Codes de Reed-Solomon en métrique de Lee

Guillaume Quintin

Équipe PICC
Laboratoire XLIM – UMR CNRS
Université de Limoges

Mardi 25 mars 2014

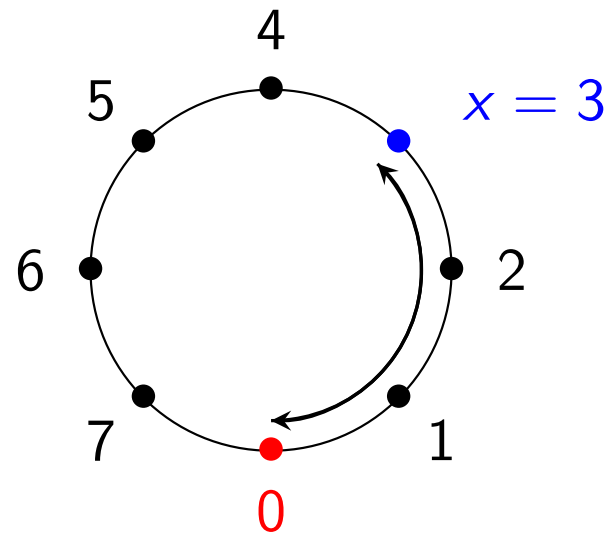
La métrique de Lee (1)

- Introduit pour les codes correcteurs par Lee en 1958 [Lee58].
- Soit q et x deux entiers positifs tels que

$$x \in [0, q-1].$$

- Le **poids de Lee** de $x \in \mathbb{Z}/q\mathbb{Z}$ est définie par

$$w_L(x) := \min(x, q-x)$$



La métrique de Lee (2)

- Pour un vecteur $(y_1, \ldots, y_n)$ son **poids de Lee** est

$$w_L(y_1, \ldots, y_n) := \sum_{i=1}^{n} w_L(y_i).$$

- Attention :
  - w_L = poids de Lee.
  - w_H = poids de Hamming.

- La **métrique de Lee** est utilisée pour
  - Les transmissions utilisant la modulation de phase.
  - La bijection [HKC+94]

$$\left\{\begin{array}{c}\text{certains codes linéaires} \\ \text{sur } \mathbb{Z}/4\mathbb{Z} \text{ en métrique de Lee}\end{array}\right\} \approx \left\{\begin{array}{c}\text{certains codes non linéaires} \\ \text{sur } \mathbb{F}_2 \text{ en métrique de Lee}\end{array}\right\}$$

Rappels sur les codes de Reed-Solomon (1)

- On fixe n et k des entiers positifs tels que $0 < k < n$.
- On se donne

$$x_1, \ldots, x_n \in \mathbb{Z}/q\mathbb{Z} \quad \text{tels que} \quad \forall i \neq j \quad (x_i - x_j) \in (\mathbb{Z}/q\mathbb{Z})^\times.$$

  C'est-à-dire $\mathrm{PGCD}(x_i - x_j, q) = 1$.
- Le **code de Reed-Solomon** de **paramètres** $[n, k]_{\mathbb{Z}/q\mathbb{Z}}$ est l'ensemble

$$\mathrm{RS} := \left\{ \begin{array}{c} (f(x_1), \ldots, f(x_n)) \in (\mathbb{Z}/q\mathbb{Z})^n \\ \text{avec} \quad \deg f < k \end{array} \right\}.$$

- Sa **distance minimale de Hamming** est telle que

$$\begin{aligned} d_H(\mathrm{RS}) &:= \min\{w_H(x) \text{ pour } x \in \mathrm{RS} \text{ et } x \neq 0\} \\ &= n - k + 1. \end{aligned}$$

Rappels sur les codes de Reed-Solomon (2)

- Le code RS est **optimal** pour la métrique de **Hamming** car

$$d_H(\mathrm{RS}) = n - k + 1.$$

- On peut **corriger** jusqu'à

$$\left\lfloor \frac{n-k}{2} \right\rfloor \text{ erreurs de } \textbf{Hamming}$$

de manière efficace.

  - Beaucoup d'algorithmes de décodage unique existent [Pet60, Ber68, Mas69, SKHN75, Jus76, Bla83, BW86, TERH88, SFWHYHAYW01, Gao02].

- Mais on peut également décoder jusqu'à

$$\left\lfloor n - \sqrt{(k-1)n} \right\rfloor \text{ erreurs de } \textbf{Hamming}$$

avec l'algorithme dû à Guruswami et Sudan.

Qu'en est-il en métrique de Lee ?

1. Roth et Siegel [RS94] ont donné un algorithme ne corrigeant pas **beaucoup d'erreurs de Lee**.

2. Roth et Tal [TR03] ont ensuite essayé d'**adapter** l'algorithme de **Guruswami-Sudan** en métrique de Lee pour corriger plus d'erreur.

3. Armand et de Taisne ont travaillé sur le même sujet que Roth et Tal mais sur les **anneaux finis**.

4. X.-W. Wu, Kuijper et Udaya ont ensuite sorti une série de papiers **introduisant une nouvelle idée** et étendant le décodage en métrique de Lee aux **codes géométriques** [WKU03, WKU04, WKU05, WKU04, WKU07, WH08].

Mais...

1. Que vaut $d_L(\mathrm{RS})$ (distance minimale) ?

2. Le code RS est-il optimal ?

3. Y a-t-il un borne de Singleton en métrique de Lee ?

4. Peut-on corriger jusqu'à

$$\left\lfloor \frac{d_L(\mathrm{RS}) - 1}{2} \right\rfloor$$

   erreurs de Lee en temps polynomial (en n et k) ?

5. Y a-t-il une borne de Johnson en métrique de Lee ?

6. Peut-on décoder en liste jusqu'à la borne de Johnson ?

La distance minimale de Lee du code RS (1)

Plusieurs cas possibles :

- On a nécessairement $d_H(\mathrm{RS}) \leq d_L(\mathrm{RS}) \leq n$.
  En effet $(1, \ldots, 1) \in \mathrm{RS}$ et $w_L(1, \ldots, 1) = n$.
- Un polynôme de petit degré doit prendre beaucoup de valeurs différentes.

$$\frac{n}{k} \leq \frac{1}{4} \quad \Rightarrow \quad d_L(\mathrm{RS}) = n$$

$$\frac{1}{4} \leq \frac{k}{n} \leq \frac{1}{3} \quad \Rightarrow \quad d_L(\mathrm{RS}) \geq 2n - 4(k-1)$$

$$\frac{1}{3} \leq \frac{k}{n} \leq \frac{1}{2} \quad \Rightarrow \quad d_L(\mathrm{RS}) = ??$$

$$\frac{1}{2} \leq \frac{k}{n} \leq 1 \quad \Rightarrow \quad d_L(\mathrm{RS}) = ??$$

- Lorsque $\mathbb{Z}/q\mathbb{Z} = \mathbb{F}_q$ et $n = q$ et $\frac{k}{n} \leq \frac{1}{2}$ alors $d_L(\mathrm{RS}) = n$.

La distance minimale de Lee du code RS (2)

- Supposons $\frac{1}{3} \leq \frac{k}{n} \leq \frac{1}{2}$.
- Nous ne savons que $d_L \geq d_H$.
- Supposons de plus que $\{x_1, \ldots, x_n\}$ soit un **sous-groupe** de $(\mathbb{Z}/q\mathbb{Z})^\times$ et tel que $\text{Card}(G) > 2k$.

Théorème
Lorsque $\left(\frac{n}{q}\right) \neq \left(\frac{n-k+1}{q}\right)$ *alors* $d_L > d_H$.

Quand $\mathbb{Z}/q\mathbb{Z} = \mathbb{F}_q$ et $n = q - 1$ alors $n = -1 \mod q$ et on a automatiquement des **critères ne dépendant** que de q et d_H.

La distance minimale de Lee du code RS (3)

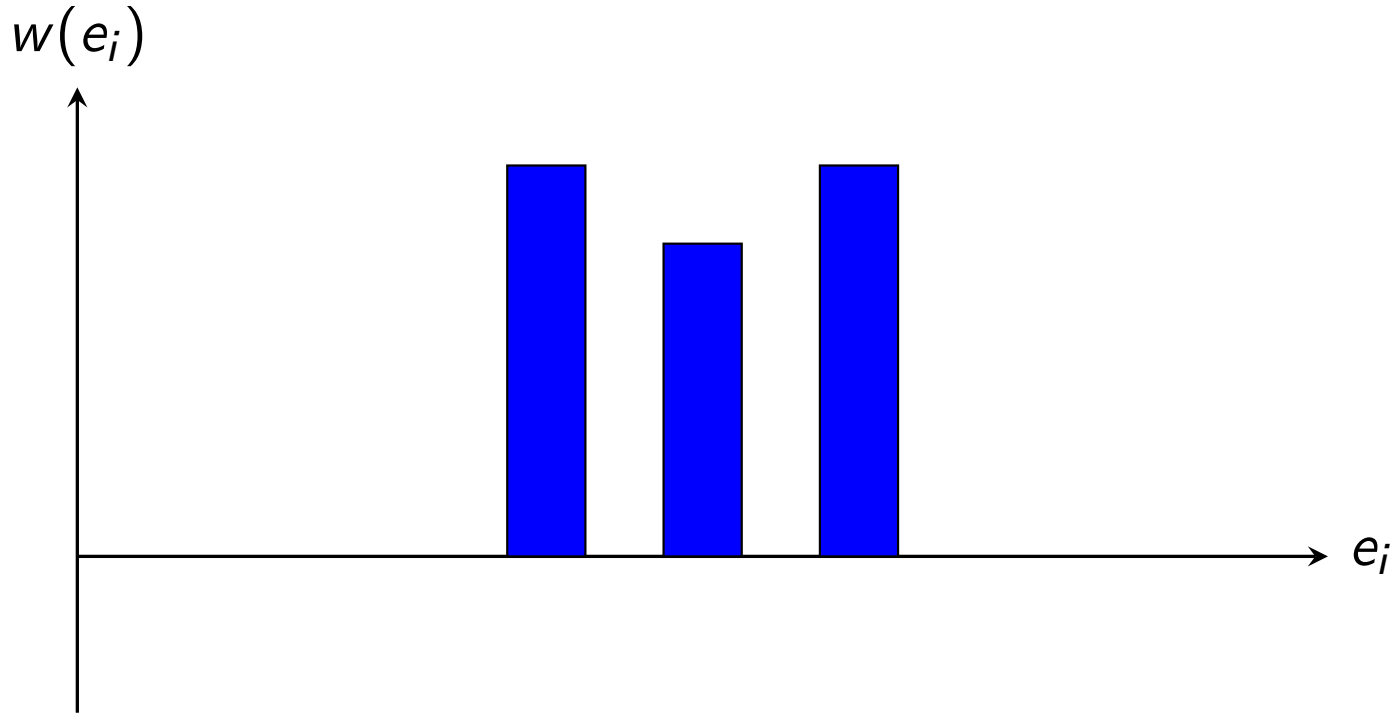
- Supposons $\frac{1}{2} \leq \frac{k}{n}$.
- Nous ne savons que $d_L \geq d_H$.
- A-t-on $d_L = d_H$?

- Recherche exhaustive de codes en `Magma`.
- Pour chaque premier $p \in [11, 31]$, il existe un code de **Reed-Solomon intéressant**.
  - Sa longueur est $p - 1$.
  - Son rendement est compris dans $[0.50, 0.56]$.
  - Et $d_L = d_H$.
- Il **existe des codes de Reed-Solomon** tels que $d_L = d_H$ pour divers rendements dans $[0.50, 1]$.
- **Aucun code de Reed-Solomon** avec $d_L = d_H$ n'a été trouvé avec un rendement dans $\left[\frac{1}{3}, \frac{1}{2}\right]$.

Décodage unique en métrique de Lee (1)

Deux situations possibles :

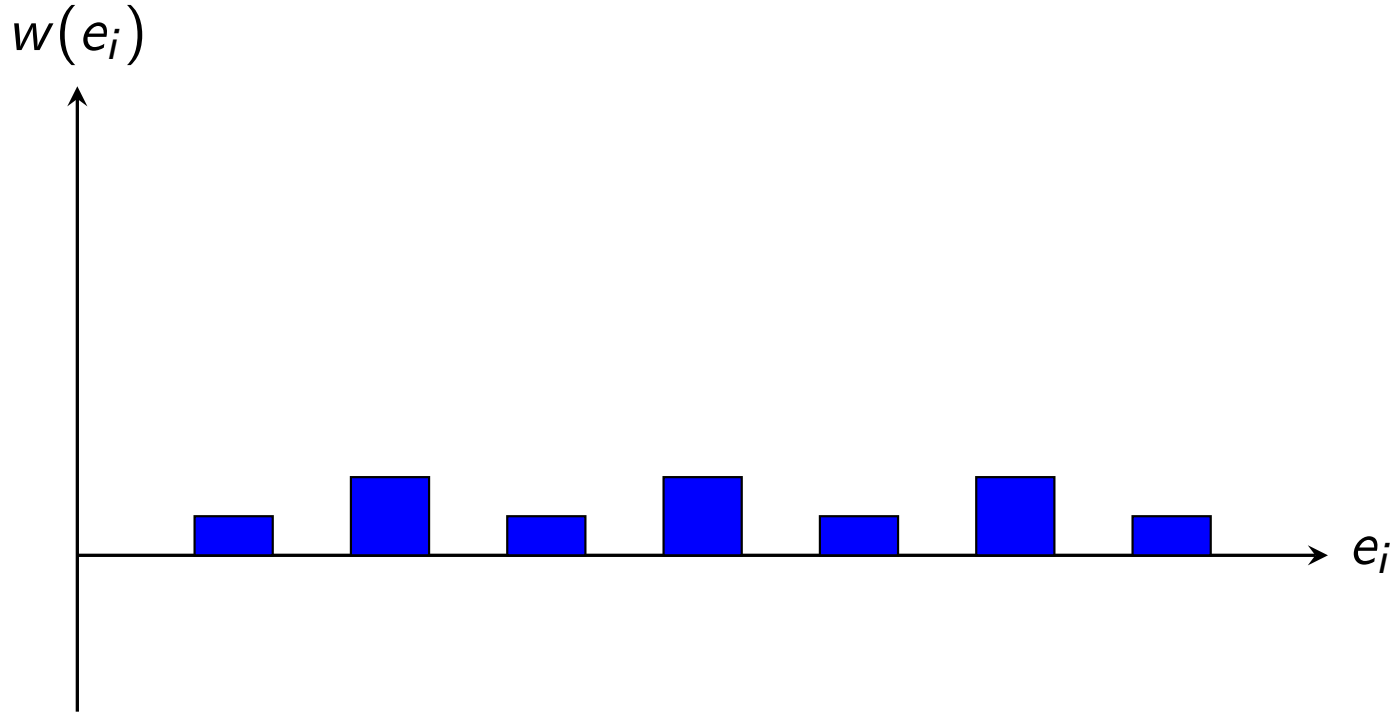
Ici $\vec{e} = (e_1, \ldots, e_n) \in (\mathbb{Z}/q\mathbb{Z})^n$ désigne l'erreur.



$w_L(\vec{e}) \approx \frac{n}{2}$ tandis que $w_H(\vec{e}) < \tau$.

(Ici τ désigne un rayon de décodage d'un décodeur en Hamming.)

Décodage unique en métrique de Lee (2)



$w_L(\vec{e}) \approx \frac{n}{2}$ tandis que $w_H(\vec{e}) \gg \tau$ mais $w_L(e_i)$ est petit pour chaque $i = 1, \ldots, n$.

Décodage unique en métrique de Lee (3)

Entrée : le mot reçu $y = (y_1, \ldots, y_n)$.
Sortie : l'unique mot de code à distance de Lee au plus $\left\lfloor \frac{n-1}{2} \right\rfloor$ de y.

1. Exécuter un décodeur de Hamming sur y.

2. **Si** le décodeur retourne $c \in \mathrm{RS}$ **alors retourner** c.

3. **Sinon** trouver une courbe $Q(X, Y) = 0$ qui passe par les points $(y_i - u, x_i), \ldots, (y_i + u, x_i)$ pour $i = 1, \ldots, n$ et pour un certain u.

4. Trouver les racines de $Q(X, Y)$.

5. **Retourner** la racine $f_0(X)$ de $Q(X, Y)$ de degré $< k$ telle que

$$w_L\left(y - (f_0(x_1), \ldots, f_0(x_n))\right) \leq \left\lfloor \frac{n-1}{2} \right\rfloor$$

Perspectives

- Et la distance minimale ?
  - Peut-on la trouver ?
  - Ou en trouver une bonne approximation ?
- On a envie de penser qu'on peut faire mieux pour décoder !
  - Pourquoi utiliser du décodage en liste (de Hamming) ?
  - Peut-on utiliser les réseaux ?
  - Ou un autre algorithme pour gagner en complexité ?
- Qu'en est-il du décodage en liste en suivant cette idée ?
  - *Avant*, peut-on "améliorer" la borne de Johnson en métrique de Lee ?
  - Peut-on atteindre la borne de Johnson ? en temps polynomial ?

References I


E.R. Berlekamp.
Algebraic Coding Theory.
McGraw Hill, New York, 1968.


R.E. Blahut.
Theory and practice of error control codes.
Addison-Wesley Pub. Co., 1983.


E. R. Berlekamp and L. R. Welch.
Error correction for algebraic block codes, 1986.
US Patent 4633470.


S. Gao.
A New Algorithm for Decoding Reed-Solomon Codes.
In *Communications, Information and Network Security, V. Bhargava, H.V. Poor, V. Tarokh, and S. Yoon*, pages 55–68.
Kluwer, 2002.

References II


Jr. Hammons, A.R., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé.
The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes.
IEEE Trans. Inform. Theory, 40(2):301–319, mar 1994.


J. Justesen.
On the complexity of decoding Reed-Solomon codes (Corresp.).
IEEE Trans. Inform. Theory, 22(2):237–238, March 1976.


C. Lee.
Some properties of nonbinary error-correcting codes.
Information Theory, IRE Transactions on, 4(2):77–82, june 1958.

References III


J. Massey.
Shift-register synthesis and BCH decoding.
IEEE Trans. Inform. Theory, 15(1):122–127, jan 1969.


W. Peterson.
Encoding and error-correction procedures for the Bose-Chaudhuri codes.
Information Theory, IRE Transactions on, 6(4):459–470, sep 1960.


R. M. Roth and P. H. Siegel.
Lee-metric BCH codes and their application to constrained and partial-response channels.
IEEE Trans. Inform. Theory, 40(4):1083–1096, 1994.

References IV


Sheng-Feng W., Huai-Yi H., and An-Yeu W.
A very low-cost multi-mode Reed-Solomon decoder based on Peterson-Gorenstein-Zierler algorithm.
In *Signal Processing Systems, 2001 IEEE Workshop on*, pages 37–48, 2001.


Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa.
A method for solving key equation for decoding goppa codes.
Information and Control, 27(1):87–99, 1975.


T. K. Truong, W. L. Eastman, I. S. Reed, and I. S. Hsu.
Simplified procedure for correcting both errors and erasures of Reed-Solomon code using Euclidean algorithm.
IEEE Proc. Comput. and Digit. Tech., 135(6):318–324, 1988.

References V


I. Tal and R. M. Roth.
On list decoding of alternant codes in the hamming and lee metrics.
In *Information Theory, 2003. Proceedings. IEEE International Symposium on*, page 364, 2003.


Y. Wu and C. N. Hadjicostis.
Decoding algorithm and architecture for BCH codes under the Lee Metric.
Communications, IEEE Transactions on, 56(12):2050–2059, 2008.


X.-W. Wu, M. Kuijper, and P. Udaya.
Lee-metric decoding of BCH and Reed-Solomon codes.
Electronics Letters, 39(21):1522–1524, 2003.

References VI


X.-W. Wu Wu, M. Kuijper, and P. Udaya.
A class of algebraic-geometric codes for Lee-Metric and their decoding.
In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 75, 2004.


X.-W. Wu Wu, M. Kuijper, and P. Udaya.
On the decoding radius of Lee-metric decoding of algebraic-geometric codes.
In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 1191–1195, 2005.


X.-W. Wu, M. Kuijper, and P. Udaya.
Lower bound on minimum lee distance of algebraic-geometric codes over finite fields.
Electronics Letters, 43(15):820–821, 2007.