Глава 21

Допирателни кодове

Нека $X \subseteq \overline{\mathbb{F}_q}^n$ е афинно многообразие с абсолютен идеал $I(X) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, породен от полиноми $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ с коефициенти от $\mathbb{F}_q$. В настоящата тема интерпретираме крайните допирателни пространства на Зариски $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ към X в $a \in X$ над дефиниционното поле $\mathbb{F}_{q^{\delta(a)}}$ на a като линейни кодове. Чрез глобални геометрични свойства на X ще характеризираме минималното разстояние на $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ в обща точка $a \in X$ и ще построим алгоритъм за едновременно декодиране на допирателни кодове след намиране на носителя на грешката.

1. Схема за построение на неприводими афинни алгебрични множества

За да опишем някои свойства на допирателните кодове $T_a(X, \mathbb{F}_{q^{\delta(a)}})$, съществено използваме неприводимостта на афинното алгебрично множество $X \subseteq \overline{\mathbb{F}_q}^n$. Настоящият параграф построява афинни многообразия $X \subseteq \overline{\mathbb{F}_q}^n$ с размерност $\dim X = k$ чрез явни изоморфизми на X с хиперповърхнини в $\overline{\mathbb{F}_q}^{k+1}$.

Лема 21.1. *Нека $f(x, y, z) = y^2 z^{2m-1} + h(x, z) \in \mathbb{F}_q[x, y, z]^{(2m+1)}$ е хомогенен полином от нечетна степен $2m + 1 \geq 3$ с $h(x, 0) = x^{2m+1}$. Тогава $f(x, y, z) \in \overline{\mathbb{F}_q}[x, y, z]$ е неразложим като полином с коефициенти от алгебричната обвивка $\overline{\mathbb{F}_q}$ на $\mathbb{F}_q$.*

Доказателство: Нека $f = f_1 f_2$ е разлагане в произведение на полиноми $f_1, f_2 \in \overline{\mathbb{F}_q}[x, y, z]$. Разглеждаме $f_j \in \overline{\mathbb{F}_q}[x, z][y]$ като полиноми на y с коефициенти от $\overline{\mathbb{F}_q}[x, z]$. От $f(x, y, z) \not\equiv 0 \in \overline{\mathbb{F}_q}[x, y, z]$ следва $f_j \not\equiv 0$, така че степените $\deg_y f_j \geq 0$ на f_j относно y са неотрицателни цели числа със сума $\deg_y f_1 + \deg_y f_2 = \deg_y f = 2$. Без ограничение на общността ще считаме, че $\deg_y f_1 \geq \deg_y f_2$. По този начин получаваме, че или $\deg_y f_1 = 2$, $\deg_y f_2 = 0$ или $\deg_y f_1 = \deg_y f_2 = 1$.
Ако $\deg_y f_1 = 2$, $\deg_y f_2 = 0$, то

$$y^2 z^{2m-1} + h(x, z) = f = [a(x, z)y^2 + b(x, z)y + c(x, z)]d(x, z)$$

за някакви полиноми $a, b, c, d \in \overline{\mathbb{F}_q}[x, z]$. Сравнявайки коефициентите на y^2 и 1 от $\overline{\mathbb{F}_q}[x, z]$ получаваме

$$a(x, z)d(x, z) = z^{2m-1}, \quad c(x, z)d(x, z) = h(x, z).$$

След евентуално умножение на $a(x, z)$ и $d(x, z)$ с ненулеви константи от $\overline{\mathbb{F}_q}$ можем да считаме, че $d(x, z) = z^s$ и $a(x, z) = z^{2m-1-s}$ за някое $s \in \mathbb{Z}$, $0 \leq s \leq 2m - 1$. Сега $h(x, z) = c(x, z)d(x, z) = z^s c(x, z)$ с $h(x, 0) = x^{2m+1} \not\equiv 0$ изисква $s = 0$, така че $d(x, z) \equiv 1 \in \overline{\mathbb{F}_q}[x, z]$ и разлагането е тривиално.
Ако $\deg_y f_1 = \deg_y f_2 = 1$, то

$$y^2 z^{2m-1} + h(x, z) = f = [a(x, z)y + b(x, z)][c(x, z)y + d(x, z)]$$

за някакви полиноми $a,b,c,d \in \overline{\mathbb{F}_q}[x,z]$. Сравнявайки коефициентите на y^2, y и 1 от $\overline{\mathbb{F}_q}[x,z]$ извеждаме равенствата

$$a(x,z)c(x,z) = z^{2m-1}, \quad a(x,z)d(x,z)+b(x,z)c(x,z) = 0, \quad b(x,z)d(x,z) = h(x,z).$$

След евентуално умножение на $a(x,z)$ и $c(x,z)$ с елементи от $\overline{\mathbb{F}_q}^*$ имаме $a(x,z) = z^s$, $c(x,z) = z^{2m-1-s}$ за някое $s \in \mathbb{Z}$, $0 \leq s \leq 2m-1$. С точност до размяна на f_1 с f_2 можем да предполагаме, че $s \geq 2m-1-s$. Сега от

$$z^{2m-1-s}[z^{2s-2m+1}d(x,z) + b(x,z)] \equiv 0$$

следва $b(x,z) = -z^{2s-2m+1}d(x,z)$, откъдето

$$h(x,z) = -z^{2s-2m+1}d(x,z)^2.$$

Но $h(x,0) = x^{2m+1} \not\equiv 0$ изисква $2s-2m+1 = 0$, което не е изпълнено за нито едно цяло число s. Това доказва несъществуването на разлагане $f = f_1 f_2$ с $\deg_y f_1 = \deg_y f_2 = 1$ и неразложимостта на $f(x,y,z) \in \overline{\mathbb{F}_q}[x,y,z]$, Q.E.D.

Лема 21.2. *Ако $f = f_1 f_2$ е разлагане на хомогенен полином $f \in k[x_1,\ldots,x_n]^{(\delta)}$ от степен $\delta \in \mathbb{Z}^{\geq 0}$ с коефициенти от поле k в произведение на полиноми $f_1, f_2 \in k[x_1,\ldots,x_n]$, то f_1 и f_2 са хомогенни.*

Доказателство: Представяме

$$f_1 = f_1^{(a)} + f_1^{(a+1)} + \ldots + f_1^{(a+b)} \quad \text{и} \quad f_2 = f_2^{(c)} + f_2^{(c+1)} + \ldots + f_2^{(c+d)}$$

като суми на хомогенни компоненти от неотрицателни степени. Без ограничение на общността можем да считаме, че $f_1^{(a)} \not\equiv 0$, $f_1^{(a+b)} \not\equiv 0$ за някакви $a,b \in \mathbb{Z}^{\geq 0}$ и $f_2^{(c)} \not\equiv 0$, $f_2^{(c+d)} \not\equiv 0$ за някакви $c,d \in \mathbb{Z}^{\geq 0}$. Полиномът $f = f_1 f_2$ има хомогенна компонента $f^{(a+c)} = f_1^{(a)} f_2^{(c)} \not\equiv 0$ от степен $a+c \geq 0$ и хомогенна компонента $f^{(a+b+c+d)} = f_1^{(a+b)} f_2^{(c+d)} \not\equiv 0$ от степен $a+b+c+d \geq 0$. Сега хомогенността на $f = f^{(\delta)}$ изисква $a+c = \delta = a+b+c+d$, откъдето $b+d = 0$ за $b,d \in \mathbb{Z}^{\geq 0}$. Това е в сила само когато $b = d = 0$ и $f_1 = f_1^{(a)} \in k[x_1,\ldots,x_n]^{(a)}$, $f_2 = f_2^{(c)} \in k[x_1,\ldots,x_n]^{(c)}$ са хомогенни полиноми, Q.E.D.

Лема 21.3. *Ако $g \in \mathbb{F}_q[x_1,\ldots,x_n]^{(\delta)}$ е хомогенен полином на $n \geq 3$ променливи, за който $g(x_1,x_2,x_3,0,\ldots,0) \in \overline{\mathbb{F}_q}[x_1,x_2,x_3]^{(\delta)}$ е неразложим, то $g \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ е неразложим като полином на $x_1,\ldots,x_n$ с коефициенти от алгебричната обвивка $\overline{\mathbb{F}_q}$ на $\mathbb{F}_q$.*

Доказателство: С индукция по броя на променливите n, за $n = 3$ няма какво да се доказва. Допускаме, че лемата е вярна за хомогенни полиноми $h \in \mathbb{F}_q[x_1,\ldots,x_{n-1}]^{(\delta)}$ на $n-1$ променливи с неразложими $h(x_1,x_2,x_3,0\ldots,0) \in \overline{\mathbb{F}_q}[x_1,x_2,x_3]^{(\delta)}$. Всяко разлагане $g = g_1 g_2$ на хомогенен полином $g \in \mathbb{F}_q[x_1,\ldots,x_n]^{(\delta)}$ има хомогенни множители $g_1 \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]^{(s)}$, $g_2 \in \overline{\mathbb{F}_q}[x_1,\ldots,x_n]^{(\delta-s)}$ за някое $0 \leq s \leq \delta$, съгласно Лема 21.2. Полагаме $x_n = 0$ и получаваме разлагане

$$g(x_1,\ldots,x_{n-1},0) = g_1(x_1,\ldots,x_{n-1},0)g_2(x_1,\ldots,x_{n-1},0)$$

на хомогенния полином $g(x_1,\ldots,x_{n-1},0) \in \mathbb{F}_q[x_1,\ldots,x_{n-1}]^{(\delta)}$ в произведение на хомогенни множители $g_1(x_1,\ldots,x_{n-1},0) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_{n-1}]^{(s)}$, съответно, $g_2(x_1,\ldots,x_{n-1},0) \in \overline{\mathbb{F}_q}[x_1,\ldots,x_{n-1}]^{(\delta-s)}$. По предположение,

$$g(x_1,\ldots,x_{n-1},0)|_{x_4=\ldots=x_{n-1}=0} = g(x_1,x_2,x_3,0,\ldots,0) \in \overline{\mathbb{F}_q}[x_1,x_2,x_3]^{(\delta)}$$

е неразложим, така че

$$g_1(x_1,\ldots,x_{n-1},0) \in \overline{\mathbb{F}_q}^* = \overline{\mathbb{F}_q}[x_1,\ldots,x_{n-1}]^{(0)} = \overline{\mathbb{F}_q}[x_1,\ldots,x_{n-1}]^{(s)}$$

или

$$g_2(x_1,\ldots,x_{n-1},0)\in\overline{\mathbb{F}_q}^*=\overline{\mathbb{F}_q}[x_1,\ldots,x_{n-1}]^{(0)}=\overline{\mathbb{F}_q}[x_1,\ldots,x_{n-1}]^{(\delta-s)}.$$

Оттук, $s=0$ или $s=\delta$, така че $g_1(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}^*$ или $g_2(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}^*$ и полиномът $g(x_1,\ldots,x_n)\in\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ е неразложим, Q.E.D.

Твърдение 21.4. *Нека $g(x_1,\ldots,x_n)\in\mathbb{F}_q[x_1,\ldots,x_n]^{(\delta)}$ е хомогенен полином от степен $\delta\in\mathbb{N}$, за който $g(x_1,x_2,x_3,0,\ldots,0)\in\overline{\mathbb{F}_q}[x_1,x_2,x_3]^{(\delta)}$ е неразложим, а $f_1,\ldots,f_k\in\mathbb{F}_q[x_1,\ldots,x_n]$ са произволни полиноми за някое $k\in\mathbb{Z}^{\geq 0}$. Тогава идеалът*

$$I=\langle g,x_{n+j}-f_j\,|\,1\leq j\leq k\rangle\lhd\overline{\mathbb{F}_q}[x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+k}]$$

е прост и $X=Z(I)\subset\overline{\mathbb{F}_q}^{n+k}$ е неприводимо афинно алгебрично множество с размерност $\dim X=n-1$.

Доказателство: Нека

$$J:=\langle x_{n+j}-f_j\,|\,1\leq j\leq k\rangle\lhd\overline{\mathbb{F}_q}[x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+k}]$$

е идеалът, породен от полиномите $\varphi_j=x_{n+j}-f_j$ за $\forall 1\leq j\leq k$. Тогава ограничението на пунктирането

$$\Pi:\overline{\mathbb{F}_q}^{n+k}\longrightarrow\overline{\mathbb{F}_q}^n,$$
$$\Pi(x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+1})=(x_1,\ldots,x_n)$$

в последните k компоненти върху множеството $Z(J)\subseteq\overline{\mathbb{F}_q}^{n+k}$ на нулите на J е бирегулярно и изоморфизмът $\Pi:Z(J)\to\overline{\mathbb{F}_q}^n$ има обратен

$$\mu:\overline{\mathbb{F}_q}^n\longrightarrow Z(J),$$
$$\mu(x_1,\ldots,x_n)=(x_1,\ldots,x_n,f_1(x_1,\ldots,x_n),\ldots,f_k(x_1,\ldots,x_n)).$$

Индуцираният изоморфизъм

$$\mu^*:\overline{\mathbb{F}_q}[Z(J)]=\overline{\mathbb{F}_q}[x_1,\ldots,x_{n+k}]/r(J)\longrightarrow\overline{\mathbb{F}_q}[\overline{\mathbb{F}_q}^n]=\overline{\mathbb{F}_q}[x_1,\ldots,x_n],$$

на афинните координатни пръстени замества $x_{n+j}+r(J)$ с $f_j+r(J)$, където $r(J)\lhd\overline{\mathbb{F}_q}[x_1,\ldots,x_{n+k}]$ е радикалът на $J\lhd\overline{\mathbb{F}_q}[x_1,\ldots,x_{n+k}]$. Комбинирайки μ^* с изоморфизмите на $\overline{\mathbb{F}_q}$-алгебри

$$\begin{aligned}\overline{\mathbb{F}_q}[Z(J)]&\simeq\overline{\mathbb{F}_q}[x_1+r(J),\ldots,x_n+r(J),x_{n+1}+r(J),\ldots,x_{n+k}+r(J)]=\\&=\overline{\mathbb{F}_q}[x_1+r(J),\ldots,x_n+r(J)]\simeq\overline{\mathbb{F}_q}[x_1,\ldots,x_n]+r(J)/r(J)\simeq\\&\simeq\overline{\mathbb{F}_q}[x_1,\ldots,x_n]/\overline{\mathbb{F}_q}[x_1,\ldots,x_n]\cap r(J),\end{aligned}$$

стигаме до извода, че $\overline{\mathbb{F}_q}[x_1,\ldots,x_n]\cap r(J)=\{0\}$. Оттук, $\overline{\mathbb{F}_q}[x_1,\ldots,x_n]\cap J=\{0\}$, съгласно $J\subseteq r(J)$.
Да означим $A:=\overline{\mathbb{F}_q}[x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+k}]$, $B:=\overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ и да забележим, че $J\subseteq I$. Идеалът $I\lhd A$ е прост точно когато фактор-пръстенът

$$A/I\simeq(A/J)/(I/J)$$

няма делители на нулата. Съгласно

$$\begin{aligned}&A/J\simeq\overline{\mathbb{F}_q}[x_1+J,\ldots,x_n+J,x_{n+1}+J,\ldots,x_{n+k}+J]=\overline{\mathbb{F}_q}[x_1+J,\ldots,x_n+J]=\\&=\overline{\mathbb{F}_q}[x_1,\ldots,x_n]+J/J\simeq\overline{\mathbb{F}_q}[x_1,\ldots,x_n]/\overline{\mathbb{F}_q}[x_1,\ldots,x_n]\cap J=\overline{\mathbb{F}_q}[x_1,\ldots,x_n]=B,\end{aligned}$$

факторът

$$I/J=gA+J/J=gB+J/J\simeq gB/gB\cap J\simeq gB$$

изоморфен на идеала gB на B, съгласно $gB\cap J\subseteq B\cap J=0$. Следователно

$$(A/J)/(I/J)\simeq B/gB$$

е област поради неразложимостта на $g \in B = \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ като полином на $x_1, \ldots, x_n$ с коефициенти от $\overline{\mathbb{F}_q}$. Това доказва простотата на идеала $I \lhd A = \overline{\mathbb{F}_q}[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+k}]$.
Сега от $IZ(I) = r(I) = I$ следва неприводимостта на $X = Z(I) \subseteq \overline{\mathbb{F}_q}^{n+k}$. Морфизмът $\mu : \overline{\mathbb{F}_q}^n \to Z(J)$ се ограничава до изоморфизъм $\mu : Z_n(g) \to Z(I)$ с хиперповърхнината $Z_n(g) := \{a \in \overline{\mathbb{F}_q}^n \,|\, g(a) = 0\}$. Оттук, размерността $\dim Z(I) = \dim Z_n(g) = n - 1$, Q.E.D.

2. Минимално разстояние на допирателен код в обща точка. Намаляване на дължината на допирателен код в обща точка със запазване на размерността и минималното разстояние.

Определение 21.5. *Рационално изображение $f : X \dashrightarrow Y$ е етално в своя точка на регулярност $a \in \mathcal{D}_f$, ако диференциалът*

$$(df)_a : T_a(X, \overline{\mathbb{F}_q}) \longrightarrow T_{f(a)}(Y, \overline{\mathbb{F}_q})$$

е $\overline{\mathbb{F}_q}$-линейно влагане.

Отсега нататък, за произволно $d \in \mathbb{N}$, $d < n$ ще означаваме със $\Sigma_d(1, \ldots, n)$ съвкупността на d-елементните подмножества $\gamma = \{\gamma_1, \ldots, \gamma_d\} \subset \{1, \ldots, n\}$ на числата от 1 до n.

Лема 21.6. *Нека $X \subseteq \overline{\mathbb{F}_q}^n$ е афинно многообразие, чийто абсолютен идеал $I(X) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ е породен от полиноми $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ с коефициенти от $\mathbb{F}_q$. В такъв случай, допирателното пространство на Зариски $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ към X в $a \in X$ има минимално разстояние $d(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \geq d + 1$ тогава и само тогава, когато за $\forall \gamma \in \Sigma_d(1, \ldots, n)$ пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ в γ е етално в a.*

Доказателство: Да забележим, че $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d$ точно когато съществува допирателен вектор $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq \mathbb{F}^n_{q^{\delta(a)}}$, чийто носител $\mathrm{Supp}(v) := \{1 \leq i \leq n \,|\, v_i \neq 0\}$ е непразно множество с $\leq d$ елемента. Това е еквивалентно на съществуването на $\gamma \in \Sigma_d(1, \ldots, n)$ с $\emptyset \neq \mathrm{Supp}(v) \subseteq \gamma$ и е в сила точно когато $v \in \ker(\Pi_\gamma) \setminus \{0^n\}$ за пунктирането

$$\Pi_\gamma : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow \Pi_\gamma T_a(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq \mathbb{F}^{n-d}_{q^{\delta(a)}}$$

в γ. Но съгласно забележката след Следствие 20.9,

$$\Pi_\gamma = (d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

съвпада с диференциала на $\Pi_\gamma : X \to \Pi_\gamma(X)$ и условието $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d$ е равносилно на $\ker(d\Pi_\gamma)_a \neq \{0^n\}$ за някое $\gamma \in \Sigma_d(1, \ldots, n)$. С други думи, допирателното пространство на Зариски $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ към X в a има ненулева дума с тегло $\leq d$ тогава и само тогава, когато $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е етално в $a \in X$ за някое $\gamma \in \Sigma_d(1, \ldots, n)$, Q.E.D.

Лема 21.7. *Нека $X \subseteq \overline{\mathbb{F}_q}^n$ е афинно многообразие с абсолютен идеал $I(X) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, породен от $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ за някое $m \geq n$, $\Pi_\gamma : X \to \Pi_\gamma(X)$ е пунктиране в $\gamma \in \Sigma_D(1, \ldots, n)$ и $\mathrm{Etale}(\Pi_\gamma)$ е множеството на точките $a \in X$, в които Π_γ е етален морфизъм. Тогава $\mathcal{E}_\gamma := \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ е Зариски отворено подмножество на X.*

Доказателство: В Твърдение-Определение 20.10 установихме, че множеството $\Pi_\gamma(X)^{\mathrm{smooth}}$ на гладките точки на $\Pi_\gamma(X)$ е непразно и Зариски отворено в $\Pi_\gamma(X)$. Съгласно непрекъснатостта на $\Pi_\gamma : X \to \Pi_\gamma(X)$ относно топологията

на Зариски, $\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ е Зариски отворено подмножество на X. Достатъчно е да провирем, че $\mathrm{Etale}(\Pi_\gamma)$ е Зариски отворено в X, за да докажем лемата. Еквивалентно, твърдим, че $X \setminus \mathrm{Etale}(\Pi_\gamma)$ е Зариски затворено в X. Наистина, $a \in X \setminus \mathrm{Etale}(\Pi_\gamma)$ точно когато $\ker(d\Pi_\gamma)_a \neq \{0^n\}$ и съществува допирателен вектор $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \setminus \{0^n\} \subseteq \mathbb{F}^n_{q^{\delta(a)}} \setminus \{0^n\}$ с носител $\mathrm{Supp}(v) \subseteq \gamma$. Последното е равносилно на линейната зависимост на стълбовете на $\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(a)$, номерирани с γ. Но

$$\mathrm{rk}\frac{\partial(f_1,\ldots,f_m)}{\partial(x_1,\ldots,x_n)}(a) = \mathrm{rk}\frac{\partial f}{\partial x_\gamma}(a) < d$$

точно когато всички минори на матрицата

$$\frac{\partial(f_1,\ldots,f_m)}{\partial(x_{\gamma_1},\ldots,x_{\gamma_d})}(a) \in M_{m\times d}(\mathbb{F}_{q^{\delta(a)}})$$

от ред d са нулеви. С други думи,

$$X \setminus \mathrm{Etale}(\Pi_\gamma) = X \cap Z\left(\det \frac{\partial f_\beta}{\partial x_\gamma} \,\middle|\, \beta \in \Sigma(1,\ldots,m)\right) \tag{21.1}$$

за

$$\frac{\partial f_\beta}{\partial x_\gamma} = \begin{pmatrix} \frac{\partial f_{\beta_1}}{\partial x_{\gamma_1}} & \ldots & \frac{\partial f_{\beta_1}}{\partial x_{\gamma_d}} \\ \ldots & \ldots & \ldots \\ \frac{\partial f_{\beta_d}}{\partial x_{\gamma_1}} & \ldots & \frac{\partial f_{\beta_d}}{\partial x_{\gamma_d}} \end{pmatrix} \quad \text{с} \quad 1 \leq \beta_1 < \ldots < \beta_d \leq m, 1 \leq \gamma_1 < \ldots < \gamma_d \leq n,$$

Q.E.D.

Определение 21.8. *Крайно доминантно разионално изображение $f : X \dashrightarrow\!\!\!\!\!\rightarrow Y$ е сепарабелно, ако крайното разширение $f^*\overline{k}(Y) \subseteq \overline{k}(X)$ на функционалните полета е сепарабелно.*

Твърдение 21.9. **Нека $X \subseteq \overline{\mathbb{F}_q}^n$ е афинно многообразие с абсолютен идеал $I(X) = \langle \varphi_1, \ldots, \varphi_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ за някои $\varphi_1, \ldots, \varphi_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ и $\Pi_\gamma : X \to \Pi_\gamma(X)$ е пунктиране в $\Sigma_d(1, \ldots, n)$.*
(i) Ако пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен сепарабелен морфизъм, то $\mathcal{E}_\gamma := \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ е непразно, Зариски отворено, Зариски гъсто подмножество на X. Във всяка точка $a \in \mathcal{E}_\gamma$ диференциалът

$$(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

е $\mathbb{F}_{q^{\delta(a)}}$-линеен изоморфизъм и $\mathcal{E}_\gamma \subseteq X^{\mathrm{smooth}}$ се състои от гладки точки на X.
(ii) Ако пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е краен морфизъм, то Π_γ не е етално в нито една точка на X, $\mathrm{Etale}(\Pi_\gamma) = \emptyset$.

Доказателство: (i) Ако пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен сепарабелен морфизъм, то $\Pi_\gamma^*\overline{\mathbb{F}_q}(\Pi_\gamma(X)) = \overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(X)$ е крайно сепарабелно разширение. Полето $\overline{\mathbb{F}_q}(X) = \overline{\mathbb{F}_q}(\Pi_\gamma(X))(x_{\gamma_i} + I(X) \,|\, 1 \leq i \leq d)$ се поражда от $x_{\gamma_i} + I(X)$, $1 \leq i \leq d$ над $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ и $\overline{\mathbb{F}_q}(X) \supseteq \overline{\mathbb{F}_q}(\Pi_\gamma(X))$ е крайно сепарабелно разширение точно когато всяко $x_{\gamma_i} + I(X) \in \overline{\mathbb{F}_q}(X)$ е сепарабелно над $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$. Ако $g_i \in \overline{\mathbb{F}_q}(\Pi_\gamma(X))[x_{\gamma_i}]$ е минималният полином на $x_{\gamma_i} + I(X)$ над $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$, то твърдим, че $\frac{\partial g_i}{\partial x_{\gamma_i}} \notin I(\Pi_\gamma(X))\overline{\mathbb{F}_q}(\Pi_\gamma(X))$. В противен случай, g_i дели $\frac{\partial g_i}{\partial x_{\gamma_i}} \in I(X)$ в $\overline{\mathbb{F}_q}(\Pi_\gamma(X))[x_{\gamma_i}]$ и съгласно $\deg_{x_{\gamma_i}} \frac{\partial g_i}{\partial x_{\gamma_i}} < \deg_{x_{\gamma_i}} g_i$ следва $\frac{\partial g_i}{\partial x_{\gamma_i}} \equiv 0$. Това противоречи на сепарабелността на $x_{\gamma_i} + I(X)$ над $\overline{\mathbb{F}_q}(\Pi_\gamma)$ и доказва, че $\frac{\partial g_i}{\partial x_{\gamma_i}} \notin I(\Pi_\gamma(X))\overline{\mathbb{F}_q}(\Pi_\gamma(X))$. Означаваме с $\neg\gamma = \{1, \ldots, n\} \setminus \gamma$ допълнението на γ и забелязваме, че съществуват полиноми $f_i \in \overline{\mathbb{F}_q}[x_{\neg\gamma}, x_{\gamma_i}]$,

$h_i \in \overline{\mathbb{F}_q}[x_{\neg\gamma}]$, така че

$$g_i = \frac{f_i + I(\Pi_\gamma(X))}{h_i + I(\Pi_\gamma(X))}.$$

Тук $f_i \in I(X)$, $\frac{\partial f_i}{\partial x_{\gamma_i}} \notin I(X)$ и $h_i \notin I(\Pi_\gamma(X)) \lhd \overline{\mathbb{F}_q}[x_{\neg\gamma}]$.

Съгласно $f_1, \ldots, f_d \in I(X)$, допирателното пространство на Зариски $T_a(X, \overline{\mathbb{F}_q})$ към X в $a \in X$ над $\overline{\mathbb{F}_q}$ се съдържа в пространството от решения T'_a на хомогенната линейна система с матрица от коефициенти

$$\frac{\partial(f_1, \ldots, f_d)}{\partial(x_\gamma, x_{\neg\gamma})}(a) = \begin{pmatrix} \frac{\partial f_1}{\partial x_{\gamma_1}}(a) & 0 & \ldots & 0 & \frac{\partial f_1}{\partial x_{\delta_1}}(a) & \ldots & \frac{\partial f_1}{\partial x_{\delta_{n-d}}}(a) \\ 0 & \frac{\partial f_2}{\partial x_{\gamma_2}}(a) & \ldots & 0 & \frac{\partial f_2}{\partial x_{\delta_1}}(a) & \ldots & \frac{\partial f_2}{\partial x_{\delta_{n-d}}}(a) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \frac{\partial f_d}{\partial x_{\gamma_d}}(a) & \frac{\partial f_d}{\partial x_{\delta_1}}(a) & \ldots & \frac{\partial f_d}{\partial x_{\delta_{n-d}}}(a) \end{pmatrix}$$

за $\delta = \{\delta_1, \ldots, \delta_{n-d}\} = \neg\gamma$. Стълбовете на горната Якобиева матрица са наредени така, че първите d от тях отговарят на формалните производни относно $x_{\gamma_1}, \ldots, x_{\gamma_d}$ в a, а последните $n-d$ се състоят от формалните производни относно $x_{\delta_1}, \ldots, x_{\delta_{n-d}}$ в a. Ако $a \in X \setminus Z\left(\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_i}\right)$, то за $\forall 1 \leq i \leq d$ съществува хомогенна линейна функция $v_{\gamma_i}(v_{\neg\gamma}) = v_{\gamma_i}(v_{\delta_1}, \ldots, v_{\delta_{n-d}})$, така че $v = (v_1, \ldots, v_n) \in T'_a$ точно когато $v_{\gamma_i} = v_{\gamma_i}(v_{\delta_1}, \ldots, v_{\delta_{n-d}})$ за $\forall 1 \leq i \leq d$. Следователно пунктирането

$$\Pi_\gamma : T'_a \longrightarrow \Pi_\gamma(T'_a)$$

е взаимно еднозначно върху образа си и се ограничава до $\overline{\mathbb{F}_q}$-линейни влагания

$$\Pi_\gamma = (d\Pi_\gamma)_a : T_a(X, \overline{\mathbb{F}_q}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \overline{\mathbb{F}_q}),$$

съответно,

$$\Pi_\gamma = (d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}).$$

С това проверихме, че $X \setminus Z\left(\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_{\gamma_i}}\right) \subseteq \mathrm{Etale}(\Pi_\gamma)$. Достатъчно е да установим, че $X \setminus Z\left(\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_{\gamma_i}}\right) \neq \emptyset$, за да получим, че Зариски отвореното подмножество $\mathrm{Etale}(\Pi_\gamma) \subseteq X$ е непразно, а оттам и сечението му

$$\mathcal{E}_\gamma = \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$$

с непразното Зариски отворено подмножество $\Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}}) \subseteq X$ е непразно. Но допускането $X \setminus Z\left(\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_{\gamma_i}}\right) = \emptyset$ води до $X \subseteq Z\left(\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_{\gamma_i}}\right)$, откъдето

$$\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_{\gamma_i}} \in IZ\left(\prod_{i=1}^{d} \frac{\partial f_i}{\partial x_{\gamma_i}}\right) \subseteq I(X).$$

Съгласно простотата на идеала $I(X) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, това изисква $\frac{\partial f_i}{\partial x_{\gamma_i}} \in I(X)$ за някое $1 \leq i \leq d$. Противоречието доказва, че ако $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен сепарабелен морфизъм, то $\mathcal{E}_\gamma \neq \emptyset$.

Във всяка точка $a \in \mathcal{E}_\gamma = \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$ е изпълнено неравенството $\dim X \leq \dim_{\mathbb{F}_{q^{\delta(a)}}} T_a(X, \mathbb{F}_{q^{\delta(a)}})$, съгласно Твърдение-Определение 20.10. Еталността на пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ в $a \in X$ дава

$$\dim_{\mathbb{F}_{q^{\delta(a)}}} T_a(X, \mathbb{F}_{q^{\delta(a)}}) \leq \dim_{\mathbb{F}_{q^{\delta(a)}}} T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}).$$

Сега $\Pi_\gamma(a) \in \Pi_\gamma(X)^{\rm smooth}$ гарантира, че $\dim_{\mathbb{F}_{q^{\delta(a)}}} T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X)$. Доминантното регулярно изображение $\Pi_\gamma : X \to \Pi_\gamma(X)$ индуцира влагане $\Pi_\gamma^* \overline{\mathbb{F}_q}(\Pi_\gamma(X)) = \overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(X)$ на функционалните полета, така че

$$\dim \Pi_\gamma(X) = \mathrm{trdeg}_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}(\Pi_\gamma(X)) \leq \mathrm{trdeg}_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}(X) = \dim X.$$

По този начин, от

$$\dim X \leq \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \leq \dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X) \leq \dim X$$

следва

$$\dim_{\mathbb{F}_{q^{\delta(a)}}} T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim_{\mathbb{F}_{q^{\delta(a)}}} T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X) = \dim X.$$

В резултат, $a \in X^{\rm smooth}$ се оказва гладка точка и $\mathcal{E}_\gamma \subseteq X^{\rm smooth}$. Диференциалът $(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \to T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ е $\mathbb{F}_{q^{\delta(a)}}$-линеен изоморфизъм във всяка точка $a \in \mathcal{E}_\gamma$ и $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен морфизъм, защото $\dim X = \dim \Pi_\gamma(X)$ и разширението $\Pi_\gamma^* \overline{\mathbb{F}_q}(\Pi_\gamma(X)) = \overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(X)$ е крайно.
(ii) Ако допуснем, че $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е краен морфизъм и $\mathrm{Etale}(\Pi_\gamma) \neq \emptyset$, то $\mathcal{E}_\gamma = \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\rm smooth}) \neq \emptyset$. Горните разсъждения установяват, че наличието на точка $a \in \mathcal{E}_\gamma$ води до крайност на морфизма $\Pi_\gamma : X \to \Pi_\gamma(X)$. Това доказва $\mathrm{Etale}(\Pi_\gamma) = \emptyset$ за $\forall \gamma \in \Sigma_d(1, \ldots, n)$, за които $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е краен морфизъм, Q.E.D.

Следствие 21.10. *Нека $X \subset \overline{\mathbb{F}_q}^n$ е афинно многообразие с абсолютен идеал $I(X) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ за някои $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, а $X^{(\leq d)}$, $X^{(d)}$, $X^{(\geq d+1)}$ са множествата на точките $a \in X$, в които допирателното пространство на Зариски $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ е с минимално разстояние $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d$, съответно $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) = d$ или $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \geq d+1$.*
(i) Подмножеството

$$X^{(\leq d)} = X \cap Z\left(\prod_{\gamma \in \Sigma_d(1,\ldots,n)} \frac{\partial f_{\varphi(\gamma)}}{\partial x_\gamma} \,\middle|\, \forall \varphi : \Sigma_d(1, \ldots, n) \to \Sigma_d(1, \ldots, m) \right)$$

на X е Зариски затворено.
(ii) Ако за $\forall \gamma \in \Sigma_d(1, \ldots, n)$ пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен сепарабелен морфизъм, то $X^{(\geq d+1)}$ е непразно, Зариски отворено, Зариски гъсто подмножество на X.
(iii) Ако за някое $\gamma \in \Sigma_d(1, \ldots, n)$ пунктирането $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е краен морфизъм, то $X^{(\leq d)} = X$.

Доказателство: (i) Съгласно Лема 21.6, $a \in X^{(\leq d)}$ тогава и само тогава, когато $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е етално в a за някое $\gamma \in \Sigma_d(1, \ldots, n)$. Оттук,

$$X^{(\leq d)} = \cup_{\gamma \in \Sigma_d(1,\ldots,n)} [X \setminus \mathrm{Etale}(\Pi_\gamma)] =$$
$$= \cup_{\gamma \in \Sigma_d(1,\ldots,n)} \left[X \cap Z\left(\frac{\partial f_\beta}{\partial x_\gamma} \,\middle|\, \beta \in \Sigma_d(1, \ldots, n) \right) \right],$$

вземайки предвид (21.1). В резултат,

$$X^{(\leq d)} = X \cap \left[\cup_{\gamma \in \Sigma_d(1,\ldots,n)} Z\left(\frac{\partial f_\beta}{\partial x_\gamma} \,\middle|\, \beta \in \Sigma_d(1, \ldots, m) \right) \right] =$$
$$= X \cap Z\left(\prod_{\gamma \in \Sigma_d(1,\ldots,n)} \frac{\partial f_{\varphi(\gamma)}}{\partial x_\gamma} \,\middle|\, \varphi : \Sigma_d(1, \ldots, n) \to \Sigma_d(1, \ldots, m) \right)$$

за всички изображения

$$\varphi : \Sigma_d(1, \ldots, n) \longrightarrow \Sigma_d(1, \ldots, m)$$

на съвкупността $\Sigma_d(1,\dots,n)$ на d-елементните подмножества $\gamma=\{\gamma_1,\dots,\gamma_d\}$ на $\{1,\dots,n\}$ в съвкупността $\Sigma_d(1,\dots,m)$ на d-елементните подмножества $\varphi(\gamma)=\beta=\{\beta_1,\dots,\beta_d\}$ на $\{1,\dots,m\}$.
(ii) От (i) следва, че $X^{(\geq d+1)}=X\setminus X^{(\leq d)}$ е Зариски отворено подмножество на X. Достатъчно е да докажем, че $X^{(\geq d+1)}\neq\emptyset$ е непразно, за да получим, че $X^{(\geq d+1)}$ е Зариски гъсто в X. Съгласно Твърдение 21.9 (i), ако $\Pi_\gamma: X\to\Pi_\gamma(X)$ е краен сепарабелен морфизъм за $\forall\gamma\in\Sigma_d(1,\dots,n)$, то $\mathrm{Etale}(\Pi_\gamma)\neq\emptyset$ е непразно, Зариски отворено, Зариски гъсто подмножество на X. По Лема 21.6, оттук следва, че Зариски отвореното подмножество

$$X^{(\geq d+1)}=\cap_{\gamma\in\Sigma_d(1,\dots,n)}\mathrm{Etale}(\Pi_\gamma)\neq\emptyset$$

е непразно, а оттам и Зариски гъсто.
(iii) Ако $\Pi_\gamma: X\to\Pi_\gamma(X)$ не е краен морфизъм за някое $\gamma\in\Sigma_d(1,\dots,n)$, то съгласно Твърдение 21.9, $\mathrm{Etale}(\Pi_\gamma)=\emptyset$. Следователно

$$X^{(\geq d+1)}=\cap_{\beta\in\Sigma_d(1,\dots,n)}\mathrm{Etale}(\Pi_\beta)=\emptyset$$

и $X^{(\leq d)}=X\setminus X^{(\geq d+1)}=X$, Q.E.D.

Лема 21.11. *Нека $G=\{g_1,\dots,g_s\}$ е базис на Groebner на абсолютния идеал $I(X)\lhd\overline{\mathbb{F}_q}[x_1,\dots,x_n]$ на афинно многообразие $X\subseteq\overline{\mathbb{F}_q}^n$ относно лексикографска наредба с $x_\gamma>x_{\neg\gamma}$ и $G_o:=G\cap\overline{\mathbb{F}_q}[x_{\neg\gamma}]$. Тогава G_o е базис на Groebner на абсолютния идеал*

$$I(\Pi_\gamma(X))=I(X)\cap\overline{\mathbb{F}_q}[x_{\neg\gamma}]$$

на образа $\Pi_\gamma(X)$ на X под действие на пунктирането $\Pi_\gamma: X\to\Pi_\gamma(X)$ в $\gamma\in\Sigma_d(1,\dots,n)$.

Доказателство: Съгласно Теоремата за елиминация, G_o е базис на Groebner на елиминационния идеал $I_o:=I(X)\cap\overline{\mathbb{F}_q}[x_{\neg\gamma}]$ на $I(X)$. Теоремата за затворената обвивка гласи съвпадението $Z_{n-d}(I_o)=\overline{\Pi_\gamma(X)}$ на афинното алгебрично множество $Z_{n-d}(I_o)\subseteq\overline{\mathbb{F}_q}^{n-d}$ на $I_o\lhd\overline{\mathbb{F}_q}[x_{\neg\gamma}]$ в $\overline{\mathbb{F}_q}^{n-d}$ със Зариски затворената обвивка $\overline{\Pi_\gamma(X)}$ на $\Pi_\gamma(X)\subseteq\overline{\mathbb{F}_q}^{n-d}$. Абсолютният идеал

$$I(\Pi_\gamma(X))=I(\overline{\Pi_\gamma(X)})=IZ_{n-d}(I_o)=r(I_o)$$

съвпада с радикала $r(I_o)\lhd\overline{\mathbb{F}_q}[x_{\neg\gamma}]$ на I_o. Остава да докажем, че $r(I_o)=I_o$ е радикален идеал. Наистина, ако $\varphi\in r(I_o)\lhd\overline{\mathbb{F}_q}[x_{\neg\gamma}]$, то $\varphi^N\in I_o\subset I(X)$ за някое $N\in\mathbb{N}$. Простотата на абсолютния идеал $I(X)\lhd\overline{\mathbb{F}_q}[x_1,\dots,x_n]$ на афинното многообразие $X\subseteq\overline{\mathbb{F}_q}^n$ изисква $\varphi\in I(X)$. Следователно $\varphi\in I(X)\cap\overline{\mathbb{F}_q}[x_{\neg\gamma}]=I_o$ и $r(I_o)=I_o$, Q.E.D.
Следващото твърдение дава критерий за крайност и сепарабелност на пунктиране $\Pi_\gamma: X\to\Pi_\gamma(X)$ на езика на базиси на Groebner.

Твърдение 21.12. *Нека $X\subseteq\overline{\mathbb{F}_q}^n$ е афинно многообразие и $\Pi_\gamma: X\to\Pi_\gamma(X)$ е пунктиране на X в някое $\gamma\in\Sigma_d(1,\dots,n)$. За произволно $1\leq i\leq d$ разглеждаме базис на Groebner $G_{\gamma\setminus\gamma_i,\gamma_i,\neg\gamma}$ на $I(X)\lhd\overline{\mathbb{F}_q}[x_1,\dots,x_n]$ относно лексикографска наредба с $x_{\gamma\setminus\gamma_i}>x_{\gamma_i}>x_{\neg\gamma}$, както и сеченията $G_i:=G_{\gamma\setminus\gamma_i,\gamma_i,\neg\gamma}\cap\overline{\mathbb{F}_q}[x_{\gamma_i},x_{\neg\gamma}]$, $G_o:=G_{\gamma\setminus\gamma_i,\gamma_i,\neg\gamma}\cap\overline{\mathbb{F}_q}[x_{\neg\gamma}]$ с полиномите, не зависещи от $x_{\gamma\setminus\gamma_i}$, съответно, от x_γ.*
(i) Пунктирането $\Pi_\gamma: X\to\Pi_\gamma(X)$ е краен морфизъм тогава и само тогава, когато разликите $G_i\setminus G_o\neq\emptyset$ са непразни множества за $\forall 1\leq i\leq d$.
(ii) Ако за $\forall 1\leq i\leq d$ съществува полином $a_i\in G_i\setminus G_o$, чиято формална производна $\frac{\partial a_i}{\partial x_{\gamma_i}}\in\overline{\mathbb{F}_q}[x_{\gamma_i},x_{\neg\gamma}]$ има ненулев остатък $\overline{\frac{\partial a_i}{\partial x_{\gamma_i}}}^{G_i}\neq 0$ при деление с G_i, то пунктирането $\Pi_\gamma: X\to\Pi_\gamma(X)$ е краен сепарабелен морфизъм.

Доказателство: (i) Ако за $\forall 1 \leq i \leq d$ съществува полином $a_i \in G_i \setminus G_o$, то $a_i \in \overline{\mathbb{F}_q}[x_{\gamma_i}, x_{\neg\gamma}] \setminus \overline{\mathbb{F}_q}[x_{\neg\gamma}]$ зависи от x_{γ_i} и задава алгебрична зависимост на $x_{\gamma_i} + I(X)$ над $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$. Затова разширението $\Pi_\gamma^* \overline{\mathbb{F}_q}(\Pi_\gamma(X)) = \overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(X)$ е крайно и $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен морфизъм.
Обратно, да допуснем че $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен морфизъм, но съществува $1 \leq i \leq d$ с $G_i \setminus G_o = \emptyset$. Тогава от $G_o \subseteq G_i$ следва $G_i = G_o$. Зариски затворената обвивка

$$\overline{\Pi_{\gamma\setminus\gamma_i}(X)} = Z_{n-d+1} I(\Pi_{\gamma\setminus\gamma_i}(X)) = Z_{n-d+1}(G_o) = \overline{\mathbb{F}_q} \times Z_{n-d}(G_o),$$

защото G_o поражда $I(\Pi_{\gamma\setminus\gamma_i}(X)) \lhd \overline{\mathbb{F}_q}[x_{\gamma_i}, x_{\neg\gamma}]$. Аналогично,

$$\overline{\Pi_\gamma(X)} = Z_{n-d} I(\Pi_\gamma(X)) = Z_{n-d}(G_o),$$

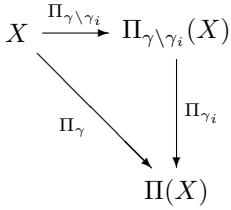
откъдето

$$\overline{\Pi_{\gamma\setminus\gamma_i}(X)} = \overline{\mathbb{F}_q} \times \overline{\Pi_\gamma(X)}.$$

Размерността

$$\dim \Pi_{\gamma\setminus\gamma_i}(X) = \dim \overline{\Pi_{\gamma\setminus\gamma_i}(X)} = 1 + \dim \overline{\Pi_\gamma(X)} = 1 + \dim \Pi_\gamma(X),$$

така че пунктирането $\Pi_{\gamma_i} : \Pi_{\gamma\setminus\gamma_i}(X) \to \Pi_\gamma(X)$ не е краен морфизъм и разширението $\overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subset \overline{\mathbb{F}_q}(\Pi_{\gamma\setminus\gamma_i}(X))$ е безкрайно. Разлагането



на Π_γ индуцира влаганията

$$\overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subset \overline{\mathbb{F}_q}(\Pi_{\gamma\setminus\gamma_i}(X)) \subseteq \overline{\mathbb{F}_q}(X)$$

на съответните функционални полета изисква $[\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_\gamma(X))] = \infty$. С това доказахме, че ако $G_i = G_o$ за някое $1 \leq i \leq d$, то $\Pi_\gamma : X \to \Pi_\gamma(X)$ не е краен морфизъм. С други думи, ако $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен морфизъм, то $G_i \setminus G_o \neq \emptyset$ за $\forall 1 \leq i \leq d$.

(ii) Да допуснем, че за $\forall 1 \leq i \leq d$ съществува $a_i \in G_i \setminus G_o$ с $\overline{\frac{\partial a_i}{\partial x_{\gamma_i}}}^{G_i} \neq 0$, но крайното разширение $\overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(X)$ не е сепарабелно. Тогава за някое $1 \leq j \leq d$ минималният полином $g_j \in \overline{\mathbb{F}_q}(\Pi_\gamma(X))[x_{\neg\gamma}]$ на $x_{\gamma_j} + I(X)$ над $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ има нулева формална производна $\frac{\partial g_j}{\partial x_{\gamma_j}} \equiv 0$. Полиномът $a_j \in G_j \setminus G_o$ се дели на $g_j \in \overline{\mathbb{F}_q}(\Pi_\gamma(X))[x_{\gamma_j}]$ с частно $\varphi_j \in \overline{\mathbb{F}_q}(\Pi_\gamma(X))[x_{\gamma_j}]$ и

$$\frac{\partial a_j}{\partial x_{\gamma_j}} = \frac{\partial (g_j \varphi_j)}{\partial x_{\gamma_j}} = g_j \frac{\partial \varphi_j}{\partial x_{\gamma_j}}$$

се анулира в $x_{\gamma_j} + I(X)$. Следователно $\frac{\partial a_j}{\partial x_{\gamma_j}} \in I(X) \cap \overline{\mathbb{F}_q}[x_{\gamma_j}, x_{\neg\gamma}] = I(\Pi_{\gamma\setminus\gamma_j}(X))$. Съгласно Лема 21.11, G_j е базис на Groebner на $I(\Pi_{\gamma\setminus\gamma_j}(X))$ и полиномът $\frac{\partial a_j}{\partial x_{\gamma_j}} \in I(\Pi_{\gamma\setminus\gamma_j}(X))$ има нулев остатък $\overline{\frac{\partial a_j}{\partial x_{\gamma_j}}}^{G_j} = 0$ при деление с G_j. Това противоречи на предположението $\overline{\frac{\partial a_j}{\partial x_{\gamma_j}}}^{G_j} \neq 0$ и доказва твърдението, Q.E.D.

Изчислителна задача 21.13. *Да се намери афинно многообразие $X \subset \overline{\mathbb{F}_q}^n$ с непразно, Зариски гъсто $X^{(\geq d+1)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \geq d+1\}$.*

Изчислителна задача 21.14. *Да се намери афинно многообразие* $X \subset \overline{\mathbb{F}_q}^n$ *с* $X^{(\leq d)} = X$ *за* $X^{(\leq d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d\}$.

Твърдение 21.15. *Нека* $X \subseteq \overline{\mathbb{F}_q}^n$ *е* k*-мерно афинно многообразие,* $1 \leq i \leq n$ *е такова естествено число, ненадминаващо* n*, че за всички* $\gamma \in \Sigma_d(1, \ldots, n)$ *с* $i \in \gamma$ *пунктирането* $\Pi_\gamma : X \to \Pi_\gamma(X)$ *е краен сепарабелен морфизъм и пунктирането* $\Pi_\beta : X \to \Pi_\beta(X)$ *не е краен морфизъм за някое* $\beta \in \Sigma_d(1, \ldots, n)$ *с* $i \notin \beta$*. Тогава пунктирането* $\Pi_i : X \to \Pi_i(X)$ *в* i *е краен сепарабелен морфизъм, крайните допирателни пространства към* X *в обща точка са* $[n.k.d]$*-кодове, а крайните допирателни пространства към* $\Pi_i(X)$ *в обща точка са* $[n-1, k, d]$*-кодове.*

Доказателство: За произволно $\alpha \in \Sigma_{d-1}(1, \ldots, n)$ с $i \notin \alpha$ разглеждаме комутативната диаграма

$$\begin{array}{ccc} X & \xrightarrow{\Pi_i} & \Pi_i(X) \\ \downarrow{\scriptstyle \Pi_\alpha} & & \downarrow{\scriptstyle \Pi_\alpha} \\ \Pi_\alpha(X) & \xrightarrow{\Pi_i} & \Pi_{\alpha\cup i}(X) \end{array} .$$

По предположение, $\Pi_\gamma : X \to \Pi_\gamma(X)$ са крайни сепарабелни морфизми за $\forall \gamma = \alpha \cup \{i\} \in \Sigma_d(1, \ldots, n)$ с $i \in \gamma$. Следователно $\overline{\mathbb{F}_q}(\Pi_{\alpha\cup i}(X)) \subseteq \overline{\mathbb{F}_q}(X)$ е крайно сепарабелно разширение. От

$$\overline{\mathbb{F}_q}\Pi_{\alpha\cup i}(X)) \subseteq \overline{\mathbb{F}_q}(\Pi_i(X)) \subseteq \overline{\mathbb{F}_q}(X)$$

следва, че $\overline{\mathbb{F}_q}(\Pi_{\alpha\cup i}(X)) \subseteq \overline{\mathbb{F}_q}(\Pi_i(X))$ и $\overline{\mathbb{F}_q}(\Pi_i(X)) \subseteq \overline{\mathbb{F}_q}(X)$ са крайни сепарабелни разширения. Съгласно Твърдение 21.9 (i), щом $\Pi_\alpha : \Pi_i(X) \to \Pi_{\alpha\cup i}(X)$ са крайни сепарабелни морфизми за $\forall \alpha \in \Sigma_{d-1}(1, \ldots, n)$ с $i \notin \alpha$, Зариски отвореното подмножество

$$\Pi_i(X)^{(\geq d)} := \{\Pi_i(a) \in \Pi_i(X) \mid d(T_{\Pi_i(a)}(\Pi_i(X), \mathbb{F}_{q^{\delta(\Pi_i(a))}})) \geq d\}$$

е непразно, а оттам и Зариски гъсто. Освен това, пунктирането $\Pi_i : X \to \Pi_i(X)$ е краен сепарабелен морфизъм. От

$$\overline{\mathbb{F}_q}(\Pi_{\alpha\cup i}(X)) \subseteq \overline{\mathbb{F}_q}(\Pi_\alpha(X)) \subseteq \overline{\mathbb{F}_q}(X)$$

следва, че пунктиранията $\Pi_\alpha : X \to \Pi_\alpha(X)$ в $\alpha \in \Sigma_{d-1}(1, \ldots, n)$ с $i \notin \alpha$ са крайни сепарабелни морфизми. Ако $\alpha \in \Sigma_{d-1}(1, \ldots, n)$ и $i \in \alpha$, то за $\forall j \in \{1, \ldots, n\} \setminus \alpha$ имаме $\gamma = \alpha \cup \{j\} \in \Sigma_d(1, \ldots, n)$ с $i \in \gamma$. По предположение, $\Pi_\gamma : X \to \Pi_\gamma(X)$ е краен сепарабелен морфизъм. Разлагането

$$\begin{array}{ccc} X & \xrightarrow{\Pi_\alpha} & \Pi_\alpha(X) \\ & {\scriptstyle \Pi_\gamma}\searrow & \downarrow{\scriptstyle \Pi_j} \\ & & \Pi_\gamma(X) \end{array}$$

на Π_γ в композиция $\Pi_\gamma = \Pi_j \Pi_\alpha$ индуцира включванията

$$\overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(\Pi_\alpha(X)) \subseteq \overline{\mathbb{F}_q}(X)$$

на съответните функционални полета. От това, че $\overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subseteq \overline{\mathbb{F}_q}(X)$ е крайно сепарабелно разширение следва, че $\overline{\mathbb{F}_q}(\Pi_\alpha(X)) \subseteq \overline{\mathbb{F}_q}(X)$ е крайно сепарабелно разширение. Това доказва, че $\Pi_\alpha : X \to \Pi_\alpha(X)$ са крайни сепарабелни морфизми за $\forall \alpha \in \Sigma_{d-1}(1, \ldots, n)$ с $i \in \alpha$. Щом $\Pi_\alpha : X \to \Pi_\alpha(X)$ са крайни сепарабелни морфизми за $\forall \alpha \in \Sigma_{d-1}(1, \ldots, n)$, Зариски отвореното подмножество $X^{(\geq d)} \subseteq X$ е непразно, а оттам и Зариски гъсто в X.

По предположение съществува $\beta \in \Sigma_d(1,\dots,n)$ с $i \notin \beta$, така че $\Pi_\beta : X \to \Pi_\beta(X)$ не е краен морфизъм. Съгласно Следствие 21.10 (iii) имаме $X^{(\leq d)} = X$. Следователно $X^{(\geq d)} = X^{(d)} \subseteq X$ е Зариски гъсто в X. Разглеждаме комутативната диаграма

$$\begin{array}{ccc} X & \xrightarrow{\Pi_i} & \Pi_i(X) \\ \downarrow{\scriptstyle \Pi_\beta} & & \downarrow{\scriptstyle \Pi_\beta} \\ \Pi_\beta(X) & \xrightarrow{\Pi_i} & \Pi_{\beta\cup i}(X) \end{array},$$

в която пунктирането $\Pi_{\beta\cup i} : X \to \Pi_{\beta\cup i}(X)$ не е краен морфизъм, защото степента

$$[\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_{\beta\cup i}(X))] = [\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_\beta(X))][\overline{\mathbb{F}_q}(\Pi_\beta(X)) : \overline{\mathbb{F}_q}(\Pi_{\beta\cup i}(X))] = \infty$$

е безкрайна съгласно $[\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_\beta(X))] = \infty$. Сега

$$\infty = [\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_{\beta\cup i}(X))] = [\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_i(X))][\overline{\mathbb{F}_q}(\Pi_i(X)) : \overline{\mathbb{F}_q}(\Pi_{\beta\cup i}(X))]$$

с $[\overline{\mathbb{F}_q}(X) : \overline{\mathbb{F}_q}(\Pi_i(X))] < \infty$ показва, че $\overline{\mathbb{F}_q}(\Pi_i(X)) \supseteq \overline{\mathbb{F}_q}(\Pi_{\beta\cup i}(X))$ е безкрайно разширение и $\Pi_\beta : \Pi_i(X) \to \Pi_{\beta\cup i}(X)$ не е краен морфизъм. Прилагаме Следствие 21.10 и получаваме, че $\Pi_i(X)^{(\leq d)} = \Pi_i(X)$. В резултат, $\Pi_i(X)^{(\geq d)} = \Pi_i(X)^{(d)} \subseteq \Pi_i(X)$ е Зариски гъсто в $\Pi_i(X)$, Q.E.D.

Изчислителна задача 21.16. *Да се намери афинно многообразие $X \subseteq \overline{\mathbb{F}_q}^n$ с размерност k, чиито крайни допирателни кодове в обща точка имат минимално разстояние d и такова число $1 \leq i \leq n$, че $\Pi_i : X \to \Pi_i(X) \subseteq \overline{\mathbb{F}_q}^{n-1}$ е краен сепарабелен морфизъм и общите допирателни кодове към $\Pi_i(X)$ са с минимално разстояние d.*

3. Едновременно декодиране на допирателни кодове чрез предварително намиране на носителя на грешката.

Определение 21.17. *Дума $w \in \mathbb{F}_q^n$ има единствена грешка с носител $\gamma \in \Sigma_t(1,\dots,n)$ относно $\mathbb{F}_q$-линеен код $C \subset \mathbb{F}_q^n$, ако съществува единствена дума $e \in \mathbb{F}_q^n$ с носител* $\mathrm{Supp}(e) := \{1 \leq i \leq n \,|\, e_i\} \subseteq \gamma$, *така че $w - e = c \in C$.*

Нека $H = \begin{pmatrix} H_1 & \dots & H_n \end{pmatrix} \in M_{m\times n}(\mathbb{F}_q)$ е проверочна матрица на $\mathbb{F}_q$-линеен код $C \subset \mathbb{F}_q^n$ със стълбове $H_i \in M_{m\times 1}(\mathbb{F}_q)$. Тогава произволна грешка $e \in \mathbb{F}_q^n$ на дума $w \in \mathbb{F}_q^n$ относно $C \subset \mathbb{F}_q^n$ е решение на системата линейни уравнения

$$H\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = H\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix},$$

защото

$$H\begin{pmatrix} c_1 \\ \dots \\ c_n \end{pmatrix} = 0_{m\times 1}$$

за произволна дума $c = (c_1,\dots,c_n) \in C$. Ако $w \in \mathbb{F}_q^n$ има единствена грешка $e \in \mathbb{F}_q^n$ с $\mathrm{Supp}(e) \subseteq \gamma$, то $\Pi_{\neg\gamma}(e) = (e_{\gamma_1},\dots,e_{\gamma_t})$ е единственото решение на системата

$$\begin{pmatrix} H_{\gamma_1} & \dots & H_{\gamma_t} \end{pmatrix}\begin{pmatrix} e_{\gamma_1} \\ \vdots \\ e_{\gamma_t} \end{pmatrix} = H\begin{pmatrix} w_1 \\ \dots \\ w_n \end{pmatrix}$$

от m линейни уравнения с t неизвестни. Съгласно $\Pi_\gamma(e) = 0^{n-t}$, грешката $e \in \mathbb{F}_q^n$ се определя еднозначно от $\Pi_{\neg\gamma}(e) = (e_{\gamma_1},\dots,e_{\gamma_t})$.

Твърдение 21.18. *Нека $X \subset \overline{\mathbb{F}_q}^n$ е афинно многообразие, а $\Pi_\gamma : X \to \Pi_\gamma(X)$ е пунктиране на X в $\gamma \in \Sigma_t(1,\ldots,n)$. За $\forall 1 \leq i \leq t$ разглеждаме базис на Groebner $G_{\gamma\setminus\gamma_i,\gamma_i,\neg\gamma} \subset \mathbb{F}_q[x_1,\ldots,x_n]$ на $I(X) \lhd \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ относно лексикографска наредба с $x_{\gamma\setminus\gamma_i} > x_{\gamma_i} > x_{\neg\gamma}$, базиса на Groebner $G_i := G_{\gamma\setminus\gamma_i,\gamma_i,\neg\gamma} \cap \mathbb{F}_q[x_{\gamma_i}, x_{\neg\gamma}]$ на $I(\Pi_{\gamma\setminus\gamma_i}(X)) = I(X) \setminus \mathbb{F}_q[x_{\gamma_i}, x_{\neg\gamma}]$ и базиса на Groebner $G_o := G_{\gamma\setminus\gamma_i,\gamma_i,\neg\gamma} \cap \mathbb{F}_q[x_{\neg\gamma}]$ на $I(\Pi_\gamma(X)) = I(X) \cap \overline{\mathbb{F}_q}[x_{\neg\gamma}]$. Предполагаме, че за всяко $1 \leq i \leq t$ съществува полином $g_i \in G_i \setminus G_o$, чиято формална производна $\frac{\partial g_i}{\partial x_{\gamma_i}} \in \mathbb{F}_q[x_{\gamma_i}, x_{\neg\gamma}]$ има ненулев остатък $\overline{\frac{\partial g_i}{\partial x_{\gamma_i}}}^{G_i} \neq 0$ при деление с G_i и $g_1,\ldots,g_t, I(\Pi_\gamma(X))$ пораждат абсолютния идеал $I(X) \lhd \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ на X. Тогава $X \setminus Z\left(\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}}\right)$ е непразно, Зариски отворено, Зариски гъсто подмножество на X и във всяка точка $a \in X \setminus Z\left(\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}}\right)$, дума $w \in \mathbb{F}^n_{q^{\delta(a)}}$ има единствена грешка с носител γ относно $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ тогава и само тогава, когато $\Pi_\gamma(w) \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ се допира до $\Pi_\gamma(X)$ в $\Pi_\gamma(a)$.*

Доказателство: Ако допуснем, че $X \setminus Z\left(\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}}\right) = \emptyset$, то $X \subseteq Z\left(\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}}\right)$, откъдето

$$\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}} \in IZ\left(\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}}\right) \subseteq I(X).$$

Поради простотата на идеала $I(X) \lhd \overline{\mathbb{F}_q}[x_1,\ldots,x_n]$ на неприводимото афинно алгебрично множество $X \subset \overline{\mathbb{F}_q}^n$ получаваме $\frac{\partial g_i}{\partial x_{\gamma_i}} \in I(X)$ за някой индекс $1 \leq i \leq t$. Полиномът $\frac{\partial g_i}{\partial x_{\gamma_i}} \in I(X) \cap \overline{\mathbb{F}_q}[x_{\gamma_i}, x_{\neg\gamma}] = I(\Pi_{\gamma\setminus\gamma_i}(X))$ има нулев остатък $\overline{\frac{\partial g_i}{\partial x_{\gamma_i}}}^{G_i} = 0$ при деление с базиса на Groebner G_i на $I(\Pi_{\gamma\setminus\gamma_i}(X))$. Това противоречи на предположението и доказва, че Зариски отвореното подмножество $X \setminus Z\left(\prod_{i=1}^t \frac{\partial g_i}{\partial x_{\gamma_i}}\right) \subseteq X$ е непразно, а оттам и Зариски гъсто.

В произволна точка $a \in X \setminus Z\left(\frac{\partial g_i}{\partial x_{\gamma_i}}\right)$ твърдим, че всеки допирателен вектор $v_{\neg\gamma} \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ към $\Pi_\gamma(X)$ в $\Pi_\gamma(a)$ има единствено продължение до допирателен вектор $v = (v_\gamma, v_{\neg\gamma}) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ към X в a. За целта забелязваме, че от $I(\Pi_\gamma(X)) = I(X) \cap \overline{\mathbb{F}_q}[x_{\neg\gamma}] \subseteq I(X)$ следва

$$I(\Pi_\gamma(X)) \otimes_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}[x_\gamma] = I(\Pi_\gamma(X)) \otimes_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}[x_1,\ldots,x_n] \subseteq I(X).$$

Ако $h_1,\ldots,h_s \in \overline{\mathbb{F}_q}[x_{\neg\gamma}]$ е пораждаща система на $I(\Pi_\gamma(X)) \lhd \overline{\mathbb{F}_q}[x_{\neg\gamma}]$, то полиномите $g_1,\ldots,g_t,h_1,\ldots,h_s$ образуват пораждаща система на $I(X)$ по предположение. Пространството от решения $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ на хомогенната система линейни уравнения с матрица от коефициенти

$$\frac{\partial(g,h)}{\partial(x_\gamma, x_{\neg\gamma})}(a) = \begin{pmatrix} \frac{\partial g_1}{\partial x_{\gamma_1}}(a) & 0 & \ldots & 0 & \frac{\partial g_1}{\partial x_{\neg\gamma}}(a) \\ 0 & \frac{\partial g_2}{\partial x_{\gamma_2}}(a) & \ldots & 0 & \frac{\partial g_2}{\partial x_{\neg\gamma}}(a) \\ 0 & 0 & \ldots & \frac{\partial g_t}{\partial x_{\gamma_t}}(a) & \frac{\partial g_t}{\partial x_{\neg\gamma}}(a) \\ 0 & 0 & \ldots & 0 & \frac{\partial G_o}{\partial x_{\neg\gamma}}(a) \end{pmatrix} \in M_{(t+s)\times n}(\mathbb{F}_{q^{\delta(a)}}).$$

се съдържа в пространството от решения $\mathbb{F}^t_{q^{\delta(a)}} \times T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ на хомогенната система линейни уравнения с матрица от коефициенти

$$\frac{\partial h}{\partial(x_\gamma, x_{\neg\gamma})}(a) = \begin{pmatrix} 0_{s\times t} & \frac{\partial h}{\partial x_{\neg\gamma}}(a) \end{pmatrix} \in M_{s\times n}(\mathbb{F}_{q\delta(a)}).$$

Първите t стълба в горните Якобиеви матрици отговарят на променливите $x_\gamma = (x_{\gamma_1}, \ldots, x_{\gamma_t})$, а последните $n-t$ стълба отговарят на останалите $n-t$ променливи. Вектор $v = (v_\gamma, v_{\neg\gamma}) \in \mathbb{F}^t_{q^{\delta(a)}} \times T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ принадлежи на $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ точно когато е решение на хомогенната линейна система с матрица от коефициенти

$$\frac{\partial(g)}{\partial(x_\gamma, x_{\neg\gamma})}(a) = \begin{pmatrix} \frac{\partial g_1}{\partial x_{\gamma_1}}(a) & 0 & \ldots & 0 \\ 0 & \frac{\partial g_2}{\partial x_{\gamma_2}}(a) & \ldots & 0 \\ 0 & 0 & \ldots & \frac{\partial g_t}{\partial x_{\gamma_t}}(a) \end{pmatrix} \in M_{t\times n}(\mathbb{F}_{q^{\delta(a)}}).$$

Следователно, във всяка точка $a \in X \setminus Z\left(\prod_{i=1}^{t} \frac{\partial g_i}{\partial x_{\gamma_i}}\right)$, произволен допирателен вектор $v_{\neg\gamma} \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ към $\Pi_\gamma(X)$ в $\Pi_\gamma(a)$ има еднозначно определено продължение $v = (v_\gamma, v_{\neg\gamma}) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ с

$$v_{\gamma_i} = -\left[\frac{\partial g_i}{\partial x_{\gamma_i}}(a)\right]^{-1} \frac{\partial g_i}{\partial x_{\neg\gamma}}(a) v_{\neg\gamma} \quad \text{за} \quad \forall 1 \le i \le t.$$

В резултат, за $\forall w \in \mathbb{F}^n_{q^{\delta(a)}}$ с $\Pi_\gamma(w) \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ съществува единствен вектор $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ с $\Pi_\gamma(v) = \Pi_\gamma(w)$. Оттук, $e := w - v$ принадлежи на ядрото на $\Pi_\gamma = (d\Pi_\gamma)_a$ и $\mathrm{Supp}(e) \subseteq \gamma$. За произволна грешка $e' \in \mathbb{F}^n_{q^{\delta(a)}}$ на $w = v' + e' \in \mathbb{F}^n_{q^{\delta(a)}}$ с носител $\mathrm{Supp}(e') \subseteq \gamma$ имаме

$$\Pi_\gamma(v) = \Pi_\gamma(v+e) = \Pi_\gamma(w) = \Pi_\gamma(v'+e') = \Pi_\gamma(v'),$$

откъдето $v = v'$ и $e = e'$ е единствената грешка на $w \in \mathbb{F}^n_{q^{\delta(a)}}$ относно $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ с носител $\mathrm{Supp}(e) \subseteq \gamma$.
Обратно, ако $w = v + e$ за $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ и $e \in \mathbb{F}^n_{q^{\delta(a)}}$ с $\mathrm{Supp}(e) \subseteq \gamma$, то $\Pi_\gamma(w) = \Pi_\gamma(v) \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^\delta(a)})$, Q.E.D.

Изчислителна задача 21.19. *Нека $g \in \mathbb{F}_q[x_1, \ldots, x_n]^{(d)}$ е хомогенен полином от степен $d \in \mathbb{N}$ с неразложим $g(x_1, x_2, x_3, 0, \ldots, 0) \in \overline{\mathbb{F}_q}[x_1, x_2, x_3]$, $f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$ са произволни полиноми и $\gamma = \{n+1, \ldots, n+k\} \in \Sigma_k(1, \ldots, n+k)$. Да се намерят достатъчни условия върху $g, f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$, $a \in X = Z(g, x_{n+1} - f_1, \ldots, x_{n+k} - f_k) \subset \overline{\mathbb{F}_q}^{n+k}$, при които w има единствена грешка с носител γ относно $T_a(X, \mathbb{F}_{q^{\delta(a)}})$.*

Твърдение 21.20. *Нека $X \subset \overline{\mathbb{F}_q}^n$ е афинно многообразие, а $\Pi_\gamma : X \to \Pi_\gamma(X)$ е пунктиране в $\gamma \in \Sigma_t(1, \ldots, n)$ с непразно, Зариски отворено, Зариски гъсто $\mathrm{Etale}(\Pi_\gamma) := \{a \in X \mid \ker(d\Pi_\gamma)_a = 0\}$ в X. Тогава във всяка точка $a \in \mathcal{E}_\gamma := \mathrm{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\mathrm{smooth}})$, дума $w \in \mathbb{F}^n_{q^{\delta(a)}}$ има единствена грешка с носител γ точно когато $\Pi_\gamma(w) \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$.*

Доказателство: Във всяка точка $a \in \mathcal{E}_\gamma$ пунктирането

$$\Pi_\gamma = (d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

е $\mathbb{F}_{q^{\delta(a)}}$-линеен изоморфизъм, съгласно Твърдение 21.9 (i). Затова, за всяка дума $w \in \mathbb{F}^n_{q^{\delta(a)}}$ с $\Pi_\gamma(w) \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ съществува единствен вектор $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ с $\Pi_\gamma(v) = \Pi_\gamma(w)$. Следователно $e := w - v \in \ker \Pi_\gamma$ има носител

$\mathrm{Supp}(e) \subseteq \gamma$. Единствеността на грешката на $w \in \mathbb{F}_{q^{\delta(a)}}^n$ относно $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ се дължи на единствеността на $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ с $\Pi_\gamma(v) = \Pi_\gamma(w)$.
Обратно, ако $w = v + e$ за $v \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ и $e \in \mathbb{F}_{q^{\delta(a)}}^n$ с $\mathrm{Supp}(e) \subseteq \gamma$, то $\Pi_\gamma(e) = 0^{n-t}$, откъдето $\Pi_\gamma(w) = \Pi_\gamma(v) \in T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$, Q.E.D.

4. Разслоено произведение на многообразия и $(u \,|\, u+v)$-конструкция на допирателните им кодове

Твърдение-Определение 21.21. *Нека $C_1, C_2 \subset \mathbb{F}_q^n$ са линейни кодове с размерности $k_i = \dim_{\mathbb{F}_q} C_i$ и минимални разстояния $d_i = d(C_i)$. Тогава множеството*

$$(C_1|C_1 + C_2) := \{(u, u+v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n = \mathbb{F}_q^{2n} | u \in C_1,\, v \in C_2\}$$

е линеен код с дължина $2n$, размерност $k_1 + k_2$ и минимално разстояние $\min(2d_1, d_2)$, за който казваме, че е получен от C_1 и C_2 чрез $(u|u+v)$-конструкция. Ако $G_i \in M_{k_i \times n}(\mathbb{F}_q)$ са пораждащи матрици на C_i, а $H_i \in M_{(n-k_i)\times n}(\mathbb{F}_q)$ са проверочни матрици на C_i, то

$$G = \begin{pmatrix} G_1 & G_1 \\ 0_{k_2 \times n} & G_2 \end{pmatrix} \in M_{(k_1+k_2)\times(2n)}(\mathbb{F}_q) \tag{21.2}$$

е пораждаща матрица на $(C_1|C_1 + C_2)$, а

$$H = \begin{pmatrix} H_1 & 0_{(n-k_1)\times n} \\ -H_2 & H_2 \end{pmatrix} \in M_{(2n-k_1-k_2)\times(2n)}(\mathbb{F}_q) \tag{21.3}$$

е проверочна матрица на $(C_1|C_1 + C_2)$.

Доказателство: Ако $(u_1, u_1+v_1), (u_2, u_2+v_2) \in (C_1|C_1+C_2)$ с $u_i \in C_1$, $v_i \in C_2$ и $\lambda \in \mathbb{F}_q$, то $(u_1, u_1+v_1)+(u_2, u_2+v_2) = (u_1+u_2, (u_1+u_2)+(v_1+v_2)) \in (C_1, C_1+C_2)$, защото $u_1+u_2 \in C_1$, $v_1+v_2 \in C_2$ и $\lambda(u_1, v_1+v_2) = (\lambda u_1, \lambda u_1+\lambda v_1) \in (C_1|C_1+C_2)$, защото $\lambda u_1 \in C_1$ и $\lambda v_1 \in C_2$. Това доказва, че $(C_1|C_1 + C_2)$ е $\mathbb{F}_q$-линейно подпространство на $\mathbb{F}_q^{2n}$.
Ако $u^{(i)} \in \mathbb{F}_q^n$, $1 \le i \le k_1$ е базис на C_1, а $v^{(j)} \in \mathbb{F}_q^n$, $1 \le j \le k_2$ е базис на C_2, твърдим, че $B = \{(u^{(i)}, u^{(i)}), (0^n, v^{(j)}) \,|\, 1 \le i \le k_1,\, 1 \le j \le k_2\}$ е базис на $(C_1|C_1 + C_2)$, откъдето $\dim(C_1|C_1 + C_2) = \dim C_1 + \dim C_2 = k_1 + k_2$. Наистина, ако

$$0^{2n} = \sum_{i=1}^{k_1} x_i(u^{(i)}, u^{(i)}) + \sum_{j=1}^{k_2} y_j(0^n, v^{(j)}) = \left(\sum_{i=1}^{k_1} x_i u^{(i)}, \sum_{i=1}^{k_1} x_i u^{(i)} + \sum_{j=1}^{k_2} y_j v^{(j)} \right),$$

то

$$0^n = \sum_{i=1}^{k_1} x_i u^{(i)} = 0^n \quad \text{и} \quad 0^n = \sum_{i=1}^{k_1} x_i u^{(i)} + \sum_{j=1}^{k_2} y_j v^{(j)} = \sum_{j=1}^{k_2} y_j v^{(j)},$$

откъдето $x_i = 0$ за $\forall 1 \le i \le k_1$ и $y_j = 0$ за $\forall 1 \le j \le k_2$, съгласно линейната независимост на $u^{(1)}, \ldots, u^{(k_1)}$ и линейната независимост на $v^{(1)}, \ldots, v^{(k_2)}$. Това доказва линейната независимост на B. От друга страна, произволен елемент на $(C_1|C_1 + C_2)$ е от вида

$$(u, u+v) = \left(\sum_{i=1}^{k_1} x_i u^{(i)}, \sum_{i=1}^{k_1} x_i u^{(i)} + \sum_{j=1}^{k_2} y_j v^{(j)} \right) =$$

$$= \sum_{i=1}^{k_1} x_i(u^{(i)}, u^{(i)}) + \sum_{j=1}^{k-2} y_j(0^n, v^{(j)}) \in l_{\mathbb{F}_q}(B),$$

така че линейната обвивка $l_{\mathbb{F}_q}(B) = (C_1|C_1+C_2)$ и B е базис на $(C_1|C_1+C_2)$. Това доказва, че $\dim(C_1|C_1+C_2) = k_1+k_2$. Освен това, ако пораждащата матрица G_1 на C_1 се състои по редове от компонентите на базиса $u^{(1)},\ldots,u^{(k_1)}$ на C_1, а G_2 се състои по редове от компонентите на $v^{(1)},\ldots,v^{(k_2)}$, то редовете на матрицата G от (21.2) се състоят от компонентите на векторите на базиса B на $(C_1|C_1+C_2)$ и G е пораждаща матрица на $(C_1|C_1+C_2)$.
За да докажем, че $(C_1|C_1+C_2)$ има минимално разстояние $d(C_1|C_1+C_2) = d = \min(2d_1,d_2)$ да забележим, че ако $c'\in C_1$ е дума с минимално тегло d_1, то $(c',c')\in(C_1|C_1+C_2)$ е дума с тегло $2d_1$. Аналогично, ако $c''\in C_2$ е дума с минимално тегло d_2, то $(0^n,c'')\in(C_1|C_1+C_2)$ е дума с тегло d_2, така че $d\le\min(2d_1,d_2)$. Ако допуснем, че $d<\min(2d_1,d_2)$, то съществува $(\lambda,\lambda+\mu)\in(C_1|C_1+C_2)$ с $\lambda\in C_1$, $\mu\in C_2$ и тегло $\mathrm{wt}(\lambda,\lambda+\mu)=d$. От $\lambda\in C_1$ следва $\mathrm{wt}(\lambda)\ge d_1$, откъдето $\mathrm{wt}(\lambda+\mu)=d-\mathrm{wt}(\lambda)\le d-d_1$. Произволни думи $a,b\in\mathbb{F}_q^n$ имат сума $a+b\in\mathbb{F}_q^n$ с тегло $\mathrm{wt}(a+b)\le\mathrm{wt}(a)+\mathrm{wt}(b)$. В резултат,

$$d_2\le\mathrm{wt}(\mu)=\mathrm{wt}((\lambda+\mu)+(-\lambda))\le\mathrm{wt}(\lambda+\mu)+\mathrm{wt}(-\lambda)=\mathrm{wt}(\lambda+\mu)+\mathrm{wt}(\lambda)=d,$$

съгласно $\mu\in C_2$ и $\mathrm{wt}(\lambda,\lambda+\mu)=\mathrm{wt}(\lambda)+\mathrm{wt}(\lambda+\mu)$. Почленното изваждане на d_2 от $d<\min(2d_1,d_2)$ дава

$$0\le d-d_2<\min(2d_1-d_2,0)\le 0,$$

което е противоречие, доказващо $d=\min(2d_1,d_2)$.
За да установим, че H от (21.3) е проверочна матрица за $(C_1|C_1+C_2)$ да забележим, че ако вектор-редовете $R_1,\ldots,R_{n-k_1}$ на H_1 са линейно независими и вектор-редовете $R'_1,\ldots,R'_{n-k_2}$ на H_2 са линейно независими, то вектор-редовете на H са линейно независими, защото от допускането

$$\sum_{i=1}^{n-k_1}x_i(R_i,0_{1\times n})+\sum_{j=1}^{n-k_2}y_j(-R'_j,R'_j)=0_{1\times(2n)}$$

за някои $x_i,y_j\in\mathbb{F}_q$ следва

$$0_{1\times n}=\sum_{j=1}^{n-k_2}y_jR'_j\quad\text{и}\quad 0_{1\times n}=\sum_{i=1}^{n-k_1}x_iR_i-\sum_{j=1}^{n-k_2}y_jR'_j=\sum_{i=1}^{n-k_1}x_iR_i.$$

Следователно H е от ранг $\mathrm{rk}(H)=(n-k_1)+(n-k_2)=2n-(k_1+k_2)$. Достатъчно е да проверим, че $(C_1|C_1+C_2)$ се съдържа в пространството от решения $U\subseteq\mathbb{F}_q^{2n}$ на хомогенната линейна система уравнения с матрица от коефициенти H, за да получим, че $U=(C_1|C_1+C_2)$ и H е проверочна матрица на $(C_1|C_1+C_2)$. Наистина, за произволни $u=(u_1,\ldots,u_n)\in C_1\subset M_{1\times n}(\mathbb{F}_q)$ и $v=(v_1,\ldots,v_n)\in C_2\subset M_{1\times n}(\mathbb{F}_q)$ е в сила

$$H\begin{pmatrix}u^t\\(u+v)^t\end{pmatrix}=\begin{pmatrix}H_1&0_{(n-k_1)\times n}\\-H_2&H_2\end{pmatrix}\begin{pmatrix}u^t\\(u+v)^t\end{pmatrix}=$$
$$=\begin{pmatrix}H_1u^t\\-H_2u^t+H_2u^t+H_2v^t\end{pmatrix}=\begin{pmatrix}H_1u^t\\H_2v^t\end{pmatrix}=\begin{pmatrix}0_{(n-k_1)\times 1}\\0_{(n-k_2)\times 1}\end{pmatrix}=0_{[2n-(k_1+k_2)]\times 1},$$

защото $H_1u^t=0_{(n-k_1)\times 1}$ и $H_2v^t=0_{(n-k_2)\times 1}$. Това доказва твърдението, Q.E.D.

Определение 21.22. *Ако $U\subseteq\overline{\mathbb{F}_q}^n$ и $V\subseteq\overline{\mathbb{F}_q}^m$ са квази-афинни многообразия с регулярни изображения $\varphi:U\to W$ и $\psi:V\to W$, то разслоеното произведение на U и V над W е множеството*

$$U\times_W V:=\{(u,v)\in U\times V\,|\varphi(u)=\psi(v)\}.$$

Еквивалентно, разслоеното произведение се определя от комутативната диаграма

$$\begin{array}{ccc} U & \xleftarrow{\mathrm{pr}_1} & U \times_W V \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{pr}_2} \\ W & \xleftarrow{\psi} & V \end{array},$$

където pr_j е каноничната проекция върху j-тия множител и изображенията, означени с успоредни струлки имат изоморфни слоеве.
В частност, ако $X \subset \overline{\mathbb{F}_q}^n$ е афинно многообразие и $g = (g_1, \ldots, g_s) : \overline{\mathbb{F}_q}^n \to \overline{\mathbb{F}_q}^s$ е регулярно изображение, зададено с полиноми $g_1, \ldots, g_s \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, то разслоеното произведение

$$X \times_{g(X)} \overline{\mathbb{F}_q}^n = \{(a, b) \in X \times \overline{\mathbb{F}_q}^n \mid g(a) = g(b)\}$$

на X и $\overline{\mathbb{F}_q}^n$ над $g(X)$ се разслоява естествено над X чрез нулите на подходящи транслации на $g_1, \ldots, g_s$,

$$X \times_{g(X)} \overline{\mathbb{F}_q}^n = \coprod_{a \in X} Z(g_1(x_1, \ldots, x_n) - g_1(a), \ldots, g_s(x_1, \ldots, x_n) - g_s(a)).$$

Твърдение 21.23. *Нека $X \subset \overline{\mathbb{F}_q}^n$ е афинно многообразие с абсолютен идеал $I(X) = \langle f_1, \ldots, f_m \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ за някои $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, а $g_1, \ldots, g_s \in \mathbb{F}_q[x_1, \ldots, x_n]$ са такива полиноми, пораждащи прост идеал*

$$I_a = \langle g_1 - g_1(a), \ldots, g_s - g_s(a) \rangle \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n],$$

че слоят

$$Y_a = \{b \in \overline{\mathbb{F}_q}^n \mid g_1(b) = g_1(a), \ldots, g_s(b) = g_s(a)\}$$

на $g = (g_1, \ldots, g_s) : \overline{\mathbb{F}_q}^n \to \overline{\mathbb{F}_q}^s$ през някоя гладка точка $a \in X^{\mathrm{smooth}}$ на X е с размерност $\dim Y_a = n - s$ и съдържа a като своя гладка точка, $a \in Y_a^{\mathrm{smooth}}$. Тогава $(u|u+v)$-конструкцията

$$(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \mid T_a(X, \mathbb{F}_{q^{\delta(a)}}) + T_a(Y_a, \mathbb{F}_{q^{\delta(a)}})) = T_{(a,a)}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}),$$

приложена към допирателните пространства $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ и $T_a(Y_a, \mathbb{F}_{q^{\delta(a)}})$ дава допирателното пространство на Зариски към $X \times_{g(X)} \overline{\mathbb{F}_q}^n$ в (a, a).

Доказателство: Абсолютният идеал $I(X \times_{g(X)} \overline{\mathbb{F}_q}^n) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ на разслоеното произведение $X \times_{g(X)} \overline{\mathbb{F}_q}^n$ съдържа полиномите

$$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$$

и

$$g_1(y_1, \ldots, y_n) - g_1(x_1, \ldots, x_n), \ldots, g_s(y_1, \ldots, y_n) - g_s(x_1, \ldots, x_n).$$

Затова допирателното пространство на Зариски $T_{(a,b)}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}})$ се съдържа в пространството от решения $C_{(a,b)} \subset \mathbb{F}_{q^{\delta(a)}}^{2n}$ на хомогенната система линейни уравнения с матрица от коефициенти

$$H_{(a,b)} = \begin{pmatrix} \frac{\partial f}{\partial x}(a) & 0 \\ -\frac{\partial g}{\partial x}(a) & \frac{\partial g}{\partial y}(b) \end{pmatrix}.$$

Допирателното пространство на Зариски $T_a(X, \mathbb{F}_q^{\delta(a)})$ има проверочна матрица $\frac{\partial f}{\partial x}(a)$, защото полиномите $f_1, \ldots, f_m$ пораждат $I(X) \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$. По Теоремата на Hilbert за нулите, идеалът

$$\begin{aligned} I(Y_a) &= IZ(g_j(y_1, \ldots, y_n) - g_j(a) \,|\, 1 \leq j \leq n) = \\ &= r\langle g_j(y_1, \ldots, y_n) - g_j(a) \,|\, 1 \leq j \leq n\rangle = r(I_a) \end{aligned}$$

съвпада с радикала на $I_a \lhd \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ От простотата на I_a имаме $r(I_a) = I_a$, така че допирателното пространство на Зариски $T_b(Y_a, \overline{\mathbb{F}_{q^{\delta(a)}}})$ към Y_a в $b \in Y_a$ има проверочна матрица $\frac{\partial g}{\partial y}(b)$. Съгласно Твърдение-Определение 21.21,

$$C_{(a,a)} = (T_a(X, \mathbb{F}_{q^{\delta(a)}}) \,|\, T_a(X, \mathbb{F}_{q^{\delta(a)}}) + T_a(Y_a, \mathbb{F}_{q^{\delta(a)}}))$$

се получава от $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ и от $T_a(Y_a, \mathbb{F}_{q^{\delta(a)}})$ чрез $(u|u+v)$-конструкция. Предположението $a \in X^{\mathrm{smmooth}} \cap Y_a^{\mathrm{smooth}}$ води до

$$\dim_{\mathbb{F}_{q^{\delta(a)}}} T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim X, \quad \dim_{\mathbb{F}_{q^{\delta(a)}}} T_a(Y_a, \mathbb{F}_{q^{\delta(a)}}) = \dim Y_a = n - s,$$

откъдето

$$\dim C_{(a,a)} = \dim X + n - s.$$

От друга страна, разслоеното произведение $X \times_{g(X)} \overline{\mathbb{F}_q}^n$ се задава с s уравнения $g_i(y) = g_i(x)$, $1 \leq i \leq s$ в директното произведение $X \times \overline{\mathbb{F}_q}^n$ и размерността му е

$$\dim(X \times_{g(X)} \overline{\mathbb{F}_q}^n) \geq \dim X + n - s.$$

Комбинирайки с включването

$$T_{(a,a)}(X \times_{g(X)}, \mathbb{F}_{q^{\delta(a)}}) \subseteq C_{(a,a)}$$

получаваме, че

$$\begin{aligned} \dim X + n - s \leq \dim(X \times_{g(X)} \overline{\mathbb{F}_q}^n) \leq \dim_{\mathbb{F}_{q^{\delta(a)}}} T_{(a,a)}(X \times_{g(X)} \overline{\mathbb{F}_q}, \mathbb{F}_{q^{\delta(a)}}) \leq \\ \leq \dim_{\mathbb{F}_{q^{\delta(a)}}} C_{(a,a)} = \dim X + n - s, \end{aligned}$$

откъдето

$$T_{(a,a)}(X \times_{G(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}) = C_{(a,a)}$$

и $(a, a) \in (X \times_{g(X)} \overline{\mathbb{F}_q}^n)^{\mathrm{smooth}}$ е гладка точка на афинното многообразие $X \times_{g(X)} \overline{\mathbb{F}_q}^n$ с размерност $\dim(X \times_{g(X)} \overline{\mathbb{F}_q}^n) = \dim X + n - s$, Q.E.D.

Изчислителна задача 21.24. *Да се изследва минималното разстояние на* $T_{(a,a)}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}})$ *с* $a \in X^{\mathrm{smooth}} \cap Y_a^{\mathrm{smooth}}$ *в зависимост от полиномите* $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ *и* $g_1, \ldots, g_s \in \mathbb{F}_q[x_1, \ldots, x_n]$.