Téléinformatique & Protocoles
TD7 : Codes d'erreur

Corrigé

Janvier 1991

1. Ce code est linéaire parce que tous les mots de code s'obtiennent par combinaison linéaire des bits de données. Le mot de code est représenté par le vecteur ligne $[I]$ et le mot de code par le vecteur ligne $[C]$:

$$\begin{aligned} [I] &= (i_1, i_2, i_3, i_4, i_5, i_6, i_7) \\ [C] &= (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \end{aligned}$$

   où :

$$\begin{aligned} &c_1 = i_1 \\ &c_2 = i_2 \\ &c_3 = i_3 \\ &c_4 = i_4 \\ &c_5 = i_5 \\ &c_6 = i_6 \\ &c_7 = i_7 \\ &c_8 = i_1 + i_2 + i_3 + i_4 + i_5 + i_6 + i_7 \end{aligned}$$

   Dans ce cas, la matrice génératrice G vérifie :

$$[C] = [I][G]$$

   avec

$$G = \begin{pmatrix} 1 & & & & & & & 1 \\ & 1 & & & & & & 1 \\ & & 1 & & & & & 1 \\ & & & 1 & & & & 1 \\ & & & & 1 & & & 1 \\ & & & & & 1 & & 1 \\ & & & & & & 1 & 1 \end{pmatrix}$$

   Sa matrice génératrice do Ce code est-il un code linéaire ? Si oui donner sa matrice génératrice son poids minimal et en déduire ses capacités de détection et de correction d'erreur.
   Lorsqu'on change un bit dans $[I]$, alors deux bits changent dans $[C]$. Donc le poids minimal est de 2. (Somme des éléments d'une ligne).
   Par conséquent ce code peut détecter une erreur par mot de code et ne peut en corriger aucune.
2. Le code de parité impaire n'est pas linéaire car le mot 0 n'appartient pas au code. Les mots de code ne sont pas obtenus par combinaison linéaire des mots d'information.
3. $p(1)$ est toujours la somme des coefficients du polynôme $p(X)$. $p(1) = 0$ équivaut à ce que la somme des coefficients de $p(X)$ soit nulle et équivaut aussi à ce que $p(X)$ puisse s'exprimer sous la forme $p(X) = (1 + X)q(X)$. (CQFD)

4. D'après la question précédente, si la somme des digits d'un mot est nulle alors forcément ce mot est divisible par $1 + X$. Donc la parité paire est polynomiale est son polynôme générateur est $1 + X$.
5. Les codes polynomiaux sont forcément linéaires (? ? ? ? ? ? ?) Le code à parité impaire n'est pas linéaire donc il ne peut pas être polynomial.

Janvier 1995

1. Montrer que $e(X)$ est détectable par C si et seulement si $g(X)$ ne divise pas $e(X)$.
   Je croyais que c'était la définition des codes polynomiaux. ...
2. La valeur du bit de poids faible d'un mot de C' est toujours 0 puisque les mots de C' sont les multiples de $Xg(X)$ donc de X. La distance entre deux mots de C est la même qu'entre deux mots de C' donc les pouvoirs détecteurs et correcteurs de C' sont les mêmes que ceux de C. Conclusion : Ca ne sert à rien d'avoir un polynôme générateur qui soit divisible par X (? ? ? ? ? ? ?)
3. $X^iP(X) = g(X)Q_1(X)$ Donc le polynôme $g(X)Q_1(X)$ a aussi 0 comme racine d'ordre i. Or $g(X)$ n'a pas de racine nulle donc c'est $Q_1(X)$ qui a les i racines nulles. Autrement dit, $Q_1(X) = X^iQ_2(X)$. $X^iP(X) = X^iQ_2(X)g(X)$. Donc $P(X) = Q_2(X)g(X)$.
4. La différence $\Delta(X)$ entre deux mots de C est toujours un polynôme multiple de $g(X)$. Autrement dit $\Delta(X) = g(X)Q(X)$.
   - Pour que C détecte une erreur, il faut et il suffit que la distance minimale entre deux mots distincts de C soit de 2. Autrement dit, il faut et il suffit donc qu'au moins deux des coefficients de $g(X)Q(X)$ soient non-nuls. Pour cela, il faut et il suffit que $g(X)Q(X) \neq 0$ et $g(X)Q(X) \neq X^i$ (avec $i \in [0, n]$) Or $g(X)Q(X) \neq 0$ puisque les deux mots de codes sont distincts et $g(X)Q(X) \neq X^i$ puisque $g(X)$ ne divise pas X^i.
     Donc la seule condition sur $g(X)$ est qu'il ne soit pas divisible par X et qu'il soit différent de $X^0 = 1$.
   - Pour que C détecte deux erreurs, il faut et il suffit que la distance minimale entre deux mots distincts de C soit de 3. Pour cela, il faut et il suffit que $g(X)Q(X) \neq 0$, que $g(X)Q(X) \neq X^i$ et enfin que $g(X)Q(X) \neq X^i + X^j$. Les deux premières conditions sont celles de la question précédente. La troisième condition est équivalente à : $g(X)Q(X) \neq 1 + X^j$ et $g(X)Q(X) \neq X^i(1 + X^j)$
     Donc $g(X)$ ne doit pas être divisible par X^i ni par $1 + X^i$ (? ? ? ? ? ? ? ?)

   On dit qu'un code détecte des paquets d'erreurs de longueur p si et seulement si toute configuration d'erreurs portant sur p bits consécutifs est détectable. Par exemple des erreurs sur les bits 2 et 4 forment un paquet d'erreur de longueur 3.
5. Donner une condition nécessaire et suffisante sur $g(X)$ pour que C détecte les paquets d'erreur de longueur 2, et plus généralement de longueur p.
6. Quelles sont les capacités de détection d'erreurs indépendantes et de paquets d'erreur du code de longueur 12 engendré par $g(X) = X^2 + X + 1$.