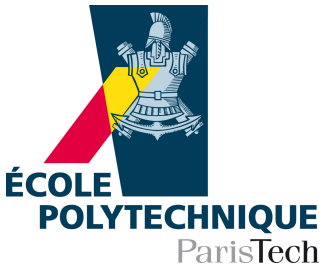
Logarithme discret et décodage des codes de Reed-Solomon

http://arxiv.org/abs/1202.4361

D. Augot, F. Morain
équipe Grace
LIX et INRIA Saclay–Île-de-France



Plan

- Les codes de Reed-Solomon et le problème de leur décodage.
- Les travaux de Cheng et Wan, et la connexion avec le logarithme discret.
- Le sens direct : algorithmes de décodage pour résoudre le problème du logarithme discret.

Codes de Reed-Solomon

Définition

- *Soit* $S = \{x_1, x_2, \ldots, x_n\} \in \mathbb{F}_q$, *avec* $x_i \neq x_j$.
- *La fonction d'évaluation associée est*

$$\begin{array}{rccc} \mathrm{ev}_S : & \mathbb{F}_q[X] & \to & \mathbb{F}_q^n \\ & f(X) & \mapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

- *Pour* $k \leq n$, *le code de Reed-Solomon code* C_k *est*

$$C_k = \{\mathrm{ev}_S(f(X)) \mid \quad \deg f(X) < k\}.$$

C'est un code de paramètres $[n, k, d = n - k + 1]_q$.
Maximal pour la borne de Singleton : c'est un code *MDS (Maximum Distance Separable)*.

Décodage des codes de Reed-Solomon

Problème du décodage (en liste) de C_k

Étant donnés $S = \{x_1, x_2, \ldots, x_n\} \in \mathbb{F}_q$,
$k \leq n$, *un rayon* $\tau \in [1 \ldots n]$,
un mot $y \in \mathbb{F}_q^n$,
trouver : $L_\tau(y) = \{c \in C_k; \quad d(c, y) \leq \tau\}$.

- Quand $n - \tau = \mu < k$, il y a un nombre exponentiel de solutions : interpolation sur μ positions quelconques.
- i.e $\tau > n - k$, qui est le *rayon de recouvrement* de C_k.

Décodage unique, en liste

Proposition (décodage unique)

Soit $\tau \leq \frac{n-k}{2}$. *Alors, pout tout mot* $y \in \mathbb{F}_q^n$, $|L_\tau(y)| \leq 1$.

- Algorithmes de Berlekamp-Massey, Euclide, Gao, etc.

Proposition (Décodage en liste, « borne de Johnson »)

Soit $\tau < n - \sqrt{n(n-d)}$. *Alors, pour tout* $y \in \mathbb{F}_q^n$,

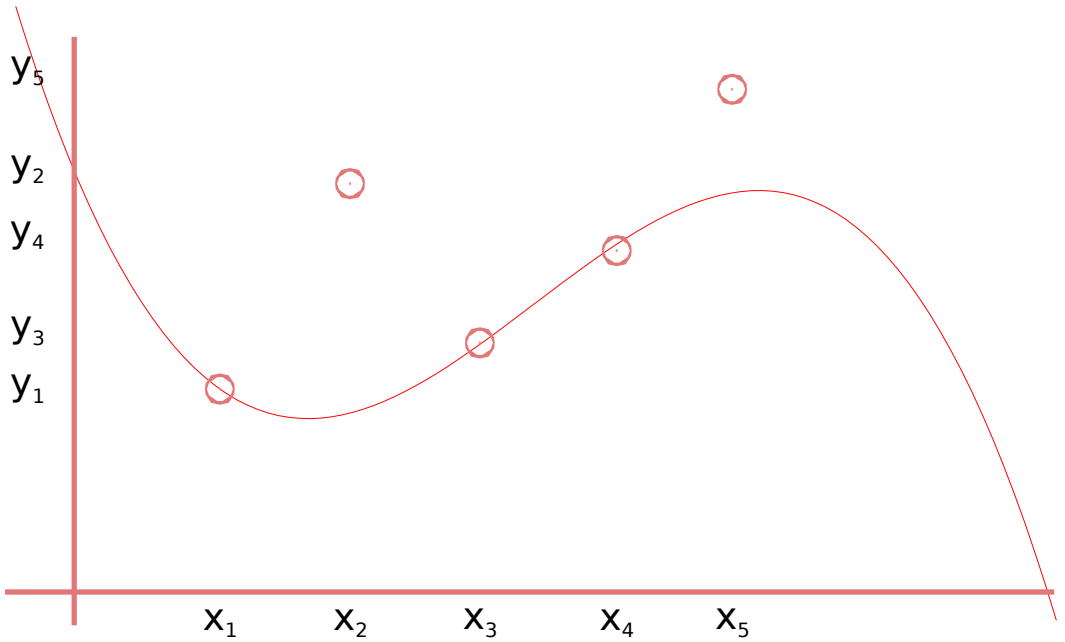
$$|L_\tau(y)| \leq \frac{nd}{(n-\tau)^2 - n(n-d)} = O(n^2).$$

- Algorithme de Guruswami-Sudan.

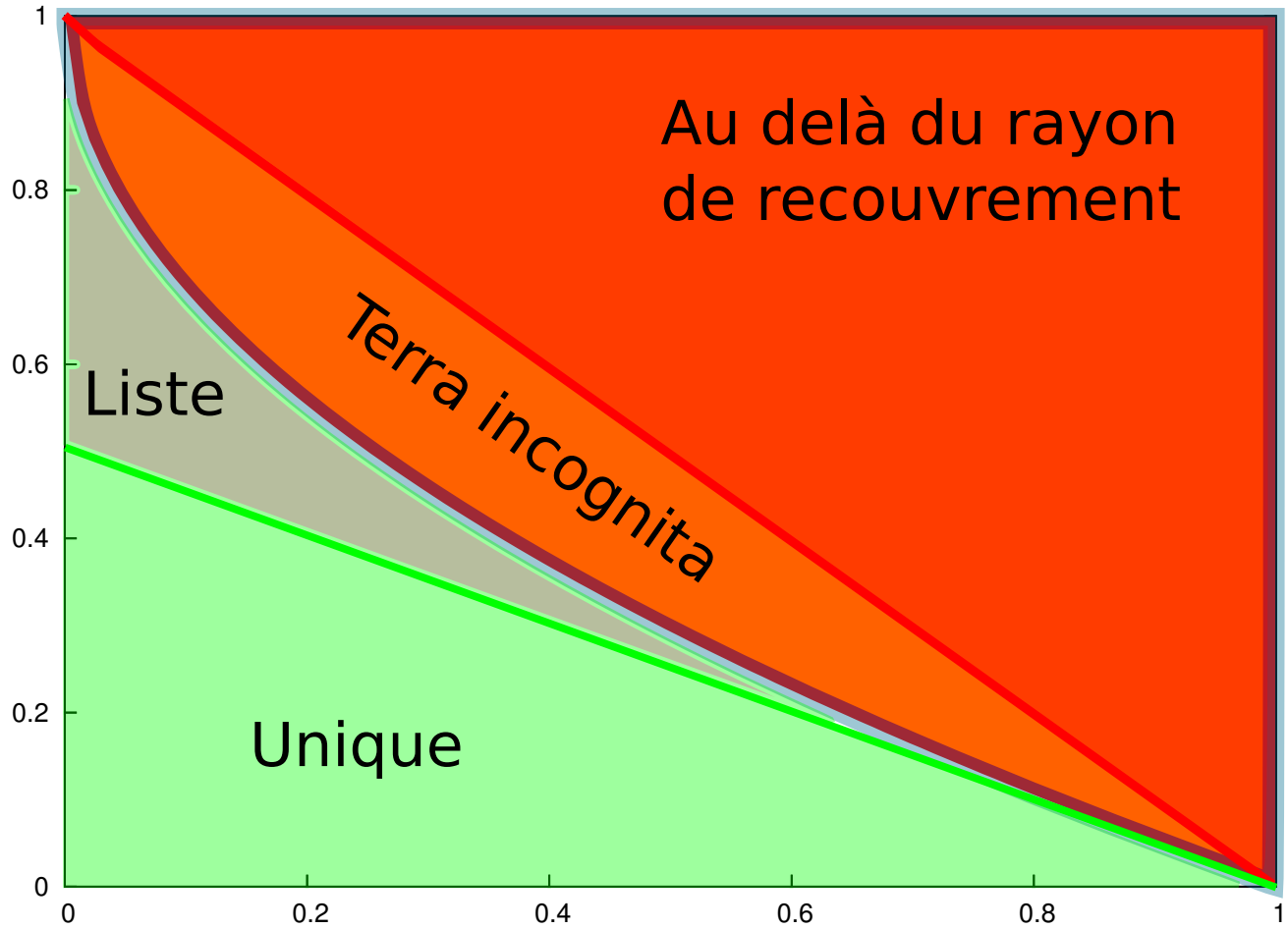
Formulation polynomiale

Problème de la reconstruction de polynômes

Étant donnés $S = \{x_1, x_2, \ldots, x_n\} \in \mathbb{F}_q$,
$k \leq n$, $\mu \in [1 \ldots n]$,
un mot $y \in \mathbb{F}_q^n$,
trouver : $L_\tau(y) = \{f(X) \in \mathbb{F}_q[X]_k;\ |\{i, f(x_i) = y_i\}| \geq \mu\}$.



Comparaison de $\frac{n-k}{2}$, $n - \sqrt{(k-1)n}$, $n-k$



Rayon de décodage relatif $\tau/n \in [0,1]$
en fonction du taux $k/n \in [0,1]$.

Difficulté du décodage

Problème

Le problème du décodage à maximum de vraisemblance est :

étant donné un code linéaire $C \subset \mathbb{F}_q^n$,
un mot $y \in \mathbb{F}_q^n$,
un rayon $\tau \in [1 \dots n]$,
existe-t-il $c \in C$ *tel que* $d(c, y) \leq \tau$ *?*

- NP-complet pour les codes linéaires généraux (Berlekamp et al. 1978).
- Même avec un précalcul infini (Bruck et Naor, 1990).

On ne sait pas bien pour quels codes C, ni pour quels mots y cela va être difficile.

Cas des codes de Reed-Solomon

Les codes de Reed-Solomon sont très structurés, on pourrait s'attendre à ce que le problème deviennent facile.

- Le décodage des codes de Reed-Solomon est NP-complet (Guruswami-Vardy 2005).
- Même avec précalcul infini.
- Une conséquence est que le problème de reconnaître un *"deep-hole"* est difficile.
- On dit que $y \in \mathbb{F}_q^n$ est un *deep-hole* de C_k si et seulement si $d(y, C_k) = n - k$.

  Similaires aux fonctions courbes associées aux codes de Reed-Muller.

Pour quels codes de Reed-Solomon ?

- Pour quelles tailles de corps ?

  Taille de l'alphabet exponentielle en n.

- Pour quels ensembles « support » S ?

  Seul un petit sous-ensemble de $\mathbb{F}_q$ est pris.

- Taux k/n ?

  Arbitraire.

Questions sur le rayon de décodage

- Pour quel rayon $\tau = \tau(n, k, q)$ le décodage jusqu'au rayon τ est difficile ?
- Guruswami-Sudan a une complexité polynomiale pour

$$\tau < n - \sqrt{(k-1)n}.$$

Guruswami-Rudra 2006 : peut-être que c'est le seuil.

- Construire, un code C_k, τ, un mot y in $\mathbb{F}_q^n$ tel que $L_\tau(y)$ est $\ll$ grand $\gg$.

Justesen-Høholdt 2001, BenSasson-Koparty-Radhakrishnan 2006.

- Même question, mais avec un volet algorithmique.

Reed-Solomon codes en cryptographie ?

"Come on, $\mathbb{F}_{2^8}$ is so small".

- Oui, mais le code peut-être gros :

  Le code standard $RS_{256}(255, 239)$ *est de taille* $2^{8 \cdot 239} = 2^{1912}$.

- Quand on quitte le monde du décodage algébrique, pas de méthode efficace quand $\tau > n - \sqrt{(k-1)n}$.
- Difficile de mettre une trappe.

  Sidelnikov-Chestakov 1992
  Augot-Finiasz 2003

Autres primitives (non computationnelles) : secret-sharing, etc.

Cheng-Wan

- Connexion entre le problème du décodage des codes de Reed-Solomon sur $\mathbb{F}_q$ et le logarithme discret dans $\mathbb{F}_q^h$.
- Volonté d'étudier les codes standards.
- Pas de NP-complétude, des réductions à des problèmes considérés durs.
- Complexité heuristique du logarithme discret sur les corps finis :

$$L_x[\alpha, c] = \exp(c(\log x)^{\alpha}(\log\log x)^{1-\alpha}).$$

"sous-exponentiel" : $\begin{cases} \text{polynomial} & \alpha = 0 \\ \text{exponentiel} & \alpha = 1 \end{cases}$

Problème du logarithme discret dans un corps fini

Problème du logarithme discret dans $\mathbb{F}_{q^h}$

Étant donnés $\mathbb{F}_{q^h}$ *une extension de* $\mathbb{F}_q$,
g *un générateur de* $\mathbb{F}_{q^h}^*$,
$a \in \mathbb{F}_{q^h}^*$,
trouver x *tel que*

$$a = g^x.$$

- ElGamal, Diffie-Hellman, Schnorr, DSA, etc.

Le $\hat{\mu}$ de Justesen et Høholdt.

Remarque

Soit C_k un code de Reed-Solomon $[n, k, \_]_q$, et $\mu < n$, il existe une boule de Hamming de rayon $\tau = n - \mu$ qui contient

$$N(\mu) = \binom{n}{\mu} / q^{\mu-k} \sim q^k \cdot \frac{1}{\mu!} \left(\frac{n}{q}\right)^{\mu}$$

mots de C_k.

Définition

On note $\hat{\mu}$ le plus petit μ tel que $N(\mu) \leq 1$. On a

$$n - \sqrt{(k-1)n} \leq \hat{\tau} = n - \hat{\mu} \leq n - k.$$

Résultats de Cheng et Wan

Théorème

S'il existe un algorithme de décodage (en temps polynomial en q) du code C_k jusqu'à $\hat{\tau} = n - \hat{\mu}$, il existe un algorithme qui résout le DLP (en temps polynomial en q) dans le corps

$$\mathbb{F}_{q^{\hat{\mu}-k}}.$$

Exemple numérique

- $q = 1024$, code $[n = 1023, k = 359, d = 665]_q$,
- décodage unique $t = 332$, décodage en liste $\tau = 417$,
- Justesen-Hoholdt : $\hat{\mu} = 461$, $\hat{\tau} = n - \hat{\mu} = 562$,
- DLP sur le corps de degré d'extension $\hat{\mu} - k = 102$

$$\mathbb{F}_{1024^{102}} \equiv \mathbb{F}_{2^{1020}}.$$

Le cœur de la réduction

- Soit $\mathbb{F}_{q^h}$ une extension de $\mathbb{F}_q$, $\mathbb{F}_{q^h} = \mathbb{F}_q[X]/Q(X) = \mathbb{F}_q[\overline{X}]$.
- Soit $S \subset \mathbb{F}_q$ de taille $n \leq q$.

Proposition

Pour tout $f(X)$, $\deg f(X) < h$, il existe $A \subset S$, $|A| = \mu$, tel que

$$f(X) \equiv \prod_{a \in A} (X - a) \bmod Q(X)$$

si et seulement si le mot

$$y = \mathrm{ev}_S\left(-f(X)/Q(X) - X^k\right)$$

est exactement à distance $\tau = n - \mu$ du code de Reed-Solomon C_k de dimension $k = \mu - h$.

Preuve

- Soit $A \subset S$, $|A| = \mu$, tel que

$$\prod_{a \in A}(X - a) \equiv f(X) \bmod Q(X).$$

- Il existe $t(X) \in F[X]$, $\deg t(X) = \mu - h = k$, tel que

$$\prod_{a \in A}(X - a) = f(X) + t(X)Q(X).$$

- En écrivant $t(X) = X^k + r(X)$, avec $\deg r(X) < k$:

$$r(X) = -\frac{f(X)}{Q(X)} - X^k + \frac{\prod_{a \in A}(X - a)}{Q(X)}.$$

- Alors $r(a) = -f(a)/Q(a) - a^k$, pour $a \in A$, et $|A| = \mu$.
- Donc $y = \mathrm{ev}_S\left(-f(X)/Q(X) - X^k\right)$ est à distance $n - \mu$ de C_k.

Les méthodes d'index-calculus

Soit $\mathbb{F}_{q^h}$, et $B \subset \mathbb{F}_{q^h}$, $|B| = n$, dont on connait les $\log_g(b)$, $b \in B$.

- Soit a dont on cherche $\log_b(a)$.
- On calcule $a \cdot g^r$, pour r aléatoire, et on cherche une relation

$$ag^r = \prod_{b \in B} b^{e_b}, \tag{1}$$

- Si une relation (1) existe, alors

$$x = \log_b a = -r + \sum_{b \in B} e_b \log_b b.$$

- Sinon, on tire un autre r aléatoire, jusqu'à ce que (1) se produise.

Cela s'appelle la *search phase*.

Les méthodes d'index-calculus

Mais comment trouver les $\log_g b$, pour $b \in B$?

- On calcule g^r, pour r aléatoire, et on cherche une relation

$$g^r = \prod_{b \in B} b^{e_b}. \tag{2}$$

- Alors (2) donne une relation linéaire entre les $\log_g b$:

$$\sum_{b \in B} e_b \log_g b = r \bmod (q^h - 1).$$

- En collectant $n = O(|B|)$ telles relations, et si le système est de rang plein, alors on trouve les $\log_g b$, $b \in B$.

Cela s'appelle la *collection phase*.

Pour résumer

Soit $n = |B|$, et $\pi = \pi(B)$ la probabilité de trouver une relation.

Précalcul

1. Phase de collection :
$$O(n\frac{1}{\pi}n^{\delta}),$$
2. Algébre linéaire :
$$O(n^{\nu}).$$

En direct live

$$O(\frac{1}{\pi}n^{\delta})$$

Il y a un compromis entre la taille de n et π.

Adleman

- La base est typiquement :

$$B = \{P(X) \in \mathbb{F}_q[X], \text{irréductible de degré} \leq e\}$$

- $n = |B| \sim \frac{q^e}{e}$
- Le coût est $O(n^{\delta+1}/\pi) + O(n^\nu)$.

Théorème

On a $\pi \sim (h/e)^{-(1+o(1))h/e}$ *(si h et e croissent ensemble).*

- On optimise e, et obtient

$$\exp(c\sqrt{h \log q \log(h \log q)}) = L_{q^h}[1/2, c]$$

- où les exposants δ et ν se retrouvent dans c.

Records

Algorithms with complexity $L_{q^h}[1/3, c]$

- Coppersmith : special case of $\mathbb{F}_{2^n}$ (idea : find $D \equiv C^k \mod Q$ with balanced degrees) ; later Semaev for $\mathbb{F}_{p^n}$; $O(\exp(cn^{1/3}(\log n)^{2/3}))$; record : $\mathbb{F}_{2^{613}}$ (Joux/Lercier).
- Number Field Sieve (NFS) : Adleman/Huang, Schirokauer, etc. $\mathbb{F}_p$. Record : $160dd$ (Kleinjung).
- Function Field Sieve (FFS) : Adleman, Joux/Lercier, etc. Records : $\mathbb{F}_{65537^{25}}$ (120 dd, 400b) ; $\mathbb{F}_{p^{18}}$ (101dd) ; $\mathbb{F}_{370801^{30}}$ (168 dd, 556b).

Index calculus à base de codes de Reed-Solomon

0. Auxiliary $S \subset \mathbb{F}_q$, $|S| = n$, and $\mu = n - \tau$.
1. (Randomize) $f(X) \leftarrow X^u \bmod Q(X)$ pour u aléatoire.
2. (Decode-Decompose) Trouver $A \subset S$, $|A| = \mu$, tel que

$$f(X) \equiv \prod_{a \in A} (X - a) \bmod Q(X). \tag{3}$$

3. (AddRow) Si (3) se produit, ajouter la ligne

$$u \equiv \sum_{a \in A} \log(\overline{X} - a) \bmod (q^h - 1).$$

   à un système d'équations linéaires d'inconnues les $\log(\overline{X} - a)$.
4. (Iterate) Si on a moins de n relations, goto 2.
5. (Linear Algebra) résoudre le système $n \times n$ sur $\mathbb{Z}/(q^h - 1)\mathbb{Z}$.

Algorithmes de décodage

- Équation clé : $O(n^2)$. Berlekamp-Massey, or EEA (Sugiyama et al.), voire $\widetilde{O}(n)$.
- Méthode de Gao, à base d'algorithme d'Euclide étendu.

Notre but

Étant donnés $S = \{x_1, x_2, \ldots, x_n\} \in \mathbb{F}_q$, $k \leq n$, $\mu \leq n$
un mot $y \in \mathbb{F}_q^n$,
trouver le polynôme localisateur d'erreur

$$\tau(X) = \prod_{y_i \neq f(a_i)} (X - a_i)$$

ou, le polynôme localisateur de vérité

$$\mu(X) = \prod_{y_i = f(a_i)} (X - a_i).$$

Gao1a

Input : $(x_i) \in \mathbb{F}_q^n$, dimension k, $d = n - k + 1$. $(y_i) \in \mathbb{F}_q^n$.

Output le polynôme localisateur $\tau(x)$ or `failure`.

0. Compute $G(X) = \prod_{i=1}^{n}(X - x_i)$.
1. (Interpolation) Trouver $I(X)$ tel que $I(x_i) = y_i$, $i \in [1 \dots n]$.
2. (Partial gcd) Appliquer l'algorithme d'Euclide étendu sur

$$s_0 = G \div X^k, \qquad s_1 = I \div X^k.$$

   Stop quand le reste $g(X) = u(X)s_0(X) + v(X)s_1(X)$ vérifie $\deg(g(X)) < (d-1)/2$.
3. (Division) Calculer $r(X) = G(X) \operatorname{rem} v(X)$
4. Si $r(X) = 0$, alors $\tau(X) = v(X)$, sinon `failure`.

Analyse de complexité de Gao1a

- Le temps total

$$T_G + T_{G \div X^k} + T_{I \div X^k} + T_{PEEA} + T_{v|G?},$$

- Si $G(X) = X^q - X$, $T_G = O(1)$ et $T_{G \div X^k} = O(1)$.
- T_I and $T_{I \div X^k} = O(M(n))$.
- $T_{PEEA} = O(M(d) \log d)$
- $T_{v|G?} = O(M(d) \log q)$
- Recherche de racines : $O(dM(d) \log q)$

Question

Qui est grand, qui est petit ?

Exemple numérique I

- Soit $\mathbb{F}_{13^3} = \mathbb{F}_{13}[X]/(X^3 + 2X + 11)$. Le support est $S = \mathbb{F}_{13}$.
- On utilise $\mathbb{F}_{13}$, et $[n, k, d] = [13, 7, 10]$.
- On considère $f(X) = X^{15}$. Il faut décoder

$$y = \mathrm{ev}_S(-X^{15}/Q(X) - X^7) = (7, 1, 1, 0, 1, 3, 6, 8, 9, 12, 4, 11, 10)$$

- L'algorithme d'Euclide étendu donne

$$u(X) = X^2 + 5X + 3,\ v(X) = 5X^3 + 2X^2 + 3,\ g(X) = 7X + 6,$$

- La factorisation de v est $(X - 3)(X - 8)(X - 12)$, de sorte que

$$X^{15}(X - 3)(X - 8)(X - 12) \equiv G(X) \bmod (Q(X), 13).$$

- On écrit $13^3 - 1 = 2^2 \cdot 3^2 \cdot 61$ (Pohlig-Hellman).

Exemple numérique II

- La matrice M des relations modulo 61 est

$$M = \begin{pmatrix}
15 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
19 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
33 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
40 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
48 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
51 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
8 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
15 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
25 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
31 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
36 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
48 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
14 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
16 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
17 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
22 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
24 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
27 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

- Une solution est

$$V = (1\,3\,52\,24\,57\,9\,41\,54\,42\,27\,41\,35\,5\,36)^T \bmod 61.$$

Quels paramètres ?

Proposition

Pour tout $f(X)$, $\deg f(X) < h$, *il existe* $A \subset S$, $|A| = \mu$, *tel que*

$$f(X) \equiv \prod_{a \in A} (X - a) \bmod Q(X)$$

si et seulement si le mot

$$y = \mathrm{ev}_S \left(-f(X)/Q(X) - X^k \right)$$

est exactement à distance $\tau = n - \mu$ *du code de Reed-Solomon* C_k *de dimension* $k = \mu - h$.

- On a le choix du code de Reed-Solomon $[n, k, n - k + 1]$, et on veut décoder jusqu'au rayon $n - k - h$.

Décodage unique

- On suppose $n - k$ pair.
- Le décodage unique atteint un rayon $\tau = \frac{n-k}{2}$, et donc

$$\mu = n - \tau = \frac{n+k}{2}$$

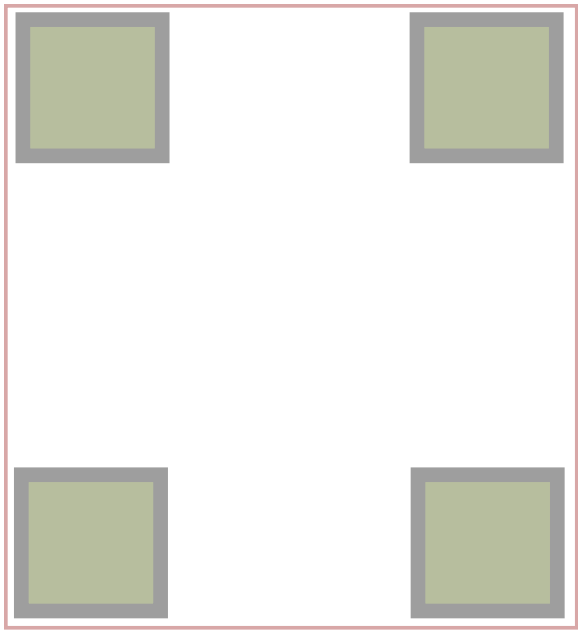
- On a aussi $k = \mu - h$: $\Longrightarrow$

$$k = n - 2h, \quad \tau = h.$$

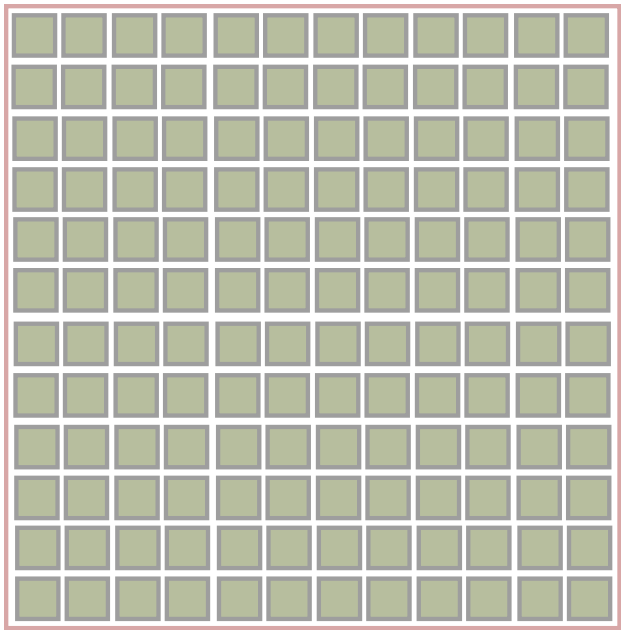
- Densité

$$\frac{\text{toutes les boules de décodage}}{\text{tout l'espace}} = \frac{V_q(n,\tau) \times q^k}{q^n}.$$

Faible taux k/n et fort taux k/n

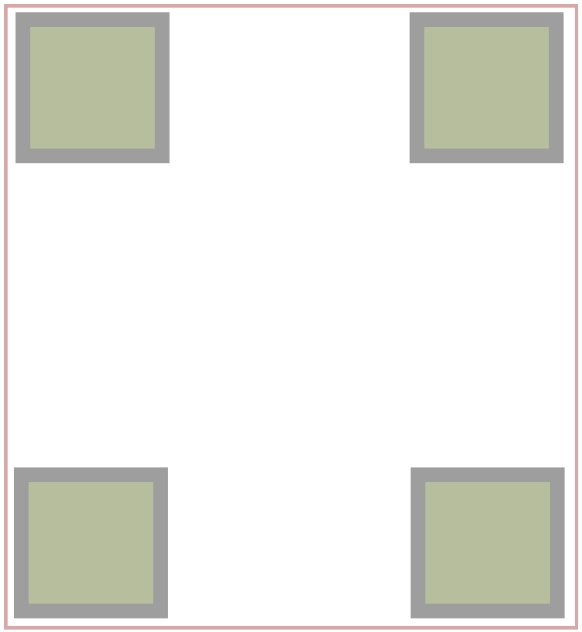


$k = O(1)$,
$t \to \frac{1}{2}$
$n \to \infty$,

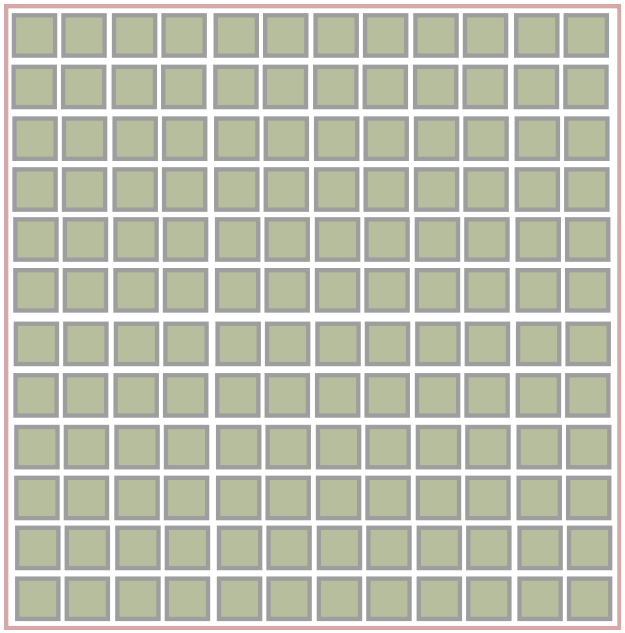


$k = n - O(1)$,
$t = O(1)$
$n \to \infty$,

Faible taux k/n et fort taux k/n



$k = O(1)$,
$t \to \frac{1}{2}$
$n \to \infty$,



$k = n - O(1)$,
$t = O(1)$
$n \to \infty$,

Photographies non contractuelles !

Pas de collisions

- Pour $|A| = \mu > h$, une relation

$$f(X) \equiv \prod_{a \in A} (X - a) \bmod Q(X)$$

devrait être lue $\prod_{a \in A} (X - a) \equiv f(X) \bmod Q(X)$.

- Décodage unique : pas de « collisions » pour la fonction

$$A \mapsto \prod_{a \in A} (X - a) \bmod Q(X).$$

- On a une probabilité

$$\frac{\binom{n}{n-\tau}}{q^h} = \frac{\binom{n}{\tau}}{q^h} = \frac{\binom{n}{h}}{q^h}$$

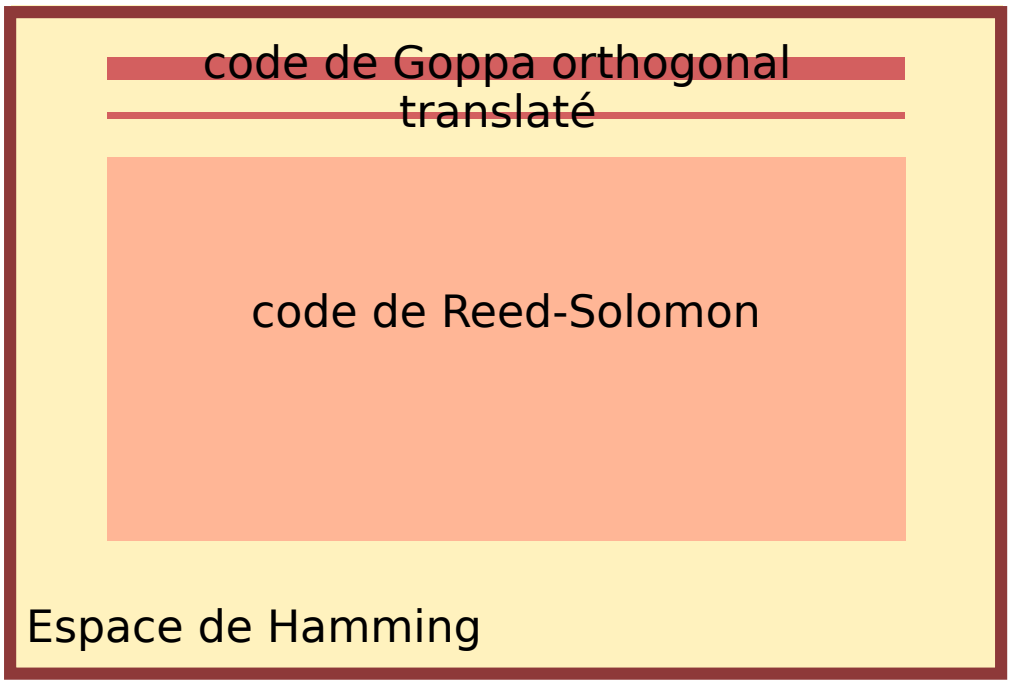
- à peu près $\sim \frac{1}{h!}$ quand $n = q$.

On ne décode pas tout l'espace

Pourquoi $1/h$!

On cherche à décoder

$$y = \mathrm{ev}_S\left(-f(X)/Q(X) - X^k\right) = \mathrm{ev}_S\left(-f(X)/Q(X)\right) - \mathrm{ev}_S\left(X^k\right).$$



Analyse

- Le coût est

$$O\left(n\frac{1}{\pi}\left(M(n)+M(h)\log h\right)+nhM(h)\log q\right)+O(h\cdot n^2M(h)),$$

- avec $\pi=\frac{\binom{n}{h}}{q^h}\sim\frac{n^h}{h!q^h}$, pour h constant et n croissant.
- Si $n>\log q$ and $n>h$, le coût devient

$$O\left(h!(q/n)^h nM(n)\right)+O(h\cdot n^2M(h)).$$

- En prenant $n=q$, on obtient

$$O(h!\cdot qM(q)),$$

- avec h constant et $q\to\infty$.

Corps de secours (helper field)

- Quand q est trop petit, on cherche des points dans une extension $\mathbb{F}_{q^e}$.
- On augmente le support S de la fonction d'évaluation.
- Exemple, $e = 2$:

$$S = S_1 \cup S_2,$$

avec $S_2 \subset \mathbb{F}_q$, et $S_2 \subset \mathbb{F}_{q^2}$.

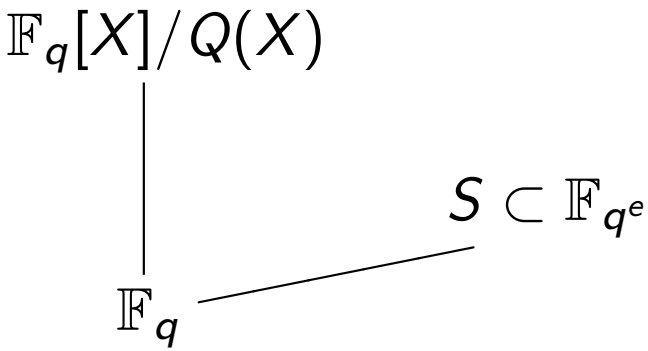
- Fonction d'évaluation :

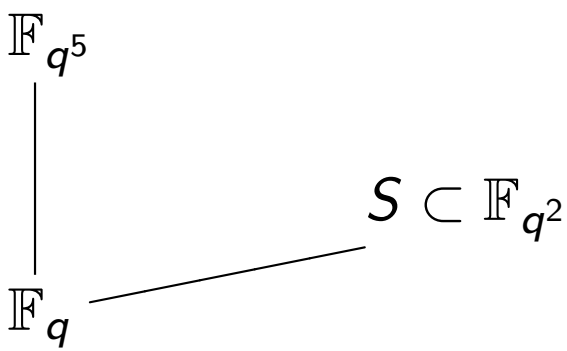
$$\begin{array}{rccl} \mathrm{ev}_S : & \mathbb{F}_q[X] & \to & \mathbb{F}_q^{n_1} \times \mathbb{F}_{q^2}^{n_2} \\ & f(X) & \mapsto & (f(u) : u \in S_1) || (f(v) : v \in S_2) \end{array}$$

- But : avoir une plus grande probabilité de décomposition.

Corps de secours $\neq$ sous corps

Helper field





Proposition (Relations de conjugaison)

Soit $\mathbb{F}_{q^h} = \mathbb{F}_q[X]/Q(X)$. *Soit* $\mu > h$.
Soit $f(X) \in K[X]$, *tel qu'il existe un unique* $A \subset \mathbb{F}_{q^e}$ *tel que*

$$f(X) \equiv \prod_{a \in A} (X - a) \bmod Q(X).$$

Alors $A^q = A$.

Probabilités

- S est l'ensemble des polynômes irréductibles de degré e.
- Pour h constant q croissant, on a une probabilité

$$\pi(q, h, e) \to c_e(h)$$

indépendante de q.

Les probabilités $c_e(h)$

h	3	7	11	13	31	67
$1/h!$	0.167	0.000198	$2.51\ 10^{-8}$	$1.61\ 10^{-10}$	$1.22\ 10^{-34}$	$2.74\ 10^{-95}$
$c_2(h)$	0.667	0.0460	0.000895	$9.13\ 10^{-5}$	$4.46\ 10^{-16}$	$2.36\ 10^{-45}$
$c_3(h)$		0.0697	0.00356	0.000783	$1.13\ 10^{-11}$	$1.32\ 10^{-31}$
$c_4(h)$		0.213	0.0333	0.0113	$3.24\ 10^{-8}$	$1.03\ 10^{-22}$
$c_6(h)$		0.407	0.117	0.0605	$1.48\ 10^{-5}$	$4.11\ 10^{-15}$
$c_8(h)$			0.117	0.0696	$9.79\ 10^{-5}$	$5.71\ 10^{-12}$

- Bonne probabilité, mais $n = O(q^e/e)$.

Analyse asymptotique

- Analyse non classique, car h et e sont constants, et $q \to \infty$.
- Il semblerait que (Romain Cosset)

$$\log c_e(h) \sim -\frac{h \log h}{e}.$$

Comportement sous-exponentiel

- Le logarithme de la complexité est

$$\log C = \log\left(\frac{1}{c_e(h)} n^{\delta'}\right) \sim \frac{h \log h}{e} + e \cdot \delta' \log q.$$

- Minimum pour $e \sim \sqrt{\frac{h \log h}{\delta' \log q}}$:

$$\log C \sim c\sqrt{h \log h \log q} = O\left(\sqrt{\log(q^h) \log\log(q^h)}\right).$$

- Dans un modèle de dépendance des paramètres pas clair...

What next ?

Ce qu'on fait de plus :

- Dérandomisation : $X^u \to X^{u+1}$: permet de simplifier certains calculs, etc.
- Test rapide d'échec : test du degré, `IsSquareFree`, etc.
- Décoder une erreur de plus : proba ≥ 1.
- NTL.

Ce qu'on veut faire :

- Utiliser des multiplicités (bornées) : *Derivative codes*.
- Utiliser Guruswami-Sudan (à faible taille de liste).
- Se donner des cibles. . .

Autres codes que les codes de Reed-Solomon :

- Codes géométriques et DLP sur les courbes elliptiques.