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

à rendre pour le cours du 21 mai 2013.

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: Codes de Hadamard (6 points)

1. Montrer que parmi les codes de longueur 11 pouvant corriger deux erreurs, le code linéaire le plus grand contient au plus 16 mots code.

Nous allons construire un code plus performant. Une matrice d'Hadamard de taille n est une matrice carrée $n \times n$ à coefficicents dans $\{-1, +1\}$ et telle que: $HH^T = nI$, i.e. le produit scalaire dans $\mathbb{R}$ de deux lignes distinctes est nul et le produit scalaire d'une ligne avec elle-même est n. Comme $H^{-1} = \frac{1}{n}H^T$, on a aussi $H^T H = nI$ et donc les colonnes de H ont la même propriété.

2. Etant donné H, montrer qu'on peut toujours construire à partir de H une matrice de Hadamard telle que la première colonne ainsi que la première ligne soient constituées de $+1$.

On dira qu'une telle matrice de Hadamard est normalisée. Voici des exemples de matrices de Hadamard normalisées (avec la convention $-$ au lieu de -1):

$$H_1 = (1), \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}. \tag{1}$$

3. Montrer que si H est une matrice d'Hadamard de taille n alors $n = 1, 2$ ou n est multiple de 4 (Il suffit de considerer les 3 premières lignes d'une matrice normalisée).

L'existence de matrices de Hadamard pour tout n multiple de 4 est une question ouverte. Une construction simple repose sur l'observation que si H_n est une matrice de Hadamard de taille n alors

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

est une matrice de Hadamard de taille $2n$. Cette construction permet d'obtenir les matrices de Sylvester $H_1, H_2, \ldots$ (1). On définit un (n, M, d) code un ensemble de M mots code de longueur n ayant distance minimale d.

4. Montrer qu'à partir d'une matrice de Hadamard normalisée H_n, il est possible de construire des codes binaires ayant les caractéristiques suivantes: $(n-1, n, n/2)$, $(n-1, 2n, n/2-1)$ et $(n, 2n, n/2)$. Conclure.

Problème 2: (3 points)
Pour n et d fixés, soit $M_L(n,d)$ le nombre maximum de mots code d'un code linéaire binaire de longueur n et de distance minimale $\geq d$. Montrer que

$$M_L(n,d) \geq \frac{2^n}{1+\binom{n-1}{1}+\cdots+\binom{n-1}{d-2}}.$$

Problème 3: Quelques propriétés des codes BCH (3 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 4: 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:

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

Donc si on trouve deux polynômes W et N tels que

$$deg(W) \leq k,\ deg(N) \leq k + d,\ W \neq 0, \text{ et } \forall i\, W(x_i)s_i = N(x_i) \tag{3}$$

et en plus W divise N, alors on a trouvé deux polynômes W et K qui vérifient (2).

5. Montrer que si N, W et L, U sont deux solutions de (3) 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 $1/4$.