TP8 : Codes correcteurs

Exercice 1. CODE DE HAMMING (7,3,1)

Alice veut transmettre à Bob un message $m = (m_1, m_2, m_3, m_4) \in (\mathbb{F}_2)^4$. Elle l'encode via l'application linéaire C définie par

$$\begin{aligned} C(1,0,0,0) &= (1,1,0,1,0,0,0), \\ C(0,1,0,0) &= (0,1,1,0,1,0,0), \\ C(0,0,1,0) &= (0,0,1,1,0,1,0), \\ C(0,0,0,1) &= (0,0,0,1,1,0,1). \end{aligned}$$

1. À l'aide de la fonction `VectorSpace` de `sage`, définir l'espace vectoriel $V4 = (\mathbb{F}_2)^4$ de dimension 4 sur $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. Toujours à l'aide de `sage`, déterminer la liste des éléments de $V4$, son cardinal ainsi que la base canonique.
2. À l'aide de la fonction `matrix` de `sage` définir la matrice de l'application C comme une matrice de taille 7×4 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Déterminer son rang et son noyau. Toujours à l'aide de `sage`, calculer l'image de $(1,1,1,1)$ par C. On rappelle que `V4([1,1,1,1])` permet de définir l'élément $(1,1,1,1)$ de $V4$.
3. Faire la liste des éléments du code, c'est-à-dire de l'image de C.
4. Soit
$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$
Montrer que $\mathrm{Ker}(H) = \mathrm{Im}(C)$. On pourra utiliser la méthode `right_kernel`.
5. Produire dans `sage` la liste de tous les $H.e_i$, où les e_i sont les vecteurs de la base canonique de $(\mathbb{F}_2)^7$.
6. Soit v un mot du code ; on suppose que v devient après transmission un autre mot $w = v + e$, où e a une seule coordonnée non nulle. Calculer Hw. Expliquer comment Bob peut utiliser H pour retrouver v.
7. Ecrire une fonction qui, à partir d'un élément v de $(\mathbb{F}_2)^7$, à distance au plus un d'un élément $w \in \mathrm{Im}(C)$, renvoie le message m tel que $C(m) = w$. On pourra utiliser la méthode `solve_right`.

Exercice 2.

Soit q une puissance d'un nombre premier, et m et e deux entiers tels que $n := m + 2e = q - 1$. Les *codes de Reed-Solomon* sont des sous-espaces de dimension $m + 1$ de $(\mathbb{F}_q)^n$.

Pour les construire, on choisit un élément $\alpha \in \mathbb{F}_q$ non nuls, d'ordre multiplicatif $q - 1$. Supposons qu'Alice veuille transmettre un message $w = (w_0, \ldots, w_m) \in \mathbb{F}_q^{m+1}$. Elle forme le polynôme $W = \sum_{i=0}^{m} w_i x^i \in \mathbb{F}_q[X]$ et transmet à Bob le vecteur $\Phi(w) = (W(1), W(\alpha), \ldots, W(\alpha^{q-2})) \in (\mathbb{F}_q)^n$.

1. Dans cette question on prend $q = 11$ et $m = 2$. Vérifier que $2 \in \mathbb{F}_{11}$ est d'ordre multiplicatif 10. Ecrire une fonction qui prend un argument le nombre q ainsi que le message w, et renvoie le vecteur $\Phi(w) = (W(1), W(2), \ldots, W(2^{10})) \in (\mathbb{F}_{11})^{10}$.

2. Comment vérifier si un mot $f \in (\mathbb{F}_q)^n$ est bien un mot du code ?
3. Expliquer comment, en supposant qu'il n'y a pas d'erreur de transmission, Bob peut retrouver le message w. En supposant $q = 11$ et $m = 2$, écrire une fonction qui prend en argument un vecteur $R \in (\mathbb{F}_{11})^{10}$ et renvoie le message $w \in (\mathbb{F}_{11})^3$ tel que $\Phi(w) = R$, si c'est possible, et une erreur sinon.
4. Toujours pour $q = 11$ et $m = 2$, faire la liste de tous les éléments du code. Vérifier que deux éléments du code sont toujours à distance de Hamming au moins 8, et donc que ce code permet de corriger au minimum 3 erreurs.
5. On prend maintenant $q = 16$ et $e = 3$.
   (a) Trouver un $\alpha \in \mathbb{F}_{16}$ d'ordre multiplicatif égal à 15.
   (b) Calculer la bonne valeur de m. Reprendre les questions 1) à 3) avec le nouveau code obtenu. Vérifier sur des messages aléatoires que le décodage de $\Phi(w)$ renvoie bien w.