Théorie de l'Information et Codage: Fiche d'exercices 3

à rendre pour le 9 juin 2014.

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: Codes localement décodables (8 points)

On généralise la définition des codes de Reed Muller vue en TD à l'alphabet q-aire. Soit q premier, n un entier et $d < q-1$. A toute fonction $f : \mathbb{F}_q^n \to \mathbb{F}_q$ on associe le vecteur $\langle f \rangle = (f(\mathbf{x}), \mathbf{x} \in \mathbb{F}_q^n) \in \mathbb{F}_q^{q^n}$ appelé la $\mathbb{F}_q^n$-évaluation de f. Le code de Reed Muller $[n, q, d]$ est constitué des $\mathbb{F}_q^n$-évaluations de tous les polynômes de degré total au plus d dans $\mathbb{F}_q[X_1, \ldots, X_n]$.

1. Montrer que le code de Reed Muller $[n, q, d]$ est un code linéaire dont on donnera la dimension.

Soit $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ et $\mathbf{y} \in \mathbb{F}_q^{q^n}$ tel que $d_H(\langle P \rangle, \mathbf{y}) \leq \delta q^n$ pour $\delta \in (0, 1)$ avec d_H la distance de Hamming. Pour $\mathbf{w} \in \mathbb{F}_q^n$, on cherche à retrouver $P(\mathbf{w})$ à partir de $\mathbf{y}$. Si tout $\mathbf{y}$ est connu, on est dans un cadre classique de décodage. Pour certaines applications, il est utile de retrouver $P(\mathbf{w})$ à partir de très peu d'entrées du vecteur $\mathbf{y}$ (décodage local). On introduit alors une probabilité d'erreur. Le but du problème est de comprendre le lien entre cette probabilité d'erreur, le nombres d'entrées dévoilées et le paramètre δ.

$P \in \mathbb{F}_q[X_1, \ldots, X_n]$ et $\mathbf{w} \in \mathbb{F}_q^n$ sont donc fixés. Voici un premier algorithme simple: prendre un vecteur $\mathbf{v} \in \mathbb{F}_q^n$ au hasard et considérer la ligne

$$L = \{\mathbf{w} + \lambda \mathbf{v},\ \lambda \in \mathbb{F}_q\}.$$

Soit S un sous-ensemble arbitraire de $\mathbb{F}_q^*$ tel que $|S| = d+1$. L'algorithme demande les coordonnées du vecteur $\mathbf{y}$ correspondant aux points $\mathbf{w} + \lambda \mathbf{v}$ pour $\lambda \in S$ et obtient les valeurs $\{e_\lambda\}$. L'algorithme calcule l'unique polynôme univarié h de degré au plus d tel que $h(\lambda) = e_\lambda$ pour tout $\lambda \in S$. L'algorithme renvoie $h(0)$.

2. Vérifier que l'algorithme est bien défini, i.e. qu'il existe bien un unique polynôme h tel que décrit ci-dessus.

3. Montrer que l'algorithme retrouve $P(\mathbf{w})$ avec probabilité au moins $1-(d+1)\delta$ en faisant $d+1$ requêtes.

En particulier, si l'on veut une probabilité d'erreur inférieure à $1/2$, il faut $\delta < \frac{1}{2(d+1)}$. Pour améliorer cet algorithme, nous avons besoin de résoudre le problème suivant, noté (P): données: m paires de points $(x_i, s_i) \in \mathbb{F}_q \times \mathbb{F}_q$ avec les x_i distincts telles qu'il existe un polynôme K de degré au plus d tel que $s_i = K(x_i)$ pour tous les i sauf au plus k, avec $2k + d < m$; but: trouver K.

4. Montrer qu'il est équivalent de résoudre le problème (P) ou de trouver des polynômes W et K tels que:

$$deg(W) \leq k,\ deg(K) \leq d,\ W \neq 0, \text{ et } \forall i\ W(x_i)s_i = W(x_i)K(x_i). \tag{1}$$

Donc si on trouve deux polynômes W et N tels que

$$deg(W) \leq k,\ deg(N) \leq k+d,\ W \neq 0, \text{ et } \forall i\ W(x_i)s_i = N(x_i) \tag{2}$$

et en plus W divise N, alors on a trouvé deux polynômes W et K qui vérifient (1).

5. Montrer que si N, W et L, U sont deux solutions de (2) alors $\frac{N}{W} = \frac{L}{U}$.

6. Conclure que le problème (P) se réduit à un problème d'algèbre linéaire.

Nous revenons maintenant au problème de décodage local en faisant l'hypothèse supplémentaire que $d \leq \sigma(q-1)-1$ pour un réel $\sigma < 1$. On modifie l'algorithme comme suit: l'algorithme demande les coordonnées du vecteur $\mathbf{y}$ correspondant aux points $\mathbf{w} + \lambda\mathbf{v}$ pour $\lambda \in \mathbb{F}_q^*$ et obtient les valeurs $\{e_\lambda\}$. L'algorithme calcule l'unique polynôme univarié h tel que $h(\lambda) = e_\lambda$ pour toutes les valeurs de $\lambda \in \mathbb{F}_q^*$ sauf au plus $\lfloor (1-\sigma)(q-1)/2 \rfloor$. Si un tel polynôme h n'existe pas, l'algorithme renvoie 0 sinon il renvoie $h(0)$.

7. Vérifier que l'algorithme est bien défini et a un temps d'execution polynomial en n (q et d étant fixés).

8. Montrer que l'algorithme retrouve $P(\mathbf{w})$ avec probabilité au moins $1 - 2\delta/(1-\sigma)$ en faisant $q-1$ requêtes.

En particulier, si σ est faible, cet algorithme tolère une fraction d'erreur δ de presque $1/4$.

Problème 3: Codes MDS (4 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 qu'un code est MDS si et seulement si tout ensemble de $n-k$ colonnes de la matrice de parité H sont linéairement indépendent.

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

3. 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.

4. 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 (6 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:

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