Cryptographie

26 septembre 2023

1 Codes

1.1 Définitions

Définition 1.1.1. La distance de Hamming sur $\mathbb{F}_q^n$ est donnée par $d(x, y) = \#\{i | x_i \neq y_i\}$.

Définition 1.1.2. Un $[n, k]_q$ code linéaire est un sev de $\mathbb{F}_q^n$ de dim k. Un $[n, k, d]_q$ code définit une distance minimale des élts du sev.

Définition 1.1.3. On peut def un code par une matrice génératrice est une matrice dont les colonnes engendre le code. (on la suppose de taille $n * l$, $l = k$.)

Définition 1.1.4. On peut aussi def par une matrice de parité. (i.e. $[n, k]_q = \ker(H)$)

(Le nom parité vient, du cas $\mathbb{F}_2$.)

Définition 1.1.5. Matrice génératrice systématique:

$$M = [id_k, A]$$

Elle est unique (combinais lineaire de A $\implies$ tjr une base mais pas le mm sev)

Définition 1.1.6 (Distance minimale)**.** Etant donné un code C, $d_C = \inf\{d(x, y) | x \neq y\}$. Ou

$$\inf\{d(x, 0)\}$$

Lemme 1.1.7. *Etant donné un $[n, k, d]_q$-code linéaire C, pour tout deux x, y:*

$$B(x, [(d-1)/2]) \cap B(y, [(d-1)/2]) = \emptyset$$

Théorème 1.1.8 (Singleton)**.** $d_C \leq n - k + 1$.

Théorème 1.1.9 (Pas de redondance inutile)**.** *Les codes MDS (qui atteignent la borne) vérifient:*

- *Tout ensemble de k colonnes d'une matrice génératrice G d'un MDS est inversible.*
- *Tout ensemble de $n - k$ colonnes d'une matrice de parité de G d'un MDS est inversible.*

2 Codes étendus

Définition 2.0.1. C un $[n, k]_q$-code tel que $\exists c \in C$, $\sum c_i \neq 0$. Le code étendu de C est

$$Ext(C) = \{(c_1, \dots, c_n, -\sum c_i) | (c_i) \in C\}$$

Proposition 2.0.2. $H' = \begin{pmatrix} H & & 0 \\ & & \vdots \\ & & 0 \\ 1 & \dots & 1 \end{pmatrix}$ *est une matrice de parité de $Ext(C)$ et $Ext(C)$ est un $[n+1, k]_q$*

2.1 Poinconnage

Définition 2.1.1. C un $[n, k, d]_q$-code et $I \subset [1, n]$.

$$P_I(C) := \{(c_i)_{i \in [1,n] - I}\}$$

(On enleve des lignes de la matrice)

Notation: Etant donné M une matrice et I des indices, on note M_I la matrice indexée par I.

Proposition 2.1.2. *Soit $G \in \mathbb{F}_q^{k*n}$ une matrice génératrice de C, alors $G_{i \in [1,n] - I}$ est une matrice génératrice de $P_I(C)$.*

Proposition 2.1.3. *$P_I(C)$ est un $[n', k', d']_q$ code avec $n' = n - \#I$, $k' \leq K$ et $d - \#I \leq d' \leq d$.*

Preuve: Pour d', soit $c \in C$, alors

$$|c| - \#I \leq |c_{i \in [1,n] - I}|$$

2.2 Raccourcissement

Définition 2.2.1.

$$R_I(C) := \{(c_i)_{i\in[1,n]-I} | c \in C \text{ } et \text{ } (c_i)_{i\in I} = 0\}$$

(On enleve des lignes de la matrice de parité)

Proposition 2.2.2. *Si H est une matrice de parité de C alors $H_{[1,n]-I}$ est une matrice de parité de $R_I(C)$.*

Preuve: $H' := H_{[1,n]-I}$
(*) Mq $R_I(C) \in Ker(H')$. Soit $c' \in R_I(C)$, $\exists c \in C$ tq $c_{[1,n]-I} = c'$, or $Hc^T = 0 = H'c' + H_I c_I = H'c'$ (**) Mq $Ker(H') \subseteq R_I(C)$. Soit $c' \in Ker(H')$ donc $H'c'^T = 0$. Soit $c \in \mathbb{F}_q^n$ tq $c_I = 0$ et $c_{[1,n]-I} = c'$. On a alors $Hc^T = H'c'^T + H_I c_I = H'c'^T = 0$ donc $c \in C$ et donc $c' \in R_I(C)$.

Proposition 2.2.3. *$R_I(C)$ est un $[n', k', d']_q$-code avec $n' = n - \#I$, $k' \geq k - \#I$, $d' \geq d$.*

Preuve: Pour d', $\{c | c_{[1,n]-I} \in R_I(C) + c_I = 0\} \subseteq C$ d'ou $d' \geq d$.

Proposition 2.2.4. *$P_I(C)^\perp = R_I(C)$ et $R_I(C)^\perp = P_I(C)$.*

2.3 Subfield Subcode

Dans la suite $m \geq 1$.

Définition 2.3.1. Soit C un $[n, k]_{q^m}$ code linéaire. Le subfield subcode de C est $C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$.

Proposition 2.3.2. *Si C est $[n, n-r, d]_{q^m}$. Alors $C|_{\mathbb{F}_q}$ est $[n, \geq n - mr, \geq d]_q$.*

Preuve: $C|_{\mathbb{F}_q} \subseteq C$ donc $d' \geq d$. Pour la dimension on pose

$$\phi : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$$

$$(x_i) \mapsto (x_i^q - x_i)$$

. On a $Ker(\phi) = C|_{\mathbb{F}_q}$. Restreindre à C et conclure.

2.4 Code trace

Définition 2.4.1. Soit $a \in \mathbb{F}_q^n$.

$$Tr_{\mathbb{F}_q^m/\mathbb{F}_q}(a) := a + a^q + \ldots + q^{m-1}$$

Remarque 1. Trace donnée par la mul ! (regarder une base du type $(\alpha^i)_i$)

Proposition 2.4.2. *Tr est à valeur dans $\mathbb{F}_q$*

(juste appliquer frob, sinon trouver la matrice et le pol char qui sont dans $\mathbb{F}_q$)

Proposition 2.4.3. *La trace est $\mathbb{F}_q$-linéaire, surjective et non dégénérée.*

Proposition 2.4.4. *Soit C un $[n, k, d]_{q^m}$ code linéaire, alors $Tr(C)$ est un $[n', k', d']_q$ un code linéaire avec $n' = n$ et $k' \leq mk$.*

Théorème 2.4.5 (Delsarte)**.** $(C|_{\mathbb{F}_q})^\perp = Tr(C^\perp)$ *et* $(Tr(C))^\perp = C|_{\mathbb{F}_q}$.

Preuve: a faire.

3 Reed-Solomon

Définition 3.0.1. Soit $x \in \mathbb{F}_q^n$, (x_i) deux à deux distincts, avec $n \leq q$ et soit $k \leq n$. Le code de Reed-Solomon associé à x est

$$RS_k(x) := \{c = (f(x_1), \ldots, f(x_n)) | f \in \mathbb{F}_q[X]_{<k}\}$$

Proposition 3.0.2. *Une matrice génératrice de $RS_k(x)$ est:* $\begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \vdots & \ldots & \vdots \\ x_1^{k-1} & x_2^{k-1} \ldots & x_n^{k-1} & \end{pmatrix}$

Proposition 3.0.3. *Les RS sont MDS.*

Preuve: On regarde $\phi_{k,x} : \mathbb{F}_q[X]_{<k} \to \mathbb{F}_q^n$ qui a f associe $(f(x_i))_i$. Elle est injective, clair. Soit maintenant, $c = (f(x_1), \ldots, f(x_n)) \neq 0$. Alors $f \neq 0$ et f a au plus $k - 1$ racines distinctes donc $|c| \geq n - k + 1$ donc $d_C \geq n - k + 1$ or avec singleton, on a aussi $d_C \leq n - k + 1$.

Définition 3.0.4 (GRS)**.** On regarde $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ avec $n \leq q$ et (x_i) deux à deux distincts. Soit $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^{*n}$. On déf

$$GRS_k(x, y) = \{c = (y_i f(x_i))_{i \in [1,n]} | f \in \mathbb{F}_q[X]_{<k}\}$$

Proposition 3.0.5. *A nouveau, les GRS sont MDS.*

Preuve: Tous isomorphes, via une isométrie, à des RS. (y_i sont non nuls)

Théorème 3.0.6 ($q <= n$)**.** *L'orthogonal de $RS_q(x)$ est $RS_{q-k}(x)$.*

preuve a faire: (produit scalaire)

Théorème 3.0.7. *Maintenant si $x \in \mathbb{F}_q^n$ tq les x_i sont deux à deux distincts et $y \in (\mathbb{F}_q^*)^n$. Alors,*

$$GRS_k(x, y)^{perp} = GRS_{n-k}(x, y')$$

avec $y'_i = \frac{-1}{y_i \prod_{i \neq j}(x_i - x_j)}$

Preuve: Noter $Q(\alpha) = \prod_{\alpha \neq x_i}(x - \alpha)$. Alors $y'_i = Q(x_i)/y_i$. Puis

$$< (y_i f(x_i))_i, y'_i g(x_i) >= \sum_{\alpha \in \mathbb{F}_q} Q(\alpha) f(\alpha) g(\alpha)$$

Et on se ramène au RS normal.

3.1 Décodeurs uniques

-Berlekamp-Welch: interpolation.
-Euclide etendu: Berlekamp-Massey (vision BCH).

On corrige au plus $[(n-k)/2]$ erreur.

3.2 Décodage en liste

A part quelques exception, les codes sont généralement pas parfait (on atteint pas la borne de Hamming). On a meme souvent que l'union des boules centrées sur le code de rayon $t = (d_C - 1)/2$ ne représentent qu'une petite partie de l'espace ambiant. On peut généralement décoder au delà de $(d_C - 1)/2$.

Idée: On va décoder au delà de $[(d_C - 1)/2]$. Généralement on a seul mot dans la liste de décodage. Si on en a plusieurs, on teste lequel est le plus proche du mot reçu.Pour que le décodeur reste en temps polynomial , il faut que la liste soit de taille polynomiale.

Théorème 3.2.1 (Borne de Johnson)**.** *Soit C un $[n, Rn, \delta n]_q$ un code linéaire. Pour R, δ des constantes. Soit*

$$\rho = (1 - \frac{1}{q})\left(1 - \sqrt{1 - \frac{q\delta}{q-1}}\right)$$

Alors $\forall a \in \mathbb{F}_q^n$,

$$\#(B(y, \rho n) \cap C) \leq q\delta n^2$$

Remarque 2. Pour $q = 2$,

$$\rho = \frac{1}{2}(1 - \sqrt{1 - 2\delta})$$

Pour $q \to \infty$, on a

$$\rho = (1 - \sqrt{1 - \delta})$$

En particulier, pour un GRS, lorsque $n \to \infty$ et donc $q \to \infty$, on a

$$\rho = 1 - \sqrt{R}$$

4 Codes LDPC

Lemme 4.0.1 (Pilling-Up-Lemma)**.** *(p_i), $(p_i = P(b_i = 1)$, b_i une variable aléatoire dans $\mathbb{F}_2$). Soit $y = c + e$ avec $c \in C$ et $e_i \leftarrow$ Bernoulli:*

Pour tout $h \in C^{\perp}$ t.q. $|h| = w$

$$P(< y, h >= 0) = (1 + \prod_{i \in Supp(h)} (1 - 2Pi))$$

(Dans le pdf) En gros l'application c'est que on suppose les équations de parités n'ayant pas de 1 en commun. (Conditionnellement indépendants par rapport à b)

Questions:

1. Etant donné un code LDPC et une matrice de parité quelconque, est-ce qu'on peut trouver une matrice de parité creuse ?

2. $E(\#(mots\ de\ poids\ w\ dans\ code\ dual\ aleatoires)) := E(w) = 2^{n-k} binom(n, w)/2^n$