Département COMELEC

UE COM105

Corrigé du TD 1

1. $k = 3$ et $d_{\min} = 2$. De plus, le code a une matrice génératrice systématique

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

et donc une matrice de contrôle de parité systématique

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}.$$

2. $k = 1$ et $d_{\min} = 4$. De plus, le code a une matrice génératrice systématique

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

et donc une matrice de contrôle de parité systématique

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

On observe qu'en permutant les colonnes de la matrice de contrôle de parité du code à répétition on obtient la matrice génératrice du code de parité de la même longueur, et vice versa. Les deux codes sont donc *duaux*.

3. Chaque pair $\boldsymbol{u} \in \mathcal{C}_1$ et $\boldsymbol{v} \in \mathcal{C}_2$ donne lieu à un autre mot de code $\mathbf{c} = (\boldsymbol{u}|\boldsymbol{v})$. Ils existent donc $2^{k_1} \cdot 2^{k_2} = 2^{k_1+k_2}$ mots de code de $\mathcal{C}_{\text{naive}}$ et la dimension de $\mathcal{C}_{\text{naive}}$ est $k_{\text{naive}} = k_1 + k_2$.

4. Comme le code $\mathcal{C}_{\text{naive}}$ enchaîne un mot de code de $\mathcal{C}_1$ et un mot de code de $\mathcal{C}_2$ (les deux mots de code étant choisis par des mots d'information différents), sa matrice génératrice G_{naive} peut s'écrire comme

$$G_{\text{naive}} = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}.$$

5. Par linéarité du code $\mathcal{C}_{\text{naive}}$, il suffit de trouver le plus petit poids de Hamming d'un mot non nul du code $\mathcal{C}_{\text{naive}}$. Soit $\boldsymbol{c} = (\boldsymbol{u}|\boldsymbol{v}) \in \mathcal{C}_{\text{naive}}$. Par la définition du poids de Hamming :

$$w_H(\boldsymbol{c}) = w_H(\boldsymbol{u}|\boldsymbol{v}) = w_H(\boldsymbol{u}) + w_H(\boldsymbol{v}).$$

Comme $\boldsymbol{c}$ est non nul, soit $\boldsymbol{u}$ est non nul soit $\boldsymbol{v}$ est non nul. Si $\boldsymbol{u}$ est non nul, alors $w_H(\boldsymbol{u}) \geq d_1$ et pour certains $\boldsymbol{u}$ il y a égalité. Si $\boldsymbol{v}$ est non nul, alors $w_H(\boldsymbol{v}) \geq d_2$, et pour certains $\boldsymbol{v}$ il y a égalité. En résumé, pour tout $\boldsymbol{c}$ non nul, $w_H(\boldsymbol{c}) \geq \min\{d_1, d_2\}$ et pour certains $\boldsymbol{c}$ il y a égalité. Donc $d_{\text{naive}} = \min\{d_1, d_2\}$.

6. Les deux codes $\mathcal{C}_1(n, k_1, d_1)$ et $\mathcal{C}_2(n, k_2, d_2)$ nécessairement satisfont la borne de Singleton. Donc

$$d_1 \leq n - k_1 + 1 \qquad \text{et} \qquad d_2 \leq n - k_2 + 1.$$

En prenant la somme des deux inégalités et en utilisant $k_{\text{naive}} = k_1 + k_2$ et $d_{\text{naive}} = \min\{d_1, d_2\}$, on arrive à l'inégalité

$$2d_{\text{naive}} = 2\min\{d_1, d_2\} \leq d_1 + d_2 \leq 2n - k_{\text{naive}} + 2.$$

7. La matrice génératrice $G_{\text{carré}}$ peut s'écrire comme

$$G_{\text{carré}} = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}.$$

Cette matrice a $k_1 + k_2$ lignes et $2n$ colonnes, comme G_1 a k_1 lignes et n colonnes et G_2 a k_2 lignes et n colonnes. De plus, la matrice est de rang plein, $k_1 + k_2$, comme G_1 et G_2 sont de rang plein. En fait, le rang d'une matrice en forme triangulaire par blocs est au moins égale à la somme des rangs des matrices en blocs sur la diagonale.

Donc, $k_{\text{carré}} = k_1 + k_2$, et $\mathcal{C}_{\text{carré}}$ a la même dimension que $\mathcal{C}_{\text{naive}}$.

8. Par linéarité du code $\mathcal{C}_{\text{carré}}$, il suffit de trouver le plus petit poids de Hamming d'un mot non nul du code $\mathcal{C}_{\text{carré}}$. Par la définition du poids de Hamming :

$$w_H(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}) = w_H(\boldsymbol{u}) + w_H(\boldsymbol{u}+\boldsymbol{v}).$$

Nous distinguons les trois cas suivants :
— Si $\boldsymbol{u} = 0$ et $\boldsymbol{v} \neq 0$, alors $\boldsymbol{c} = (\boldsymbol{0}|\boldsymbol{v})$ et $w_H(\boldsymbol{c}) \geq d_2$ avec égalité si $\boldsymbol{v}$ est un mot code de poids minimal dans $\mathcal{C}_2$.
— Si $\boldsymbol{v} = 0$ et $\boldsymbol{u} \neq 0$, alors $\boldsymbol{c} = (\boldsymbol{u}|\boldsymbol{u})$ et $w_H(\boldsymbol{c}) \geq 2d_1$ avec égalité si $\boldsymbol{u}$ est un mot code de poids minimal dans $\mathcal{C}_1$.
— Si $\boldsymbol{u} \neq 0$ et $\boldsymbol{v} \neq 0$, alors $\boldsymbol{c} = (\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v})$ et

$$w_H(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}) = w_H(\boldsymbol{u}) + w_H(\boldsymbol{u}+\boldsymbol{v})$$

Il nous faut donc caractériser $w_H(\boldsymbol{u}+\boldsymbol{v})$ avec une borne inférieure. Pour cela on peut remarquer que le poids de Hamming satisfait pour tous les mots $\boldsymbol{a}$ et $\boldsymbol{b}$ la relation suivante :

$$w_H(\boldsymbol{a}+\boldsymbol{b}) \leq w_H(\boldsymbol{a}) + w_H(\boldsymbol{b}), \tag{1}$$

parce que le mot $(\boldsymbol{a}+\boldsymbol{b})$ contient 1 à une certaine position si et seulement si un seul des deux mots $\boldsymbol{a}$ et $\boldsymbol{b}$ contient 1 à cette position. Donc le nombre de 1 dans $(\boldsymbol{a}+\boldsymbol{b})$ ne peut pas dépasser la somme des nombres de 1 dans $\boldsymbol{a}$ et dans $\boldsymbol{b}$. Nous pouvons également obtenir cette inégalité en remarquant que $w_H(\boldsymbol{a}+\boldsymbol{b}) = d_H(0, \boldsymbol{a}+\boldsymbol{b})$ et que d_H, en tant que distance, satisfait l'inégalité triangulaire.

Grâce à l'équation (1), nous obtenons

$$w_H(\boldsymbol{v}) = w_H(\boldsymbol{u}+\boldsymbol{u}+\boldsymbol{v}) \leq w_H(\boldsymbol{u}) + w_H(\boldsymbol{u}+\boldsymbol{v}),$$

donc

$$w_H(\boldsymbol{u}+\boldsymbol{v}) \geq w_H(\boldsymbol{v}) - w_H(\boldsymbol{u}).$$

ce qui implique que

$$w_H(\boldsymbol{u}|\boldsymbol{u}+\boldsymbol{v}) \geq w_H(\boldsymbol{u}) + w_H(\boldsymbol{v}) - w_H(\boldsymbol{u}) = w_H(\boldsymbol{v}) \geq d_2.$$

En résumé,

$$d_{\text{carré}}(\mathcal{C}) = \min\{2d_1, d_2\}$$

car il existe au moins un mot code de $\mathcal{C}$ de poids $\min\{2d_1, d_2\}$ et le poids de tout mot code de $\mathcal{C}$ non nul est borné soit par $2d_1$ soit par d_2.

9. Le code $\mathcal{C}_{\text{carré}}$ est un code $(8, 4, 4)$. En utilisant les réponses aux questions 1., 2., et 7., on trouve la matrice génératrice

$$G_{\text{carré}} = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

10. Il n'y a pas de code $C_{\text{naive}}(8, 4, 4)$, car ces valeurs $2n = 8$, $k = 4$, et $d_{\text{naive}} = 4$ ne satisfont pas l'inégalité prouvée dans la question 6., c'est-à-dire l'inégalité (1) de l'énoncé.