Глава 9

Теорема на Bezout. Полиномиални кодове върху равнинни криви.

Определение 9.1. *Множеството*

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

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

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

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

с коефициенти от поле K, резултантата се определя като

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

Непосредствено се вижда, че

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

и $R(f, g) = 0$ за $f(t) \not\equiv 0_K$, $g(t) \not\equiv 0_K$ точно когато f и g имат общ корен.
Дискриминантата на $f(t)$ се определя като

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

Лема 9.2. *Нека $f(t), g(t) \in K[t]$ са полиноми на една променлива t с коефициенти от поле K, а P е простото подполе на K. Тогава дискриминантата $D(f) \in P[a_0, \ldots, a_n]$ на $f(t)$ е полином на коефициентите на $f(t)$, резултантата $R(f, g) \in P[a_0, \ldots, a_n, b_0, \ldots, b_m]$ на f и g е полином на коефициентите на f и g.*

Доказателство: Нека $\sigma_1, \ldots, \sigma_n$ са елементарните симетрични полиноми на $\alpha_1, \ldots, \alpha_n$, а $\tau_1, \ldots, \tau_m$ са елементарните симетрични полиноми на $\beta_1, \ldots, \beta_m$. Непосредствено се вижда, че $\prod_{n \geq i > j \leq 1} (\alpha_i - \alpha_j)^2$ е симетричен полином на $\alpha_1, \ldots, \alpha_n$,

откъдето и полином $\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2 \in P[\sigma_1,\ldots,\sigma_n]$ на елементарните симетрични полиноми $\sigma_1,\ldots,\sigma_n$ на $\alpha_1,\ldots,\alpha_n$ с коефициенти от P. От формулите на Виет $\sigma_i=(-1)^i\frac{a_i}{a_0}$ за $1\leq i\leq n$ получаваме, че

$$\prod_{n\geq i>j\leq 1}(\alpha_i-\alpha_j)^2 \in P\left[\frac{a_1}{a_0},\ldots,\frac{a_n}{a_0}\right].$$

Съгласно алгоритъма за представяне на симетричен полином на $\alpha_1,\ldots,\alpha_n$ като полином на $\sigma_1,\ldots,\sigma_n$, мономите на $\prod_{n\geq i>j\leq 1}(\alpha_i-\alpha_j)^2$ са от вида

$$\mu=\left(\frac{a_1}{a_0}\right)^{k_1-k_2}\left(\frac{a_2}{a_0}\right)^{k_2-k_3}\ldots\left(\frac{a_{n-1}}{a_0}\right)^{k_{n-1}-k_n}\left(\frac{a_n}{a_0}\right)^{k_n}$$

с $k_1\geq k_2\geq\ldots\geq k_{n-1}\geq k_n\geq 0$. Тук k_1 не надминава максималната степен $2n-2$, в която α_1 участва в моном на $\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2$. Следователно мономите на $D(f)=a_0^{2n-2}\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2$ са от вида

$$a_0^{2n-2}\mu=a_0^{2n-2-k_1}a_1^{k_1-k_2}a_2^{k_2-k_3}\ldots a_{n-1}^{k_{n-1}-k_n}a_n^{k_n}$$

с $2n-2\geq k_1\geq k_2\geq\ldots\geq k_{n-1}\geq k_n\geq 0$, така че $a_0^{2n-2}\mu\in P[a_0,a_1,\ldots,a_n]$ и $D(f)\in P[a_0,a_1,\ldots,a_n]$.

Полиномът $\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)$ от степен m относно α_i и от степен n относно β_j е симетричен полином на $\alpha_1,\ldots,\alpha_n$ и симетричен полином на $\beta_1,\ldots,\beta_m$. Следователно

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)\in P[\sigma_1,\ldots,\sigma_n,\tau_1,\ldots,\tau_m]=P\left[\frac{a_1}{a_0},\ldots,\frac{a_n}{a_0},\frac{b_1}{b_0},\ldots,\frac{b_m}{b_0}\right],$$

съгласно основната теорема за симетричните полиноми и формулите на Виет $\sigma_i=(-1)^i\frac{a_i}{a_0}$ за $1\leq i\leq n$, $\tau_j=(-1)^j\frac{b_j}{b_0}$ за $1\leq j\leq m$. Мономите на

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)$$

са от вида

$$\nu=\left(\frac{a_1}{a_0}\right)^{k_1-k_2}\ldots\left(\frac{a_{n-1}}{a_0}\right)^{k_{n-1}-k_n}\left(\frac{a_n}{a_0}\right)^{k_n}\left(\frac{b_1}{b_0}\right)_{l_1-l_2}\ldots\left(\frac{b_{m-1}}{b_0}\right)^{l_{m-1}-l_m}\left(\frac{b_m}{b_0}\right)^{l_m}$$

за $m\geq k_1\geq k_2\geq\ldots\geq k_{n-1}\geq k_n\geq 0$, $n\geq l_1\geq l_2\geq\ldots\geq l_{m-1}\geq l_m\geq 0$. Следователно мономите на $R(f,g)=a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j)$ са от вида

$$a_0^m b_0^n\nu=$$

$$=a_0^{m-k_1}a_1^{k_1-k_2}\ldots a_{n-1}^{k_{n-1}-k_n}a_n^{k_n}b_0^{n-l_1}b_1^{l_1-l_2}\ldots b_{m-1}^{l_{m-1}-l_m}b_m^{l_m}\in P[a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_m]$$

и $R(f,g)\in P[a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_m]$, Q.E.D.

Лема 9.3. *Нека*

$$f(t)=a_0t^n+a_1t^{n-1}+\ldots+a_{n-1}t+a_n \quad u$$

$$g(t)=b_0t^m+b_1t^{m-1}+\ldots+b_{m-1}t+b_m$$

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

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

са запълнени последователно от m екземпляра на коефициентите на $f(t)$, записани от диагоналните позиции надясно и n екземпляра на коефицинетите 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

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

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

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

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

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

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 адюнгирани 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 адюнгирани количества относно $(m+n)$-ти стълб, $(m+n-1)$-ви стълб, ... $(m+1)$-ви стълб в първоначалната номерация на стълбовете и т.н. Получаваме

$$(-1)^{mn}a_0^m\left[\prod_{i=1}^{n}g(\alpha_i)\right](-1)^{\frac{n(n-1)}{2}}\prod_{1\le j<i\le n}(\alpha_i-\alpha_j)=$$

$$=\det(M)(-1)^{mn}(-1)^{\frac{n(n-1)}{2}}\prod_{1\le j<i\le n}(\alpha_i-\alpha_j).$$

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

$$R(f,g)D(f)=\det(M)D(f) \tag{9.1}$$

за дискриминантата $D(f)$ 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 $\mathrm{char}(K)=0$ или $\mathrm{char}(K)=p$ не дели степента $\deg(f)=n$, то $f(t)=t^n+1$ и $f'(t)=nt^{n-1}$ нямат общ корен. В случая на степн $\deg(f)=n$, кратна на характеристиката $\mathrm{char}(K)=p$ 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 $Z(f)\subset\mathbb{P}^2(\overline{k})$ и $Z(g)\subset\mathbb{P}^2(\overline{k})$ 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 9.4. (Слаб вариант на Теоремата на Bezout) *Ако $Z(f)\subset\mathbb{P}^2(\overline{k})$ и $Z(g)\subset\mathbb{P}^2(\overline{k})$ са проективни равнинни криви с крайно сечение $Z(f)\cap Z(G)$, то*

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

Доказателство: Разглеждаме проекцията

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

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

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

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

е проективизацията на равнината

$$\{(x,y,z)\in\overline{k}^3\ \mid\ x_oy-xy_o=0\}\simeq\overline{k}^2$$

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

Твърдим, че съществува такава координатна система в $\overline{k}^3$, спрямо която сечението $Z(f)\cap Z(g)\subseteq\mathbb{P}^2(\overline{k})\setminus\{[0:0:1]\}$ се съдържа в дефиниционната област на Π и ограничението $\Pi:Z(f)\cap Z(g)\to\Pi(Z(f)\cap Z(g))$ е взаимно еднозначно върху образа си. За целта разглеждаме правите през началото $l_i=\{(\lambda p_i,\lambda q_i,\lambda r_i)\ \mid\ \lambda\in\overline{k}\}$, $1\le i\le n$, до които се повдигат точките от

$Z(f)\cap Z(g)=\{[p_i:q_i:r_i]\ \mid\ 1\le i\le n\}$ и равнините α_{ij} през началото, минаващи през l_i и l_j за $\forall 1\le i<j\le n$. Всеки две различни прави l_i и l_j, $i<j$ в $\overline{k}^3$ през началото определят единствена равнина α_{ij}. Избираме третата координатна ос Oz така, че да не лежи в нито една от равнините α_{ij}, $1\le i<j\le n$. Тогава $[0:0:1]\notin Z(f)\cap Z(g)$, защото Oz не лежи върху нито една от правите l_i. Ако допуснем, че две различни прави $l_i\neq l_j$ се проектират върху една и съща права $\{(\lambda p_i,\lambda q_i)\ \mid\ \lambda\in\overline{k}\}=\{(\mu p_j,\mu q_j)\ \mid\ \mu\in\overline{k}\}$ в $\overline{k}^2$, то можем да представим l_j във вида $l_j=\{(\nu p_i,\nu q_i,\nu r'_j)\ \mid\ \nu\in\overline{k}\}\subset\overline{k}^3$. От $l_i\neq l_j$ следва $r_i\neq r'_j$, така че векторът $v_{ij}=(0,0,r_i-r'_j)$ е ненулев. Но $v_{ij}\in\alpha_{ij}$ принадлежи на линейната обвивка α_{ij} на l_i и l_j, което противоречи на избора на Oz и доказва взаимната еднозначност на $\Pi: Z(f)\cap Z(g)\to\Pi(Z(f)\cap Z(g))$ при направения избор на координати.

Представяме хомогенния полином

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

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

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

за хомогенни полиноми $b_j(x,y)\in\overline{k}[x,y]$ 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 $R_z(f,g)(x,y)\in\overline{k}[x,y]$ на f и g като полиноми на z. Достатъчно е да докажем, че $R_z(f,g)(x,y)$ е хомогенен полином от степен $d\le mn$ за $\deg(f)=n$, $\deg(g)=m$, за да получим, че $|Z(f)\cap Z(g)|\le mn$. Поточно, $R_z(f,g)(x,y)$ от степен d има най-много d корена, които отговарят на различни точки от $Z(f)\cap Z(g)$ съгласно взаимната еднозначност на проекцията $\Pi: Z(f)\cap Z(g)\to\Pi(Z(f)\cap Z(g))$.

За произволен параметър t резултантата

$$R_z(f,g)(tx,ty)=$$

$$\det\begin{pmatrix}
t^{n-s}a_{n-s} & t^{n-s+1}a_{n-s+1} & \ldots & & t^na_n & & \\
 & t^{n-s}a_{n-s} & t^{n-s+1}a_{n-s+1} & \ldots & & t^na_n & \\
 & & & t^{n-s}a_{n-s} & t^{n-s+1}a_{n-s+1} & \ldots & t^na_n \\
t^{m-l}b_{m-l} & t^{m-l+1}b_{m-l+1} & \ldots & & t^mb_m & & \\
 & t^{m-l}b_{m-l} & t^{m-l+1}b_{m-l+1} & \ldots & & t^mb_m & \\
 & & & t^{m-l}b_{m-l} & t^{m-l+1}b_{m-l+1} & \ldots & t^mb_m
\end{pmatrix}$$

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

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

Изнасянето на степените на t от стълбовете на получената детерминанта дава

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

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

$$\Delta = \delta(s+l) + \frac{(s+l-1)(s+l)}{2} - (m-l)l - \frac{(l-1)l}{2} - (n-s)s - \frac{(s-1)s}{2} = \\ = ms + nl - sl \leq mn,$$

защото $(m-l)(n-s) \geq 0$, Q.E.D.

Равенството $|Z(f) \cap Z(g)| = \deg(f)\deg(g)$ за крайно сечение $Z(f) \cap Z(h)$ се извежда от неравенствата

$$|Z(f) \cap Z(h)| = \sum_{p \in Z(f) \cap Z(g)} \dim_{\overline{k}} \mathcal{O}_p / \langle f, g \rangle_p \leq \dim_{\overline{k}} \overline{k}[x,y]/\langle f, g \rangle \leq \deg(f)\deg(g),$$

които после се доказват че са изпълнени като равенства.

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 афинна равнинна крива, зададена чрез неразложим над $\overline{\mathbb{F}_q}$ (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 $\sum_{i=0}(i+1) = \frac{(l+1)(l+2)}{2}$. Избираме n различни $\mathbb{F}_q$-рационални точки $P_1, \ldots, P_n \in Z(h)(\mathbb{F}_q)$ за някое естествено $n > ml$ и разглеждаме остойностяващото изображение

$$\mathcal{E} : U_l \longrightarrow \mathbb{F}_q^n,$$
$$\mathcal{E}(f) = (f(P_1), \ldots, f(P_n)).$$

Ядрото $\ker \mathcal{E} = \{g \in U_l \mid g(P_i) = 0, \ \ 1 \leq i \leq n\}$ се състои от онези полиноми $g \in U_l$, за които $P_1, \ldots, P_n \in Z(g) \cap Z(h)$. Ако сечението $Z(g) \cap Z(h)$ е крайно, то броят на точките в него е

$$n = |\{P_1, \ldots, P_n\}| \leq |Z(g) \cap Z(h)| \leq lm,$$

което противоречи на избора на $n > lm$. Следователно $Z(g) \cap Z(h)$ е крива за всички $g \in U_l \setminus \{0\}$. От $Z(g) \cap Z(h) \subseteq Z(h)$ е неприводимостта на $Z(h)$ получаваме $Z(g) \cap Z(h) = Z(h)$, откъдето $Z(h) \subseteq Z(g)$. Следователно идеалите $r(\langle h \rangle = IZ(h) \supseteq IZ(g)$ изпълняват противоположното включване. Неразложимият над $\overline{\mathbb{F}_q}$ полином h поражда прост идеал $\langle h \rangle$, така че $r(\langle h \rangle) = \langle h \rangle$. Оттук, $g \in IZ(g) \subseteq \langle h \rangle$. Обратно, ако $g \in \langle h \rangle$, то $g(P_i) = 0$ за $\forall P_i \in Z(h)$ и $g \in \ker \mathcal{E}$. С това доказахме, че

$$\ker \mathcal{E} = \langle h \rangle \cap U_l = \{hf \mid \deg(hf) \leq l\} = \{hf \mid \deg f \leq l-m\} \simeq U_{l-m} \quad \text{за} \quad l \geq m$$

и $\ker \mathcal{E} = \{0\}$ за $l < m$.

Образът $C = \mathcal{E}(U_l)$ на U_l под действие на $\mathcal{E}$ е $\mathbb{F}_q$-линеен код с дължина n и размерност

$$\dim C = \dim U_l - \dim \ker \mathcal{E} = \begin{cases} \binom{l+2}{2} - \binom{l-m+2}{2} & \text{за } l \geq m, \\ \binom{l+2}{2} & \text{за } l < m. \end{cases}$$

Твърдим, че минималното разстояние d на C е $d \geq n - lm$. За целта използваме съвпадението на d с минималното тегло w на C. Ненулева дума $c = (g(P_1), \ldots, g(P_n) \in C$ има нулева компонента $g(P_i) = 0$ точно когато $P_i \in Z(g) \cap Z(h)$. Съгласно $c \neq (0, \ldots, 0)$ сечението $Z(g) \cap Z(h)$ е крайно и броят на точкте в него е $|Z(g) \cap Z(h)| \leq lm$. Следователно кодова дума $c \in C \setminus \{(0, \ldots, 0)\}$ има най-много lm нулеви компоненти или поне $n - ml$ ненулеви компоненти. С други думи, $d = w \geq n - ml$.

Задача 9.5. *Да се намерят $\mathbb{F}_9$-рационалните точки $P_1, \ldots, P_n \in V(\mathbb{F}_9)$ на афинната равнинна крива*

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

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

$$\mathcal{E} : U_1 = \{f(x, y) = a_0 + a_1 x + a_2 y \mid a_i \in \mathbb{F}_9\} \longrightarrow \mathbb{F}_9^n,$$
$$\mathcal{E}(f) = (f(P_1), \ldots, f(P_n)).$$

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

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

За $\forall (x, y) \in V(\mathbb{F}_9)$ имаме $y^2 = \mathrm{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) \in \mathbb{F}_3$. Затова решенията на $y^2 = x^3 + x$ са точно решенията на системите

$$\left| \begin{array}{l} y^2 = a \\ x^3 + x = a \end{array} \right. \quad \text{за} \quad \forall a \in \mathbb{F}_3.$$

Ако $\mathrm{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = 0$, то $x \in \{0, \pm(\alpha + 1)\} = \ker \mathrm{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}$ и $y = 0$. Забелязваме, че $x = -1 \in \mathbb{F}_3$ е решение на $x^3 + x = 1$. Съгласно линейността на следата, всички решения на $\mathrm{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = 1$ са $-1 + \ker \mathrm{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9} = \{-1, \alpha, 1 - \alpha\}$. От друга страна, $y^2 = 1$ има решения $y = \pm 1$. Аналогично, $x_2 = 1$ е решение на $x^3 + x = -1$. Всички решения на това уравнение са $1 + \ker \mathrm{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9} = \{1, -\alpha, -1 + \alpha\}$. Вече пресметнахме, че корените на $y^2 = -1$ в $\mathbb{F}_9$ са $y \in \{\pm(1 + \alpha)\}$. Следователно $\mathbb{F}_9$-рационалните точки на V са:

$$P_1 = (0, 0), \quad P_2 = (\alpha + 1, 0), \quad P_3 = (-\alpha - 1, 0),$$
$$P_4 = (-1, 1), \quad P_5 = (\alpha, 1), \quad P_6 = (1 - \alpha, 1),$$
$$P_7 = (-1, -1), \quad P_8 = (\alpha, -1), \quad P_9 = (1 - \alpha, -1),$$
$$P_{10} = (1, 1 + \alpha), \quad P_{11} = (-\alpha, 1 + \alpha), \quad P_{12} = (-1 + \alpha, 1 + \alpha),$$
$$P_{13} = (1, -1 - \alpha), \quad P_{14} = (-\alpha, -1 - \alpha), \quad P_{15} = (-1 + \alpha, -1 - \alpha).$$

Остойностяващото изображение $\mathcal{E} : U_1 \to \mathbb{F}_9^{15}$, $\mathcal{E}(f) = (f(P_1), \ldots, f(P_{15})$ е влагане , защото неразложимият над $\overline{\mathbb{F}_9}$ полином $y^2 - x^3 - x$ е от степен $m = 3$, строго по-голяма от степента $l = 1$ на полиномите в които заместваме с P_i. Следователно $C = \mathcal{E}(U_1) \subset \mathbb{F}_9^{15}$ е $\mathbb{F}_9$-линеен код с дължина $n = 15$ и размерност $\dim C = \dim U_1 = \binom{1+2}{2} = \binom{3}{2} = 3$. Горните разглеждания доказват, че минималното разстояние $d \geq n - ml = 15 - 3.1 = 12$. Достатъчно е да забележим съществуването на дума

$$\mathcal{E}(y) = (0, 0, 0, 1, 1, 1, -1, -1, -1, 1+\alpha, 1+\alpha, 1+\alpha, -1-\alpha, -1-\alpha, -1-\alpha) \in C$$

с тегло 12, за да стигнем до извода, че минималното разстояние на C е $d = 12$.