TD 11 : Codes correcteurs d'erreur

Exercice 1. *Échauffement*

Soit $\mathcal{C}$ un $(n, M, d)_\Sigma$-code, avec d pair.

✎ Montrer qu'on peut corriger jusqu'à $d/2 - 1$ erreurs, mais pas $d/2$ erreurs.

Exercice 2. *Codes dérivés*

1. Soit $\mathcal{C}$ un $(n, M, d)_2$-code avec d impair. Montrer qu'on peut déduire de $\mathcal{C}$ un $(n+1, M, d+1)_2$-code.
2. **i.** Soit $\mathcal{C}$ un $(n, M, d)_\Sigma$-code. Montrer qu'on peut déduire de $\mathcal{C}$ un $(n-1, M, d-1)_\Sigma$-code.
   ii. En déduire une nouvelle preuve de la borne de Singleton.

Étant donné un code $\mathcal{C}$ de paramètres $(n, M, d)_\Sigma$ et un ensemble $I \subset \{1, \dots, n\}$, on définit le *code poinçonné* $\mathcal{C}_I = \{(c_j)_{j \notin I} : (c_i)_i \in \mathcal{C}\}$ obtenu en supprimant de chaque mot de code les lettres d'indices $i \in I$.

3. Calculer les paramètres de $\mathcal{C}_I$ pour $\#I \leq d$.

Exercice 3. *Erreurs et effacements*

Soit $\mathcal{C}$ un $(n, M, d)_\Sigma$-code. On considère un canal bruité qui ajoute des erreurs (symbole remplacé par un autre symbole de l'alphabet) et des effacements (symbole remplacé par `?` par exemple). On note e le nombre d'erreurs et s le nombre de symboles effacés dans le mot reçu.

1. Montrer que si $e = 0$ et $s < d$, il est toujours possible de décoder le mot reçu de manière unique.
2. Montrer que tant que $2e + s < d$, on peut décoder le mot reçu de manière unique.

On considère un code binaire $(n, M, d)_2$. On suppose qu'on dispose d'un algorithme de décodage qui permet de décoder un mot comportant $e < d/2$ erreurs (mais pas d'effacement), en temps $T(n)$.

3. Montrer qu'on peut décoder un mot comportant e erreurs et s effacements avec $2e + s < d$, en temps $O(T(n))$.

Exercice 4. *Codes de Reed-Solomon*

Soit $\mathcal{C}$ un code de Reed-Solomon sur $\mathbb{F}$, de dimension k et de longueur n, défini par les points d'évaluation $\alpha_1, \dots, \alpha_n$.

1. Montrer que $\mathcal{C}$ est un code linéaire.
2. On veut calculer la distance minimale de $\mathcal{C}$. Soit m_1 et m_2 deux messages, et c_1 et c_2 les mots de code correspondant. On note F_1 et F_2 les polynômes obtenus à partir des deux messages.
   i. Montrer que la distance entre c_1 et c_2 est $n - t$ où $t = \#\{\alpha_i : F_1(\alpha_i) = F_2(\alpha_i)\}$.
   ii. En déduire que la distance minimale est $\geq n - k + 1$.
   iii. Montrer que la distance minimale est $\leq n - k + 1$ en exhibant deux mots de $\mathcal{C}$ à distance $n - k + 1$.
   iv. De quelle autre manière aurait-on pu démontrer que la distance minimale est $\leq n - k + 1$?