TD 3

Exercice 1.
Le but de cet exercice est l'étude de certains résultats sur le code de Golay binaire $\mathcal{G}_{23}$ et le code de Golay binaire étendu $\mathcal{G}_{24}$.

Commençons par deux petits résultats généraux qui serviront ensuite à déterminer la distance des codes de Golay binaires (c-à-d sur $\mathbb{F}_2$). On se fixe un code binaire C, de paramètres $[n, k, d]$, et G une matrice génératrice de C. On suppose pour toute la suite que les lignes de G sont orthogonales entre elles.

(a) Montrer que C est inclus dans $C^\perp$.

On s'intéresse maintenant aux poids des vecteurs d'un tel code.
(b.1) Soient L et K deux lignes de G.
Montrer que $w(L+K) = w(L) + w(K) - 2\#\{i\,;\, L_i = K_i = 1\}$ (où $\#$ désigne le cardinal d'un ensemble et L_i désigne le $i$ème coefficient de L).

(b.2) On suppose que le poids des lignes de G est multiple de 4. Montrer que la somme de deux lignes a un poids multiple de 4.

(b.3) En déduire que, sous la même hypothèse qu'en (b.2), tout élément du code a un poids multiple de 4.

On définit maintenant le code de Golay binaire étendu $\mathcal{G}_{24}$ par sa matrice génératrice $G = (I_{12}\vdots A)$ obtenue en mettant côte à côte deux matrices 12×12 où

$$A = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & B & \\ 1 & & & \end{pmatrix}$$

et B est la matrice circulante de taille 11×11 définie par sa première ligne

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

Précisément $B_{i,j}$ vaut 1 lorsque $i + j - 2$ est un carré modulo 11 (c-à-d $0, 1, 3, 4, 5, 9$) et vaut 0 sinon.
On admet que les lignes de G sont orthogonales entre elles.

(c.1) Vérifier que le poids des lignes de G est multiple de 4.

(c.2) En déduire que la distance du code est 4 ou 8, et que $\mathcal{G}_{24} = \mathcal{G}_{24}^\perp$.

(c.3) Montrer que $A = {}^tA$.

(c.4) En déduire que $H = (A\vdots I_{12})$ est à la fois une matrice de contrôle et une matrice génératrice de $\mathcal{G}_{24}$.

On veut maintenant montrer que la distance du code de $\mathcal{G}_{24}$ est 8.
Supposons par l'absurde qu'il existe un mot c du code, de poids 4. Soit r le nombre de lignes de G dont on a fait la somme pour obtenir c.
(d.1) Justifier que $r \leq 4$.

(d.2) Démontrer que $r = 1$ est impossible.

(d.3) Démontrer que $r = 4$ est impossible. (On pourra admettre que A est inversible)

(d.4) Démontrer que $r = 3$ est impossible (on pourra écrire c sous la forme $(x\vdots xA)$ et sous la forme $(yA\vdots y)$ où x et y sont dans $\mathbb{F}_2^{12}$).

(d.5) Sans faire tout le raisonnement en détails, expliquer ce qu'il faut vérifier pour éliminer le cas $r = 2$.

On considère maintenant le code $\mathcal{G}_{23}$ (toujours sur $\mathbb{F}_2$) obtenu en enlevant la dernière coordonnée aux mots de $\mathcal{G}_{23}$.

(e.1) Démontrer que $\mathcal{G}_{23}$ est de paramètres $[23, 12, 7]$. Combien d'erreurs les codes $\mathcal{G}_{23}$ et $\mathcal{G}_{24}$ peuvent-ils corriger ?

(e.2) Montrer que le code $\mathcal{G}_{23}$ est parfait (on pourra utiliser les égalités $\binom{23}{2} = 253$ et $\binom{23}{3} = 1771$).