

Теорема на Bezout. Полиномиални кодове върху равнинни криви.

ОПРЕДЕЛЕНИЕ 9.1. Множеството

$$Z(f) = \{[x : y : z] \in \mathbb{P}^2(\bar{k}) \mid f(x, y, z) = 0\}$$

на нулите на (евентуално разложим) хомогенен полином $f(x, y, z) \in \bar{k}[x, y, z]$ в двумерното проективно пространство $\mathbb{P}^2(\bar{k})$ се нарича проективна равнинна крива.

Степента на проективна равнинна крива $Z(f) \subset \mathbb{P}^2(\bar{k})$ се определя като общата степен на хомогенния полином $f(x, y, z)$, $\deg Z(f) = \deg(f)$.

Ще докажем Слаба форма на Теоремата на Bezout с помощта на резултанта на два полинома на една променлива. Да напомним, че за полиноми

$$f(t) = a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n = a_0 \prod_{i=1}^n (t - \alpha_i),$$

$$g(t) = b_0 t^m + b_1 t^{m-1} + \dots + b_{m-1} t + b_m = b_0 \prod_{j=1}^m (t - \beta_j)$$

с коефициенти от поле K , резултантата се определя като

$$R(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

ЛЕМА 9.2. Нека

$$f(t) = a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n \quad \text{и}$$

$$g(t) = b_0 t^m + b_1 t^{m-1} + \dots + b_{m-1} t + b_m$$

са полиноми с коефициенти от поле K , а редовете на $(m+n) \times (m+n)$ -матрицата

$$\begin{pmatrix} a_0 & a_1 & \dots & a_n & & & \\ & a_0 & a_1 & \dots & & & \\ & & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & & b_m & & & \\ & b_0 & b_1 & \dots & & b_m & & \\ & & & & b_0 & b_1 & \dots & b_m \end{pmatrix}$$

са запълнени последователно от m екземпляра на коефициентите на $f(t)$, записани от диагоналните позиции надясно и n екземпляра на коефициентите на $g(t)$, записани от диагоналните позиции надясно. Тогава резултантата $R(f, g)$ на $f(t)$ и $g(t)$ е равна на детерминантата на M ,

$$R(f, g) = \det(M).$$

Доказателство: Разглеждаме матрицата

$$L = \begin{pmatrix} W^{(m)}(\alpha_1, \dots, \alpha_n) & E_m \\ W(\alpha_1, \dots, \alpha_n) & 0_{n \times m} \end{pmatrix},$$

където

$$W(\alpha_1, \dots, \alpha_n) = \begin{pmatrix} \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \dots & \alpha_n^{n-2} \\ \dots & \dots & \dots & \dots \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 1 & \dots & 1 \end{pmatrix} \in M_{n,n}(K),$$

$$W^{(m)}(\alpha_1, \dots, \alpha_n) = \begin{pmatrix} \alpha_1^{n+m-1} & \alpha_2^{n+m-1} & \dots & \alpha_n^{n+m-1} \\ \alpha_1^{n+m-2} & \alpha_2^{n+m-2} & \dots & \alpha_n^{n+m-2} \\ \dots & \dots & \dots & \dots \\ \alpha_1^{n+1} & \alpha_2^{n+1} & \dots & \alpha_n^{n+1} \\ \alpha_1^n & \alpha_2^n & \dots & \alpha_n^n \end{pmatrix} \in M_{m,n}(K),$$

E_m е единичната $m \times m$ -матрица, а $0_{n \times m}$ е нулевата матрица с n реда и m стълба. Произведението

$$ML = \begin{pmatrix} 0_{m \times n} & T_m \\ r(\alpha_1, \dots, \alpha_n; g) & N_{n \times m} \end{pmatrix}$$

с триъгълна матрица

$$T_m = \begin{pmatrix} a_0 & * & * & \dots & * & * \\ 0 & a_0 & * & \dots & * & * \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_0 & * \\ 0 & 0 & 0 & \dots & 0 & a_0 \end{pmatrix} \in M_{m,m}(K),$$

$$r(\alpha_1, \dots, \alpha_n; g) = \begin{pmatrix} \alpha_1^{n-1}g(\alpha_1) & \alpha_2^{n-1}g(\alpha_2) & \dots & \alpha_n^{n-1}g(\alpha_n) \\ \alpha_1^{n-2}g(\alpha_1) & \alpha_2^{n-2}g(\alpha_2) & \dots & \alpha_n^{n-2}g(\alpha_n) \\ \dots & \dots & \dots & \dots \\ \alpha_1g(\alpha_1) & \alpha_2g(\alpha_2) & \dots & \alpha_ng(\alpha_n) \\ g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \end{pmatrix} \in M_{n,n}(K)$$

и някаква матрица $N_{n \times m} \in M_{n,m}(K)$.

По Теоремата за умножение на детерминанти, $\det(ML) = \det(M)\det(L)$. Развиваме $\det(ML)$ по адюнгираните количества относно n -ти ред, $(n-1)$ -ви ред, $\dots$, 1 -ви ред в първоначалната номерация на ердовете на ML и т.н. Развиваме $\det(L)$ по адюнгираните количества относно $(m+n)$ -ти стълб, $(m+n-1)$ -ви стълб, $\dots$, $(m+1)$ -ви стълб в първоначалната номерация на стълбовете и т.н. Получаваме

$$\begin{aligned} & (-1)^{mn} a_0^m \left[\prod_{i=1}^n g(\alpha_i) \right] (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j) = \\ & = \det(M) (-1)^{mn} (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j). \end{aligned}$$

Резултантата $R(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i)$, защото $g(\alpha_i) = b_0 \prod_{j=1}^m (\alpha_i - \beta_j)$. След почленно умножение с $(-1)^{mn} (-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)$ имаме

$$R(f, g)D(f) = \det(M)D(f) \quad (9.1)$$

за дискриминантата

$$D(f) = a_0^{2n-2} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)^2$$

на $f(t)$.

Достатъчно е да докажем, че $D(f) \in P[a_0, \dots, a_n]$ не се анулира тъждествено като полином на $a_0, \dots, a_n$ с коефициенти от простото подполе P на K , за да получим $R(f, g) = \det(M)$. Да допуснем, че $D(f) \equiv 0$ се анулира тъждествено като полином на $a_0, \dots, a_n$. Тогава всеки полином $f(t) \in K[t]$ има кратен корен или $\forall f(t) \in K[t]$ има общ корен с формалната си производна $f'(t) \in K[t]$. Ако характеристиката $\text{char}(K) = 0$ или $\text{char}(K) = p$ не дели степента $\deg(f) = n$, то $f(t) = t^n + 1$ и $f'(t) = nt^{n-1}$ нямат общ корен. В случая на степен $\deg(f) = n$, кратна на характеристиката $\text{char}(K) = p$ полиномът $f(t) = t^n + t + 1 \in K[t]$ и формалната му производна $f'(t) = 1$ нямат общи корени. Полученото противоречие доказва, че $D(f) \not\equiv 0 \in P[a_0, \dots, a_n]$ и $R(f, g) = \det(M)$, Q.E.D. Теоремата на Bezout за проективни равнинни криви $Z(f) \subset \mathbb{P}^2(\bar{k})$ и $Z(g) \subset \mathbb{P}^2(\bar{k})$ гласи, че ако сечението $Z(f) \cap Z(g)$ е крайно, то броят на точките в него е равен на произведението на степените на $Z(f)$ и $Z(g)$, т.е.

$$|Z(f) \cap Z(g)| = \deg Z(f) \deg Z(g).$$

Ние ще докажем и използваме

ТВЪРДЕНИЕ 9.3. (Слаб вариант на Теоремата на Bezout) Ако $Z(f) \subset \mathbb{P}^2(\bar{k})$ и $Z(g) \subset \mathbb{P}^2(\bar{k})$ са проективни равнинни криви с крайно сечение, то

$$|Z(f) \cap Z(g)| \leq \deg Z(f) \deg Z(g).$$

Доказателство: Разглеждаме проекцията

$$\Pi : \mathbb{P}^2(\bar{k}) \dashrightarrow \mathbb{P}^1(\bar{k}),$$

$$\Pi([x : y : z]) = [x : y],$$

която е определена върху $\mathbb{P}^2 \setminus \{[0 : 0 : 1]\}$. За всяка фиксирана точка $[x_o : y_o] \in \mathbb{P}^1(\bar{k})$ слоят

$$\Pi^{-1}[x_o : y_o] = \{[x : y : z] \in \mathbb{P}^2(\bar{k}) \mid x_o y - x y_o = 0\}$$

е проективизацията на равнината

$$\{(x, y, z) \in \bar{k}^3 \mid x_o y - x y_o = 0\} \simeq \bar{k}^2$$

през началото в $\bar{k}^3$, така че $\Pi^{-1}[x_o : y_o] \simeq \mathbb{P}^1(\bar{k})$ е проективна права.

Искаме да изберем такива хомогенни координати x, y, z върху $\mathbb{P}^2(\bar{k})$, че Π да е определено във всички точки на $Z(f) \cap Z(g)$ и $\Pi : Z(f) \cap Z(g) \rightarrow \Pi(Z(f) \cap Z(g))$ да е взаимно еднозначно. За регулярността на Π върху $Z(f) \cap Z(g)$ е достатъчно $[0 : 0 : 1] \notin Z(f) \cap Z(g)$. Изображението $\Pi : Z(f) \cap Z(g) \rightarrow \Pi(Z(f) \cap Z(g))$ е взаимно еднозначно, ако за $\forall p = [p_0 : p_1 : p_2] \in Z(f) \cap Z(g)$ слоят на Π над $\Pi(p) = [p_0 : p_1]$ не съдържа друга точка на $Z(f) \cap Z(g)$ освен p . По-точно,

$$\Pi^{-1}(\Pi(p)) = \Pi^{-1}([p_0 : p_1]) = \{[x : y : z] \in \mathbb{P}^2(\bar{k}) \mid p_0 y - p_1 x = 0\} \simeq \mathbb{P}^1(\bar{k}),$$

така че е нужно $p_0 q_1 - p_1 q_0 \neq 0$ за $\forall q = [q_0 : q_1 : q_2] \in (Z(f) \cap Z(g)) \setminus \{p\}$. Да означим с x', y', z' поризволни хомогенни координати върху $\mathbb{P}^2(\bar{k})$. Търсим хомогенни координати x, y, z с

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = T \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} x \\ y \\ z \end{pmatrix} = T^{-1} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

за подходяща $T \in GL(3, \bar{k})$. Ако p_i, q_j са старите хомогенни координати на $p = [p_0 : p_1 : p_2], q = [q_0 : q_1 : q_2] \in Z(f) \cap Z(g)$, избираме матрицата $T^{-1} \in GL(3, \bar{k})$ така, че

$$T^{-1} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} x(p) \\ y(p) \\ z(p) \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} \quad \text{за } \forall p \in Z(f) \cap Z(g), \quad \forall \lambda \in \bar{k}^* \quad \text{и}$$

$$x(p)y(q) - y(p)x(q) \neq 0 \quad \text{за всички различни } p, q \in Z(f) \cap Z(g).$$

Представяме хомогенния полином

$$f(x, y, z) = a_{n-k}z^k + a_{n-k+1}z^{k-1} + \dots + a_{n-1}z + a_n$$

като полином на z , чиито коефициенти са хомогенни полиноми a_i на x, y от степен i . Аналогично,

$$g(x, y, z) = b_{m-l}z^l + b_{m-l+1}z^{l-1} + \dots + b_{m-1}z + b_m$$

за хомогенни полиноми $b_j(x, y) \in \bar{k}[x, y]$ от степен j . Точката $[x_o : y_o : z_o]$ е общ корен на $f(x, y, z) = 0$ и $g(x, y, z) = 0$ тогава и само тогава, когато $[x_o : y_o]$ е корен на резултантата $R_z(f, g)(x, y) \in \bar{k}[x, y]$ на f и g като полиноми на z . Достатъчно е да докажем, че $R_z(f, g)(x, y)$ е хомогенен полином от степен $d \leq mn$ за $\deg(f) = n, \deg(g) = m$, за да получим, че $|Z(f) \cap Z(g)| \leq mn$. По-точно, $R_z(f, g)(x, y)$ от степен d има най-много d корена, които отговарят на различни точки от $Z(f) \cap Z(g)$ съгласно взаимната еднозначност на проекцията $\Pi : Z(f) \cap Z(g) \rightarrow \Pi(Z(f) \cap Z(g))$.

За произволен параметър t резултантата

$$R_z(f, g)(tx, ty) = \det \begin{pmatrix} t^{n-k}a_{n-k} & t^{n-k+1}a_{n-k+1} & \dots & t^n a_n & & \\ & t^{n-k}a_{n-k} & t^{n-k+1}a_{n-k+1} & \dots & t^n a_n & \\ & & & t^{n-k}a_{n-k} & t^{n-k+1}a_{n-k+1} & \dots & t^n a_n \\ t^{m-l}b_{m-l} & t^{m-l+1}b_{m-l+1} & \dots & & t^m b_m & \\ & t^{m-l}b_{m-l} & t^{m-l+1}b_{m-l+1} & \dots & & t^m b_m \\ & & & t^{m-l}b_{m-l} & t^{m-l+1}b_{m-l+1} & \dots & t^m b_m \end{pmatrix}$$

Умножаваме по редове с $t^{m-l}, t^{m-l+1}, \dots, t^{m-1}, t^{n-k}, t^{n-k+1}, \dots, t^{n-1}$, така че стълбовете да са хомогенни от степен $d = (n-k) + (m-l), d+1, \dots, d+k+l-1$,

$$\begin{pmatrix} t^d a_{n-k} & t^{d+1} a_{n-k+1} & \dots & t^{d+k} a_n & & \\ & t^{d+1} a_{n-k} & t^{d+2} a_{n-k+1} & t^{d+k+1} a_n & \dots & \\ & & & & t^{d+l-1} a_{n-k} & t^{d+l} a_{n-k+1} & t^{d+l-1+k} \\ t^d b_{m-l} & t^{d+1} b_{m-l+1} & \dots & & & t^{d+l} b_m & \\ & t^{d+1} b_{m-l} & t^{d+2} b_{m-l+1} & t^{d+l+1} b_m & \dots & & \\ & & & & & t^{d+k-1} b_{m-l} & t^{d+k} b_{m-l} & t^{d+k-1+l} \end{pmatrix}.$$

Изчисляването на степените на t от стълбовете на получената детерминанта дава

$$t^{(m-l)l + \frac{(l-1)l}{2} + (n-k)k + \frac{(k-1)k}{2}} R_z(f, g)(tx, ty) = t^{d(k+l) + \frac{(k+l-1)(k+l)}{2}} R_z(f, g)(x, y).$$

Следователно $R_z(f, g)(x, y) \in \bar{k}[x, y]$ е хомогенен полином от степен

$$\Delta = d(k+l) + \frac{(k+l-1)(k+l)}{2} - (m-l)l - \frac{(l-1)l}{2} - (n-k)k - \frac{(k-1)k}{2} = mk + nl - kl \leq mn,$$

защото $(m-l)(n-k) \geq 0$, Q.E.D.

Сега ще построим полиномиални кодове върху афинни равнинни криви над крайни полета. Ще пресметнем размерностите на тези кодове и ще оценим отдолу минималните им разстояния.

Нека $Z(h) = \{(x, y) \in \overline{\mathbb{F}_q}^2 \mid h(x, y) = 0\}$ е неприводима афинна равнинна крива, зададена от (необезателно хомогенен) полином $h(x, y) \in \mathbb{F}_q[x, y]$ от обща степен m . Да означим с U_l множеството на полиномите от $\mathbb{F}_q[x, y]$ с обща степен $\leq l$. Тогава U_l е $\frac{(l+1)(l+2)}{2}$ -мерно линейно пространство над $\mathbb{F}_q$, защото мономите $x^s y^{i-s}$ с $0 \leq s \leq i$, $0 \leq i \leq l$ образуват $\mathbb{F}_q$ -базис на U_l и техният брой е $\sum_{i=0}^l (i+1) = \frac{(l+1)(l+2)}{2}$. Избираме n различни $\mathbb{F}_q$ -рационални точки $P_1, \dots, P_n \in Z(h)(\mathbb{F}_q)$ за някое естествено $n > ml$ и разглеждаме остойносттаващото изображение

$$\mathcal{E} : U_l \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}(f) = (f(P_1), \dots, f(P_n)).$$

Образът $C = \mathcal{E}(U_l)$ на U_l е линеен код с дължина n и размерност

$$\dim C = \begin{cases} \frac{(l+1)(l+2)}{2} - \frac{(l-m+1)(l-m+2)}{2} & \text{за } l \geq m; \\ \frac{(l+1)(l+2)}{2} & \text{за } l < m. \end{cases}$$

За $l < m$ минималното разстояние $d \geq n - ml$. По-точно, ядрото $\ker(\mathcal{E}) = \{f \in U_l \mid f(P_i) = 0, 1 \leq i \leq n\}$ се състои от онези полиноми $f \in U_l$, за които $P_1, \dots, P_n \in Z(f) \cap Z(h)$. Ако сечението $Z(f) \cap Z(h)$ не е крайно, то неприводимата крива $Z(h)$ се съдържа в $Z(f)$ или $f \in \langle h \rangle = h\mathbb{F}_q[x, y]$ е полином от идеала, породен от h . Обратно, $\langle h \rangle \subseteq \ker(\mathcal{E})$, така че за $l \geq m$ имаме $\ker(\mathcal{E}) = hU_{l-m}$ с размерност $\dim \ker(\mathcal{E}) = \frac{(l-m+1)(l-m+2)}{2}$ и $\dim C = \dim U_l - \dim U_{l-m}$. Ако $l < m$, то $\ker(\mathcal{E}) = 0$ и $\dim C = \dim U_l$.

Минималното разстояние d съвпада с минималното тегло на линейния код C . За $l < m$ нулевите компоненти $f(P_i)$ в дума $(f(P_1), \dots, f(P_n)) \in C$ отговарят на точките $P_i \in Z(f) \cap Z(h)$ от сечението на афинните криви $Z(f)$ и $Z(h)$. По Теоремата на Bezout, техният брой не надминава $\deg(f) \deg(h) = lm$, така че всяка дума от C има поне $n - ml$ ненулеви компоненти и $d \geq n - ml$.

ЗАДАЧА 9.4. Да се намерят $\mathbb{F}_9$ -рационалните точки $P_1, \dots, P_n \in V(\mathbb{F}_9)$ на афинната равнинна крива

$$V = \{(x, y) \in \overline{\mathbb{F}_3} \mid y^2 = x^3 + x\}.$$

Да се пресметнат размерността и минималното разстояние на линейния код $C = \text{im}(\mathcal{E})$, където

$$\mathcal{E} : U_1 = \{f(x, y) = a_0 + a_1x + a_2y \mid a_i \in \mathbb{F}_9\} \longrightarrow \mathbb{F}_9^n,$$

$$\mathcal{E}(f) = (f(P_1), \dots, f(P_n)).$$

Решение: Нека $\mathbb{F}_9 = \{a + b\alpha \mid a, b \in \mathbb{F}_3\}$ за порождащия α на $\mathbb{F}_9^*$ с $\alpha^2 = \alpha + 1$. Вземайки предвид $\text{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \langle \Phi_3 \rangle \simeq (\mathbb{Z}_2, +)$ с $\Phi_3(x) = x^3$, представяме уравнението на V във вида

$$y^2 = \text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x).$$

За $\forall (x, y) \in V(\mathbb{F}_9)$ имаме $y^2 = \text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) \in \mathbb{F}_3$. Ако $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = 0$, то $x \in \{0, \pm(\alpha+1)\}$ и $y = 0$. Ако $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = 1$, то $x \in \{-1, \alpha, 1-\alpha\}$ и $y = \pm 1$. От $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = -1$ следва $x \in \{1, -\alpha, -1+\alpha\}$ и $y \in \{\pm(1+\alpha)\}$. Следователно $\mathbb{F}_9$ -рационалните точки на V са:

$$P_1 = (0, 1), \quad P_2 = (-1, 1), \quad P_3 = (-1, -1) \in \mathbb{F}_3^2,$$

$$P_4 = (1+\alpha, 0), \quad P_5 = (-1-\alpha, 0), \quad P_6 = (\alpha, 1), \quad P_7 = (1-\alpha, 1) \in \mathbb{F}_9^2,$$

$$P_8 = (\alpha, -1), \quad P_9 = (1-\alpha, -1), \quad P_{10} = (1, 1+\alpha), \quad P_{11} = (-\alpha, 1+\alpha) \in \mathbb{F}_9^2,$$

$P_{12} = (-1+\alpha, 1+\alpha), P_{13} = (1, -1-\alpha), P_{14} = (-\alpha, -1-\alpha), P_{15} = (-1+\alpha, -1-\alpha) \in \mathbb{F}_9^2$.

Нека $M \in M_{3,15}(\mathbb{F}_9)$ е пораждаща матрица на C , съставена по редове от стойностите на $1, x, y$ в $P_1, \dots, P_{15}$. По-точно, ако $P_j = (x(P_j), y(P_j))$, то

$$\begin{aligned} M_{1,j} &= 1 \quad \text{за } \forall 1 \leq j \leq 15, \\ M_{2,j} &= x(P_j) \quad \text{за } \forall 1 \leq j \leq 15, \\ M_{3,j} &= y(P_j) \quad \text{за } \forall 1 \leq j \leq 15. \end{aligned}$$

Търсим проверочна матрица $H \in M_{12,15}(\mathbb{F}_9)$ с максимален ранг 12. Редовете на H са съставени от фундаментална система решения на хомогенната линейна система

$$M \begin{pmatrix} z_1 \\ \dots \\ z_{15} \end{pmatrix} = 0_{3 \times 1}. \quad (9.2)$$

Да означим с $R_1, R_2, R_3 \in M_{1,15}(\mathbb{F}_9)$ редовете на матрицата M . Тогава елементарните преобразувания

$$\begin{aligned} R_1 &\mapsto -R_1 - R_2, \\ R_2 &\mapsto -R_1 + R_2 + R_3, \\ R_3 &\mapsto R_1 - R_3 \end{aligned}$$

свеждат първите три стълба към $-E_3$, където E_3 е единичната 3×3 -матрица. За произволно $4 \leq j \leq 15$ стълбът $(1, u_j, v_j)^t$ на M с номер j се трансформира в

$$(-1 - u_j, -1 + u_j + v_j, 1 - v_j)^t.$$

Общото решение на (9.2) е

$$\begin{aligned} z_1 &= -\sum_{j=4}^{15} (1 + u_j) z_j, \\ z_2 &= \sum_{j=4}^{15} (-1 + u_j + v_j) z_j, \\ z_3 &= \sum_{j=4}^{15} (1 - v_j) z_j. \end{aligned}$$

Редовете $H_j \in M_{1,15}(\mathbb{F}_9)$, $1 \leq j \leq 12$ на $H \in M_{12,15}(\mathbb{F}_9)$ могат да се изберат по следния начин:

$$\begin{aligned} H_{j,j+3} &= 1, \\ H_{j,s} &= 0 \quad \text{за } s \in \{4, \dots, j+2, j+4, \dots, 15\}, \\ H_{j,1} &= -1 - u_{j+3}, \\ H_{j,2} &= -1 + u_{j+3} + v_{j+3}, \\ H_{j,3} &= 1 - v_{j+3}. \end{aligned}$$

Знаем, че минималното разстояние на C е $d \geq 12$. Затова е достатъчно да намерим 12 линейно зависими стълба на H , за да твърдим, че $d = 12$. Стълбовете $C_1, \dots, C_{15} \in M_{12,1}(\mathbb{F}_9)$ на проверочната матрица H са

$$\begin{aligned} C_1^t &= (-1 - u_4, -1 - u_5, \dots, -1 - u_{15})^t, \\ C_2^t &= (-1 + u_4 + v_4, -1 + u_5 + v_5, \dots, -1 + u_{15} + v_{15})^t, \\ C_3^t &= (1 - v_4, 1 - v_5, \dots, 1 - v_{15})^t, \\ C_j &= e_{j-3}, \quad 4 \leq j \leq 15, \end{aligned}$$

където $e_{j-3} \in M_{12,1}(\mathbb{F}_9)$ има единствен ненулев елемент 1 в $(j-3)$ -та позиция. Твърдим, че стълбовете $C_1, \dots, C_9, C_{13}, C_{14}, C_{15}$ на H са линейно зависими. За целта е достатъчно анулирането на детерминантата

$$\Delta = \det(C_1 \dots C_9 C_{13} C_{14} C_{15}) = \begin{vmatrix} H_{71} & H_{72} & H_{73} \\ H_{81} & H_{82} & H_{83} \\ H_{91} & H_{92} & H_{93} \end{vmatrix},$$

след развитие по адюнгирани количества относно последните стълбове. По-точно,

$$\Delta = \begin{vmatrix} -1 - u_{10} & -1 + u_{10} + v_{10} & 1 - v_{10} \\ -1 - u_{11} & -1 + u_{11} + v_{11} & 1 - v_{11} \\ -1 - u_{12} & -1 + u_{12} + v_{12} & 1 - v_{12} \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & u_{10} & v_{10} \\ 1 & u_{11} & v_{11} \\ 1 & u_{12} & v_{12} \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 + \alpha \\ 1 & -\alpha & 1 + \alpha \\ 1 & -1 + \alpha & 1 + \alpha \end{vmatrix} = 0.$$