Codes de Reed-Solomon

Lancelot Pecquet[1]

Résumé

Les codes correcteurs d'erreurs inventés [8] en 1960 par Irving Reed et Gus Solomon sont performants et on connaît leur distance minimale ainsi que des méthodes de décodage rapide (quadratique) telle celle de Berlekamp [1] dont il existe de nombreuses variantes [5, 3, 2]. James Massey a popularisé cet algorithme dans le contexte cryptologique par son application à la cryptanalyse des registres à décalage [6]. On pourra consulter [9, Chapter 7, pp. 197–203] et [4] pour un traitement plus approfondi. Voici le principe de ces algorithmes résumé en une page. L'accélération de l'algèbre linéaire provient de la structure de la matrice.

Définition 1 *Soit $\mathbb{F}_q$ un corps fini à q éléments et n un entier naturel. L'espace $\mathbb{F}_q^n$ peut être muni de la* ***distance de* Hamming** *: $\mathrm{d}(x, x')$ est le nombre d'indices j tels que $x_j \neq x'_j$. Soit $p = (p_1, \ldots, p_n)$ un n-uplet d'éléments de $\mathbb{F}_q$. On note $\mathrm{ev}_p : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q^n$ l'application linéaire d'évaluation : $f \longmapsto \big(f(p_1), \ldots, f(p_n)\big)$. Soit $k \in \mathbb{N}$ et L_k le sous-espace vectoriel de dimension k de $\mathbb{F}_q[x]$ constitué des polynômes de degré inférieur à k. Le sous-espace vectoriel $C = \mathrm{ev}_p(L_k)$ de $\mathbb{F}_q^n$ s'appelle un* ***code de* Reed-Solomon** *(il y a des variantes dans la littérature). Si les p_j sont distincts et que $k < n$, ev_p est un isomorphisme de L_k sur C et la* ***distance minimale*** *entre deux mots distincts vaut $d = n - k + 1$. Le* ***rayon d'empilement*** *de C, $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ est la plus grande distance τ telle qu'une boule fermée de rayon τ contient au plus un mot de C.*

Théorème 1 *Soit c un mot de C et y un vecteur de $\mathbb{F}_q^n$ à distance inférieure à t l'un de l'autre et soit $m \stackrel{\text{def}}{=} \left\lfloor \frac{n+k-1}{2} \right\rfloor + 1$, alors la matrice :*

$$M \stackrel{\text{def}}{=} \begin{pmatrix} p_1^0 & \cdots & p_n^0 \\ \vdots & \ddots & \vdots \\ p_1^{m-1} & \cdots & p_n^{m-1} \\ p_1^0 y_1 & \cdots & p_n^0 y_n \\ \vdots & \ddots & \vdots \\ p_1^{m-k} y_1 & \cdots & p_n^{m-k} y_n \end{pmatrix} \tag{1}$$

a un noyau non trivial et $c = \mathrm{ev}_p(f)$ où f est le quotient exact de la division de $-a_0(x)$ par $a_1(x)$, où η est un vecteur non-nul tel que $\eta \cdot M = 0$ à partir duquel on a construit les polynômes $a_0(x) = \eta_1 + \cdots + \eta_m x^{m-1}$ et $a_1(x) = \eta_{m+1} + \cdots + \eta_{2m-k+1} x^{m-k}$ de telle sorte que :

$$\eta = \Big(\boxed{a_{0,0}, \ldots, a_{0,m-1}}, \boxed{a_{1,0}, \ldots, a_{1,m-k}} \Big) . \tag{2}$$

Démonstration : La matrice étant $(2m - k + 1) \times n$, elle a un noyau non-trivial si $2m - k + 1 > n$, ce qui est le cas pour le m choisi. Le fait que $\eta \cdot M = 0$ signifie que le polynôme non-nul $G(T) = (a_{0,0}x^0 + \cdots + a_{0,m-1}x^{m-1}) + (a_{1,0}x^0 + \cdots + a_{1,m-k}x^{m-k})T$ satisfait la propriété que $\big(G(y_j)\big)(p_j) = 0$ pour tout j. Soit f un polynôme de L_k tel que $c = \big(f(p_1), \ldots, f(p_n)\big)$, on a $f(p_j) = y_j$ pour $n - \tau$ valeurs de j. Comme $\tau \leq t$, on a $n - \tau \geq m$ donc le polynôme $G(f)$ s'annule au moins m fois. Or, puisque $\deg f < k$, degré (et le nombre de racines) du polynôme $G(f)$ est majoré par $m-1$. Par conséquent $G(f)$ est le polynôme nul *i.e.* $f = -a_0/a_1$. □

Références

[1] Elwyn R. Berlekamp. On decoding the Bose-Chauduri-Hocqenghem codes. *IEEE Transactions on Information Theory*, 11 :577–579, 1965.

[2] Elwyn R. Berlekamp. Bounded distance+1 soft-secision Reed-Solomon decoding. *IEEE Transactions on Information Theory*, 42(3) :704–720, 1996.

[3] Elwyn R. Berlekamp and Lloyd R. Welch. Error correction of algebraic block codes. patent 4,633,470. dec 30th, 1986.

[4] Richard E. Blahut. Decoding cyclic codes and codes on curves. Chapter 19 dans [7], pp. 1569–1633.

[5] James L. Massey. Step-by-step decoding of the Bose-Chaudhuri-Hocqenghem codes. *IEEE Transactions on Information Theory*, 11 :580–585, 1965.

[6] James L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, IT-15(1) :122–127, 1969.

[7] Vera S. Pless and William C. Huffman, editors. *Handbook of Coding Theory*. North-Holland, 1998.

[8] Irving S. Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the SIAM*, 8 :300–304, 1960.

[9] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[1] `lancelot@pecquet.org` – Merci à Valerie Viet Triem Tong qui m'a motivé pour écrire ce petit document. V. 1.0 du 28/03/2006