Codes détecteurs et correcteurs

Question préliminaire

1. Soient a et b deux nombres entiers.
Montrer que le nombre $a+b$ est pair si, et seulement si, a et b sont de la même parité.

Par disjonction de cas :

- Si a et b sont pairs tous les deux :
  Il existe deux entiers n et p tels que $a = 2n$ et $b = 2p$.
  On a donc : $a + b = 2(n + p)$, donc $a + b$ est pair.
- Si a et b sont impairs tous les deux :
  Il existe deux entiers n et p tels que $a = 2n + 1$ et $b = 2p + 1$.
  On a donc : $a + b = 2(n + p) + 2 = 2(n + p + 1)$, donc $a + b$ est pair.
- Si a et b sont de parités différentes :
  Considérons par exemple le cas a pair et b impair : Il existe deux entiers n et p tels que $a = 2n$ et $b = 2p + 1$.
  On a donc : $a + b = 2(n + p) + 1$, donc $a + b$ est impair.

Ainsi $a + b$ est pair si, et seulement si, a et b sont de même parité.

Codage d'un message

Un message est ici un nombre M codé sous la forme d'un quadruplet (x_1, x_2, x_3, x_4) où x_1, x_2, x_3 et x_4 sont des « bits », c'est-à-dire des nombres ne pouvant valoir que 0 ou 1. Le nombre M que représente le quadruplet (x_1, x_2, x_3, x_4), appelé aussi demi-octet d'information, vaut par définition :

$$M = x_1 + 2 \times x_2 + 4 \times x_3 + 8 \times x_4.$$

Par exemple, le code $(0, 0, 1, 1)$ représente le nombre $M = 12$ puisque $12 = 0 + 2 \times 0 + 4 \times 1 + 8 \times 1$.

2.

a. Quel est le message M que code le quadruplet $(1, 0, 0, 1)$?
Le quadruplet $(1, 0, 0, 1)$ code le message $M = 1 + 2 \times 0 + 4 \times 0 + 8 \times 1 = 9$

b. Trouver un code qui représente $M = 10$. Trouver un code qui représente $M = 15$.
$10 = 2 + 8 = 0 + 2 \times 1 + 4 \times 0 + 8 \times 1$. Le quadruplet $(0, 1, 0, 1)$ représente $M = 10$.
$15 = 1 + 2 + 4 + 8 = 1 + 2 \times 1 + 4 \times 1 + 8 \times 1$. Le quadruplet $(1, 1, 1, 1)$ représente $M = 15$.

c. Peut-on trouver un code pour représenter $M = 20$? Le plus grand nombre que l'on peut représenter avec 4 un quadruplet est $1 + 2 \times 1 + 4 \times 1 + 8 \times 1 = 15$. On ne peut pas représenter $M = 20$.

d. Quels sont les différents messages possibles ?
Il y a 16 messages possibles : les 16 entiers de 0 à 15.

Un message est parfois altéré (on dit aussi « corrompu ») lors de sa transmission du fait d'un matériel défectueux ou de signaux parasites. Des erreurs modifient des bits, un 0 se transformant en 1 ou un 1 se transformant en 0. Aussi des techniques permettant de détecter et de corriger ces anomalies ont-elles été mises au point. Ceci fait l'objet de la suite.

Codage d'un message avec protection contre les erreurs

3. Principe du bit de parité
Le code (x_1, x_2, x_3, x_4) est transformé en le quintuplet (x_1, x_2, x_3, x_4, y), dont le dernier bit y, dit de parité, vaut 0 si la somme $x_1 + x_2 + x_3 + x_4$ est paire, et 1 si elle est impaire. C'est ce quintuplet qui est transmis, il

représente le même message M que le code (x_1, x_2, x_3, x_4), à savoir $M = x_1 + 2 \times x_2 + 4 \times x_3 + 8 \times x_4$. Les bits dits d'information demeurent x_1, x_2, x_3, x_4 et le bit de parité, y, est transmis avec les plus grandes précautions.

Par exemple, pour transmettre le nombre $M = 12$ correspondant à $x_1 = 0, x_2 = 0, x_3 = 1$ et $x_4 = 1$, on calcule d'abord $x_1 + x_2 + x_3 + x_4 = 2$, qui est pair ; on pose donc $y = 0$ et on émet le quintuplet $(0, 0, 1, 1, 0)$.

4. Principe des bits de contrôle

Le code (x_1, x_2, x_3, x_4) est transformé en l'heptuplet $(x_1, x_2, x_3, x_4, y_1, y_2, y_3)$, où $y_1 = 0$ si $x_1 + x_2 + x_3$ est pair, $y_1 = 1$ sinon ; $y_2 = 0$ si $x_2 + x_3 + x_4$ est pair, $y_2 = 1$ sinon ; $y_3 = 0$ si $x_1 + x_3 + x_4$ est pair, $y_3 = 1$ sinon. Les bits dits d'information demeurent x_1, x_2, x_3, x_4.
L'heptuplet $(x_1, x_2, x_3, x_4, y_1, y_2, y_3)$ code toujours le message $M = x_1 + 2 \times x_2 + 4 \times x_3 + 8 \times x_4$.

a. Quels sont les bits y_1, y_2, y_3, dits de contrôle, associés au quadruplet $(1, 0, 0, 1)$ codant le nombre $M = 9$?
On a :

- $x_1 + x_2 + x_3 = 1 + 0 + 0 = 1$, donc $y_1 = 1$.
- $x_2 + x_3 + x_4 = 0 + 0 + 1 = 1$, donc $y_2 = 1$.
- $x_1 + x_3 + x_4 = 1 + 0 + 1 = 2$, donc $y_3 = 0$.

b. Pourquoi est-on certain que l'heptuplet reçu $(1, 1, 0, 1, 0, 0, 1)$ résulte d'une altération de transmission dans le cas où on est sûr des bits de contrôle ?
Ici $x_1 + x_3 + x_4 = 1 + 0 + 1 = 2$, donc y_3 devrait être égal à 0. Ce n'est pas le cas dans le triplet transmis.

c. Si on est sûr de la justesse des bits de contrôle, dans l'hypothèse où exactement un des quatre bits d'information est erroné, pourquoi peut-on détecter qu'il y a eu une altération et pourquoi peut-on la localiser (et donc la corriger) ? Peut-on détecter l'erreur quand exactement deux des quatre bits d'information sont erronés ?
Dans le cas où exactement un des quatre bits d'information est erroné :

- Si x_1 est erroné, alors y_1 et y_3 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_2 est erroné, alors y_1 et y_2 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_3 est erroné, alors y_1, y_2 et y_3 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_4 est erroné, alors y_2 et y_3 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).

On peut donc localiser l'erreur à partir du calcul de y_1, y_2 et y_3.

Dans le cas où exactement deux des quatre bits d'information sont erronés :

- Si x_1 et x_2 sont erronés, alors y_2 et y_3 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_1 et x_3 sont erronés, alors y_2 ne correspondra pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_1 et x_4 sont erronés, alors y_1 et y_2 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_2 et x_3 sont erronés, alors y_3 ne correspondra pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_2 et x_4 sont erronés, alors y_1 et y_3 ne correspondront pas au quadruplet (x_1, x_2, x_3, x_4).
- Si x_3 et x_4 sont erronés, alors y_1 ne correspondra pas au quadruplet (x_1, x_2, x_3, x_4).

On peut donc localiser l'erreur à partir du calcul de y_1, y_2 et y_3.