Théorie de l'information et du codage

TD n^{o}9

Erreurs en cascade

Une cascade d'erreurs de taille $l < n/2$ survient lorsque, sur un mot-code transmis de taille n, des erreurs se produisent uniquement au sein de l symboles consécutifs ; on dira qu'une cascade d'erreurs a une taille *exactement* l lorsqu'au moins le premier et le dernier symboles de la zone de taille l sont erronés. La capacité de *détection* (resp. *correction*) de cascades d'erreurs d'un code est la taille maximum l telle que le code détecte (resp. corrige) toutes les cascades d'erreurs de taille $\leq l$.

1. Combien y-a-il de cascades d'erreurs de taille exactement l.
2. Donner une borne supérieure (simple) sur la capacité de détection τ_d de cascades d'erreurs d'un code q-aire de paramètres (n, k).
3. Soit $\mathcal{C}$ un code cyclique de polynôme générateur $g(X)$ de degré $r \geq 1$, avec $g_0 \neq 0$. Montrer que $\tau_d(\mathcal{C}) = r$, et que la fraction non détectée de cascades d'erreurs de taille exactement $l = r + 1$ est $q^{-r}(1 - 1/q)^{-1}$ et celle de cascades d'erreurs de taille exactement $l > r + 1$ est q^{-r}.
4. Montrer que la capacité de correction τ_c d'un code q-aire de paramètres (n, k) vérifie $2\tau_c \leq n - k$ (borne de Rieger) et aussi $\tau_c \leq n - k - \log_q n$.

On définit l'efficacité d'un code linéaire pour la correction d'erreurs en cascade (ou efficacité BEC, pour *burst error correction*) par la quantité $\frac{2\tau_c}{n-k}$. Un code cyclique $\mathcal{C}$ de polynôme générateur $g(X)$ est un code de Fire si $g(X) = (X^{2l-1} - 1)p(X)$, où $p(X)$ est un polynôme irréductible de degré $r \geq l$ et d'ordre m sur $\mathbb{F}_q$, et $p(X)$ ne divise pas $X^{2l-1} - 1$. La longueur de mot-code utilisée est le plus petit entier n tel que $g(X)$ divise $X^n - 1$, c-a-d $n = \mathrm{lcm}(m, 2l - 1)$.

5. Quelle est la taille du code $\mathcal{C}$?
6. Si $e_1(X) = X^i b(X)$ et $e_2(X) = X^j b'(X)$, avec $b_0, b'_0 \neq 0$ et $i \leq j < n$, sont les polynômes correspondant à deux cascades d'erreurs de taille $\leq l$, montrer que les syndromes correspondants sont dans différents cosets. En déduire que $\tau_c(\mathcal{C}) \geq l$.
7. Montrer également que $\tau_c(\mathcal{C}) \leq m$. Quelle est l'éfficacité BEC de $\mathcal{C}$ dans le cas $m = l$?

Afin de construire facilement de grands codes avec une bonne efficacité BEC et facilement décodables, on utilise des méthodes dites d'*entrelacement* (interleaving). Supposons que l'on ait à notre disposition λ codes $\mathcal{C}_1, \ldots, \mathcal{C}_\lambda$ de paramètres (n, k) et de capacité BEC l. Le code $\widetilde{\mathcal{C}}$ obtenu par entrelacement de $\mathcal{C}_1, \ldots, \mathcal{C}_\lambda$ a ses mots-codes construits de la manière suivante : soient $c_1, \ldots, c_\lambda$ des mots de codes de $\mathcal{C}_1, \ldots, \mathcal{C}_\lambda$ respectivement, et M la matrice de taille $\lambda \times n$ de lignes $c_1, \ldots, c_\lambda$. On obtient un mot-code de $\widetilde{\mathcal{C}}$ en listant les éléments de M colonne par colonne, i.e. le mot-code $\tilde{c}$ obtenu est $(M_{1,1}, M_{2,1}, \ldots, M_{\lambda,1}, M_{1,2}, \ldots, M_{\lambda,n})$.

8. Quelle sont les paramètres de $\widetilde{\mathcal{C}}$ et quelle est sa capacité BEC ?

Quelques exos sur les corps finis

1. Soit F une extension finie de $F(p)$ qui contient tous les zéros de $X^{p^m} - X$. Montrer (i) que $X^{p^m} - X$ a tous ses zéros distincts dans F ; (ii) directement que ces zéros forment un corps.
2. Soit G un groupe commutatif contenant des éléments g et h d'ordres r et s respectivement. (i) Montrer que si $g^n = 1$ alors $r|n$. (ii) Montrer que si $\text{pgcd}(r, s) = 1$ alors gh a pour ordre rs. (iii) Montrer que si $r = r_1 r_2$ alors g^{r_1} a pour ordre r_2.
3. (i) Montrer que dans tout corps :

$$X^s - 1 | X^r - 1 \Leftrightarrow s|r.$$

(ii) Montrer que $\text{pgcd}(X^r - 1, X^s - 1) = X^d - 1$ avec $d = \text{pgcd}(r, s)$.