M1MI2016 Codes et Cryptologie

Feuille d'exercices n° 10.

Matrice de parité, code dual

1 Soit la matrice

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

1. Vérifiez que H est bien une matrice de parité d'un code C dont on précisera la longueur et la dimension.
2. Les mots suivants appartiennent-ils à C ?
   (a) $x = 00011100$
   (b) $x = 01000011$
   (c) $x = 11111000$
   (d) $x = 10101010$
3. Donnez une matrice génératrice de C.

2 Donner une matrice de parité des codes suivants :

1. Le code de Hamming (TD 9 exo 8).
2. Le code de parité (TD 9 exo 9).
3. Le code de Hamming étendu (TD 9 exo 10). Montrez que ce code est égal à son code dual.
4. Le code C de l'exercice 12 TD 9.

3 Soit C un code linéaire de matrice de parité H. Montrez les propriétés suivantes :

1. C contient un mot de poids 1 si et seulement si H contient une colonne nulle.
2. C contient un mot de poids 2 si et seulement si H contient deux colonnes identiques.
3. C contient un mot de poids w si et seulement si H contient w colonnes dont la somme est nulle.

4 Utilisez l'exercice précédent pour calculer la distance minimale du code C de l'exercice 1.

5 **Les codes de Hamming généralisés :** Soit $r \geq 2$, un code de Hamming généralisé de paramètre r est un code dont une matrice de parité est une matrice dont les colonnes sont exactement l'ensemble des vecteurs non nuls de $\{0,1\}^r$, pris sans répétition et dans un ordre arbitraire.

1. Explicitez une matrice de parité, puis une matrice génératrice d'un code de Hamming de paramètre $r = 2$, $r = 3$, puis $r = 4$. Quelle est la longueur et la dimension de ces codes ?
2. Pour $r \geq 2$ quelconque, montrez qu'un code de Hamming de paramètre r est de longueur $n = 2^r - 1$ et de dimension $n - r$.
3. Montrez qu'un code de Hamming de paramètre $r \geq 2$ est de distance minimale 3.

6 **Le poids des mots du dual d'un code de Hamming.** Soit C un code de Hamming généralisé de paramètre r,

1. Vérifiez que pour $r = 2$, les mots non nuls de $C^\perp$ sont tous de poids 2, puis que pour $r = 3$, ils sont de poids 4.
2. On montre dans cette question que, pour $r \geq 2$ quelconque, les mots non nuls de $C^\perp$ sont tous de poids 2^{r-1}.
   (a) Soit H une matrice de parité de C. Montrez que
   $$x \in C^\perp \Leftrightarrow \text{il existe } u \in \{0,1\}^r \text{ tel que } x = uH.$$
   (b) Soit $u \in \{0,1\}^r$, $u \neq 0^r$, et soit
   $$\begin{aligned} f : \{0,1\}^r &\to \{0,1\} \\ y &\mapsto u_1 y_1 + \cdots + u_r y_r. \end{aligned}$$
   Montrez que f est une application linéaire et que $|\operatorname{Ker}(f)| = 2^{r-1}$.
   (c) En déduire que $x = uH$ est de poids 2^{r-1} et conclure.

7 **La borne de Singleton :** Montrez que, si C est un code linéaire de paramètres $[n, k, d]$, alors $d \leq n - k + 1$. Indication : utilisez la forme échelonnée réduite d'une matrice génératrice de C pour montrer que C contient un mot non nul de poids inférieur ou égal à $n - k + 1$.

8 **La borne de Hamming :** Soit C un code de longueur n et de distance minimale d. Soit $t = \lfloor (d-1)/2 \rfloor$.

1. Montrez que les boules $B_n(x,t)$ de centre $x \in C$ sont disjointes (on pourra utiliser l'exercice 5 de la feuille de TD 9).
2. Montrez que (c'est l'exo 4 TD 9) :
   $$|B_n(x,t)| = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}.$$
3. En déduire que
   $$|C| \leq \frac{2^n}{1 + \binom{n}{1} + \cdots + \binom{n}{t}}.$$