Théorie de l'Information et Codage: Fiche d'exercices 4

à rendre pour le 20 juin 2012.

Instructions: merci à chacun de rendre une copie manuscrite. Si vous avez réfléchi à plusieurs sur un problème, mettez les noms de vos collaborateurs.

Problème 1: Quelques propriétés des codes BCH (2 points)

1. Un code est dit réversible si $(c_0, c_1, \ldots, c_{n-1})$ est un mot code alors $(c_{n-1}, c_{n-2}, \ldots, c_0)$ est aussi un mot code. Montrer qu'un code BCH$(-t, 2t+2)$ est réversible.

2. Montrer que si $n = k\ell$ alors le code binaire BCH(b, ℓ) a pour distance minimale ℓ.

Problème 2: construction de codes binaires à partir de codes de Reed-Solomon (4 points)
Soit $\xi_1, \ldots, \xi_m$ une base de l'espace vectoriel $F(2^m)$ sur $F(2)$. Alors si $\beta = \sum_{i=1}^{m} b_i \xi_i$ est un élément de $F(2^m)$ avec $b_i \in F(2)$, on représente β par $b_1, \ldots, b_m$.

1. Montrer que cette correspondance transforme un code linéaire sur $F(2^m)$ en un code linéaire sur $F(2)$. Donner la dimension et une borne sur la distance minimale du code obtenu.

2. En utilisant la base $1, \alpha$ pour $F(4)$ sur $F(2)$ avec $\alpha^2 + \alpha + 1 = 0$, expliciter les mots code du code binaire de longueur 6 obtenu à partir du code de Reed-Solomon sur $F(4)$ vu en cours (de polynôme générateur $g(X) = X + \alpha^2$).

3. Donner la dimension et une borne sur la distance minimale des deux codes suivants: si $c = (c_1, \ldots, c_{N-1})$ est un mot code d'un code de Reed-Solomon sur $F(2^m)$ de distance D,

   (i) on remplace chaque c_i par un m-uplet binaire auquel on rajoute un bit de parité (de tel sorte que le nombre de 1 dans le $m+1$ uplet est paire).

   (ii) on rajoute d'abord un bit de parité au mot code c (i.e. code de Reed-Solomon étendu), puis on fait la meme construction que précédement.

Problème 3: Codes MDS (7 points) Pour un code linéaire de dimension k et de longueur n, la distance minimale du code doit satisfaire $d \leq n - k + 1$. Un code MDS (maximum distance separable) est un code tel que $d = n - k + 1$.

1. Montrer que les codes de Reed-Solomon étendus (i.e. à chaque mot code est ajouté un bit de parité $c_N = -\sum_{i=0}^{N-1} c_i$) sont MDS.

2. Montrer qu'un code est MDS si et seulement si tout ensemble de $n - k$ colonnes de la matrice de parité H sont linéairement indépendent.

3. Montrer que si un code est MDS, son dual aussi.

4. En utilisant les deux résultats précédents, montrer qu'un code est MDS si et seulement si pour tout ensemble de d coordonnées, il existe un mot-code de poids minimal chargeant uniquement ces d coordonnées.

5. Montrer que pour tout $k \in \{1, \ldots, 2^m + 1\}$, il existe un code cyclique MDS de longueur $2^m + 1$ et dimension k sur $F(2^m)$. On pourra montrer au préalable que tous les facteurs sur $F(2^m)$ de $X^{2^m+1} + 1$ autres que $X + 1$ sont quadratiques.

Problème 4: Codes de Justesen (7 points) La classe des codes de Justesen est la seule classe de codes linéaires binaires explicitement connue contenant des codes $(\mathcal{C}_i)_{i\geq 1}$ dont les paramètres de longueur, dimension et distance minimale $(n_i, k_i, d_i)_{i\geq 1}$ satisfont:

$$n_i \xrightarrow[i\to\infty]{} +\infty, \qquad \liminf_{i\to\infty} \frac{k_i}{n_i} > 0 \qquad \text{et} \qquad \liminf_{i\to\infty} \frac{d_i}{n_i} > 0.$$

Notons $\mathcal{P}_r$ l'ensemble des polynômes de degré au plus r sur le corps fini $\mathbb{F}_{q^m}$ et soit $L = (\alpha_1, \ldots, \alpha_n)$ une famille de $n > r$ éléments 2 à 2 distincts de $\mathbb{F}_{q^m}$.

1. À chaque $f \in \mathcal{P}_r$, on associe le vecteur de ses évaluations sur L, i.e. le mot-code

$$c(f) = (f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_{q^m}^n,$$

et l'on note $\mathcal{C}_{L,r}$ l'ensemble des vecteurs ainsi obtenus. Vérifier que $\mathcal{C}_{L,r}$ est un code linéaire, puis calculer sa dimension et sa distance.

2. Montrer que cette famille de codes généralise celle des codes de Reed-Solomon.

3. À chaque $f \in \mathcal{P}_r$, on associe à présent le mot-code

$$\widetilde{c}(f) = (f(\alpha_1), \alpha_1 f(\alpha_1), \ldots, f(\alpha_n), \alpha_n f(\alpha_n)) \in \mathbb{F}_{q^m}^{2n},$$

et l'on note $\widetilde{\mathcal{C}}_{L,r}$ l'ensemble des vecteurs ainsi obtenus. Quelles sont les longueur et dimension de $\widetilde{\mathcal{C}}_{L,r}$? Montrer qu'un mot-code non-nul contient toujours au moins $n-r$ couples $(f(\alpha_i), \alpha_i f(\alpha_i))$ 2 à 2 distincts.

4. Expliquer comment transformer simplement un code linéaire q^m-aire de dimension k et de longueur n en un code linéaire $q-$aire de dimension mk et de longueur mn.

5. Pour tout $m \geq 1$ et tout $\varrho \in [0, 1)$, on appelle code de Justesen d'ordre m et de paramètre ϱ le code binaire obtenu en appliquant la transformation de la question (4) au code de la question (3) avec $q = 2$, $r = \lfloor 2^m \varrho \rfloor$ et $L = \mathbb{F}_{2^m}$. Montrer que la classe des codes de Justesen vérifie bien la propriété annoncée.

Indication: on pourra démontrer le résultat suivant: si $x_1, \ldots, x_M$ sont des mots binaires 2 à 2 distincts de longueur N, alors la proportion totale de 1, $\gamma = \frac{1}{MN} \sum_{i=1}^{M} w(x_i)$, vérifie:

$$NH(\gamma) \geq \log_2(M).$$