windows: (proc mon) C:\Users\Sorin\AppData\Local\webplatformchannel.exe

Curs 3 STLS II

Coduri de evaluare

K corp, $|K| = q = p^\alpha$

$k, n : 1 \leq k \leq n \leq q$

$M = \{a_1, \dots, a_n\} \subseteq K$ etichete identificate

$i \neq j \Rightarrow a_j \neq a_i$

$C = \{(f(a_1), \dots, f(a_n)) \mid f \in K[X], \deg f < k\} \leq K^n$ (polinom, num. vect.)

(Classic) Reed-Solomon Code $\leftrightarrow$ Shamir Secret Sharing

$f = s + t_1 X + \dots + t_{k-1} X^{k-1}$

"x_i" $\leftarrow f(x_i)$ $(x_i, f(x_i))$

Th $[n, k, n-k+1]$ R-S code (Reed-Solomon)

$\forall$ cuvânt de cod are cel puțin $n-(k-1)$ coordonate diferite de 0.

$\forall c \in C \quad wt(c) \geq n-k+1$

Dacă $f(x) = (x-a_1)(x-a_2)\cdots(x-a_{k-1})$,

$wt(c_f) = n-k+1 \Rightarrow \boxed{d(C) = n-k+1}$

Algoritmul Berlekamp-Welch

$t \geq 1, \quad n = 3t+1$

Th $\exists$ procedură rapidă ($\mathcal{O}(n^2)$) pt. a corecta un nr de $e < t$ erori în C

Idee: Se consideră un polinom $Q(x,y) = f_0(x) - f_1(x)\,y$.

$f_0, f_1 \in K[x]$, $\deg f_0 \leq 2t$ [$2t+1$ necunoscute], $\deg f_1 \leq t$ [t necunoscute] cu $f_1(0) = 1$.

Se recepționează cuvântul $(y_1, \ldots, y_n)$ și s-a stabilit că este incorect (nu știm var. corectă).

Construim sistem de necunoscute pt. el. (x_k - cunoscut (elem. construcție cod), y_k - cunoscut)

$$\begin{cases} Q(x_k, y_k) = 0 \\ k = 1, \ldots, n \end{cases} \qquad \begin{matrix} (2t+1)+t = 3t+1 \\ \text{necunoscute} \end{matrix}$$

$n = 3t+1$ ecuații

Din rezolvare $\Rightarrow f_1(x), f_0(x)$. Se face împărțirea cu rest în $K[x]$ (cu algoritmul lui Euclidian cu gradul polinoamelor).

Se află $f(x) = \dfrac{f_0(x)}{f_1(x)}$ cu rest $= 0$

De ce? $P(x) = Q(x, f(x))$, f polinom necunoscut.

$\deg P(x) \leq 2t$, are cel puțin $n-e$ rădăcini (coordonatele y_i corecte)

Dar $n-e > n-t > 3t-t = 2t$ (polinom cu mai multe rădăcini decât gradul lui)

Dacă $P \equiv 0 \Rightarrow f_0(x) = f(x) f_1(x)$ este identitate polinomială

$c_f = (f(x_1), \dots, f(x_n))$. □

Codul Reed-Müller (1950) pt. $K = \mathbb{F}_2$

$\mathbb{F}_2[x_1, \dots, x_m] \quad 0 \neq f = \sum k_{e_1 \dots e_m} x_1^{e_1} \cdots x_m^{e_m}$

$\deg f = \max \{ e_1 + e_2 + \dots + e_m \mid k_{e_1 \dots e_m} \neq 0 \}$

$\deg 0 = -\infty$.

$\mathbb{F}_2^m = \{P_1, \dots, P_n\}, \quad n = 2^m$

$f \rightsquigarrow c_f = (f(P_1), \dots, f(P_n)) \in K^n$.

asociere cuvânt de cod

peste $\mathbb{F}_2$, funcția x și x^2 se comportă la fel

$0 \leq e_i \leq 1 \quad ; \quad 0^0 = 1$

$V_r = \{ f \in K[x_1, \dots, x_m] \mid \deg f \leq r \}$ $= V$

$\dim V_r = \sum_{i=0}^{r} \binom{m}{i}$, $\dim V = 2^m$.

$0 \leq r \leq m$

$RM(r, m) = \{ (f(P_1), \dots, f(P_n)) \mid f \in V_r \}$ comb

codul Reed-Müller (Reed-Müller)

(Th) $[2^m, \sum_{j=0}^{r} \binom{m}{j}, 2^{m-r}]$

• Construcția Plotkin pt. coduri Reed-Muller

Lemă $i = 1, 2$ C_i de parametri $[n, k_i, d_i]$.

Def $C = C_1 \,\&\, C_2 = \{(c_1, c_1 + c_2) \mid c_1 \in C_1,\ c_2 \in C_2\}$

Este un cod $[2n, k_1 + k_2, \min(2d_1, d_2)]$ K^{2n} // subsp. v.

Dem. Consider apl. lin. $\alpha : C_1 \oplus C_2 \longrightarrow C$

$\alpha(c_1, c_2) = (c_1, c_1 + c_2)$ injectivă

$\Rightarrow \dim C = k_1 + k_2$ (dim injectivității)

Obs $wt(c_1) \geq |\underset{\text{suport}}{supp}(c_1) \cap supp(c_2)|$

$wt(c) = wt(c_1) + wt(c_1 + c_2) \geq wt(c_1) + wt(c_1) + wt(c_2) - 2|supp(c_1) \cap supp(c_2)| \leq$

dacă $c_2 \neq 0$

$d_2 \leq wt(c_2)$

dacă $c_2 = 0$: $wt(c) = 2\, wt(c_1) \geq 2 d_1$

dacă $c_i = 0$ și c_j $(j \neq i)$ are pondere minimală, această pondere se atinge pt. c. □

$RM(r, m)$: $RM(0, m) = [2^m, 1, 2^m]$ cod de repetiție

$RM(m, m) = \{0,1\}^{2^m}$

$RM(r, m) = RM(r, m-1) \,\&\, RM(r-1, m-1)$

$RM(r, m)$: lungimea 2^m, $d = \min\left(2 \cdot 2^{m-1-r}, \underset{m-1-(r-1)}{2}\right) = 2^{m-r}$

$\dim RM(r, m) = \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} =$

$= 1 + \sum_{i=0}^{r-1} \left[\binom{m-1}{i+1} + \binom{m-1}{i}\right] =$

$= 1 + \sum_{i=0}^{r-1} \binom{m}{i+1} = \sum_{i=0}^{r} \binom{m}{i}$

Ex: $RM(1,5) = [32, 6, 16]$ Mariner Mars Mission

Coduri Reed-Solomon generalizate

K corp, $|K| = q$, $2 \le d \le n \le q$

fixăm $a = (a_1, \dots, a_n) \in K^n$, $i \neq j \Rightarrow a_i \neq a_j$ (structură)

fixăm $v = (v_1, \dots, v_n) \in K^n$, $v_i \neq 0$

$H \in \mathcal{M}_{(d-1)\times n}(K)$

$$H = \begin{pmatrix} v_1 & \dots & \dots & v_n \\ a_1 v_1 & \dots & \dots & a_n v_n \\ a_1^2 v_1 & \dots & \dots & a_n^2 v_n \\ \vdots & & & \vdots \\ a_1^{d-2} v_1 & \dots & \dots & a_n^{d-2} v_n \end{pmatrix}$$

matricea de control

Orice minor $(d-1)\times(d-1)$ al lui H are $\det \neq 0$.

$v_{i_1} \cdots v_{i_{d-1}} \prod (a_j - a_i)$

$$GRS_d(a, v) = \{ c \mid c \in K^n \text{ și } Hc^T = 0 \}$$

generalized Reed-Solomon

$d(GRS_d(a, v)) = d$

$d_{dim} = n - rk(H) = n - d + 1$ $\Rightarrow [n, n-d+1, d]$

Obs. K corp finit $\Rightarrow K^\times$ ciclic

α generator al lui $K^\times$ $\langle \alpha \rangle = K^\times$.

$v = a = (1, \alpha, \alpha^2, \dots, \alpha^{q-2})$ Reed-Solomon dim $q-2$

Def Un cod s.n. ciclic dacă $\forall c = (c_1, \dots, c_n) \in C$, atunci $(c_n, c_1, c_2, \dots, c_{n-1}) \in C$.

Th Un cod Reed-Solomon $\langle \alpha \rangle$ este ciclic.

Grupuri ciclice $(\mathbb{Z}_n, +, 0)$ izomorfism

"logaritmul discret este dificil" → numai în grupuri multiplicative, respectiv în grupuri aditive pentru curbe eliptice

x generator $\Leftrightarrow \gcd(x, n) = 1$

$y \in \mathbb{Z}_n$, x a.î. $\langle x \rangle = (\mathbb{Z}_n, +, 0)$ grup aditiv

Cum se calc. r a.î. "x^r" $= rx = y$?

$\gcd(x, n) = 1 \Rightarrow x$ multiplicativ inversabil $\Rightarrow$

$\exists\, x^{-1} \bmod n$ (Euclid extins) $\mathcal{O}((\log_n)^3)$

$r = x^{-1} y \bmod n$ "logaritmul discret"

$(\mathbb{Z}_n, +, \cdot, 0, 1)$ apare grupul unităților (elem. inversabile)

$(\mathbb{Z}_n^\times, \cdot, 1) = \{x \mid \gcd(x, n) = 1\}$ = generatorii lui $(\mathbb{Z}_n, +, 0)$

Th1 $(\mathbb{Z}_n^\times, \cdot, 1)$ ciclic $\Leftrightarrow n \in \{2, 4, p^\alpha, 2p^\alpha\}$ (p prim impar)

Th2 K corp, G finit $\leq (K^\times, \cdot, 1)$ (subgrup; grupul multiplicativ al corpului K)

$\Rightarrow G$ ciclic

- $\mathbb{R}$, $G = \{+1, -1\}$
- $\mathbb{C}$, $G = \langle \cos\frac{2\pi i}{n} + i \sin\frac{2\pi i}{n} \rangle$ $|G| = n$

$(G, \cdot, 1) \simeq (\mathbb{Z}_n, +, 0)$

- K corp finit $\Rightarrow K^\times$ ciclic

$\forall \alpha\ \exists!$ K corp finit cu p^α elemente, p prim $\rightarrow \mathbb{F}_{p^\alpha}$

$\alpha = 1 \Rightarrow K = \mathbb{Z}_p$ $\quad \mathbb{F}_p = \mathbb{Z}_p$

$\alpha > 1 \rightarrow \exists\, \mathbb{F}_{p^\alpha}$ $\quad \mathbb{F}_{p^\alpha} \neq \mathbb{Z}_{p^\alpha}$

- se găsește un polinom ireductibil $f \in \mathbb{Z}_p[X]$ de grad α și $\mathbb{F}_{p^\alpha} = \mathbb{Z}_p[X]/(f)$ — idealul generat de polinomul f în inelul $\mathbb{Z}_p[X]$.

$p=2$, $k=2$ → $f = X^2+X+1$ ireductibil peste $\mathbb{F}_2$

Fie ω „soluție" a lui X^2+X+1 $(\omega^2+\omega+1=0) \Rightarrow$

$2=0$, $1=-1$

$\Rightarrow \omega^2 = \omega+1$

$\omega^n : \omega,\ \omega^2 = \omega+1,$

$\omega^3 = \omega^2+\omega = 2\omega+1 = 1$

$\mathbb{F}_4 = \{0, 1, \omega, \omega+1\}$ ⟸

ω generator ⇒ $\mathbb{F}_4$ ciclic

$\mathbb{Z}_7$ ciclic: $2^n \bmod 7$: 2, 4, 1 ord 2 = 3

$3^n \bmod 7$: 3, 2, 6, 4, 5, 1 ⇒ 3 generator

$(\mathbb{Z}_7^*, \cdot, 1) \simeq (\mathbb{Z}_6, +, 0)$

generatorii: numerele relativ prime cu 6 : 1, 5

generator 3, 5 $\quad 3^k \longleftrightarrow g \cdot k \,/\, 1 \cdot k$ — generator

$5^n \bmod 7$: 5, 4, 6, 2, 3, 1

$\log_5 2 \bmod 7 = 4$ (log discret)

$\mathbb{Z}_{11}$: $2^n \bmod 11$: 2, 4, 8, 5, 10, 9, 7, 3, 6, 1

2 generator pt $(\mathbb{Z}_{11}^*, \cdot, 1) \simeq (\mathbb{Z}_{10}, +, 0)$

generatorii: 1, 3, 7, 9

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\} \simeq (\mathbb{Z}_4, +, 0)$

Generatorii lui $\mathbb{Z}_{11}^*$: $2^1, 2^3, 2^7, 2^9$ (2, 8, 7, 6) 6 generator multiplicativ