Sécurité Appliquée
Codes Correcteurs de Hamming (TP)

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

11 mars 2021

1 Mise en place des algorithmes

Exercice 1.1 (Mise en place du produit matriciel dans $\mathbb{B}$). *Définir une fonction qui prend en paramètre deux matrices booléennes et effectue le produit matriciel de celles-ci, toujours dans $\mathbb{B}$.*

Exercice 1.2 (Génération des matrices H_k et G_k). *Définir une fonction qui prend en paramètres k et qui retourne H_k et G_k, respectivement les matrices de contrôle et de génération pour un code de Hamming systématique.*

Exercice 1.3 (Vérification et correction éventuelle). *Définir la fonction testEtCorrige(w,H) telle que :*
- *w est un vecteur de taille $2^k - 1$, contenant possiblement une erreur,*
- *H est la matrice de contrôle construite à la question précédente*

et qui retourne le mot associé à w, après correction éventuelle d'un bit.

2 Evaluation des codes systématiques

Exercice 2.1 (Vérification de correction). *Pour $k \in \{3, \ldots, 8\}$, vérifier que pour tous les mots de $\mathbb{B}^{2^k-k-1}$ et pour toutes les erreurs possibles sur le mot généré (à la position 1, à la position 2, ..., la position, $2^k - 1$), l'algorithme corrige bien l'erreur.*