d възникват не повече от $t = \left[\dfrac{d-1}{2}\right]$ грешки, то декодирането е еднозначно. По-точно, ако дума $y \in \mathbb{F}_q^n$ е на разстояние $< \left[\dfrac{d-1}{2}\right]$ от две кодови думи $a, b \in C$, то по неравенството на триъгълника

$$\mathrm{d}(a,b) \leq \mathrm{d}(a,y) + \mathrm{d}(y,b) \leq 2\left[\frac{d-1}{2}\right] < d.$$

Това противоречи на $\mathrm{d}(a,b) \geq d$ и доказва, че за всяка дума $y \in \mathbb{F}_q^n$, на разстояние $\leq t = \left[\dfrac{d-1}{2}\right]$ от C, съществува единствена кодова дума $a \in C$ на разстояние $\mathrm{d}(y,a) \leq t$ от y.

Определение Ако кодът C е линейно подпространство на $\mathbb{F}_q^n$, казваме, че C е *линеен код.*

Основни свойства на линеен код C са:

1) $(0,0,\dots,0) \in C$

2) $\mathrm{d}(C)$ съвпада с минималното тегло на дума от C

3) Ако $t_1, t_2, \dots, t_n \in C$ са кодови думи, то произволна тяхна линейна комбинация $a_1t_1 + a_2t_2 + \cdots + a_nt_n \in C$ с коефициенти $a_i \in \mathbb{F}_q$ е кодова дума.

Определение *Размерност* на линеен код $C \subset \mathbb{F}_q^n$ е размерността на C като линейно пространство над $\mathbb{F}_q$. Ще я означаваме с $\dim_{\mathbb{F}_q} C$.

Определение Ако $t_1, \dots, t_k$ е базис на линеен код $C \subset \mathbb{F}_q^n$, то матрицата

$$\mathbf{G} = \begin{pmatrix} t_1 \\ t_2 \\ \dots \\ t_k \end{pmatrix},$$

образувана по редове от компонентите на тези вектори, се нарича *пораждаща матрица на* C.

Ако $c = a_1t_1 + a_2t_2 + \cdots + a_kt_k$ е кодова дума, то векторът

$$\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_k \end{pmatrix}$$

се нарича *информационен.* На матричен език $c^t = G^t a$.

Множеството $\mathbb{F}_q^n$ на наредените n-торки с елементи от крайно поле $\mathbb{F}_q$ е линейно пространство над $\mathbb{F}_q$ относно покомпоненнтно определените събиране и умножение с $\alpha \in \mathbb{F}_q$. В частност, $\mathbb{F}_q^n$ е абелева група относно събирането. Произволен линеен код C е подгрупа $(C, +)$ на адитивната група $(\mathbb{F}_q^n, +)$ на линейното пространство $\mathbb{F}_q^n$. Съседните класове на $\mathbb{F}_q^n$ относно C са от вида $y+C = \{y+c \mid c \in C\}$ за някое $y \in \mathbb{F}_q^n$.

Ако $\dim_{\mathbb{F}_q} C = k$, C съдържа q^k думи, колкото е броят на всички линейни комбинации на базисните вектори. Всеки съседен клас съдържа $|y+C| = |C| = q^k$ думи. Два съседни класа или нямат общи думи, или съвпадат. Класовете $y+C = t+C$ с $y, t \in \mathbb{F}_q^n$ съвпадат точно когато $y \in t + C$.

Определение *Лидерът* на съседния клас $t+C$ е думата $y \in t+C$ с най-малко тегло.

Определение Максималното тегло на лидер y на съседен клас на $\mathbb{F}_q^n$ относно C се нарича *радиус на покритие* за C и се бележи с $\mathrm{r}(C)$.

ТВЪРДЕНИЕ 1.1. *Радиусът на покритие* $\mathrm{r}(C)$ *на линеен код* $C \subset \mathbb{F}_q^n$ *с минимално разстояние* d *изпълнява неравенството*

$$\mathrm{r}(C) \geq t = \left[\frac{d-1}{2}\right].$$

Доказателство: Достатъчно е да посочим дума от $\mathbb{F}_q^n$ с тегло t, която е лидерът на своя съседен клас. Твърдим, че

$$y = (1, \dots, 1, 0, \dots, 0) \in \mathbb{F}_q^n$$

е лидерът на $y+C$. Да допуснем, че лидерът на $y+C$ е $z \neq y$. Ако при предаване на кодова дума $c \in C$ са възникнали не повече от t грешки и е получена дума $w \in y + C = z + C$, то c се определя еднозначно от w. Както $w-y \in C$, така и $w-z \in C$ са на разстояние $\mathrm{d}(w, w-y) = \mathrm{d}(0, y) = t$, съответно $\mathrm{d}(w, w-z) = \mathrm{d}(0, z) \leq t$ от получената дума w, така че $c = w - y = w - z$, откъдето следва, че $y = z$. Това противоречи на $y \neq z$ и доказва, че $y = (1, \dots, 1, 0, \dots, 0)$ е лидерът на своя съседен клас $y + C$ и $\mathrm{r}(C) \geq t$. □

Определение Ако линеен код $C \subset \mathbb{F}_q^n$ има минимално разстояние d и радиус на покритие $\mathrm{r}(C) = t + 1 = \left[\frac{d-1}{2}\right] + 1$, казваме, че C е *квазиперфектен*.

Определение *Проверочно съотношение* за C се нарича такова хомогенно линейно уравнение $p\colon a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$, което е изпълнено за всяка дума $c = (c_1, c_2, \dots, c_n) \in C$, $c_i \in \mathbb{F}_q$, тоест $a_1c_1 + a_2c_2 + \cdots + a_nc_n = 0$ за $\forall c \in C$.

Да напомним, че рангът на матрица $H \in M_{m\times n}(\mathbb{F}_q)$ е максималният размер на ненулев минор на H. Рангът на H съвпада с максималния брой линейно независими вектор-редове на H и с максималния брой линейно независими вектор-стълбове на H. Произволен линеен код $C \subset \mathbb{F}_q^n$ с размерност k е пространството от решения на хомогенна линейна система уравнения, чиято матрица от коефициенти има ранг $n-k$.

Определение Ако $C \subset \mathbb{F}_q^n$ е пространството от решения на хомогенна система линейни уравнения

$$\begin{array}{c} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = 0 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{s,1}x_1 + a_{s,2}x_2 + \cdots + a_{s,n}x_n = 0 \end{array},$$

то матрицата

$$H = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ a_{s,1} & a_{s,2} & \dots & a_{s,n} \end{pmatrix}$$

се нарича *проверочна матрица* на C.

Дума $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ е кодова точно когато $c_1, \dots, c_n$ са решения на горната система. На матричен език $Hc^t = (0, \dots, 0)$.

Носителят на c е множеството

$$\mathrm{Supp}(c) = \{1 \le i \le n \mid c_i \ne 0\}$$

на индексите i на ненулевите компоненти $c_i \ne 0$ на c. Нека $H_1, \dots, H_n$ са стълбовете на матрицата H. Тогава C има ненулева дума c с носител $\mathrm{Supp}(c) \subseteq \{i_1, \dots, i_s\}$, $1 \le i_1 < \dots < i_s \le n$ точно когато $H_{i_1}, \dots, H_{i_s}$ са линейно зависими. Това доказва следващото

Твърдение 1.2. *Ако $C \subset \mathbb{F}_q^n$ е линеен код с минимално разстояние d и проверочна матрица H, то произволни $d-1$ стълба на H са линейно независими и съществуват d линейно зависими стълба $H_{i_1}, \dots, H_{i_d}$, $1 \le i_1 < \dots < i_d \le n$ на H.*

Определение *Цикличната пермутация* на вектор $c = (c_1, \dots, c_n)$ е векторът $(c_n, c_1, \dots, c_{n-1})$.

Определение Линеен код, който заедно с всеки свой вектор c съдържа и неговата циклична пермутация, се нарича *цикличен код*.

Ако на вектор $a = (a_0, a_1, \dots, a_{n-1}) \in C$ от цикличен код C съпоставим полинома $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]$ от степен $\le n-1$, то цикличната пермутация на a трансформира полинома $a(x)$ в полинома $xa(x)$ по модул идеала $(x^n - 1) \triangleleft \mathbb{F}_q[x]$, породен от полинома $x^n - 1 \in \mathbb{F}_q[x]$. По този начин, всеки цикличен код C е затворен относно умножение с полином от фактор-пръстена $R = \mathbb{F}_q[x]/(x^n - 1)$. Вземайки предвид, че C е затворено относно събиране, стигаме до извода, че C е идеал в R. Всеки елемент на R има единствен представител $r(x) \in \mathbb{F}_q[x]$ от степен $\deg r(x) \leq n-1$. Произведението на полиномите $a(x), b(x) \in R$ е равно на остатъка $r(x)$ при деление $a(x)b(x) = (x^n-1)q(x) + r(x)$ на $a(x)b(x) \in \mathbb{F}_q[x]$ с $x^n - 1$ с частно $q(x) \in \mathbb{F}_q[x]$ и остатък $r(x) \in \mathbb{F}_q[x]$ от степен $0 \leq \deg r(x) \leq n-1$.

Всеки идеал C в R се повдига до идеал в $\mathbb{F}_q[x]$ и е главен, т. е. $C = (g(x) + (x^n-1)) \lhd R$ за някакъв полином $g(x) \in \mathbb{F}_q[x]$ от степен $\deg(g) \leq n-1$.

Определение Произволен полином $g(x) \in \mathbb{F}_q[x]$ от степен $\deg(g) \leq n-1$, чийто съседен клас $g(x)+(x^n-1)$ поражда C като идеал в R, се нарича пораждащ полином на C. Записваме накратко $C = \langle g(x) \rangle$.

Теорема 1.3. *Нека $C = \langle g(x) \rangle$ е цикличен код с пораждащ полином $g(x)$ от степен $\deg(g) \leq n-1$. Тогава:*

1) $g(x) \mid x^n - 1$

2) *$c \in C$ точно когато $g(x) \mid c(x)$*

3) *Ако $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, то кодът има размерност $n-r$ и пораждащата матрица за C е*

$$\begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & 0 & g_0 & \dots & g_{r-2} & g_{r-1} & g_r & \dots & 0 \\ \multicolumn{9}{c}{\dotfill} \\ 0 & 0 & 0 & g_0 & \dots & \dots & \dots & \dots & g_r \end{pmatrix}$$

Доказателство: Повдигането $\widetilde{C}$ на идеала $C \lhd R$ до идеал в $\mathbb{F}_q[x]$ съдържа идеала (x^n-1). Следователно $x^n - 1 \in \widetilde{C} = \langle g(x) \rangle \lhd \mathbb{F}_q[x]$ или $g(x)$ дели x^n-1. Това доказва условие **1**).

Условие **2**) е тривиално следствие от факта, че C е идеал в R.

Ако $x^n - 1 = g(x)h(x)$ за някакъв полином $h(x) \in \mathbb{F}_q[x]$ от степен $\deg(h) = n-r$, то елементите на $C = (g + (x^n-1)) \lhd R$ са от вида $g(x)f(x) + (x^n-1) = g(x)s(x) + (x^n-1)$ за остатъка $s(x) \in \mathbb{F}_q[x]$ от степен $\deg(s) < n-r$ при деление $f(x) = h(x)q(x) + s(x)$ на $f(x) \in \mathbb{F}_q[x]$ с $h(x)$. Следователно кодът C има базис $g(x), xg(x), \dots, x^{n-r-1}g(x)$ над $\mathbb{F}_q$. Това доказва **3**). $\square$

Забележка: Нека $\alpha_1, \dots \alpha_r$ са всички корени на $g(x)$, броени с кратностите. Тогава $g(x) \mid c(x)$ точно когато $c(\alpha_i) = 0, i = 1, \dots r$. Затова за „проверочна“ матрица на C можем да изберем

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \multicolumn{5}{c}{\dotfill} \\ 1 & \alpha_r & \alpha_r^2 & \dots & \alpha_r^{n-1} \end{pmatrix}$$

Нека $g(x) = M_{\beta_1}(x) \dots M_{\beta_k}(x)$ за минималните полиноми $M_{\beta_i}(x)$ на β_i над $\mathbb{F}_q$ за $i = 1, \dots k$. Ако $M_{\beta_i}(x)$ и $c(x)$ имат общ корен, то всички корени на на $M_{\beta_i}(x)$ са корени на $c(x)$, тоест $M_{\beta_i}(x) \mid c(x)$. Затова $c \in C$ точно когато c е решение на хомогенната линейна система с матрица

$$\begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \dots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \dots & \beta_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \beta_k & \beta_k^2 & \dots & \beta_k^{n-1} \end{pmatrix}$$

Тези матрици не са проверочните по дефиниция за C понеже елементите α_i и β_j са от разширение на $\mathbb{F}_q$.

Определение Ако H е „проверочна“ матрица за C, то *синдром* на вектора $c \in \mathbb{F}_q^n$ наричаме вектора Hc^t.

Понеже условието $Hx^t = Hy^t$ е еквивалентно на $H(x-y)^t = \widetilde{0}$, където $\widetilde{0} = (0, \dots, 0)$, т. е. векторът $x - y$ е кодов, векторите x и y имат един същи синдром точно когато принадлежат на един и същи съседен клас $y + C = x + C$.

Определение Ако $C \subset \mathbb{F}_q^n$ е цикличен код с пораждащ полином $g(x)$, то частното

$$h(x) := \frac{x^n - 1}{g(x)}$$

се нарича *проверочен полином* за C.

От определението следва, че степента $\deg(h(x)) = n - r$ на проверочния полином е равна на размерността $\dim_{\mathbb{F}_q} C = n - r$.

Наредена n-орка $c = (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n$ принадлежи на цикличен код C с пораждащ полином $g(x)$ и проверочен полином $h(x)$ тогава и само тогава, когато $x^n - 1 = g(x)h(x)$ дели $c(x)h(x)$.

Определение *Код на Хеминг* наричаме код с проверочна матрица, състояща се от координатите спрямо $\mathbb{F}_p$ на всички два по два непропорционални вектори от $\mathbb{F}_q^*$, мултипликативната група на полето $\mathbb{F}_q$.

Когато $p = 2$, всеки вектор е пропорционален само на себе си и на нулевия, така че това са всички ненулеви вектори от $\mathbb{F}_q^*$, следователно в този случай кодът на Хеминг е цикличен и пораждащият му полином е минималният полином $m\alpha(x)$ на α над $\mathbb{F}_2$.

Понеже всеки ненулев вектор има $p - 1$ пропорционални, дължината на кода на Хеминг е $\dfrac{q-1}{p-1}$. Тъй като проверочната матрица на кода на Хеминг няма нулев стълб и два пропорционални стълба, минималното му кодово разстояние е не по-малко от 3. Проверочната матрица на кода на Хеминг съдържа стълбовете $c = (1, 0, 0, \dots, 0)^t$, $c = (0, 1, 0, \dots, 0)^t$ и $c = (1, 1, 0, \dots, 0)^t$, които са линейно зависими, следователно минималното му кодово разстояние е точно 3.

2. Уравнения над крайни полета

Нека $\mathbb{F}_q$ е крайно поле с $q = p^k$ елемента, $p \neq 2$ е просто число и нека $\mathbb{F}_q^* = \langle b \rangle = \{b^s \mid s = 0, \dots, q-2\}$, $Q = \langle b^2 \rangle$ *множеството от квадратите* в $\mathbb{F}_q^*$ и $N = b\langle b^2 \rangle$ *множеството от неквадратите* $\mathbb{F}_q^*$. Ясно е, че $|N| = |Q| = \dfrac{q-1}{2}$.

Лема 2.1. **1**) *Произведението на елементи от Q и N е елемент от N, а на елементи от N и N и на елементи от Q и Q е елемент от Q.*

2) $-1 \in N$ *точно когато* $p \equiv 3 \pmod 4$ *и k нечетно.*

Доказателство: 1) Ако $p = b^{2m}$ и $q = b^{2n}$ са два елемента от Q, то $pq = b^{2(m+n)} \in Q$.

Нека $\alpha \in N$. Разглеждаме множеството $F_\alpha := \{\alpha x \mid x \in \mathbb{F}_q^*\}$. Допускането, че $x_1\alpha = x_2\alpha$ влече, че $(x_1 - x_2)\alpha = 0$, откъдето понеже $\alpha \neq 0$, $x_1 = x_2$. Следователно $F_\alpha = \mathbb{F}_q^*$. Нека $y \in Q$, тоест $y = t^2$ за някое $t \in \mathbb{F}_q^*$. Допускането, че $\alpha y \in Q$, тоест $\alpha y = v^2$ за някое $v \in \mathbb{F}_q^*$ влече, че $\alpha = (vt^{-1})^2 \in Q$, което е противоречие. Заключваме, че $\alpha y \in N$. Нека $\alpha_Q := \{\alpha y \mid y \in Q\}$ и $\alpha_N := \{\alpha y \mid y \in N\}$. От $y_1\alpha \neq y_2\alpha$ при $y_1 \neq y_2$, $y_1 \in Q$, $y_2 \in Q$, $|\alpha_Q| = \dfrac{q-1}{2}$, предвид $|N| = |Q| = \dfrac{q-1}{2}$ и от това, че доказахме, че $\alpha_Q \subset N$, следва, че $\alpha_Q = N$. От това, че $x_1\alpha \neq x_2\alpha$ при $x_1 \neq x_2$ заключваме, че $\alpha z \in Q$ за $z \in N$.

2) Известно е, че -1 е квадратичен остатък по модул p точно когато $p \equiv 1 \pmod 4$. Следователно в този случай -1 е квадрат и в $\mathbb{F}_q$.

Нека $p \equiv 3 \pmod 4$. Тогава -1 е квадрат в $\mathbb{F}_q$ точно когато корен на полинома $x^2 + 1 = 0$ е в $\mathbb{F}_q$. Този полином е неразложим над $\mathbb{F}_p$, корените му са пораждащи за $\mathbb{F}_{p^2}$ над $\mathbb{F}_p$ и наличието им в $\mathbb{F}_q$ води до $\mathbb{F}_{p^2} \subset \mathbb{F}_q$, което е изпълнено точно когато $2 \mid k$. Следователно единствено при k нечетно -1 е неквадрат в $\mathbb{F}_q$. $\square$

Лема 2.2 (Божилов, Великова). *Нека M е множеството от решения (x, y) на уравнението*

$$Ax^2 + By^2 = C,$$

с $A \neq 0$, $B \neq 0$ над полето $\mathbb{F}_q$ с $q = p^k$ елемента и нека $D = BA^{-1}$. Тогава

$$|M| = \begin{cases} q - \left(\dfrac{-D}{q}\right), & \text{когато } C \neq 0 \\ q + \left(\dfrac{-D}{q}\right)(q-1), & \text{когато } C = 0 \end{cases}.$$

Доказателство: Нека за фиксирано y

$$M_x(y) := \left\{ x \mid x^2 = -\frac{B}{A}\left(-\frac{C}{B} + y^2\right)\right\}.$$

Твърдим, че $|M_x(y)| = 1 + \left(\frac{-\frac{B}{A}}{q}\right)\left(\frac{y^2 - \frac{C}{B}}{q}\right)$:

При $\frac{-B}{A}(y^2 - \frac{C}{B}) \in N$,

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

Не съществува x решение на уравнението, тоест $|M_x(y)| = 0$.

При $\frac{-B}{A}(y^2 - \frac{C}{B}) = 0$, $x = 0$ е единственото решение на уравнението и $|M_x(y)| = 1$.

При $\frac{-B}{A}(y^2 - \frac{C}{B}) \in Q$,

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

Уравнението има две решения за x, тоест $|M_x(y)| = 2$.

Ясно е, че

$$(1) \quad |M| = \sum_{y\in\mathbb{F}_q} |M_x(y)| = \sum_{y\in\mathbb{F}_q} (1 + \left(\frac{-\frac{B}{A}}{q}\right)\left(\frac{y^2 - \frac{C}{B}}{q}\right)) =$$

$$= q + \left(\frac{-\frac{B}{A}}{q}\right)\sum_{y\in\mathbb{F}_q}\left(\frac{y^2 - \frac{C}{B}}{q}\right) = q + \left(\frac{-D}{q}\right)\sum_{y\in\mathbb{F}_q}\left(\frac{y^2 - \frac{C}{B}}{q}\right).$$

Твърдим, че $\sum_{y\in\mathbb{F}_q}\left(\frac{y^2 - \frac{C}{B}}{q}\right) = \begin{cases} q-1, & \text{при } C = 0 \\ -1, & \text{при } C \neq 0 \end{cases}.$

1) $C = 0$. Когато $y = 0$, $\left(\frac{0}{q}\right) = 0$, а за всички $q - 1$ на брой ненулеви стойности на $y \in \mathbb{F}_q^*$, $\left(\frac{y^2}{q}\right) = 1$.

2) $C \neq 0$. Полагаме $S := \frac{C}{B} \neq 0$. Тогава

$$\sum_{y\in\mathbb{F}_q}\left(\frac{y^2 - \frac{C}{B}}{q}\right) = \sum_{y\in\mathbb{F}_q}\left(\frac{y^2 - S}{q}\right).$$

Ще докажем, че

$$\sum_{y\in\mathbb{F}_q}\left(\left(\frac{y^2 - S}{q}\right) + 1\right) = q - 1.$$

Имаме, че

$$\left(\frac{y^2-S}{q}\right)+1=\begin{cases}1, & \text{когато } y^2-S=0\\ 2, & \text{когато } y^2-S=x^2,\ x\neq 0\\ 0, & \text{когато } y^2-S\in N\end{cases}$$

Следователно $\displaystyle\sum_{y\in\mathbb{F}_q}\left(\left(\frac{y^2-S}{q}\right)+1\right)$ е броят решения на уравнението $y^2-x^2=S$. Представяйки $y^2-x^2=(y-x)(y+x)$ и използвайки, че $S\neq 0$, забелязваме, че решенията на последното уравнение се определят еднозначно от всяка ненулева стойност на $t=y-x$, като $t^{-1}S=y+x$. Понеже смяната $t^{-1}S=y+x$, $t=y-x$ е взаимноеднозначна, броят решения на уравнението е равен на $q-1$.

Имаме $\displaystyle q+\sum_{y\in\mathbb{F}_q}\left(\frac{y^2-S}{q}\right)=\sum_{y\in\mathbb{F}_q}\left(\left(\frac{y^2-S}{q}\right)+1\right)=q-1$, откъдето следва $\displaystyle\sum_{y\in\mathbb{F}_q}\left(\frac{y^2-S}{q}\right)=-1$. □

Лема 2.3. *Нека* $f(x)=Ax^2+Bx+C,\ A\neq 0,\ B\neq 0$ *и нека* $M=\{x\mid x\in\mathbb{F}_q, f(x^2)=f(tx^2), \text{за някое } t\in N\}$. *Тогава*

$$|M|=\begin{cases}\dfrac{q-1}{2}, & \text{при } p\equiv 3 \pmod 4 \text{ и } k \text{ нечетно}\\ \dfrac{q+1}{2}, & \text{при } p\equiv 1 \pmod 4 \text{ или } k \text{ четно}\end{cases}.$$

Доказателство: Нека x е решение на

$$f(x^2)=f(tx^2),$$

за някое $t\in N$. Очевидно $x=0$ е решение. Оттук нататък ще предполагаме, че $x\neq 0$. Имаме:

$$\begin{aligned}Ax^4+Bx^2+C&=At^2x^4+Btx^2+C\\ Ax^2+B&=At^2x^2+Bt\\ A(1-t^2)x^2&=B(t-1)\\ -A(1+t)x^2&=B\end{aligned}$$

понеже $1\notin N$. Тъй като $B\neq 0$, то $t\neq -1$ и разделяйки последното равенство на $1+t$, получаваме

$$x^2=\frac{-B}{A(1+t)}.$$

Елементът $t\in N$ точно когато съществува $u\in\mathbb{F}_q^*$ такова, че $t=bu^2$, $u\neq 0$. Понеже произведението на елементи от Q и N е елемент от N, а на елементи от N и N и на елементи от Q и Q е елемент от Q, ще разгледаме 2 случая:

1) $\dfrac{-B}{A} \in N$. Тогава $\dfrac{-B}{A(1+t)} \in Q$ точно когато $1+t \in N$, тоест

$$1 + bu^2 = bv^2 \tag{2}$$

за някое $v \in \mathbb{F}q^*$.

От Лема 2.2 имаме, че всички 2-ки $(u, v) \in \mathbb{F}_q^2$, решения на (2) са $q-1$ на брой. Измежду тях няма такива с $u = 0$ понеже $1 \in Q$, а такива с $v = 0$ има точно когато $-1 \in N$, което е изпълнено точно когато $p \equiv 3 \pmod 4$ и k нечетно.

1.1) $-1 \in N$

Двойките с $v = 0$ са две: $(\pm u_0, 0)$, $u_0^2 = -1$. Следователно остават $q - 3$ ненулеви решения на (2).

1.2) $-1 \in Q$

Няма двойки с $v = 0$ и има $q - 1$ ненулеви решения на (2).

От решенията на (2) v^2 еднозначно определя x^2 за x решение на (2), а 4 двойки решения $(\pm u, \pm v)$ на (2) с ненулеви (u, v) задават едно и също v^2. Оттук и понеже всеки ненулев елемент на Q има 2 квадратни корена, решенията на (2) с $x \neq 0$ са $\dfrac{q-3}{2}$ при $p \equiv 3 \pmod 4$ и k нечетно и $\dfrac{q-1}{2}$ иначе. Добавянето на решението $x = 0$ доказва лемата в този случай.

2) $\dfrac{-B}{A} \in Q$. Тогава $\dfrac{-B}{A(1+t)} \in Q$ точно когато $1+t \in Q$, тоест

$$1 + bu^2 = v^2 \tag{3}$$

за някое $v \in \mathbb{F}_q^*$.

От Лема 2.2 имаме, че всички двойки $(u, v) \in \mathbb{F}_q^2$, решения на (3) са $q + 1$ на брой. Измежду тях тези с $u = 0$ са две: $(0, \pm 1)$, а такива с $v = 0$ отново има точно когато $-1 \in N$, което е изпълнено точно когато $p \equiv 3 \pmod 4$ и к нечетно. Тогава те са две: $(\pm u_0, 0)$. Следователно броят на ненулевите решения на (3) отново е $q - 3$ при $p \equiv 3 \pmod 4$, k нечетно и $q - 1$ при $-1 \in Q$. По същия начин, както в **1)** случай, лемата следва. □

Забележка: Понеже всеки елемент на $\mathbb{F}_q^*$ има 2 квадратни корена при $p \geq 3$, а 0 единствен такъв, ако $M^2 = \{x^2 \mid x \in \mathbb{F}_q,\ f(x^2) = f(tx^2),$ за някое $t \in N\}$, $|M^2| = \dfrac{q+1}{4}$ при $p \equiv 3 \pmod 4$ и k нечетно и $|M^2| = \dfrac{q+3}{4}$ в останалите случаи.

3. Квадратни уравнения в крайни полета с характеристика 2

Тук ще дадем някои сведения, касаещи решаването на квадратни уравнения в крайни полета с характеристика 2 (виж например, [1]).

Определение *Следа* на елемента γ от $\mathbb{F}_2^m$ наричаме

$$\mathrm{tr}(\gamma) = \gamma + \gamma^2 + \cdots + \gamma^{2^{m-1}}$$

Ще използваме следните свойства на следата:

Твърдение 3.1.
1) *За произволни α и β : $\mathrm{tr}(\alpha+\beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$.*
2) *$\mathrm{tr}(\alpha^2) = \mathrm{tr}(\alpha)$.*
3) *Половината от елементите на $\mathbb{F}_2^m$ имат следа 0, а другата половина следа 1.*
4) *$\mathrm{tr}(1) = m \pmod 2$, тоест $\mathrm{tr}(1) = 0$ при m четно и $\mathrm{tr}(1) = 1$ при m нечетно.*

Доказателство: **1**) Имаме $\mathrm{tr}(\alpha+\beta) = (\alpha+\beta)+(\alpha+\beta)^2+\cdots+(\alpha+\beta)^{2^{m-1}} = \alpha+\beta+\alpha^2+\beta^2+\cdots+\alpha^{2^{m-1}}+\beta^{2^{m-1}} = \alpha+\alpha^2+\cdots+\alpha^{2^{m-1}}+\beta+\cdots+\beta^{2^{m-1}} = \mathrm{tr}(\alpha)+\mathrm{tr}(\beta)$ (Използвали сме, че за a и b в поле с характеристика 2, $(a+b)^2 = a^2+b^2$.)

2) Понеже $\alpha^{2^m} = \alpha$, следва, че:

$$\mathrm{tr}(\alpha^2) = \alpha^2 + \alpha^4 + \cdots + \alpha^{2^m} = \alpha^2 + \alpha^4 + \cdots + \alpha = \mathrm{tr}(\alpha).$$

3) Нека $f(x) := x + x^2 + \cdots + x^{2^{m-1}}$, а $g(x) := f(x) + 1$. Имаме $f(x)g(x) = x + x^2 + \cdots + x^{2^{m-1}} + x^2 + x^4 + \cdots + x^{2^m} = x + x^{2^m}$.

Корените на последния полином са всички елементи на $\mathbb{F}_2^m$. За $\gamma \in \mathbb{F}_2^m$ $\mathrm{tr}(\gamma) = 0$ точно когато γ е корен на $f(x)$, а $\mathrm{tr}(\gamma) = 1$ точно когато γ е корен на $g(x)$. Оттук и понеже $\deg(f(x)) = \deg(g(x)) = 2^{m-1}$ следва, че броят на елементите със следа 0 е равен на броя на елементите със следа 1, който е 2^{m-1}.

4) Имаме $\mathrm{tr}(1) = 1 + 1^2 + \cdots + 1^{2^{m-1}} = m \pmod 2$ □

Теорема 3.2. *Квадратното уравнение $x^2 + x + \gamma = 0$ има решение в полето $\mathbb{F}_2^m$ тогава и само тогава, когато $tr(\gamma) = 0$.*

Доказателство: *Необходимост:* Нека $u \in \mathbb{F}_2^m$ е решение на уравнението $x^2 + x + \gamma = 0$, тоест $u^2 + u + \gamma = 0$. Следователно е изпълнено $\mathrm{tr}(u^2 + u + \gamma) = tr(0) = 0$. Сега от Твърдение 3.1 следва, че $\mathrm{tr}(u^2 + u + \gamma) = \mathrm{tr}(u^2) + \mathrm{tr}(u) + \mathrm{tr}(\gamma) = \mathrm{tr}(\gamma) = 0$.
Достатъчност: Разглеждаме изображението $f(z) = z^2 + z$, $z \in \mathbb{F}_2^m$. От Твърдение 3.1 се вижда, че $tr(f(z)) = 0$ за всяко z. За доказателството на теоремата е достатъчно да покажем, че $f(z)$ приема за стойности всички елементи от $\mathbb{F}_2^m$ със следа, равна на 0. Ако $f(u) = f(v)$, тоест $u^2 + u = v^2 + v$, то е изпълнено: $u^2 + v^2 = (u+v)^2 = u + v$. Следователно $u + v$ е решение на уравнението $x^2 + x = x(x+1) = 0$, откъдето $u + v = 0$ или $u + v = 1$, и окончателно $v = u$ или $v = u + 1$. Това означава, че когато z пробягва полето $\mathbb{F}_2^m$, $f(z)$ приема за стойности половината от елементите на $\mathbb{F}_2^m$. Вземайки предвид отново Твърдение 3.1, заключаваме, че тези

стойности са всичките елементи със следа 0 (в частност и самото γ е една от тях). □

Забележка: Това доказателство на Теорема 3.2 не е ново и може да се намери например в [7]. Тук то е дадено за пълнота на изложението. Може да се забележи също, че доказателството се различава от това, което е изложено в [1], където е използван един по-конструктивен подход. А именно, в последната книга е описан метод за намиране на решенията на квадратните уравнения от разглеждания тип, базиращ се на така наречения нормален базис на полето $\mathbb{F}_2^m$.

ГЛАВА II

Кодове на Мелас

1. p-ичен код на Мелас

Нека $\mathbb{F}_q$ е крайно поле с $q = p^m$ елемента, $p \neq 2$ е просто число и нека $\mathbb{F}_q^* = \langle b \rangle = \{b^s \mid s = 0, \ldots, q-2\}$

Определение *p-ичен код на Мелас от m род ((p, p^m) код на Мелас)* $\mathcal{M}$ се нарича цикличен код с пораждащ полином $g(x) = M_\alpha(x) M_{\alpha^{-1}}(x)$, където α е примитивен елемент (тоест пораждащ за мултипликативната група на полето $\mathbb{F}_q$), докато $M_\alpha(x)$ и $M_{\alpha^{-1}}(x)$ са минималните полиноми съответно за α и α^{-1} над $\mathbb{F}_p$.

„Проверочната“ матрица на $\mathcal{M}$ има следния вид:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & . & . & . & \alpha^{q-2} \\ 1 & \alpha^{-1} & \alpha^{-2} & . & . & . & \alpha \end{pmatrix}$$

Блоковата дължина на този код е $n = q - 1$, а от общата теория на линейните циклични кодове е ясно, че размерността му е $\dim_{\mathbb{F}_q}(\mathcal{M}) = q - 1 - 2m$.

Забележка: При $q = p = 3$ имаме, че $\alpha = 2 = \alpha^{-1}$ и 2-та реда на H са равни, тоест дефинирането на кода не е много смислено, защото не съществува вектор със „синдром“ (a, b), $a \neq b$.

2. Радиус на покритие на p-ичен код на Мелас

Теорема 2.1. *Радиусът на покритие $r(\mathcal{M})$ е не по-малък от 2. Ако $p \geq 5$ и $q \geq 13$, то $r(\mathcal{M}) \leq 3$.*

Доказателство: Нека $S = \{s = (a, b) \in \mathbb{F}_q^2, (a, b) \neq (0, 0)\}$. Ще докажем, че съществува вектор $e \in \mathbb{F}_p^{q-1}$, $\mathrm{wt}(e) \leq 3$ със синдром s. За целта трябва да докажем, че системата $(*)$:

$$a_1 X_1 + a_2 X_2 + \cdots + a_l X_l = a$$
$$a_1 X_1^{-1} + a_2 X_2^{-1} + \cdots + a_l X_l^{-1} = b$$

има решение с две по две различни $X_j \in \mathbb{F}_q^*$, $j = 1, 2, \ldots, l$ и $a_j \in \mathbb{F}_p^*$, $j = 1, 2, \ldots, l$ за някое естествено число $l \leq 3$.

При $l = 1$ допускането, че $a = 0$ ($b = 0$) влече $a_1 = 0$ и $b = 0$ ($a = 0$). Ако $a \neq 0$ и $b \neq 0$, изразявайки от първото уравниние $X_1 = a a_1^{-1}$ и замествайки във второто, получаваме $a_1^2 = ab$, което означава, че системата има решение точно когато ab е ненулев квадрат в $\mathbb{F}_p$. Понеже ненулевите квадрати в $\mathbb{F}_p$ са $\dfrac{p-1}{2}$ на брой, винаги можем да изберем a и b такива, че ab да не е измежду тях. Следователно $r \geq 2$. Нека разгледаме системата

$$\begin{aligned} X_1 + X_2 + X_3 &= a \\ X_1^{-1} + X_2^{-1} + X_3^{-1} &= b \end{aligned}$$

с $(a,b) \in \mathbb{F}_q^2, (a,b) \neq (0,0)$, $ab \neq 1$. Нейно решение е еквивалентно на такова за $(*)$ с $a_j = 1$ за $X_j \neq 0$.

Ако допуснем, че $b = 0$, полагайки $Y_i = X_i^{-1}, i = 1,2,3$, получаваме

$$\begin{aligned} Y_1 + Y_2 + Y_3 &= 0 \\ Y_1^{-1} + Y_2^{-1} + Y_3^{-1} &= a \end{aligned}$$

с $a \neq 0$ и от решението за Y_i намираме X_i. Затова можем да считаме, че $b \neq 0$.

Разглеждаме функцията $D_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a$, $y \in \mathbb{F}_q$.

1) $-a^2b^2 + 6ab + 3 \neq 0$.

От Лема 2.3, Глава I, следва, че за поне $\dfrac{q+1}{4}$ при $q \equiv 3 \pmod 4$ и $\dfrac{q+3}{4}$ при $q \equiv 1 \pmod 4$ на брой стойности на c^2 за $c \in \mathbb{F}_q$ съществува $t \in N$ такова, че $D_1(c^2) = D_1(tc^2)$. Понеже едното от c^2 и (tc^2) е от Q, а другото от N, предвид Лема 2.1, Глава I, независимо от това дали $-D_1(y) \in Q$, или $-D_1(y) \in N$, можем да изберем $y = c^2$ или $y = tc^2$, така че $-yD_1(y) \in Q$. Тъй като при $q \geq 13$, $\dfrac{q+3}{4} > 3$, можем да изберем $y \neq 0$, $y \neq -b^{-1}$, $y \neq -a$ такова, че системата има решение:

$X_1 = \dfrac{a+y}{1+by}$, $X_2 = \dfrac{(ab-1)y + \sqrt{D}}{2(1+by)}$, $X_3 = \dfrac{(ab-1)y - \sqrt{D}}{2(1+by)}$, където $D = -yD_1(y)$.

Изборът $y \neq -a$ гарантира, че $X_1 \neq 0$. Допускането, че $X_2 = 0$ или $X_3 = 0$ при $y \neq 0$, води до уравнението $4by^2 + 4(ab+1)y + 4a = 0$, чиито корени са $y = -a$ и $y = -b^{-1}$, като тези възможности за y вече сме изключили. Следователно, изключвайки най-много 3 стойности за y, избрано по горния начин, гарантираме ненулево решение на системата. Ако $X_i = X_j$ за някои $1 \leq i < j \leq 3$, то получаваме решение на $(*)$ с $a_j = 2$ и $a_k = 1$ за единственото $k \neq i = j$, тоест вектор с тегло 2, имащ синдрома s.

2) $-a^2b^2 + 6ab + 3 = 0$.

Ясно е , че $a \neq 0$ и $b \neq 0$. Разглеждаме системата

$$X_1 + X_2 + X_3 = ak^{-1}$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = bk^{-1},$$

$k \in \mathbb{F}_p^*$. За нея коефициентът пред y в $D_1(yk^{-1})$ е $-a^2b^2k^{-4}+6abk^{-2}+3$ и допускането, че той е нулев, води до $ab(k^4-1) = 6(k^4-k^2)$, тоест до уравнението

$$k^4(ab-6) + 6k^2 - ab = 0,$$

имащо най-много 4 решения за k. При $p = 5$ уравнението е

$$k^4(ab-1) + k^2 - ab = 0$$

и има по-малко от 4 корена понеже 4-те елемента на $\mathbb{F}_5^*$ са корени на единствен унитарен полином от 4 степен k^4-1, който не е асоцииран с този в уравнението. Следователно можем да изберем k такова, че коефициентът пред y в $D_1(yk^{-1})$ е ненулев и последната система има решение за поне $\dfrac{q+1}{4} - 3$ стойности на y при $q \equiv 3 \pmod 4$ и $\dfrac{q+3}{4} - 3$ при $q \equiv 1 \pmod 4$, за които $yk^{-1} \neq 0$, $yk^{-1} \neq -b^{-1}$, $yk^{-1} \neq -a$. Това решение е еквивалентно на такова и за $(*)$ с $a_i = k$, $i = 1, 2, 3$. $\square$

Теорема 2.2. *Нека $p = 3$. При $q > 9$ също е в сила, че $r(\mathcal{M}) \leq 3$.*

Доказателство: В случая, когато $-a^2b^2 + 6ab + 3 = -a^2b^2 \neq 0$, твърдението следва от разсъжденията в предната теорема.

Когато $-a^2b^2 = 0$, $D = 2by^3 + 2ay = 2by^3$, защото $a = 0$, тъй като $b \neq 0$. Избираме y, удовлетворяващо условията:

$$y \neq 0, \quad y \neq -b^{-1}, \quad y \neq -a, \quad \text{и полагаме} \quad z^2 := 2by \in Q.$$

Функцията $f(t) := 2bt$ приема всички стойности на $\mathbb{F}_q$, когато t пробягва $\mathbb{F}_q$, а $|Q| = \dfrac{q-1}{2}$, следователно съществуват поне $\dfrac{q-1}{2}$ стойности на y, за които горните свойства са удовлетворени. Тогава

$$x_1 = \frac{2z^2b^{-1}}{1+2z^2}, \quad x_2 = \frac{2z^2b^{-1} + yz}{1+2z^2}, \quad x_3 = \frac{2z^2b^{-1} - yz}{1+2z^2}$$

са решения на системата. $\square$

Теорема 2.3. *Когато $q = p \geq 5$, тоест $\mathbb{F}_q$ е просто поле, $r(\mathcal{M}) = 2$.*

Доказателство: Наличието на вектор с тегло ≤ 2, имащ синдрома $(a, b) \neq (0, 0)$ е еквивалентно на решение на системата:

$$a_1X_1 + a_2X_2 = a$$
$$a_1X_1^{-1} + a_2X_2^{-1} = b$$

за $a_i \in \mathbb{F}_p$, $X_1 \neq X_2$, $X_i \in \mathbb{F}_q^*$. Умножаваме второто уравнение с $X_1X_2 \neq 0$ и получаваме, че системата е еквивалентна на

$$X_1a_1 + X_2a_2 = a$$
$$X_2a_1 + X_1a_2 = bX_1X_2$$

Детерминантата на последната система е равна на $X_1^2 - X_2^2 = 4 - 1 = 3 \neq 0$, избирайки $X_1 = 2$, $X_2 = 1$, и системата има решение за a_1 и a_2, като направеният избор $X_i \in \mathbb{F}_p^*$ гарантира $a_i \in \mathbb{F}_p$. $\square$

3. Минимално разстояние на код на Мелас

Следствие 3.1. *Минималното кодово разстояние на p-ичния код на Мелас е по-малко от 9.*

Доказателство: Съгласно Твърдение 1.1 $r(\mathcal{M}) \geq t$, $t = \left[\dfrac{d-1}{2}\right]$. От Теорема 2.2 имаме, че $t \leq 3$, откъдето $\dfrac{d-1}{2} < 4$ и $d(\mathcal{M}) < 9$. $\square$

Теорема 3.2. *В сила е, че $d(\mathcal{M}) = 2$.*

Доказателство: Наличието на кодова дума с тегло 1 е еквивалентно на решение с $a_1 \in \mathbb{F}_p$, $x_1 \in \mathbb{F}_q^*$ на системата:

$$a_1X_1 = 0$$
$$a_1X_1^{-1} = 0$$

Понеже в поле няма делители на 0, то такава дума не съществува. Следователно $d(\mathcal{M}) \geq 2$. Остава да докажем, че $d(\mathcal{M}) \leq 2$, което е еквивалентно на решение с $a_i \in \mathbb{F}_p$, $i = 1, 2$ и $x_j \in \mathbb{F}_q^*, j = 1, 2$, $(x_1, x_2) \neq (0, 0)$ (при това x_j са различни) на системата:

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_1^{-1} + a_2X_2^{-1} = 0$$

Изборът $a_1 = a_2 = 1 = 1$, $X_1 = 1$, $X_2 = -1$ води до такова решение. $\square$

Забележка: Горните твърдения са в сила и когато $p \neq 2^k$ е съставно, като единственото прецизиране е в доказателството на Теорема 2.3 в случая, когато $p = 3^k$. Тогава избираме $X_1 = \beta$, където β е пораждащ за $\mathbb{F}_p$ като разширение над $\mathbb{F}_3$, тоест $\mathbb{F}_p = \mathbb{F}_3(\beta)$, $X_2 = 1$. Понеже $x^2 - 1$ е разложим над $\mathbb{F}_3$, е ясно, че $\beta^2 \neq 1$.

ГЛАВА III

Кодове, подобни на код на Мелас

Развитата теория до сега може да се приложи и за други циклични кодове над $\mathbb{F}_q$, $q = p^m$, с блоковата дължина $n = q - 1$. При горните означения и $p \geq 3$ нека разгледаме кода $\mathcal{D}$ с „проверочна" матрица H, имаща следния вид:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & . & . & . & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & . & . & . & \alpha^{2(q-2)} \end{pmatrix}$$

Пораждащ полином за $\mathcal{D}$ е $g(x) = M_\alpha(x)M_{\alpha^2}(x)$, където $\mathbb{F}_q^* = \langle\alpha\rangle$, докато $M_\alpha(x)$ и $M_{\alpha^2}(x)$ са минималните полиноми съответно за α и α^2 над $\mathbb{F}_p$.

Забележка: При $p = 2$ имаме, че $M_\alpha(x) = M_{\alpha^2}(x)$. Тогава $\mathcal{D}$ съвпада с кода на Хеминг и вторият ред на H е излишен. Затова ще считаме, че $p \geq 3$.

Твърдение 1. *Размерността на* $\mathcal{D}$ $\dim_{\mathbb{F}_p}(\mathcal{D}) = q - 1 - 2m$.

Доказателство: От Теорема 1.3, Глава I, следва, че твърдението е еквивалентно на това полиномът $g(x)$ да е от степен, равна на $2m$.

Всички корени на $M_\alpha(x)$ са от вида α^{p^k}, а тези на $M_{\alpha^2}(x)$ са от вида α^{2p^k} за $k = 0, \dots, m-1$. Всички те са различни понеже допускането, че $\alpha^{2p^i} = \alpha^{2p^j}$ за $i > j$ влече

$$p^m - 1 \mid 2(p^i - p^j) = 2p^j(p^{i-j} - 1)$$

и от $(p^j, p^m - 1) = 1$ следва, че $p^m - 1 \mid 2(p^{i-j} - 1)$. От

$$p^{i-j} - 1 \leq p^{m-1} - 1$$

следва, че

$$2(p^{i-j} - 1) \leq 2p^{m-1} - 2 < p^m - 1$$

и делението е възможно само когато $2(p^{i-j} - 1) = 0$, откъдето $i = j$ и получаваме противоречие. Следователно

$$\deg(M_\alpha(x)) = \deg(M_{\alpha^2}(x)) = m.$$

Освен това 2-та полинома нямат общ корен. Наистина допускането, че $\alpha^{p^i} = \alpha^{2p^j}$ за някои $0 \leq i, j \leq m-1$ влече $p^m - 1 \mid (p^i - 2p^j)$. Понеже $1 \leq p^i \leq p^{m-1}$ и $2 \leq 2p^j \leq 2p^{m-1}$, то

$$-p^m + 1 < -2p^{m-1} + 1 \leq p^i - 2p^j \leq p^{m-1} - 2 < p^m - 1$$

и от $p^m - 1 \mid (p^i - 2p^j)$ следва, че $p^i - 2p^j = 0$, което е невъзможно понеже $p \geq 3$. Следователно $g(x) = M_\alpha(x)M_{\alpha^2}(x)$ е от степен $2m$. $\square$

За $\mathcal{D}$ наличието на вектор с тегло ≤ 3, имащ синдром $(a, b) \neq (0, 0)$ е еквивалентно на решение на системата:

$$a_1X_1 + a_2X_2 + a_3X_3 = a$$
$$a_1X_1^2 + a_2X_2^2 + a_3X_3^2 = b$$

с две по две различни $X_j \in \mathbb{F}_q^*$, $j = 1, 2, 3$, $a_j \in \mathbb{F}_p$. Тъй като векторът с компоненти $X_j \in \mathbb{F}_q^*$, $j = 1, 2, 3$ е ненулев, можем да считаме, че $a_1 \neq 0$. Ще търсим решение с $a_1 = 1$, $a_2 = a_3$. Фиксирайки $y := X_1$, изразявайки $X_2+X_3 = (a-X_1)a_2^{-1}$, замествайки във второто уравнение, намираме X_2X_3 и от формулите на Виет получаваме, че X_2 и X_3 са корени на уравнението

$$t^2 + (y - a)a_2^{-1}t + \frac{y^2 - b + a_2^{-1}(y - a)^2}{2a_2} = 0$$

с дискриминанта

$$D = \frac{(-1 - 2a_2)y^2 + 2ay - a^2 + 2ba_2}{a_2^2}.$$

Ще разгледаме няколко случая:

1) $a = 0$. Тогава $b \neq 0$

1.1) $p \geq 5$. Изборът $a_2 = 1$ води до $D = -3y^2+2b$. Понеже $b \neq 0$, съгласно Лема 2.2, Глава I, съществуват поне $q - 1$ 2-ки $(y, t) \in \mathbb{F}_q^2$, за които $D = t^2$, като поне $q - 3$ от тях са с $y \neq 0$. Получаваме, че за поне $\dfrac{q-1}{2}$ $\left(\dfrac{q+1}{2}\right.$, когато $t = 0$ е решение$\left.\right)$ стойности на y $D = t^2$, $t \in \mathbb{F}_q$. Ако $X_i = X_j$ за $i \neq j$, както и ако някое $X_k = 0$, то следва, че имаме вектор с тегло ≤ 2, имащ синдрома (a, b).

1.2) $p = 3$. Изборът $a_2 = 1$ води до $D = 2b$. Ако $2b$ е неквадрат, избираме $a_2 = 2$. Тогава за $D = y^2+b$ и по Лема 2.2, Глава I, отново следва, че има поне $\dfrac{q-1}{2}$ стойности на y, за които $D = t^2$, $t \in \mathbb{F}_q$.

2) $a \neq 0$. Изборът $a_2 = -2^{-1}$ води до $D = 4(2ay - a^2 - b)$, който израз приема всички стойности на $\mathbb{F}_q$, когато y пробягва $\mathbb{F}_q$. Следователно за $\dfrac{q+1}{2}$ стойности на y е изпълнено $D = t^2$, $t \in \mathbb{F}_q$ и системата има решение. Полученият резултат можем да запишем като

Теорема 2. *При $p \geq 3$ радиусът на покритие на кода $\mathcal{D}$ е $r(\mathcal{D}) \leq 3$.*

Теорема 3. *Минималното кодово разстояние на $\mathcal{D}$ е $d(\mathcal{D}) = 3$.*

Доказателство: В горните означения при $a = 0$ и $b = 0$ имаме $D = \dfrac{(-1-2a_2)y^2}{a_2^2}$. Условието $D = t^2$, $t \in \mathbb{F}_q$ е еквивалентно на $(-1-2a_2)y^2 - v^2 = 0$, където $v := ta_2$. Понеже $(-1-2a_2) \neq 0$, избирайки $a_2 \neq -2^{-1}$, от Лема 2.2, Глава I, следва, че за поне $\dfrac{q-1}{2}$ стойности на y $D = t^2$. Заключваме, че $d(\mathcal{D}) \leq 3$. Допускането, че $d(\mathcal{D}) \leq 2$ е еквивалентно на ненулево решение на системата:

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_1^2 + a_2X_2^2 = 0$$

Разглеждайки я като линейна относно a_1 и a_2, тя е с детерминанта $X_1X_2(X_2 - X_1) \neq 0$ и следователно системата няма ненулево решение и получаваме противоречие. □

Твърдение 4. *В $\mathbb{F}_p^n$ има вектор с тегло 1, имащ синдрома $(a, b) \neq (0, 0)$ точно когато $a \neq 0$, $b \neq 0$ и $a^2b^{-1} \in \mathbb{F}_p$.*

Доказателство: Съществува вектор с тегло 1, имащ синдрома $(a, b) \neq (0, 0)$, точно когато системата

$$a_1X_1 = a$$
$$a_1X_1^2 = b$$

има решение за $X_1 \in \mathbb{F}_q^*$ с $a_1 \in \mathbb{F}_p^*$. Допускането, че $a = 0$ (или $b = 0$) влече $X_1 = 0$ или $a_1 = 0$ и $b = 0$ (или и $a = 0$). Нека $a \neq 0$, $b \neq 0$. Заместваме $X_1 = \dfrac{a}{a_1}$ във второто уравнение и получаваме $a^2 = ba_1$ и изборът на $a_1 = a^2b^{-1}$ води до решението $X_1 = \dfrac{a}{a_1}$. □

Понеже синдромите (a, b), за които $a = 0$, $b \neq 0$ или $b = 0$, $a \neq 0$ нямат лидери с тегло 1, $r(\mathcal{D}) \geq 2$.

Твърдение 5. *При $q = p \geq 5$ $r(\mathcal{D}) = 2$, тоест кодът е квазиперфектен.*

Доказателство: За $\mathcal{D}$ наличието на вектор с тегло ≤ 2, имащ синдрома $(a, b) \neq (0, 0)$, е еквивалентно на решение на системата:

$$a_1X_1 + a_2X_2 = a$$
$$a_1X_1^2 + a_2X_2^2 = b$$

с две различни $X_j \in \mathbb{F}_q^*$, $j = 1, 2$. Ще намерим решение при $a_1 = 1$. Нека $a_2 := \alpha$. Търсим решение на системата:

$$X_1 + \alpha X_2 = a$$
$$X_1^2 + \alpha X_2^2 = b$$

1 случай: $a = 0$. От първото уравнение изразяваме $X_1 = -\alpha X_2$ и замествайки във второто, получаваме $(\alpha^2+\alpha)X_2^2 - b = 0$ за някое $X_2 \in \mathbb{F}_q^*$. То има решение точно когато $\dfrac{b}{\alpha^2+\alpha} = t^2$ за някое $t \in \mathbb{F}_q^*$, тоест $(\alpha^2+\alpha)t^2 = ((\alpha+2^{-1})^2 - 2^{-2})t^2 = b$ за $\alpha \neq 0, -1$

1.1) $b \in Q$. Искаме $(\alpha + 2^{-1})^2 - s^2 - 2^{-2} = 0$ за $s = \sqrt{b}t^{-1}$. От Лема 2.2, Глава I, следва, че уравнението има $q-1$ двойки решения $(\alpha+2^{-1}, s)$, на които съответстват $q-1$ двойки решения (α, s). При това $\alpha = 0, -1$ участва в решение точно когато $s = 0$. При $s \neq 0$ остават $q-3$ двойки решения. С $\alpha + 2^{-1} = 0$ имаме две решения $(-2^{-1}, \pm 2^{-1}\sqrt{-1})$ при $p \equiv 1 \pmod 4$ и нямаме решение при $p \equiv 3 \pmod 4$. Както в Лема 2.3, Глава I, заключваме, че и в двата случая имаме $\dfrac{q-3}{2}$ благоприятни стойности за α.

1.2) $b \in N$. Искаме $(\alpha + 2^{-1})^2 - bv^2 - 2^{-2} = 0$ за $v = t^{-1}$. От Лема 2.2, Глава I, следва, че уравнението има $q+1$ двойки решения $(\alpha + 2^{-1}, v)$, на които съответстват $q+1$ двойки решения (α, v). Случаят $v = 0$ ни дава две двойки решения и съответства на $\alpha = 0, -1$. При $v \neq 0$ остават $q-1$ двойки решения. Освен това $\alpha + 2^{-1} = 0$ дава 2 решения точно когато $-bv^2 = 2^{-2}$ има решение, тоест $-b \in Q$, в сила точно когато $-1 \in N$, което е изпълнено при $p \equiv 3 \pmod 4$. При $p \equiv 1 \pmod 4$ $-1 \in Q$, $-b \in N$ и $\alpha + 2^{-1} = 0$ не дава решение. И в двата случая имаме $\dfrac{q-1}{2}$ благоприятни стойности на α.

За така получената стойност на $X_2 = t$ при някоя от тези стойности на α намираме $X_1 = -\alpha X_2$.

2 случай: $a \neq 0$. Ще докажем, че при $\alpha = -1$ системата има решение. Изразявайки $X_1 = a + X_2$ от първото уравнение и замествайки във второто, получаваме $a^2 + 2aX_2 - b = 0$, което води до решение с $X_2 = \dfrac{b-a^2}{2}a$, $X_1 = a + \dfrac{b-a^2}{2}a = \dfrac{a^2+b}{2}a$. Ясно е, че или $X_1 \neq 0$, или $X_2 \neq 0$ (може и двете). □

Твърдение 6. *При $q = p = 3$ е изпълнено, че $r = 2$.*

Доказателство: Да разгледаме синдрома $(0, 1)$. Системата

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_1^2 + a_2X_2^2 = 1$$

има решение $a_1 = a_2 = 2$ с $X_1 = 1$, $X_2 = 2$.

При синдром $(0, 2)$ системата

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_1^2 + a_2X_2^2 = 2$$

има решение $a_1 = a_2 = 1$ с $X_1 = 1$, $X_2 = 2$.

За синдромите с $a \neq 0$ от разсъжденията в Твърдение 2.12, следва, че $a_1 = 1$, $a_2 = -1$ е решение. $\square$

Теорема 7. *Нека $q = p^m$. При $m = 2l+1$, $r = 2$, а при $m = 2l$, $r = 3$.*

Доказателство: Ще разгледаме два случая:

1) $a \neq 0$. Ще докажем, че $a_1 = 1$, $a_2 = -1$ е решение на системата:

$$a_1X_1 + a_2X_2 = a$$
$$a_1X_1^2 + a_2X_2^2 = b$$

при някакви $X_1X_2, \in \mathbb{F}_q$. Изразявайки $X_1 = a + X_2$ от първото уравнение и заествайки във второто, получаваме $a^2+2aX_2-b = 0$, което води до решение с $X_2 = \dfrac{b-a^2}{2a}$, $X_1 = a+\dfrac{b-a^2}{2a} = \dfrac{a^2+b}{2a}$. Ясно е, че поне едно от двете X_1, X_2 е ненулево (може и двете). Така, че има вектор с тегло 2, чийто синдром е (a, b).

2) $a = 0$. Наличието на вектор с тегло ≤ 2, имащ синдрома $(a, b) \neq (0, 0)$, е еквивалентно на това системата

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_1^2 + a_2X_2^2 = b$$

да има решение с две различни $X_j \in \mathbb{F}_q^*$, $j = 1, 2$. Ясно е, че $a_1 \neq 0$ и $a_2 \neq 0$. Последната система е еквивалентна на

$$X_1 + \frac{a_2}{a_1}X_2 = 0$$
$$X_1^2 + \frac{a_2}{a_1}X_2^2 = \frac{b}{a_1}$$

Изразявайки $X_1 = -\dfrac{a_2}{a_1}X_2$ от първото и замествайки във второто уравнение, получаваме $X_2^2 = \dfrac{ba_1}{a_2^2 + a_2a_1} = G(a_1, a_2, b)$. Последното има решение за X_2 точно когато $G(a_1, a_2, b) \in Q$.

Ще докажем, че $G(a_1, a_2, b)$ не може да приема еднакви стойности за две различни стойности на $a_1 \neq -a_2$ при фиксирани $a_2 \neq 0$ и $b \neq 0$. Наистина, допускането, че $\dfrac{\gamma b}{a_2^2 + a_2\gamma} = \dfrac{\beta b}{a_2^2 + a_2\beta}$, е равносилно на $(\gamma - \beta)a_2^2 = 0$, което обаче е невъзможно при $\gamma \neq \beta$. Така че при фиксирано a_2, менейки $a_1 \in \mathbb{F}_p^* \backslash \{-a_2\}$, $G(a_1, a_2, b)$ приема $p - 2$ стойности.

При $p \geq 5$ $p - 2 > \dfrac{p-1}{2}$. Когато $p = 3$, за $b \in N$ избираме $a_1 = 1$, $a_2 = 1$ и получаваме, че $\dfrac{a_1}{a_2^2 + a_2a_1} = 2$ (неквадрат в полето $\mathbb{F}_3$) , а за $b \in Q$ изборът $a_1 = 2$, $a_2 = 2$ води до $\dfrac{a_1}{a_2^2 + a_2a_1} = 1 \in Q$.

При $m = 2l+1$ половината $\dfrac{p-1}{2}$ елемента на $\mathbb{F}_p^*$ са в Q, а останалите, неквадратите в $\mathbb{F}_p^*$, които са $\dfrac{p-1}{2}$ на брой, са в N. Когато $m = 2l$, всички елементи на $\mathbb{F}_p^*$ са от Q. Това е така понеже $\dfrac{p-1}{2}$ елемента на $\mathbb{F}_p^*$ са квадрати на елемент от $\mathbb{F}_p^*$, а за такова $t \in \mathbb{F}_p^*$, което не е квадрат на елемент от $\mathbb{F}_p^*$, $\sqrt{t} \in \mathbb{F}_p^2$ и $\sqrt{t} \in F_q$ точно когато $\mathbb{F}_p^2 \subset \mathbb{F}_q$, което е изпълнено точно когато $2 \mid m$. Ако $b \in N(Q)$, то при $m = 2l+1$ последната има решение понеже $G(a_1, a_2, b) \in Q$, избирайки a_2 и a_1 от $\mathbb{F}_p^*$, такива че $\dfrac{a_1}{a_2^2 + a_2 a_1} \in N(Q)$ (Използваме свойството, че произведенията на елемент от N и елемент от N и на два елемента от Q са елементи от Q). При $m = 2l$, както и да избираме a_2 и a_1 от $\mathbb{F}_p^*$, $\dfrac{a_1}{a_2^2 + a_2 a_1} \in Q$ и $G(a_1, a_2, b) \in N$ за синдромите с $b \in N$. $\square$

Забележка: Горните твърдения се пренасят и при p съставно, стига $p \neq 2^k$.

Твърдение 8. *При $p = 2^k$, $k \geq 2$, е в сила, че $d(\mathcal{D}) = 3$.*

Доказателство: По същия начин, както при $p \neq 2^k$, се съобразява, че $d(\mathcal{D}) \geq 3$. Разглеждаме системата:

$$a_1 X_1 + a_2 X_2 + a_3 X_3 = 0$$
$$a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2 = 0$$

Избираме две по две различни $X_j \in \mathbb{F}_p^*$, $j = 1, 2, 3$. Системата относно a_j, $j = 1, 2, 3$ е хомогенна с ранг 2 и пространството от решения за нея е едномерно, в частност системата има ненулево решение, на което съответства кодова дума с тегло, равно на 3. $\square$

Лема 9. *В поле с $q = 2^k$ елемента $\mathbb{F}_q^* = Q$.*

Доказателство: Нека $\mathbb{F}_q^* = \langle \beta \rangle = \{\beta^l \mid l = 1, \ldots, 2^k - 1\}$. Допускането, че два различни елемента на $\mathbb{F}_q^*$ имат еднакъв квадрат, тоест $\beta^{2i} = \beta^{2j}$ за $2^k - 1 \geq i > j \geq 0$ влече, че $2^k - 1 \mid 2(i-j)$, и от $(2, 2^k - 1) = 1$ следва, че $2^k - 1 \mid i - j$, което е невъзможно. Следователно квадратите на всички елементи $\mathbb{F}_q^*$ са същите елементи в разбъркан ред. $\square$

Твърдение 10. *При $p = 2^k$, $k \geq 2$ радиусът на покритие на $\mathcal{D}$ е $r = 2$, тоест $\mathcal{D}$ е квазиперфектен.*

Доказателство: Поради същите съображения, както при $p \neq 2^k$, следва, че $r \geq 2$. Разглеждаме системата:

$$X_1 + \alpha X_2 = a$$
$$X_1^2 + \alpha X_2^2 = b$$

Изразявайки $X_1 = a + \alpha X_2$ от първото уравнение и замествайки във второто, получаваме $(\alpha^2+\alpha)X_2^2 + a^2 - b = 0$.

1) $a^2 - b \neq 0$. Избираме $\alpha \neq 0$, $\alpha \neq -1$. Тогава

$$X_2^2 = \frac{b-a^2}{\alpha^2+\alpha} \in \mathbb{F}_q^*$$

и от Лема 9 следва, че съществува $X_2 \in \mathbb{F}_q^*$, удовлетворяващо горното равенство, откъдето намираме решение на системата. При $X_1 = 0$ имаме вектор с тегло 1, имащ синдрома (a, b).

2) $a^2 - b = 0$. Тогава $X_1 = a$, $X_2 = 0$ е решение на системата и отново имаме вектор с тегло 1, имащ синдрома (a, b). $\square$

ГЛАВА IV

Двоичен код на Мелас

1. Характеристики на двоичен код на Мелас

Тук ще разгледаме кода на Мелас $\mathcal{M}$ при $p = 2$. Блоковата дължина на този код е $n = 2^m - 1$.

Твърдение 1.1. *При $m \geq 3$ размерността на $\mathcal{M}$ е $2^m - 1 - 2m$.*

Доказателство: Корените на минималния полином $M_\alpha(x)$ над $\mathbb{F}_2$ за пораждащия елемент α на $\mathbb{F}_{2^m}^*$ са от вида α^{2^l} за $0 \leq l \leq m-1$. Елементът $\alpha^{-1} = \alpha^{2^m-2}$ също е пораждащ за $\mathbb{F}_{2^m}^*$ и двата полинома са от степен m. Понеже при $m \geq 3$ за всяко $0 \leq l \leq m-1$ $2^l \neq 2^m - 2$, корените им са различни и $\deg(M_\alpha(x)M_{\alpha^{-1}}(x)) = 2m$, откъдето следва, че размерността на $\mathcal{M}$ е $2^m - 1 - 2m$. $\square$

Забележка: При $m = 2$ е изпълнено $M_{\alpha^{-1}}(x) = M_\alpha(x)$ и следователно $\mathcal{M}$ е кодът на Хеминг с дължина 3. Затова разглеждаме кода при $m \geq 3$.

Твърдение 1.2. *Кодът на Мелас е реверсивен код, тоест заедно с всяка кодова дума $\mathbf{c} = (c_0, c_1, \ldots, c_{n-2}, c_{n-1})$ в него се съдържа и думата $\mathbf{c}' = (c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$.*

Доказателство: Понеже $(\alpha^{-1})^j = \alpha^{n-j}$ и пораждащ полином за $\mathcal{M}$ е $M_\alpha(x)M_{\alpha^{-1}}(x)$, думата $\mathbf{c} = (c_0, c_1, \ldots, c_{n-2}, c_{n-1})$ принадлежи на $\mathcal{M}$ точно когато е удовлетворена системата:

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0$$
$$c_0 + c_1\alpha^{n-1} + \cdots + c_{n-1}\alpha = 0$$

Като умножим първото уравнение на системата с α, разделим второто уравнение на α и използваме, че $\alpha^n = 1$, $\alpha^{n-1} = \alpha^{-1}$, получаваме

$$c_0\alpha + c_1\alpha^2 + \cdots + c_{n-2}\alpha^{n-1} + c_{n-1} = 0$$
$$c_0\alpha^{n-1} + c_1\alpha^{n-2} + \cdots + c_{n-2}\alpha + c_{n-1} = 0$$

Тъй като $\alpha^{n-s} = (\alpha^{-1})^s$, първото уравнение е еквивалентно на това $\mathbf{c}'(\alpha^{-1}) = 0$. Второто уравнение е еквивалентно на това $\mathbf{c}'(\alpha) = 0$. От последните две равенства заключваме, че $\mathbf{c}' \in \mathcal{M}$. $\square$

2. Думи с малки тегла в двоичен код на Мелас.

Твърдение 2.1. *Минималното кодово разстояние* $d(\mathcal{M}) \geq 3$.

Доказателство: От вида на първия ред на проверочната матрица следва, че $\mathcal{M}$ е подкод на кода на Хеминг с минимално кодово разстояние 3. □

Твърдение 2.2. *Ако* $m = 3$, *то* $d(\mathcal{M}) = 7$.

Доказателство: В този случай пораждащият полином за $\mathcal{M}$ е $g(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + \cdots + x + 1$, от степен 6, откъдето за размерността на кода k получаваме $k = 7 - 6 = 1$. Следователно този реверсивен код освен нулевата дума с дължина 7 съдържа още една дума, (която е $(1, \ldots, 1)$), и съвпада с кода с повторение. Така, че $d(\mathcal{M}) = 7$, с което твърдението е доказано. □

Теорема 2.3. *В кода* $\mathcal{M}$ *има думи с тегло* 3 *само при четно* m *и техният брой е* $\dfrac{2^m - 1}{3}$.

Доказателство: Съществуването на дума с тегло 3 в $\mathcal{M}$, съгласно неговото определение (и съответните му проверочни равенства), е еквивалентно на решение на системата:

$$X_1 + X_2 + X_3 = 0$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = 0,$$

за две по две различни $X_j \in \mathbb{F}_{2^m}^*$, $j = 1, 2, 3$.

Ще докажем, че такова решение съществува. За целта от първото уравнение изразяваме $X_3 = X_1 + X_2$ и след заместване във второто получаваме, че системата има решение точно когато уравнението

$$X_1^2 + X_1 X_2 + X_2^2 = 0$$

има такова. За произволно $X_1 \in \mathbb{F}_{2^m}^*$, умножавайки последното уравнение с X_1^{-2} и полагайки $x := \dfrac{X_2}{X_1}$, получаваме следното уравнение с едно неизвестно: $x^2 + x + 1 = 0$. Съгласно Теорема 3.2, Глава I, това уравнение има решение в полето $\mathbb{F}_{2^m}$, което очевидно е $\neq 0$, 1, тогава и само тогава, когато $\mathrm{tr}(1) = 0$, тоест точно при m четно (поради Твърдение 3.1, Глава I). С това заключаваме, че разглежданата система има решение от търсения вид тогава и само тогава, когато m е четно.

Нека β е корен на $x^2 + x + 1 = 0$. Другият корен е $\beta^2 = \beta + 1$. Освен това $\beta^3 = \beta^2 + \beta = 1$ и $\beta^4 = \beta$. За дадено $a := X_1 \neq 0$ решения на системата са

$$X_1 = a, \quad X_2 = a\beta, \quad X_3 = a + a\beta = a(\beta + 1) = a\beta^2$$

и

$$X_1 = a, \quad X_2 = a\beta^2, \quad X_3 = a(1 + \beta^2) = a\beta,$$

като очевидно X_2 и X_3 също са ненулеви. Тъй като наредбата на X_1, X_2 и X_3 е без значение, то за $X_1 = a$ всъщност получаваме единствена кодова дума. Лесно се проверява също, че тази кодова дума се получава и когато $X_1 := a\beta$ и $X_1 := a\beta^2$, т.е. на всеки три стойности на X_1 от този вид съответствува една и съща кодова дума.

Така, когато X_1 пробяга всички $2^m - 1$ ненулеви елементи на $\mathbb{F}_{2^m}$, получаваме всичките $\dfrac{2^m-1}{3}$ кодови думи с тегло 3. □

От Твърдение 2.1 и последната теорема получаваме следното:

Следствие 2.4. *Ако m е четно, то $d(\mathcal{M}) = 3$.*

Теорема 2.5. *В $\mathcal{M}$ няма дума с тегло 4.*

Доказателство: Допускането, че съществува кодова дума с тегло 4, съгласно определението на код на Мелас (и съответните му проверочни равенства), е еквивалентно на съществуването на решение на системата

$$X_1 + X_2 + X_3 + X_4 = 0$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} + X_4^{-1} = 0,$$

за две по две различни $X_j \in \mathbb{F}^*_{2^m}$, $j = 1, 2, 3, 4$.

Да предположим, че такова решение наистина съществува. Тъй като $X_4 \neq 0$, можем да разгледаме елементите от полето $\mathbb{F}_{2^m}$, дефинирани като $Y_j := \dfrac{X_j}{X_4}$, за $j = 1, 2, 3$. След това лесно съобразяваме, че са удовлетворени следните равенства:

$$Y_1 + Y_2 + Y_3 = 1$$
$$Y_1^{-1} + Y_2^{-1} + Y_3^{-1} = 1,$$

с $Y_j \in \mathbb{F}_{2^m} \backslash \{0, 1\}$ и две по две различни помежду си. По-нататък можем да довършим доказателството по 2 начина:

1-ви начин: Нека $Y_3 = a \in \mathbb{F}_{2^m} \backslash \{0, 1\}$. От първото уравнение изразяваме $Y_2 = 1 + a + Y_1$, заместваме във второто уравнение и получаваме

$$\frac{1}{Y_1} + \frac{1}{1 + a + Y_1} = 1 + \frac{1}{a}$$

След привеждане под общ знаменател, виждаме, че последното уравнение е еквивалентно на

$$\frac{Y_1 + Y_2}{Y_1 Y_2} = \frac{1 + a}{a}$$

и вземайки предвид първото равенство на системата получаваме, че тя е еквивалентна на:

$$Y_1 + Y_2 = 1 + a$$
$$Y_1 Y_2 = a$$

за $a \in \mathbb{F}_{2^m} \backslash \{0, 1\}$, $Y_1 \neq Y_2$, $Y_j \in \mathbb{F}_{2^m} \backslash \{0, 1, a\}$. Последната система е удовлетворена точно когато Y_1 и Y_2 са корени на уравнението

$$Y^2 + (1 + a)Y + a = 0$$

Но негови корени са $Y_1 = 1$ и $Y_2 = a$ и получаваме противоречие.

2-ри начин: Като положим: $Z_j := Y_j + 1$, за $j = 1, 2, 3$, заместим последните величини в горните равенства, приведем лявата страна на второто от тях под общ знаменател и се освободим от него, получаваме:

$$Z_1 + Z_2 + Z_3 = 0$$
$$Z_1 + Z_2 + Z_3 = Z_1 Z_2 Z_3$$

След изразяване на $Z_3 = Z_1 + Z_2$ от първото и заместването му във второто равенство получаваме:

$$Z_1 Z_2 (Z_1 + Z_2) = 0$$

Накрая, от това последно равенство следва, че $Z_1 = 0$ (тоест $Y_1 = 1$) или $Z_2 = 0$ (тоест $Y_2 = 1$), или $Z_1 = Z_2$ (тоест $Y_1 = Y_2$), като във всички случаи получаваме необходимото противоречие. С това доказателството е завършено. $\square$

Теорема 2.6. *При $m \geq 5$ нечетно в $\mathcal{M}$ има дума с тегло 5.*

Доказателство: Както и в предишните доказателства, съществуването на дума с тегло 5 в $\mathcal{M}$ е еквивалентно на това системата

$$X_1 + X_2 + X_3 + X_4 + X_5 = 0$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} + X_4^{-1} + X_5^{-1} = 0$$

да има решение за две по две различни $X_j \in \mathbb{F}_{2^m}^*$, $j = 1, 2, 3, 4, 5$. Проверките за различие от 0 на X_j, $j = 1, 2, 3, 4, 5$ и различие на X_k от X_l при $k \neq l$ са излишни, тъй като в противен случай бихме получили, че в C има вектор с тегло < 5, което е противоречие с предишните твърдения.

Ще докажем, че съществува решение с $X_3 := a^2$, $X_4 := a$, $X_5 := 1$ за някое $a \in \mathbb{F}_{2^m}^*$. Търсим X_1 и X_2, удовлетворяващи системата:

$$X_1 + X_2 = a^2 + a + 1$$

$$\frac{X_1 + X_2}{X_1 X_2} = X_1^{-1} + X_2^{-1} = 1 + a^{-1} + a^{-2} = \frac{a^2 + a + 1}{a}^2,$$

която е еквивалентна на

$$X_1 + X_2 = a^2 + a + 1$$
$$X_1 X_2 = a^2$$

Нека $c := a^2 + a + 1$. Понеже m нечетно, ако намерим a, удовлетворяващо горните условия, то $c \neq 0$. (В противен случай a ще бъде пораждащ за $\mathbb{F}_{2^2}$, откъдето ще следва, че $\mathbb{F}_{2^2}$ е подполе на $\mathbb{F}_{2^m}$, а последното е изпълнено точно когато m четно).

От формулите на Виет следва, че X_1 и X_2 са корени на уравнението:

$$X^2 + cX + a^2 = 0,$$

което след полагането $u := \dfrac{x}{c}$ се редуцира до

$$u^2 + u + \left(\frac{a}{c}\right)^2 = 0,$$

имащо корени в $\mathbb{F}_{2^m}$ точно когато $\operatorname{tr}\left(\dfrac{a}{c}\right) = 0$.

Разглеждаме функцията $f(z) := \dfrac{z}{z^2 + z + 1}$. Ще докажем, че съществува $z_0 \in \mathbb{F}_2^m \backslash \{0\}$, за което $\operatorname{tr}(f(z_0)) = 0$. Понеже

$$f(z+1) = f(z) + \frac{1}{z^2 + z + 1},$$

то

$$\operatorname{tr}(f(z+1)) = \operatorname{tr}(f(z)) + \operatorname{tr}\left(\frac{1}{z^2 + z + 1}\right).$$

Сега ще използваме факта, че съществува елемент

$$w \in \mathbb{F}_{2^m} \backslash \{0, 1\} \text{ с } \operatorname{tr}(w) = \operatorname{tr}(w^{-1}) = 1,$$

изложен в [8]. За това w разглеждаме квадратното уравнение

$$z^2 + z + 1 = w \text{ или } z^2 + z + 1 + w = 0,$$

което има решение в $\mathbb{F}_{2^m}$ точно когато $\operatorname{tr}(1 + w) = 1 + \operatorname{tr}(w) = 0$ (последното равенство следва от това, че $\operatorname{tr}(1) = 1$ понеже m е нечетно), изпълнено, понеже $\operatorname{tr}(w) = 1$. Понеже $\operatorname{tr}(w^{-1}) = 1$ при z_0 решение на горното уравнение, едното от двете $\operatorname{tr}(f(z_0))$ или $\operatorname{tr}(f(z_0) + 1)$ е равно на 0. □

3. Радиус на покритие на двоичен код на Мелас

Лема 3.1. *Нека a, b са два елемента на полето $\mathbb{F}_{2^m}$ такива, че $\operatorname{tr}(a) = \operatorname{tr}(b) = 0$. Ако за всяко $\alpha \in \mathbb{F}_{2^m}$, за което $\operatorname{tr}(\alpha) = 0$, е изпълнено $\operatorname{tr}(\alpha^{-1}) = 0$, то $\operatorname{tr}(ab) = 0$.*

Доказателство: Нека $A = \sqrt{a} = a^{2^{m-1}}$, следователно $ab = A^2 b$. Имаме $a^{2^{m+k}} = a^{2^k}$, откъдето

$$\operatorname{tr}(A) = a^{2^{m-1}} + a + \cdots + a^{2^{m-2}} = a + \cdots + a^{2^{m-2}} + a^{2^{m-1}} = \operatorname{tr}(a) = 0.$$

Проверява се, че когато $A \neq 0$, $b \neq 0$ и $Ab \neq 1$, е в сила

$$\frac{1}{\frac{1}{A} + \frac{1}{\frac{1}{b} - A}} = A - A^2 b.$$

От допускането, че за всяко $\alpha \in \mathbb{F}_{2^m}$, за което $\mathrm{tr}(\alpha) = 0$, $\mathrm{tr}(\alpha^{-1}) = 0$, $\mathrm{tr}(a) = \mathrm{tr}(b) = 0$ и от адитивността на следата следва, че:

$$\mathrm{tr}\left(\frac{1}{\frac{1}{A} + \frac{1}{\frac{1}{b} - A}}\right) = 0,$$

тоест $\mathrm{tr}(A) = \mathrm{tr}(A^2 b) = \mathrm{tr}(ab)$. Ако $A = 0$, $a = 0$. Ако $a = 0$ или $b = 0$, $ab = 0$ и $\mathrm{tr}(ab) = 0$. Ако $Ab = 1$, $A = b^{-1}$ и $a = b^{-2}$, откъдето $ab = b^{-1}$ и от $\mathrm{tr}(b) = 0$ имаме $\mathrm{tr}(b^{-1}) = 0$. □

Твърдение 3.2. *За двоичния код на Мелас има вектор с тегло 2, имащ синдрома (a, b), точно когато* $\mathrm{tr}\left(\frac{1}{ab}\right) = 0$.

Доказателство: Наличието на такъв вектор е еквивалентно на решение на системата:

$$X_1 + X_2 = a$$
$$X_1^{-1} + X_2^{-1} = b$$

с две по две различни $X_j \in \mathbb{F}_{2^m}^*$, $j = 1, 2$.

Замествайки $X_2 = a - X_1$ във второто уравнение, получаваме $X_1^{-1} + (a - X_1)^{-1} = b$, което след освобождаване от знаменател придобива вида

$$-bX_1^2 + baX_1 - a = 0.$$

Разделяйки последното на ba^2, получаваме $\left(\frac{X_1}{a}\right)^2 - \frac{X_1}{a} - \frac{1}{ba} = 0$, което има решение точно когато $\mathrm{tr}\left(\frac{1}{ab}\right) = 0$. □

Следствие 3.3. *При m четно кодът не е квазиперфектен.*

Доказателство: Тъй като в този случай кодът поправя 1 грешка, достатъчно е да намерим синдром (a, b), така че да няма вектор, имащ този синдром. Избираме $a = 1$, а b измежду елементите от $\mathbb{F}_{2^m}$ със следа 1, които са 2^{m-1} на брой. □

Лема 3.4. *Нека $b \in \mathbb{F}_{2^m}^*$. Тогава системата:*

$$X_1 + X_2 + X_3 = 0$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = b$$

има решение в $\mathbb{F}_{2^m}^*$.

Доказателство: (виж, [2]). □

Лема 3.5. *Нека* $b \in \mathbb{F}_{2^m}$, $\mathrm{tr}(b^{-1}) = 0$. *Тогава системата:*

$$X_1 + X_2 = 1$$
$$X_1^{-1} + X_2^{-1} = b$$

има решение в $\mathbb{F}_{2^m}^*$.

Доказателство: Лемата е частен случай на Твърдение 3.2. $\square$

Лема 3.6. *Нека* $b \in \mathbb{F}_{2^m}^*$, $\mathrm{tr}(b) = 0$. *Тогава системата:*

$$X_1 + X_2 + X_3 = 1$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = b$$

има решение в $\mathbb{F}_{2^m}^*$.

Доказателство: (виж, [2]). $\square$

Лема 3.7. *Нека* $b \in \mathbb{F}_{2^m}^*$, $\mathrm{tr}(b) = \mathrm{tr}(b^{-1}) = 1$, $b^2 + b + 1 \neq 0$. *Тогава системата:*

$$X_1 + X_2 + X_3 = 1$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = b$$

има решение в $\mathbb{F}_{2^m}^*$.

Доказателство: (виж, [2]). $\square$

Лема 3.8. *Нека* $b \in \mathbb{F}_{2^m}^*$, $\mathrm{tr}(b) = \mathrm{tr}(b^{-1}) = 1$, $b^2 + b + 1 = 0$, $m > 2$. *Тогава системата:*

$$X_1 + X_2 + X_3 = 1$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = b$$

има решение в $\mathbb{F}_{2^m}^*$.

Доказателство: (виж, [2]). $\square$

Забележка: В доказателството се използва Лема 3.1.

Теорема 3.9. *Радиусът на покритие на* $\mathcal{M}$ *е* 3.

Доказателство: При $b \neq a^{-1}$ и $\mathrm{tr}\left(\frac{1}{ab}\right) = 0$ няма вектор от кода с тегло ≤ 2, имащ синдрома (a, b). Трябва да докажем, че тогава има вектор с тегло 3 със синдрома (a, b), тоест

$$X_1 + X_2 + X_3 = a$$
$$X_1^{-1} + X_2^{-1} + X_3^{-1} = b$$

има решение в $\mathbb{F}_{2^m}^*$. Можем да считаме, че $b \neq 0$. Случаят $a = 0$ е покрит от Лема 3.4. От лемите с номера 3.5, 3.6 и 3.7 следва, че системата:

$$Y_1 + Y_2 + Y_3 = 1$$
$$Y_1^{-1} + Y_2^{-1} + Y_3^{-1} = ba,$$

която е еквивалентна на първоначалната след полагането $Y_i := X_i a^{-1}$, има решение. $\square$

Нека сега разгледаме кода на Мелас $\mathcal{N}$ при $p = 2^k$, $k \geq 2$, $q = p^m$.

Теорема 3.10. *Минималното кодово разстояние на кода $\mathcal{N}$ е $d = 3$.*

Доказателство: Наличието на вектор с тегло ≤ 2 в него е еквиваленто на решение на системата:

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_1^{-1} + a_2X_2^{-1} = 0$$

с $a_i \in \mathbb{F}_p$, $a_i \neq (0,0)$, $X_1 \neq X_2$, $X_i \in \mathbb{F}_q^*$. Умножаваме второто уравнение с X_1X_2 и разглеждаме системата

$$a_1X_1 + a_2X_2 = 0$$
$$a_1X_2 + a_2X_1 = 0$$

като линейна относно a_i. Тя е с детерминанта $X_1^2 - X_2^2 \neq 0$ при $X_1 \neq X_2$ и няма ненулево решение. Заключваме, че $d \geq 3$.

Наличието на вектор с тегло 3 в $\mathcal{N}$ е еквиваленто на решение на системата:

$$a_1X_1 + a_2X_2 + a_3X_3 = 0$$
$$a_1X_1^{-1} + a_2X_2^{-1} + a_3X_3^{-1} = 0$$

с $a_i \in \mathbb{F}_p^*$, различни $X_i \in \mathbb{F}_q^*$. Изразяваме $X_3 = \dfrac{a_1X_1 + a_2X_2}{a_3}$ от първото уравнение, заместваме във второто, привеждаме под общ знаменател и получаваме:

$$a_1a_2X_1^2 + (a_1^2 + a_2^2 + a_3)X_1X_2 + a_1a_2X_2^2 = 0.$$

Разделяме последното уравнение на X_2^2, полагаме $x := \dfrac{X_1}{X_2}$, делим на a_1a_2 и получаваме уравнението:

$$X^2 + \left(\frac{a_1^2 + a_2^2 + a_3}{a_1a_2}\right)X + 1 = 0.$$

Фиксираме a_1 и a_2, избираме $a_3 \neq a_1^2 + a_2^2$, делим последното на $\left(\dfrac{a_1^2 + a_2^2 + a_3}{a_1a_2}\right)^2$ и полагайки $y := \dfrac{X}{a_1^2 + a_2^2 + a_3a_1a_2}$, получаваме уравнението

$$y^2 + y + \frac{a_1^2a_2^2}{a_1^4 + a_2^4 + a_3^2} = 0.$$

Последното има решение в $\mathbb{F}_p$ точно когато $\operatorname{tr}\left(\dfrac{a_1^2a_2^2}{a_1^4+a_2^4+a_3^2}\right)=0$.
Нека
$$\alpha := a_1^2a_2^2, \quad \beta := a_1^4+a_2^4 \quad \text{и} \quad f(t) := \frac{\alpha}{\beta+t^2}.$$
Допускането, че $f(t_1)=f(t_2)$ е еквивалентно на $\alpha(t_1^2-t_2^2)=0$ и понеже $\alpha\neq 0$ последното е изпълнено единствено при $t_1=t_2$. Следователно функцията $f(t)$ приема $p-2$ стойности, когато $t\neq 0$ и $t\neq a_1^2+a_2^2$ при $a_1^2+a_2^2\neq 0$, тоест $a_1\neq a_2$ и $p-1$ стойности при $a_1^2+a_2^2=0$, тоест $a_1=a_2$. Нека $k\geq 3$. Понеже елементите със следа, равна на 0 в $\mathbb{F}_p$ са $\dfrac{p}{2}$ и $p-2>\dfrac{p}{2}$, можем да изберем $a_3\neq 0, a_1^2+a_2^2$ такова, че
$$\operatorname{tr}\left(\frac{a_1^2a_2^2}{a_1^4+a_2^4+a_3^2}\right)=\operatorname{tr}(f(a_3))=0.$$
При $k=2$ изборът $a_1=a_2=a_3=1$ води до $f(a_3)=1$ и $\operatorname{tr}(1)=0$. Намерихме решение за y дори в $\mathbb{F}_p\subset\mathbb{F}_q$, а оттам намераме и кодов вектор с тегло 3. $\square$

Библиография

[1] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes,a North-Holland Publishing Company, 1977.

[2] S.M. Dodunekov, Some Quasiperfect Double Error-Correcting Codes, Problems of Control and Information Theory, vol. 15 (5), pp. 367–375, 1986.

[3] Stefan Dodunekov,Danyo Danev A family of ternary quasi-perfect codes, Des.Codes Cryptogr. (2008) 49:265-271 DOI 10.1007/s10623-008-9193-7

[4] Е. Д. Великова-Бандова, Записки по кодиране: Двоични шумозащитни кодове, ФОИ-КОМЕРС, София, 2004.

[5] Е. Д. Великова-Бандова, Записки по кодиране: Циклични кодове, ФОИ-КОМЕРС, София, 2001.

[6] E.D. Velikova, A.I. Bojilov, An upper bound on the covering radius of a class of cyclic codes Eleventh International Workshop on Algebraic and Combinatorial Theory June 16-22 2008 Pamporovo Bulgaria pp.300-304

[7] R.E. Blahut, Theory and Practice of Error-Control Codes, Addison-Wesley Publishing Company, 1984.

[8] H.Niederreiter, An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field, AAECC 1,119-124 (1990).

[9] C.M. Melas, A cyclic code for double error correction, IBM J. Res. Deuel., 4 (1960), 364-366. 10, 12