

Алгебро-геометрични кодове. Декодиране чрез локатор на грешката

Следващото твърдение излага конструкцията на алгебро-геометричните кодове на Reed-Solomon.

ТЕОРЕМА-ОПРЕДЕЛЕНИЕ 2. (Алгебро-геометричен код на Reed-Solomon) *Нека $D = P_1 + \dots + P_n$ е сума на \mathbb{F}_q -рационални точки от гладка проективна крива X , определена над \mathbb{F}_q , $G \in \text{Div}(F)$ е ефективен дивизор, чийто носител*

$$\text{Supp}(G) = \text{Supp} \left(\sum_Q n_Q Q \right) = \{Q \mid n_Q > 0\}$$

не се пресича с $\{P_1, \dots, P_n\}$, а

$$\mathcal{E}_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n,$$

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

е остойносттавящото изображение на линейната система $\mathcal{L}(G)$ на G върху D . Тогава образът $C(X, D, G) = \mathcal{E}_D(\mathcal{L}(G)) \subset \mathbb{F}_q^n$ е линейен код с размерност

$$k = l(G) - l(G - D)$$

и минимално разстояние

$$d \geq n - \deg(G).$$

Думата $\mathcal{E}_D(f) \in C(X, D, G)$ е с тегло $r > 0$ точно когато съществува пермутация $\sigma \in S_n$, така че $f \in \mathcal{L}(G - P_{\sigma(r+1)} - \dots - P_{\sigma(n)})$. Затова минималното разстояние d е минималното естествено число, за което съществува дивизор $D' \leq D$ от степен $\deg(D') = n - d$.

Доказателство: Остойносттавящото изображение \mathcal{E}_D е \mathbb{F}_q -линейно и

$$k = \dim(\text{im}(\mathcal{E}_D)) = l(G) - \dim(\text{ker}(\mathcal{E}_D)).$$

Условието $f \in \mathcal{L}(G)$ означава, че $(f) + G = (f)_0 - (f)_\infty + G \geq 0$ и е еквивалентно на $G - (f)_\infty \geq 0$. Ако $f \in \mathcal{L}(G)$ се анулира в P_1, \dots, P_n , то $P_1 + \dots + P_n \leq (f)_0$ и $\text{div}(f) + G - D = (f)_0 - D + G - (f)_\infty \geq 0$ и $f \in \mathcal{L}(G - D)$. Следователно $\mathcal{L}(G) \cap \text{ker}(\mathcal{E}_D) = \mathcal{L}(G - D)$.

Минималното разстояние d на $C(X, D, G)$ се достига от някаква дума $\mathcal{E}_D(f) = (f(P_1), \dots, f(P_n))$. Съществува пермутация $\sigma \in S_n$, така че така че $P_{\sigma(d+1)} + \dots + P_{\sigma(n)} \leq (f)_0$ и $f \in \mathcal{L}(G - (P_{\sigma(d+1)} + \dots + P_{\sigma(n)})) \setminus \{0\}$. Ако $\mathcal{L}(H) \neq 0$, то $\deg(H) \geq 0$. Да напомним, че всяка рационална функция $f \in F$ има равен брой нули и полюси, броени с техните кратности или $\deg(f) = 0$. Ако съществува $f \in \mathcal{L}(H) \setminus \{0\}$, то $\text{div}(f) + D \geq 0$. Ефективността на дивизора $\text{div}(f) + D$ означава неотрицателност на всичките му цели коефициенти, така че степента $\deg((f) + D) \geq 0$ като сума на коефициентите. Затова от $f \in \mathcal{L}(G - (P_{\sigma(d+1)} + \dots + P_{\sigma(n)})) \setminus \{0\}$ следва $\deg(G - (P_{\sigma(d+1)} + \dots + P_{\sigma(n)})) \geq 0$ или $\deg(G) \geq n - d$. Дума $\mathcal{E}_D(f) \in C(X, D, G)$ има тегло $w(\mathcal{E}_D(f)) = r \in (0, d]$ точно когато съществува $\sigma \in S_n$, така че $f(P_{\sigma(r+1)}) = \dots = f(P_{\sigma(n)}) = 0$. С други думи,

съществува дивизор $D' = \sum_{j=r+1}^n P_{\sigma(j)}$ от степен $\deg(D') = n - r$, така че $D \geq D'$

и $f \in \mathcal{L}(G - D')$. Минималното разстояние d на $C(X, D, G)$ е минималното естествено $d = r$ с това свойство, Q.E.D.

Използвайки резидууми на диференциални форми построяваме алгебро-геометричните кодове на Горра.

ТЕОРЕМА-ОПРЕДЕЛЕНИЕ 3. *В означенията от Теорема-Определение 2, разглеждаме \mathbb{F}_q -линейното изображение*

$$\text{Res} : \Omega_D^{\mathbb{F}_q}(G - D) \longrightarrow \mathbb{F}_q^n,$$

$$\text{Res}(\eta) = (\text{Res}_{P_1}(\eta), \dots, \text{Res}_{P_n}(\eta)),$$

където $\Omega_D^{\mathbb{F}_q}(G - D) = \Omega_D^{\mathbb{F}_q} \cap \Omega(G - D)$ и $\Omega_D^{\mathbb{F}_q} = \cap_{i=1}^n \mathbb{F}_q(X) dt_i$ за локални параметри t_i в P_i , $D = \sum_{i=1}^n P_i$. Тогава образът $C^*(X, D, G) = \text{Res} \Omega_D^{\mathbb{F}_q}(G - D) \subset \mathbb{F}_q^n$ е алгебро-геометричен код на Горра с размерност

$$k^* = l((\omega) + D - G) - l((\omega) - G)$$

за произволна диференциална форма $\omega \in \Omega \setminus \{0\}$ и минимално разстояние

$$d^* \geq \deg(G) - (2g - 2).$$

Доказателство: Да започнем с обосновка на $\text{Res}_{P_i}(\eta) \in \mathbb{F}_q$ за $\forall 1 \leq i \leq n$. Дискретното нормиране v_{P_i} , отговарящо на $P_i \in X$ има поле от остатъци $\mathcal{O}_{P_i}(X)/\mathfrak{M}_{P_i}(X) = \mathbb{F}_q$, защото P_i е \mathbb{F}_q -рационална точка. Следователно $\forall f \in \mathbb{F}_q(X)$ се представя като Лоранов ред $\sum_{j \geq j_0} a_{ij} t_i^j$ с коефициенти $a_{ij} \in \mathcal{O}_{P_i}(X)/\mathfrak{M}_{P_i}(X) = \mathbb{F}_q$.

За произволна диференциална форма $\omega \in \Omega_D^{\mathbb{F}_q} \setminus \{0\}$ и

$$\mathcal{L}(\text{div}(\omega) + D - G) = \{f \in \mathbb{F}_q(X)^* \mid \text{div}(f) + \text{div}(\omega) + D - G \geq 0\},$$

изображението

$$\begin{aligned} \varphi : \mathcal{L}(\text{div}(\omega) + D - G) &\longrightarrow \Omega_D^{\mathbb{F}_q}(G - D), \\ \varphi(f) &= f\omega \end{aligned}$$

е \mathbb{F}_q -линеен изоморфизъм. Затова можем да разглеждаме линейния код

$$C^*(X, D, G) = \text{Res} \varphi \mathcal{L}((\omega) + D - G)$$

като образ на подходяща линейна система. По определение, $f\omega \in \Omega_D^{\mathbb{F}_q}(G - D)$ означава, че

$$\text{div}(f\omega) - G + D = [(f\omega)_0 - G] + [D - (f\omega)_\infty] \geq 0.$$

За ефективни дивизори $D = P_1 + \dots + P_n$ и $G = mQ$, $m \geq 0$, оттук следват $(f\omega)_0 - G \geq 0$ и $D - (f\omega)_\infty \geq 0$. Наистина, ако $v((f\omega)_0 - G) < 0$ за някое дискретно нормиране v , то $v = v_Q$, съгласно ефективността на $(f\omega)_0$. Понеже $Q \notin \text{Supp}(D)$, получаваме $v_Q(D - (f\omega)_\infty) < 0$, което противоречи на $\text{div}(f\omega) - G + D \geq 0$. Аналогично, ако $w(D - (f\omega)_\infty) < 0$ за някое дискретно нормиране w , то w е полюс на $f\omega$. Без ограничение на общността можем да считаме, че $w \notin \text{Supp}(f\omega)_0$, откъдето $w((f\omega)_0 - G) < 0$. Това също противоречи на $\text{div}(f\omega) - G + D \geq 0$ и доказва, че $(f\omega)_0 - G \geq 0$ и $D - (f\omega)_\infty \geq 0$ за $\forall f\omega \in \Omega_D^{\mathbb{F}_q}(G - D)$. (Всъщност, за $\forall f\omega \in \Omega(G - D)$.) Условието $(f\omega)_\infty \leq D$ означава, че диференциалната форма $f\omega$ има най-много прости полюси в P_1, \dots, P_n . Сега ядрото $\ker(\text{Res} \varphi)$ се състои от рационалните функции $f \in \mathcal{L}(\text{div}(\omega) + D - G)$, за които формата $f\omega$ няма полюси, т.е. $\text{div}(f\omega) = (f\omega)_0$. Тогава $\text{div}(f\omega) \geq G$ и $f \in \mathcal{L}((\omega) - G)$. Следователно $\dim(\ker(\text{Res} \varphi)) = l((\omega) - G)$ и $k^* = l((\omega) + D - G) - l((\omega) - G)$, доколкото φ е \mathbb{F}_q -линеен изоморфизъм.

Минималното разстояние d^* на $C^*(X, D, G)$ се достига в някоя кодова дума $Res(\eta) \in C^*(X, D, G)$ с тегло d^* . След евентуална преномерация на P_1, \dots, P_n можем да считаме, че $Res_{P_i}(\eta) \neq 0$ за $\forall 1 \leq i \leq d^*$ и $Res_{P_j}(\eta) = 0$ за $\forall d^* + 1 \leq j \leq n$. С други думи, формата $\eta \in \Omega_D^{\mathbb{F}_q}(G - D)$ няма полюси в P_{d^*+1}, \dots, P_n и $\eta \in \Omega_D^{\mathbb{F}_q}(G - (P_1 + \dots + P_{d^*}))$. Оттук, линейната система $\mathcal{L}(div(\omega) - G + P_1 + \dots + P_{d^*}) \simeq \Omega_D^{\mathbb{F}_q}(G - (P_1 + \dots + P_{d^*})) \neq 0$ е ненулева и степента $\deg(div(\omega) - G + P_1 + \dots + P_{d^*}) \geq 0$. Съгласно $\deg(div(\omega)) = 2g - 2$ получаваме $2g - 2 - \deg(G) + d^* \geq 0$, Q.E.D.

ТЕОРЕМА 25. *Алгебро-геометричните кодове $C(X, D, G)$ от Теорема-Определение 2 и $C^*(X, D, G)$ от Теорема-Определение 3 са дуални.*

Доказателство: От една страна, сумата на размерностите на гореспоменатите кодове е равна на общата дължина n . По-точно,

$$\begin{aligned} k + k^* &= [l(G) - l(G - D)] + [l(div(\omega) + D - G) - l((\omega) - G)] = \\ &= [l(G) - l(div(\omega) - G)] + [l(div(\omega) + D - G) - l(G - D)] = \\ &= [\deg(G) - g + 1] + [\deg(div(\omega) + D - G) - g + 1] = \\ &= [\deg(G) - g + 1] + [2g - 2 + n - \deg(G) - g + 1] = n, \end{aligned}$$

съгласно Теоремата на Riemann-Roch

$$l(E) - l(div(\omega) - E) = \deg(E) - g + 1$$

за дивизор E върху крива с род g , $\deg div(\omega) = 2g - 2$ и избора на D от степен $\deg(D) = n$. Достатъчно е да проверим, че $C^*(X, D, G) \subseteq C(X, D, G)^\perp$, за да получим $C^*(X, D, G) = C(X, D, G)^\perp$ и да докажем теоремата.

За произволна диференциална форма $\eta \in \Omega_D^{\mathbb{F}_q}(G - D)$ и рационална функция $f \in \mathcal{L}(G)$ произведението $f\eta \in \Omega(-D)$, защото от $div(\eta) \geq G - D$ и $div(f) + G \geq 0$ следва $div(f\eta) = div(f) + div(\eta) \geq (-G) + G - D = -D$. Условието $div(f\eta) + D = (f\eta)_0 - (f\eta)_\infty + D \geq 0$ изисква $D \geq (f\eta)_\infty$ или $f\eta$ има най-много прости полюси в P_1, \dots, P_n . Освен това, $f \in \mathcal{L}(G)$ е регулярна в P_1, \dots, P_n съгласно избора на $\text{Supp}(G) \cap \{P_1, \dots, P_n\} = \emptyset$. Следователно Теоремата за резидуумите $\sum_{P \in X} Res_P(f\eta) = 0$ в този случай гласи, че

$$0 = \sum_{i=1}^n Res_{P_i}(f\eta) = \sum_{i=1}^n f(P_i) Res_{P_i}(\eta) = \sum_{i=1}^n \mathcal{E}_D(f)_i Res(\eta)_i = (\mathcal{E}_D(f), Res(\eta)),$$

за стандартното вътрешно произведение $(\mathcal{E}_D(f), Res(\eta))$ в \mathbb{F}_q^n . С други думи, всяко $Res(\eta)$ е перпендикулярно на $C(X, D, G) = \mathcal{E}_D(\mathcal{L}(D))$ или $C^*(X, D, G) \subseteq C(X, D, G)^\perp$, Q.E.D.

В останалата част от въпроса ще изложим алгоритъм за декодиране на алгебро-геометрични кодове на Горра чрез локатор на грешката.

В означенията от Теорема-Определение 3, нека $\deg(div(\omega) - G) = 2g - 2 - \deg(G) < 0$, така че $l(div(\omega) - G) = 0$, Res е влагане и размерността $\dim C^*(X, D, G) = k^* = l((\omega) + D - G)$. Да напомним, че минималното разстояние $d^* \geq \deg(G) - (2g - 2)$. Нека е предадена кодова дума $c \in C^*(X, D, G) \subset \mathbb{F}_q^n$ и е получена кодова дума $f = c + e$. За произволна рационална функция $\varphi \in F = \mathbb{F}_q(X)$ определяме синдрома на f относно φ като

$$(\varphi, f) = \sum_{i=1}^n \varphi(P_i) f_i,$$

ако φ е регулярна (определена) в P_1, \dots, P_n или $(\varphi, f) = \infty$, ако φ има полюс в някоя точка P_i . Съгласно Теорема 25, кодът $C^*(X, D, G)$ е дуален на кода $C(X, D, G)$, така че $c \in C^*(X, D, G)$ тогава и само тогава, когато $(x, c) =$

$\sum_{i=1}^n x_i c_i = 0$ за $\forall x \in C(X, D, G)$. Това условие е еквивалентно на $(\varphi, c) = 0$ за $\forall \varphi \in \mathcal{L}(G)$ и се свежда до $(\varphi_i, c) = 0$ за базис $\varphi_1, \dots, \varphi_{l(G)}$ на $\mathcal{L}(G)$. Оттук $(\varphi, f) = (\varphi, c + e) = (\varphi, e)$ за $\forall \varphi \in \mathcal{L}(G)$. Поставяме си за задача да намерим грешката e от синдромите на f .

Локатор на грешката е нетъждествено нулева рационална функция Θ от сечението $\cap_{i=1}^n \mathcal{O}_{P_i}(X)$ с $\Theta(P_i) = 0$ за всички $1 \leq i \leq n$ с $e_i \neq 0$.

ТВЪРДЕНИЕ 19.1. Нека $e \in \mathbb{F}_q^n$ е дума с тегло $w(e) \leq t$ и $A \in \text{Div}(F)$ е дивизор с $l(A) \geq t+1$, $\text{Supp}(A) \cap \text{Supp}(D) = \emptyset$. Тогава съществува локатор на грешката $\Theta \in \mathcal{L}(A)$.

Доказателство: Нека $M = \{P_i \mid e_i \neq 0, 1 \leq i \leq n\}$ е носителят на e в $D = P_1 + \dots + P_n$. Избираме базис $\varphi_1, \dots, \varphi_{l(A)}$ на $\mathcal{L}(A)$ и търсим $\Theta = \sum_{j=1}^{l(A)} a_j \varphi_j$, $a_i \in \mathbb{F}_q$, така че

$$\Theta(P_i) = \sum_{j=1}^{l(A)} a_j \varphi_j(P_i) = 0 \quad \text{за } \forall P_i \in M.$$

Получената хомогенна линейна система има $|M| = w(e) \leq t$ уравнения и $l(A) \geq t+1$ неизвестни. Следователно съществува ненулево решение $(a_1, \dots, a_{l(A)})$ и нетъждествено нулева функция $\Theta = \sum_{i=1}^{l(A)} a_i \varphi_i$, която е локатор на грешката за e , Q.E.D.

ТВЪРДЕНИЕ 19.2. Нека $e \in \mathbb{F}_q^n$ е грешка с тегло $w(e) \leq t$, A е дивизор с $\text{Supp}(A) \cap \text{Supp}(D) = \{P_1, \dots, P_n\} = \emptyset$, $\deg(A) \leq t+r$, $a Z \leq G$ е дивизор с $\deg(Z) \geq t+r+2g-1$ за някое $r \geq 0$. Ако съществува локатор на грешката $\Theta \in \mathcal{L}(A)$, то e е еднозначно определено от Θ и синдромите на e относно функциите от $\mathcal{L}(Z)$.

Доказателство: В означенията от Твърдение 19.1, ако $(\Theta)_0$ е дивизорът на нулите на Θ , то $(\Theta)_0 \supseteq M$. Избираме $r \geq 0$, така че броят на нулите $\deg(\Theta)_0 \leq t+r$. За произволна рационална функция $\varphi \in F$ без полюси в P_1, \dots, P_n имаме

$$(\varphi, e) = \sum_{i=1}^n \varphi(P_i) e_i = \sum_{P_i \in M} \varphi(P_i) e_i = \sum_{P_i \in (\Theta)_0} \varphi(P_i) e_i.$$

В частност, от $\mathcal{L}(Z) \subseteq \mathcal{L}(G)$ следва, че грешката e е решение на уравненията

$$(\varphi, f) = (\varphi, e) = \sum_{P_i \in (\Theta)_0} \varphi(P_i) x_i \quad \text{за } \forall \varphi \in \mathcal{L}(Z).$$

Ако e' е друго решение на горната система, чийто носител се съдържа в $(\Theta)_0$, то $(\varphi, e - e') = 0$, така че $e - e' \in C(X, D, Z)^\perp = C^*(X, D, Z)$. Съгласно Теорема-Определение 3, минималното разстояние

$$d^* = dC^*(X, D, Z) \geq \deg(Z) - (2g - 2) \geq (t + r + 2g - 1) - (2g - 2) = t + r + 1.$$

Понеже носителите на e и e' се съдържат в $(\Theta)_0$ от степен $\deg(\Theta)_0 \leq t+r$, теглото $w(e - e') \leq t+r$. Сега от

$$w(e - e') \geq dC^*(X, D, Z) \geq t + r + 1$$

следва $e = e'$, така че грешката e е единственото решение x на

$$(\varphi_j, f) = \sum_{P_i \in (\Theta)_0} \varphi_j(P_i) x_i$$

с $\text{Supp}(x) \subseteq (\Theta)_0$ за базис $\varphi_1, \dots, \varphi_{l(Z)}$ на $\mathcal{L}(Z)$, Q.E.D.

ТВЪРДЕНИЕ 19.3. Нека $e \in \mathbb{F}_q^n$ е дума с тегло $w(e) \leq t$ и $Y \in \text{Div}(F)$, $F = \mathbb{F}_q(X)$ е дивизор от степен $\deg(Y) \geq t+2g-1$ с носител $\text{Supp}(Y) \cap \text{Supp}(D) = \emptyset$. В такъв случай, $\Theta \in \cap_{i=1}^n \mathcal{O}_{P_i}(X)$ е локатор на грешката е тогава и само тогава, когато $(\Theta\psi, e) = 0$ за $\forall \psi \in \mathcal{L}(Y)$.

Доказателство: Твърдим, че Θ е локатор на грешката за e тогава и само тогава, когато $e' = (\Theta(P_1)e_1, \dots, \Theta(P_n)e_n) = 0_{1 \times n}$. Ако $e_i = 0$, то $\Theta(P_i)e_i = 0$. Ако $e_i \neq 0$ и Θ е локатор на грешката за e , то $\Theta(P_i) = 0$ и $\Theta(P_i)e_i = 0$. Следователно $e' = 0_{1 \times n}$, ако Θ е локатор на грешката за e . Обратно, ако $e' = 0_{1 \times n}$, то за всяко $1 \leq i \leq n$ с $e_i \neq 0$ имаме $\Theta(P_i) = 0$, така че Θ е локатор на грешката за e .

Остава да проверим, че $e' = 0$ тогава и само тогава, когато

$$(\Theta\psi, e) = \sum_{i=1}^n \psi(P_i)\Theta(P_i)e_i = (\psi, e') = 0 \quad \text{за } \forall \psi \in \mathcal{L}(Y).$$

Наистина, ако $(\psi, e') = 0$ за $\forall \psi \in \mathcal{L}(Y)$, то $e' \in C^*(X, D, Y)$ по Теорема 25. Съгласно Теорема-Определение 3, минималното разстояние

$$dC^*(X, D, y) \geq \deg(Y) - (2g - 2) \geq t + 2g - 1 - (2g - 2) = t + 1.$$

Но теглото $w(e') \leq w(e) \leq t$, така че от $(\psi, e') = 0$ за $\forall \psi \in \mathcal{L}(Y)$ следва $e' = 0$, Q.E.D.

СЛЕДСТВИЕ 19.4. В означенията от Теорема-Определение 3, нека $c \in C^*(X, D, G)$, $f = c + e$ за грешка $e \in \mathbb{F}_q^n$ с тегло $w(e) \leq t$, $A \in \text{Div}(F)$ е дивизор с $l(A) \geq t+1$, $\text{Supp}(A) \cap \text{Supp}(D) = \emptyset$, а $Y \in \text{Div}(F)$ е дивизор от степен $\deg(Y) \geq t + 2g - 1$ с носител $\text{Supp}(Y) \cap \text{Supp}(D) = \emptyset$, така че $A + Y \leq G$. Избираме \mathbb{F}_q -базис $\varphi_1, \dots, \varphi_{l(A)}$ на $\mathcal{L}(A)$, и \mathbb{F}_q -базис $\psi_1, \dots, \psi_{l(Y)}$ на $\mathcal{L}(Y)$. Образоваме матрицата $S = (S_{ij}) \in M_{l(A) \times l(Y)}(\mathbb{F}_q)$, $1 \leq i \leq l(A)$, $1 \leq j \leq l(Y)$ от синдромите

$$S_{ij} = (\varphi_i \psi_j, f) = \sum_{s=1}^n \varphi_i(P_s) \psi_j(P_s) f_s$$

на f относно рационалните функции $\varphi_i \psi_j \in \mathcal{L}(A+Y) \subseteq \mathcal{L}(G)$. В такъв случай, рационалната функция

$$\Theta = \sum_{i=1}^{l(A)} a_i \varphi_i \in \mathcal{L}(A)$$

е локатор на грешката за e тогава и само тогава, когато

$$\sum_{i=1}^{l(A)} a_i S_i = 0_{1 \times l(Y)}$$

за редовете $S_i = (S_{i,1}, \dots, S_{i,l(Y)})$ на матрицата S .

Доказателство: От $A + Y \leq G$ следва $\mathcal{L}(A + Y) \subseteq \mathcal{L}(G)$, защото ако $\text{div}(f) + A + Y \geq 0$ за $f \in F$, то $\text{div}(f) + G = [\text{div}(f) + AY] + [G - (A + Y)] \geq 0$. Освен това, $\varphi_i \in \mathcal{L}(A)$, $\psi_j \in \mathcal{L}(Y)$ означават $\text{div}(\varphi_i) + A \geq 0$, $\text{div}(\psi_j) + Y \geq 0$, така че $\text{div}(\varphi_i \psi_j) + A + Y = [\text{div}(\varphi_i) + A] + [\text{div}(\psi_j) + Y] \geq 0$. Това обяснява $\varphi_i \psi_j \in \mathcal{L}(A + Y) \subseteq \mathcal{L}(G)$. Твърдим, че $(\varphi_i \psi_j, c) = 0$ за $\forall 1 \leq i \leq l(A)$, $\forall 1 \leq j \leq l(Y)$, така че $S_{ij} = (\varphi_i \psi_j, e)$. По предположение, $c \in C^*(X, D, G) = C(X, D, G)^\perp$, така че $(\rho, c) = 0$ за $\forall \rho \in \mathcal{L}(G)$. В частност, за $\rho = \varphi_i \psi_j \in \mathcal{L}(G)$.

Съгласно Твърдение 19.3, $\Theta = \sum_{i=1}^{l(A)} a_i \varphi_i \in \mathcal{L}(A) \subset \cap_{i=1}^n \mathcal{O}_{P_i}(X)$ е локатор на грешката за e тогава и само тогава, когато

$$\begin{aligned} (\Theta \psi_j, e) &= \left(\sum_{i=1}^{l(A)} a_i \varphi_i \psi_j, e \right) = \sum_{i=1}^{l(A)} a_i \sum_{s=1}^n \varphi_i(P_s) \psi_j(P_s) e_s = \\ &= \sum_{i=1}^{l(A)} a_i (\varphi_i \psi_j, e) = \sum_{i=1}^{l(A)} a_i S_{ij} = 0 \quad \text{за } \forall 1 \leq j \leq l(Y). \end{aligned}$$

Последното е еквивалентно на

$$\sum_{i=1}^{l(A)} a_i (S_{i,1}, S_{i,2}, \dots, S_{i,l(Y)}) = \sum_{i=1}^{l(A)} a_i S_i = 0_{1 \times l(Y)},$$

Q.E.D.

ЛЕМА 19.5. Ако $\deg(G) > 2g - 2$ и съществува дивизор $A' \in \text{Div}(F)$ с $l(A') \geq t + 1$ и $0 \leq \deg(A') \leq \deg(G) - (2g - 1) - t$, то съществуват дивизори $A, Z, Y \in \text{Div}(F)$, така че $l(A) \geq t + 1$, $\text{Supp}(A) \cap \text{Supp}(D) = \emptyset$, $\deg(A) \leq t + r$, $Z \leq G$, $\deg(Z) \geq t + r + 2g - 1$, $\deg(Y) \geq t + 2g - 1$, $\text{Supp}(Y) \cap \text{Supp}(D) = \emptyset$, $A + Y \leq G$.

Доказателство: Ако $\text{Supp}(A') \cap \text{Supp}(D) = \emptyset$, вземаме $A = A'$. Ако $\text{Supp}(A') \cap \text{Supp}(D) = \{P_1, \dots, P_k\}$ за някое $1 \leq k \leq n$ и коефициентите на P_i в A' са n_i за $1 \leq j \leq k$, то избираме афинна крива $X_0 \subset X$, съдържаща P_1, \dots, P_k и рационална функция f върху X_0 с $v_{P_i}(f) = -n_i$. Тогава $A = A' + \text{div}(f)$ има $\text{Supp}(A) \cap \text{Supp}(D) = \emptyset$ и $\deg(A) = \deg(A')$, $l(A) = l(A')$. По Теоремата на Riemann $l(A') \geq \deg(A') - g + 1$. По предположение, $u = l(A') - (t + 1) \geq 0$. Следователно $u + t + 1 = l(A) \geq \deg(A) - g + 1$, откъдето $0 \leq \deg(A) = r \leq t + u + g$.

Избираме $Z = G$ и $Y = G - A$. В резултат,

$$\deg(Z) = \deg(G) \geq \deg(A') + 2g - 1 + t = t + r + 2g - 1,$$

$$\deg(Y) = \deg(G) - \deg(A) \geq t + 2g - 1$$

и $A + Y = G$, Q.E.D.

ЛЕМА 19.6. Ако $2t < \deg(G) - (3g - 2)$, то съществува дивизор $A' \in \text{Div}(F)$ с $l(A') \geq t + 1$ и $0 \leq \deg(A') \leq \deg(G) - (2g - 1) - t$ от предишната лема.

Доказателство: По предположение,

$$t + g \leq \deg(G) - 2g + 1 - t,$$

така че съществува цяло число

$$t + g = a \leq \deg(G) - 2g + 1 - t.$$

За произволна точка $Q \notin \text{Supp}(D)$ избираме $A' = aQ$. Тогава

$$l(A') = l(aQ) \geq \deg(aQ) - g + 1 = a - g + 1 = t + 1,$$

Q.E.D.

SV-АЛГОРИТЪМ ЗА ДЕКОДИРАНЕ (СКОРОВОГАТОВ-ВЛАДУТ, 1990)

Нека $c \in C^*(X, D, G)$, $f = c + e$ за дивизор G от степен $\deg(G) > 2g - 2$.

Предварително стъпка 0: Избираме дивизори $A \in \text{Div}(F)$ с $l(A) > t$, $\deg(A) \leq \deg(G) - (2g - 1) - t$ и $Z, Y \in \text{Div}(F)$ с $Z \leq G$, $A + Y \leq G$, $\deg(Z) \geq t + r + 2g - 1$, $\deg(Y) \geq t + 2g - 1$. Построяваме базис $\rho_1, \dots, \rho_{l(Z)}$ на $\mathcal{L}(Z)$, базис $\varphi_1, \dots, \varphi_{l(A)}$ на $\mathcal{L}(A)$ и базис $\psi_1, \dots, \psi_{l(Y)}$ на $\mathcal{L}(Y)$.

Стъпка 1: Пресмятаме матрицата $S = (S_{ij})$ от синдроми

$$S_{ij} = (\varphi_i \psi_j, f) = \sum_{s=1}^n \varphi_i(P_s) \psi_j(P_s) f_s \quad \text{за } 1 \leq i \leq l(A), \quad 1 \leq j \leq l(Y).$$

Стъпка 2: Намираме локатор на грешката $\Theta = \sum_{i=1}^{l(A)} a_i \varphi_i$, така че $\sum_{i=1}^{l(A)} a_i S_i = 0$ за редовете $S_i = (S_{i,1}, S_{i,2}, \dots, S_{i,l(Y)})$ на S .

Стъпка 3: Позиции на грешката

Ако $(\Theta)_0$ е дивизорът на нулите на $\Theta \in F$, то множеството $M \subseteq \{P_1, \dots, P_n\}$ на ненулевите позиции $e_i \neq 0$ на грешката e съдържа в $(\Theta)_0$, $M \subseteq (\Theta)_0$.

Стъпка 4: Пресмятане на грешката

Линейната система уравнения

$$\sum_{P_s \in \text{Supp}(\Theta)_0} \rho_i(P_s) e_s = (\rho_i, f), \quad 1 \leq i \leq l(Z)$$

има единствено решение, което продължаваме с $e_s = 0$ за $P_s \notin \text{Supp}(\Theta)_0$ и получаваме e .

ЗАДАЧА 19.7. Ако при предаване на думи $c^{(k)} \in C_{9,3}^*$ са получени

$$u^{(1)} = (-\bar{1}, \bar{0}, \bar{1}, \dots, \bar{1}), \quad u^{(2)} = (\bar{1}, -\bar{1}, \bar{0}, \bar{1}, \dots, \bar{1}) \in \mathbb{F}_9^9,$$

да се докаже, че

$$c^{(1)} = c^{(2)} = (\bar{1}, \dots, \bar{1}) \in \mathbb{F}_9^9.$$

Да се намерят грешките $e^{(k)} = u^{(k)} - c^{(k)} = u^{(k)} - c$ за $k = 1$ и 2 .

Упътване: Използвайте, че декодирането на $C_{9,3}^*$ е еднозначно при смущения на $t \leq \left\lfloor \frac{d^*-1}{2} \right\rfloor$ символа.

ЗАДАЧА 19.8. Да се намерят матриците на синдромите $S^{(k)} = (S_{ij}^{(k)})_{i=1, j=1}^3 \in M_{3,2}(\mathbb{F}_9)$,

$$S_{ij}^{(k)} = \sum_{s=1}^9 p_s^{i+j-2} u_s^{(k)}.$$

на думите $u^{(k)}$ спрямо базиса $1, x, x^2$ на $V_{9,2} = \mathbb{F}_9^{(3)}[x]$ и базиса $1, x$ на $V_{9,1} = \mathbb{F}_9^{(2)}[x]$.

ЗАДАЧА 19.9. Да се намерят нетъждествено нулеви функции

$$\Theta^{(k)} = a_1^{(k)} + a_2^{(k)} x + a_3^{(k)} x^2 \in V_{9,2} = \mathbb{F}_9^{(3)}[x] \quad c$$

$$\sum_{i=1}^3 a_i^{(k)} S_i^{(k)} = (\bar{0}, \bar{0})$$

за редовете $S_1^{(k)}, S_2^{(k)}, S_3^{(k)} \in M_{1,2}(\mathbb{F}_9)$ на $S^{(k)}$.

Така намерените $\Theta^{(k)}$ са локатори на грешките e на $C_{9,3}^*$ с тегло $w(e) \leq t = 2$, защото $\mu = 1 > t + (2g - 2) = 0$.

ЗАДАЧА 19.10. Да се намерят множествата

$$(\Theta^{(k)})_0 = \{p_i \in \mathbb{F}_9 \mid \Theta^{(k)}(p_i) = 0, \quad 1 \leq i \leq 9\} = \{p_{i(k)}, p_{j(k)}\}, \quad 1 \leq i(k) < j(k) \leq 9$$

на нулите на $\Theta^{(k)}$ за $1 \leq k \leq 2$.

ЗАДАЧА 19.11. Да се намерят единствените ненулеви решения $x^{(k)} = (x_{i(k)}, x_{j(k)}) \in \mathbb{F}_9^2$ на системите линейни уравнения

$$p_{i(k)}^s x_{i(k)} + p_{j(k)}^s x_{j(k)} = \sum_{r=1}^9 p_r^s u_r^{(k)}, \quad \forall 0 \leq s \leq 3.$$

Да се провери, че думите $\varepsilon^{(k)} \in \mathbb{F}_9^9$ с $\varepsilon_{i(k)}^{(k)} = x_{i(k)}$, $\varepsilon_{j(k)}^{(k)} = x_{j(k)}$ и $\varepsilon_r^{(k)} = 0$ за $\forall r \in \{1, \dots, 9\} \setminus \{i(k), j(k)\}$ съвпадат с грешките $e^{(k)}$ от задача 19.7.

Упътване: $\bar{0}^0 = \bar{1}$.