T. D. Codes correcteurs d'erreurs.
ESIL. 2ième année
UNIVERSITÉ DE LA MÉDITERRANÉE
Année universitaire 2010/2011

Enseignants : Alexis Bonnecaze
Odile Papini

Feuille de T. D. 1 Corrigée : Codes correcteurs d'erreurs

Exercice 1 : condition de décodage

Soit un code sur l'alphabet $A = \{0, 1\}$ tel que
$C = \{x_1 = (0, 0, 0, 0), x_2 = (1, 0, 1, 1), x_3 = (0, 1, 0, 1), x_4 = (1, 1, 1, 0)\}$.

1) La longueur du code est $n = 4$.

2) La distance minimale du code est $d = 2$ car $d(x_1, x_2) = 3$, $d(x_1, x_3) = 2$, $d(x_1, x_4) = 3$, $d(x_2, x_3) = 3$, $d(x_2, x_4) = 2$, $d(x_3, x_4) = 3$.

3) Le code C ne vérifie pas la condition de décodage d'ordre e, pour $e = 1$. Les boules centrées sur les mots du code de rayon 1 ne sont pas 2 à 2 disjointes.

$B(x_1, 1) = \{(0, 0, 0, 0), (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$
$B(x_2, 1) = \{(1, 0, 1, 1), (0, 0, 1, 1), (1, 1, 1, 1), (1, 0, 0, 1), (1, 0, 1, 0)\}$
$B(x_3, 1) = \{(0, 1, 0, 1), (1, 1, 0, 1), (0, 0, 0, 1), (0, 1, 1, 1), (0, 1, 0, 0)\}$
$B(x_4, 1) = \{(1, 1, 1, 0), (0, 1, 1, 0), (1, 0, 1, 0), (1, 1, 0, 0), (1, 1, 1, 1)\}$

$B(x_1, 1) \cap B(x_2, 1) = \emptyset$, $B(x_1, 1) \cap B(x_4, 1) = \emptyset$, $B(x_2, 1) \cap B(x_3, 1) = \emptyset$, $B(x_3, 1) \cap B(x_4, 1) = \emptyset$ mais $B(x_1, 1) \cap B(x_3, 1) = \{(0, 0, 0, 1), (0, 1, 0, 0)\}$ et $B(x_2, 1) \cap B(x_4, 1) = \{(1, 1, 1, 1), (1, 0, 1, 0)\}$.

Exercice 2 : code correcteur non binaire

Soit un code sur l'alphabet $A = \{0, 1, 2\}$ tel que $C = \{x_1 = (0, 0, 0, 0)$, $x_2 = (1, 2, 1, 2)$, $x_3 = (2, 0, 1, 1)$, $x_4 = (0, 1, 2, 1)\}$.

1) La distance minimale du code est $d = 3$ car $d(x_1, x_2) = 4$, $d(x_1, x_3) = 3$, $d(x_1, x_4) = 3$, $d(x_2, x_3) = 3$, $d(x_2, x_4) = 4$, $d(x_3, x_4) = 3$.

2) La capacité de correction de ce code est $e = \lfloor (d - 1)/2 \rfloor = 1$.

3) Le code C n'est pas parfait. Il vérifie la condition de décodage d'ordre 1 car les boules centrées sur les mots du code de rayon 1 sont 2 à 2 disjointes.

$B(x_1, 1) = \{(0, 0, 0, 0), (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1), (2, 0, 0, 0), (0, 2, 0, 0), (0, 0, 2, 0), (0, 0, 0, 2)\}$.
$B(x_2, 1) = \{(1, 2, 1, 2), (2, 2, 1, 2), (1, 0, 1, 2), (1, 2, 2, 2), (1, 2, 1, 0), (0, 2, 1, 2), (1, 1, 1, 2), (1, 2, 0, 2), (1, 2, 1, 1)\}$.
$B(x_3, 1) = \{(2, 0, 1, 1), (0, 0, 1, 1), (2, 1, 1, 1), (2, 0, 2, 1), (2, 0, 1, 2), (1, 0, 1, 1), (2, 2, 1, 1), (2, 0, 0, 1), (2, 0, 1, 0)\}$.
$B(x_4, 1) = \{(0, 1, 2, 1), (1, 1, 2, 1), (0, 2, 2, 1), (0, 1, 0, 1), (0, 1, 2, 2), (2, 1, 2, 1), (0, 0, 2, 1), (0, 1, 1, 1), (0, 1, 2, 0)\}$.

$B(x_1, 1) \cap B(x_2, 1) = \emptyset$, $B(x_1, 1) \cap B(x_4, 1) = \emptyset$, $B(x_2, 1) \cap B(x_3, 1) = \emptyset$, $B(x_3, 1) \cap B(x_4, 1) = \emptyset$, $B(x_1, 1) \cap B(x_3, 1) = \emptyset$ et $B(x_2, 1) \cap B(x_4, 1) = \emptyset$.

Le code n'est pas parfait car le nombre de mots par boule est $\mid B(x_i, 1) \mid = 9$ et le nombre de mots du code $\mid C \mid = 4$ donc $\mid B(x_i, 1) \mid . \mid C \mid = 36$. Or $\mid A \mid^n = 3^4 = 81$ donc $\Sigma_{x_i \in c} \mid B(x_i, 1) \mid = \mid B(x_i, 1) \mid . \mid C \mid < \mid A \mid^n$.

Exercice 3 : code parfait

Soit un code sur l'alphabet $A = \{0, 1\}$ tel que $C = \{x_1 = (0, 0, 0), x_2 = (1, 1, 1)\}$.

1) La capacité de correction de ce code est $e = 1$ car $d = 3$.

2) Le code C est parfait car les boules centrées sur les mots du code et de rayon 1 sont disjointes et recouvent A^n.

$B(x_1, 1) = \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.
$B(x_2, 1) = \{(1, 1, 1), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$.

$B(x_1, 1) \cap B(x_2, 1) = \emptyset$, les boules sont disjointes et $\Sigma_{x_i \in c} \mid B(x_i, 1) \mid = 8$ et $\mid A \mid^n = 8$ Donc $\Sigma_{x_i \in c} \mid B(x_i, 1) \mid = \mid A \mid^n$.

Exercice 4 (facultatif): distance de Hamming

La distance de Hamming est une distance. Soit A un alphabet, $\forall x, y, z \in A^n$

i) $d(x,y) \in \mathbb{R}^+$;
découle de la définition $d(x,y) = \mid \{i \in \{1, \cdots n\}, x_i \neq y_i\} \mid$.

ii) $d(x,y) = 0$ si et seulement si $x = y$;
si $d(x,y) = 0$ alors $\mid \{i \in \{1, \cdots n\}, x_i \neq y_i\} \mid = 0$ donc $x = y$. Si $= y$ alors $\forall i \in \{1, \cdots n\}, x_i \neq y_i$ donc $d(x,y) = 0$.

iii) $d(x,y) = d(y,x)$;
car $\mid \{i \in \{1, \cdots n\}, x_i \neq y_i\} \mid = \mid \{i \in \{1, \cdots n\}, y_i \neq x_i\} \mid$.

iv) $d(x,y) \leq d(x,z) + d(z,y)$.

Cette propriété peut être montrée par récurrence sur n, dans ce cas pour $n = 2$ il y a 5 cas à examiner cas $1 : x = y = z$, cas $2 : x = y$ et $x \neq z$, cas $3 : x \neq y$ et $x = z$, cas $4 : x \neq y$ et $y = z$, cas $5 : x \neq y \neq z$.

Bien plus élégante est la démonstration qui utilise le fait que $d(x,y) = \Sigma_{i=1}^{n} d_i(x_i, y_i)$ où $d_i(x_i, y_i) = 0$ si $x_i = y_i$ et $d_i(x_i, y_i) = 1$ si $x_i \neq y_i$.

$d(x,y) \leq d(x,z) + d(z,y)$ ssi $\Sigma_{i=1}^{n} d_i(x_i, y_i) \leq \Sigma_{i=1}^{n} d_i(x_i, z_i) + d_i(z_i, y_i)$.
On se ramène à montrer que $d_i(x_i, y_i) \leq d_i(x_i, z_i) + d_i(z_i, y_i)$.

si $x_i = y_i$ alors $d_i(x_i, y_i) = 0$,
si $x_i = z_i$ alors $d_i(x_i, z_i) = d_i(z_i, y_i) = 0$,
sinon $(x_i \neq z_i)$ $d_i(x_i, z_i) = 1$ et $d_i(z_i, y_i) = 1$ donc $d_i(x_i, y_i) \leq d_i(x_i, z_i) + d_i(z_i, y_i)$.

si $x_i \neq y_i$ alors $d_i(x_i, y_i) = 1$,
si $x_i = z_i$ alors $d_i(x_i, z_i) = 0$ et $d_i(z_i, y_i) = 1$ donc $d_i(x_i, y_i) \leq d_i(x_i, z_i) + d_i(z_i, y_i)$.
sinon $(x_i \neq z_i)$ et $d_i(x_i, z_i) = 1$ et quelque soit la valeur de $d_i(z_i, y_i)$ on a $d_i(x_i, y_i) \leq d_i(x_i, z_i) + d_i(z_i, y_i)$.