Alice transmet un 7-uple binaire $\mathbf{x} = [x_1, \ldots, x_7]$ à Bob avec la convention que le message secret associé est le syndrome $\sigma(\mathbf{x})$. Pour communiquer un secret de trois bits, on transmet donc sur le canal sept symboles binaires. On suppose que $\mathbf{x}$, et donc $\mathbf{s}$, suivent des lois uniformes dans $\{0,1\}^7$ et $\{0,1\}^3$.

On suppose maintenant que Alice communique à Bob deux secrets de trois bits, soit $\mathbf{s}$ et $\mathbf{t}$, en transmettant les deux 7-uples $\mathbf{x} = [x_1, \ldots, x_7]$ et $\mathbf{y} = [y_1, \ldots, y_7]$. Une espionne, Eve, est capable d'intercepter jusqu'à 7 des 14 symboles transmis, mais pas plus. Montrer qu'elle est capable d'obtenir un des secrets, mais que quels que soient les symboles qu'elle intercepte, elle a zéro bit d'information sur au moins un des deux secrets $\mathbf{s}$ ou $\mathbf{t}$.

– EXERCICE 6. On considère le code linéaire ternaire C de matrice de parité

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

a) Quels sont les paramètres du code C ?

b) Combien le code C a-t-il de mots de poids minimum ?

– EXERCICE 7. Montrer que si un code linéaire C a une distance minimale 4, alors il existe des mots $\mathbf{x}$ de l'espace tels que pour tout mot de code $\mathbf{c} \in C$, la distance de Hamming de $\mathbf{x}$ à $\mathbf{c}$ vérifie $d(\mathbf{x}, \mathbf{c}) \geqslant 2$. En déduire qu'il n'existe pas de code linéaire binaire de paramètres $[7, 4, 4]$.

– EXERCICE 8. On considère le code binaire C de matrice de parité

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

a) Quels sont les paramètres de ce code ?

b) On reçoit le mot

$$[? \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1]$$

où la première coordonnée a été effacée. En faisant l'hypothèse qu'au plus une coordonnée non effacée est en erreur, montrer qu'on peut retrouver le mot de code d'origine sans ambiguïté et le donner.

c) Donner une configuration minimale d'effacements (avec un nombre minimum d'effacements) non corrigible, et une configuration maximale d'effacements corrigible.

d) Quels sont les paramètres du code dual $C^\perp$?

e) Calculer le nombre de mots de l'espace $\{0,1\}^{10}$ qui ne sont pas à distance 0 ou 1 d'un mot de code.