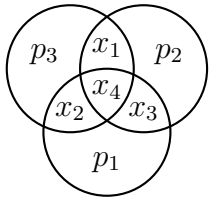
M1MI2016 Codes et Cryptologie

Feuille d'exercices n° 8.

Codes correcteurs : Introduction

On rappelle qu'un message $x = (x_1, x_2, x_3, x_4)$ est encodé par le code de Hamming en $x' = (x_1, x_2, x_3, x_4, p_1, p_2, p_3)$, où p_1, p_2, p_3 sont les bits de parités associés aux cercles de la figure suivante :



1 Vous avez reçu des messages encodés par le code de Hamming. Malheureusement ces messages ont été détériorés.

1. Ils ont été affectés par au plus deux effacements. Corrigez-les.

$$11 * 1111$$
$$000 * *00$$
$$11 * 011*$$
$$0 * 00 * 00$$
$$110 * 1 * 0$$

2. Ils ont été affectés par au plus une erreur. Corrigez-les.

$$1100010$$
$$0011100$$
$$1111110$$
$$0001111$$
$$0000111$$

2 Les messages considérés sont toujours encodés par le code de Hamming, mais trois bits sont effaçés.

1. Pouvez-vous corriger $**0*111$? Et $***1100$? Est-ce que la réponse dépend de la valeur des autres bits ?
2. Montrez dans les deux cas précédents que corriger ces effacements revient à résoudre un système linéaire de trois équations à trois inconnues.
3. En vous appuyant sur les exemples précédents, déterminez quels sont les effacements de trois bits que l'on peut corriger.

3 On transmet des messages binaires par un canal qui envoie chaque bit indépendamment, avec une probabilité d'erreur $p < 0.5$ sur chacun d'entre eux. Les messages sont de longueur n.

1. Quelle est la probabilité qu'un message soit reçu sans erreurs ?
2. Quelle est la probabilité qu'un message soit reçu avec au moins une erreur ?
3. Quelle est la probabilité qu'un message soit reçu avec au plus une erreur ?

Maintenant on veut transmettre des messages de 4 bits mais on veut comparer les deux méthodes suivantes :

(1) On transmet le message x lui-même. On note x^* le message reçu.

(2) On utilise le code de Hamming pour transformer x en x' puis on transmet x' à travers le canal ; on reçoit y', que l'on décode suivant la procédure suivante :
   – Si les trois parités de y' sont correctes, on pose $y^* = y'$.
   – Sinon, on change un bit de y', afin de les rendre correctes (comme vu en cours), et on note y^* le nouveau message.
   – On note x^* le message constitué des quatre premiers bits de y^*.

4. Quelle est la probabilité $P_1(p)$ que $x = x^*$ avec la procédure (1) ?
5. Quelle est la probabilité $P_2(p)$ que $x = x^*$ avec la procédure (2) ?
6. Comparez ces probabilités pour $p = 0.4$, $p = 0.01$.
7. Donnez une expression de $P_1(p)$ et $P_2(p)$, puis montrez que $P_2(p) \geq P_1(p)$ pour tout $p \leq 0.5$. Conclure.

4 Dans cet exercice on considère le code carré vu en cours. On rappelle qu'un message $x = (x_1, x_2, x_3, x_4)$ est encodé en $x' = (x_1, x_2, x_3, x_4, p_1, p_2, p_3, p_4)$ où p_1, p_2, p_3, p_4 sont les parités associées aux lignes et colonnes du schéma :

$$\begin{array}{ccc} x_1 & x_2 & p_1 \\ x_3 & x_4 & p_2 \\ p_3 & p_4 & \end{array}$$

1. Exprimez x' comme le produit de x par une matrice binaire à déterminer.
2. Explicitez une procédure de correction de une erreur par un tableau comme dans le cours pour le code de Hamming.
3. Explicitez cette procédure en terme du produit d'une matrice H, à déterminer, par le mot reçu y.
4. Trouvez un exemple de trois effacements qui sont corrigeables et un exemple de trois effacements qui ne le sont pas.
5. Montrez que trois effacements sur x' sont corrigeables si et seulement si les colonnes de la matrice H associées à ces positions forment une matrice de rang 3. En déduire tous les effacements de trois bits non corrigeables.