Décodage

I. Algorithme basique

II. "Error-correcting pair"

III. Guruswami-Sudan

I. On va décoder le code $\mathcal{C}_\Omega(\mathcal{X}, \mathcal{Y}, \mathcal{D})$

Notat° : $\delta_p := \deg(\mathcal{D}) - 2g + 2$ $\quad [n, k, d]$

Thm. L'algorithme basique décode jusqu'à $\left\lfloor \frac{\delta_p - g - 1}{2} \right\rfloor$ erreurs en $O(n^3)$ opérat°.

Prop : Soit $\mathcal{C}$ un code linéaire, de matrice de parité H.
Supposons que $y = c + e$, avec $c \in \mathcal{C}$
et que je connais un ensemble J tq $\{i \mid e_i = 0\} \subset J$
et $|J| \leq d_{min}(\mathcal{C}) - 2$
Alors le vecteur e est l'unique solution de l'équat°. $H^t x = H^t y$ avec $x_i = 0 \ \forall i \in J$.

→ On cherche une fct f qui localise les erreurs.

→ Soit F un diviseur de $\mathcal{X}$.

$f \in L(F)$.

→ Notons : $I = \{ i \mid e_i \neq 0 \}$, $\#I = t$

$Q = \sum_{i \in I} P_i$, $P_i \in \mathcal{P}$

→ On veut $f \in L(F-Q)$.

$\deg(F) \geq t + g_{\mathcal{X}}$ avec $g_{\mathcal{X}}$ genre de $\mathcal{X}$.

→ On connait les equat° de parité : $Hy = Hc$

$$\sum_{i=1}^{n} y_i h(P_i) = \sum_{i=1}^{n} e_i h(P_i) \quad \forall h \in L(D)$$

$$= \sum_{i \in I} e_i h(P_i)$$

→ Pour $g \in L(D-F)$, on a $fg \in L(D)$

Si $f(P_i) = 0 \quad \forall i \in I$, alors

$$\sum_{i \in I} y_i f(P_i) g(P_i) = 0$$

$$\sum_{i=1}^{n} e_i f(P_i) g(P_i) = 0 \iff \sum_{i=1}^{n} y_i f(P_i) g(P_i) = 0$$

$$K(y, F) = \left\{ f \in L(F) \mid \sum_{i=1}^{n} y_i f(P_i) g(P_i) = 0 \quad \forall g \in L(D-F) \right\}$$

→ On a $L(F-Q) \subset K(y,F)$.

Lemme : Si $\deg(D-F) > t + 2g - 2$

alors $L(F-Q) = K(y,F)$

Preuve : Soit $f \in K(y,F)$

$$\sum_{i=1}^{n} y_i f(P_i) g(P_i) = 0 \qquad \forall g \in L(D-F)$$

$$\sum_{i \in I} \underbrace{e_i f(P_i)}_{w_i} g(P_i) = 0 \qquad \forall g \in L(D-F)$$

$w = (w_i)_{i \in I} \in \mathcal{C}_L(\mathcal{X}, Q, D-F)^{\perp}$

→ on veut que $\mathcal{C}_L(\mathcal{X}, Q, D-F)^{\perp} = \{0\}$

→ on veut $\dim(\Omega(D-F-Q)) < 0$

$\dim(\Omega(D-F-Q)) = 2g-2 - \deg(D-F) + t$

J'ai $\deg(D-F) > t + 2g - 2$

Les deux conditions sur F :

(i) $\deg(F) \geq t + g_x$

(ii) $\deg(D-F) > t + 2g - 2$

Pour avoir (i) et (ii) il faut que :

$$t \leq \left\lfloor \frac{\delta_T - g - 1}{2} \right\rfloor$$

Lemme. Si $\deg(F) \leq \deg(D) - t - 2g + 1$ alors $|\{j \in \{1,\dots,n\} \mid f(P_j) = 0\}| \leq d - 1$ pour $f \in L(F - Q)$.

Preuve: $f \in L(F)$, $(f) \geq -F$

$$\#\text{zéro}(f) \leq \deg(F) \leq \deg(D) - t - 2g + 1 \leq \delta_T - 1$$

Récalcul: Choisir F satisfaisant (i) et (ii) avec $t = \left\lfloor \frac{\delta_T - g - 1}{2} \right\rfloor$. Calculer une base de $L(F)$ et $L(D-F)$

Algo: Entrée: $y = c + e$
Sortie: c ou "?" (si $w(e) > \left\lfloor \frac{\delta_T - g - 1}{2} \right\rfloor$)

- Calculer $K(y, F)$
- Si $K(y,F) = \{0\}$ (alors $w(e) > \left\lfloor \frac{\delta_T - g - 1}{2} \right\rfloor$)
  Retourner "?"

→ Sinon
- Prendre $f \in K(y,F)$
- Calculer $S = \{j \in \{1,\dots,n\} \mid f(P_j) = 0\}$
- Calculer l'ens. des solut° du système : $\begin{cases} H^t x = H^t y \\ x_i = 0 \quad \forall i \notin S. \end{cases}$ (S)

→ (Si) S a une unique sol e alors retourner $y - e$

(→ Sinon Retourner "?")

II) Error correcting pair

déf: Soient $A, B, \mathcal{C}$ codes linéaires (A,B) est appelée "t-error correcting pair" si:

(i) $A * B \subset \mathcal{C}^{\perp}$

(ii) $k(A) > t$

(iii) $d(B^{\perp}) > t$

(iv) $d(A) + d(\mathcal{C}) > n$

$A = \mathcal{C}_L(X, \mathcal{P}, F)$

$B = \mathcal{C}_L(X, \mathcal{P}, \mathcal{D} - F)$

(ii) $\deg(F) \geq t + g_X$

(iii) $\deg(\mathcal{D} - F) > t + 2g - 2$

$K(y) = \{ a \in A \mid y \cdot (a * b) = 0 \quad \forall b \in B \}$

$L(F, Q) : A(I) = \{ a \in A \mid a_i = 0 \quad \forall i \in I \}$

III) Guruswami - Sudan.

R.S $[n,k,d]$ $(x_i)_i$ support, $(y_i)_i$ mot reçu
on veut corriger t erreurs.

Pb: Trouver $p \in \mathbb{F}_q[X]_{<k}$ tq $p(x_i)=y_i$ pour au moins $n-t$ valeurs de i.

(0) $n\binom{r+1}{2} < \left(\frac{\ell}{k}+1\right)\left(\ell+1-\frac{k}{2}\left(\frac{\ell}{k}\right)\right)$
avec $\ell < r(n-t)$

1) Trouver $Q \in \mathbb{F}_q[X][Y]$, $\deg_{1,k-1}(Q)<\ell$ tq
$Q(x_i,y_i)=0 \quad \forall i$
avec multiplicité r

2) Factoriser Q
Retourner les $p \in \mathbb{F}_q[X]$ tq $Q(X,p(X))=0$
et $p(x_i)=y_i$ pour au moins $n-t$ valeurs

- On veut décoder $C_L(X, P, \alpha P_0)$

Pb: Soit $y=(y_1,\dots,y_n)$, trouver toutes les fcts $h \in L(\alpha P_0)$ tq $h(P_i)=y_i$ pour au moins $n-t$ valeurs.

(0) Choisir r et ℓ

(1) Trouver $Q \in \mathbb{F}_q(X)[Y]$ tq :
(i) $Q(\cdot,f) \in L(\ell P_0)$, $\forall f \in L(\alpha P_0)$
(ii) $\forall i \in \{1,\dots,n\}$, $\forall h \in \mathbb{F}_q(X)$
si $h(P_i)=y_i$ alors $v_{P_i}(Q(h)) \geq r$.

(2) Trouver les racines $h \in L(\alpha P_0)$ de Q
tq $h(P_i)=y_i$ pour au moins $n-t$ valeurs

coeff$(y^j) \in L((\ell-\alpha i)P_0)$

$C_L(\alpha, P_{-\alpha}P_\infty)$ $\quad P_1 \dots P_n$ $\quad$ auxiliaire π

$g=(y_1 \dots y_n)$

$\{f \in L(\alpha P_\infty),\ |\{i,\ f(P_i)=y_i\}| \geq n-t\}$

① $Q(T) \in L(\alpha P_\infty)(T)$

- $Q(T)=\sum Q_i T^i \quad Q_i \in L\left[(\pi(n-t)-i\alpha P_\infty\right]_{-1}$
- $Q(y_i)(P_i)=0$ "avec mult." $i=1..n$

$$Q(Y+y_i)=\sum \tilde{Q}_j Y^j$$

Si $v_{P_i}(\tilde{Q}_j)+j<\pi$

$\Rightarrow \tilde{Q}_j=0$

$Q(f) \in L(\pi(n-t)-1)$

$f(P_i)=y_i$ (lemme)

$\Rightarrow v_{P_i}(Q(f)) \geq \pi$

$$Q(f) \in L\Big(\underbrace{\pi(n-2)-\pi(P_{i_1}+\dots P_{i_{n-t}})}_{<0}\Big)$$

$Q(f)=0$