Théorie de l'information et du codage

TD n^{o}9 – Codes de Goppa

Dans tout ce qui suit, on se donne un entier de la forme $q = p^f$ avec p premier, ainsi qu'un polynôme G sur une extension $\mathbb{F}_{q^m}$ du corps $\mathbb{F}_q$. On notera $r = d^\circ G$.

1 Définition et propriétés

Question 1. *Si $\alpha \in \mathbb{F}_{q^m}$, à quelle condition $X - \alpha$ est-il inversible modulo G ? Quel est alors son inverse ? Expliciter ses coefficients en fonction de ceux de G.*

On se donne désormais une partie $L = \{\alpha_1, \ldots, \alpha_n\}$ de $\mathbb{F}_{q^m}$ sur laquelle G ne s'annule pas, et l'on appelle code de Goppa associé à G et L l'ensemble

$$\mathcal{G}_{G,L} := \left\{ (c_1, \ldots, c_n) \in \mathbb{F}_q^n ; \sum_{j=1}^{n} \frac{c_j}{X - \alpha_j} \equiv 0 \bmod G(X) \right\}.$$

Question 2. *Montrer que c'est un code linéaire et qu'une matrice vérificatrice est :*

$$H = \begin{pmatrix} \frac{1}{G(\alpha_1)} & \frac{1}{G(\alpha_2)} & \cdots & \frac{1}{G(\alpha_n)} \\ \frac{\alpha_1}{G(\alpha_1)} & \frac{\alpha_2}{G(\alpha_2)} & \cdots & \frac{\alpha_n}{G(\alpha_n)} \\ \vdots & \vdots & & \vdots \\ \frac{\alpha_1^{r-1}}{G(\alpha_1)} & \frac{\alpha_2^{r-1}}{G(\alpha_2)} & \cdots & \frac{\alpha_n^{r-1}}{G(\alpha_n)} \end{pmatrix}.$$

Question 3. *En déduire que la dimension est au moins $n - mr$ et la distance au moins $r + 1$.*

Question 4. *Montrer que les codes de Goppa généralisent les codes BCH.*

Question 5. *On considère le code de Goppa binaire associé à $G = X^2 + X + 1 \in \mathbb{F}_8[X]$, $L = \mathbb{F}_8$. Que sait-on à priori de sa dimension ? de sa distance ? En expliciter une matrice vérificatrice H (pour la construction de $\mathbb{F}_8$, on utilisera $X^3 + X + 1$). Quels sont les mots-codes ? Quelle est la dimension exacte ? Quelle est la distance exacte ?*

Question 6. *Montrer que pour les codes de Goppa binaires, la distance minimale d vérifie en réalité $d > d^\circ \overline{G}$, où $\overline{G}$ est le plus petit carré parfait multiple de G.*

Question 7. *Trouver une condition nécessaire et suffisante sur G pour que $\overline{G} = G^2$. On parle alors de code de Goppa binaire séparable. Combien d'erreurs un tel code peut-il corriger ?*

Question 8. *Soit $\mathcal{G}_{G,L}$ un code de Goppa binaire séparable. Soit $z_1, \ldots, z_r$ les racines de G dans une extension de $\mathbb{F}_{2^m}$ suffisament grande. Montrer qu'une matrice vérificatrice de $\mathcal{G}_{G,L}$ est la matrice de Cauchy :*

$$H = \begin{pmatrix} \frac{1}{z_1 - \alpha_1} & \frac{1}{z_1 - \alpha_2} & \cdots & \frac{1}{z_1 - \alpha_n} \\ \frac{1}{z_2 - \alpha_1} & \frac{1}{z_2 - \alpha_2} & \cdots & \frac{1}{z_2 - \alpha_n} \\ \vdots & \vdots & & \vdots \\ \frac{1}{z_n - \alpha_1} & \frac{1}{z_n - \alpha_2} & \cdots & \frac{1}{z_n - \alpha_n} \end{pmatrix}.$$

2 Un algorithme de décodage efficace

Imaginons qu'un mot-code $c = (c_1, \ldots, c_n) \in \mathcal{G}_{G,L}$ soit envoyé dans le canal et que le message reçu par le destinataire soit $r = (r_1, \ldots, r_n) \in \mathbb{F}_{q^m}$. Posons alors

$$S_r = \sum_{j=1}^{n} \frac{r_j}{X - \alpha_j} \bmod G.$$

Notons $e = r - c = (e_1, \ldots, e_n)$ le motif (inconnu) des erreurs et $J_e = \{1 \leq j \leq n; e_j \neq 0\}$ l'ensemble des positions de ces erreurs. Dans toute cette section, on fera l'hypothèse que

$$|J_e| \leq \left\lfloor \frac{d^\circ G}{2} \right\rfloor. \tag{1}$$

Question 9. *Que garantit cette condition ? Comment le receveur peut-il s'y prendre pour identifier c à partir de r ? Quelle est la complexité algorithmique de cette stratégie ?*

Il existe en réalité une méthode incroyablement plus efficace pour récupérer c à partir de r, qui explique à elle seule l'immense succès des codes de Goppa. On définit deux précieux polynômes, dits "localisateur" et "évaluateur" :

$$\sigma_e = \prod_{j \in J_e} (X - \alpha_j) \text{ et } \omega_e = \sum_{j \in J_e} e_j \prod_{k \in J_e \setminus j} (X - \alpha_k).$$

Question 10. *Montrer que la connaissance du couple (σ_e, ω_e), même à scalaire multiplicatif près, suffit à décoder aussitôt le message reçu.*

Question 11. *Montrer que le couple (σ_e, ω_e) est solution de l'"équation-clé"*

$$\sigma S_r = \omega \ mod\ G, \ et\ \sigma \wedge \omega = 1, \tag{2}$$

et que parmi toutes les solutions $(\sigma, \omega) \in \mathbb{F}_{q^m}[X] \times \mathbb{F}_{q^m}[X]$, c'est la seule à satisfaire en outre :

$$\sigma \text{ est unitaire, } d^\circ\omega < \left\lfloor \frac{d^\circ G}{2} \right\rfloor \text{ et } d^\circ\sigma \leq \left\lfloor \frac{d^\circ G}{2} \right\rfloor.$$

Étant donnés deux polynômes $a, b \in \mathbb{K}[X]$ sur un corps arbitraire $\mathbb{K}$, avec $b \neq 0$, on définit $(r_0, s_0, t_0) = (a, 1, 0)$, $(r_1, s_1, t_1) = (b, 0, 1)$, puis pour tout $k \geq 2$, tant que $r_{k-1} \neq 0$:

$$r_k = \mathcal{R}(r_{k-2}|r_{k-1}), \quad s_k = s_{k-2} - s_{k-1}\mathcal{Q}(r_{k-2}|r_{k-1}) \quad \text{et} \quad t_k = t_{k-2} - t_{k-1}\mathcal{Q}(r_{k-2}|r_{k-1}),$$

où $\mathcal{Q}(x|y)$ et $\mathcal{R}(x|y)$ sont le quotient et le reste de la division de x par y.

Question 12. *Justifier les propriétés suivantes :*

1. $k^* = \max\{k; r_k \neq 0\}$ *existe.*
2. $r_{k^*} = a \wedge b$.
3. *À tout instant* $k \leq k^*$, $s_k a + t_k b = r_k$ *et* $s_k \wedge t_k = 1$.
4. *À tout instant* $k \leq k^*$, $d^\circ t_{k+1} + d^\circ r_k = d^\circ a$ *et* $d^\circ s_{k+1} + d^\circ r_k = d^\circ b$.

Question 13. *En déduire un algorithme de décodage efficace pour les codes de Goppa.*