Université Mohammed V Agdal
Faculté des Sciences
Rabat

Année 2013-14
Master C2SI
Théorie des codes
Contrôle Final

Documents non autorisés

Exercice 1. Montrer que le code dual $Ham(r,q)^{\perp}$ d'un code de Hamming $Ham(r,q)$ est un code simplexe, et la valeur commune des poids (non nulle) est q^{r-1}.

Cas binaire : $Ham(r,2)^{\perp}$ est clairement de longueur 2^r-1, de dimension r et matrice génératrice H_r. (H_r étant une matrice de contrôle de $Ham(r,2)$.

Par récurrence sur r :

Pour $r=2$ on a

$$H_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

et le poids de tout mot de $Ham(2,2)^{\perp}$ est $2 = 2^{2-1}$

On suppose vrai pour $r-1$. On peut construire H_r à partir de H_{r-1} :

$$H_r = \left(\begin{array}{c|c|c} 0\cdots 0 & 1 & 1\cdots 1 \\ & 0 & \\ H_r & \vdots & H_r \\ & 0 & \end{array}\right)$$

est une matrice $((r-1)+1) \times ((2^{r-1}-1)+1+(2^{r-1}-1)) = r \times (2^r-1)$.

Les mots de $Ham(r,2)^{\perp}$ sont de la forme :

- première ligne de H_r :il est de poids $(1+2^{r-1}-1) = 2^{r-1}$
- $(a,0,b)$ où a et b sont des lignes de H_r, le poids de $(a,0,b)$ est $2.2^{r-2} = 2^{r-1}$
- $(a,1,b+1)$ somme de deux lignes de H_{r-1}, le poids de $(a,1,b+1)$ est $2^{r-2}+1+2^{r-2}-1 = 2^{r-1}$

Donc tous les mots de $Ham(r,2)^{\perp}$ sont de poids 2^{r-1} sauf 0.

Exercice 2. Soit C un $[n,k,d]$-code linéaire binaire auto-dual.

a) Montrer que le mot $1\cdots 1$ est dans C.

b) Montrer que soit tous les mots de C sont de poids divisibles par 4 ; ou exactement la moitié de mots de C sont de poids divisibles par 4 tandis que l'autre moitié sont de poids pairs non divisibles par 4.

c) Pour $n=6$. Déterminer d.

Exercice 3. Soit $g(x)$ le polynôme générateur d'un code cyclique binaire C.

a) Montrer que si $x+1$ divise $g(x)$ alors C ne contient aucun mot de poids impair.

b) Montrer que si n est impair et $x+1$ ne divise pas $g(x)$ alors C contient le mot $1\cdots 1$.

c) Montrer que si n est le plus petit entier tel que $g(x)$ divise x^n+1 alors la distance minimale de C est au moins 3.

d) On suppose que C contient des mots de poids pairs et impaires. Soit $A(z)$ le polynôme énumérateur de poids de C. Montrer que le polynôme $(x+1)g(x)$ engendre un code cyclique binaire de polynôme énumérateur de poids $A_1(z) = \frac{1}{2}\left[A(z)+A(-z)\right]$.

Rappel ; le polynôme énumérateur de poids $A(X) = \sum_{i=0}^{n} A_i x^n$ où $A_i = |\{c \in C \mid \omega(c) = i\}|$

a) Soit $c(x) \in C$ un mot dut code. Alors il existe un polynôme $a(x)$ tel que $c(x) = a(x).g(x)$. Puisque $x+1$ divise $g(x)$ alors $x+1$ divise $c(x)$ d'où $c(1) = 0$ donc le poids de $c(x)$ est pair.

b) On sait $X^n + 1 = (x+1)(1 + x + x^2 + \cdots + x^{n-1})$. Puisque $g(x)$ divise $X^n + 1$ et $x+1$ ne divise pas $g(x)$ alors $g(x)$ divise $1 + x + x^2 + \cdots + x^{n-1}$. Donc $1 + x + x^2 + \cdots + x^{n-1}$ est un mot du code C.

c) On suppose qu'il existe un mot de C de poids 1. Ce mot est un polynôme de la forme $c(x) = x^m$ où $0 \leq m \leq n-1$. Puisque le code est cyclique alors $1 \in C$ d'où $g(x)$ divise 1. Le code C dans ce cas est le code trivial $\mathcal{F}_n$.

On suppose qu'il existe un mot de C de poids 2. Ce mot est un polynôme de la forme $c(x) = x^r + x^s$ où $0 \leq r < s \leq n-1$. Puisque le code est cyclique $1 + x^{s-r} \in C$ d'où $g(x)$ divise $1 + x^{s-r}$. Ce qui contredit le fait que l'hypothèse puisque $s - r < n$.

d) Puisque C contient des mots de poids paires et de poids impaires $x+1$ ne divise pas $g(x)$. Or $g(x)$ divise x^n+1 d'où $(x+1)g(x)$ divise x^n+1. $(x+1)g(x)$ engendre un $[n, k-1]$-code cyclique qu'on note C'.

On montre que C' contient les mots de poids pairs de C. Soit $c(x) \in C$, alors il existe $a(x)$ tel que $c(x) = a(x)g(x)$ où $deg(a(x)) \leq k-2$. $c(x)$ est de poids pair si seulement si $c(x)$ est divisible par $x+1$. Puisque $g(x)$ n'est pas divisible par $x+1$, $c(x)$ est de poids pair si et seulement si $x+1$ divise $a(x)$ càd $a(x) = b(x)(x+1)$ et $c(x) = b(x)(x+1)g(x)$ d'où $c(x) \in C'$.

Inversement, soit $c(x) \in C'$. Clairement $c(x) = b(x)(x+1)g(x) \in C$ et de poids pair.

Soient $A_1(z)$ le polynôme énumérateur de poids de C' et $A(z)$ le polynôme énumérateur de poids de C. $\frac{1}{2}[A(z) + A(-z)]$ correspond aux mots de poids pairs de C. Donc $A_1(z) = \frac{1}{2}[A(z) + A(-z)]$.