9 Code de Hamming

Les codes de Hamming datent de 1950, ils forment une famille de codes simples et néanmoins toujours suffisants pour certaines applications telles que les mémoires RAM ECC [1].

Comme tout code bloc linéaire binaire, à une séquence de longueur k, un code de Hamming associe un mot de code de longueur $n > k$ qui comprend $m = n - k$ 'bits' de redondance. Pour un code de Hamming :

$$\begin{aligned} n &= 2^m - 1 \\ k &= 2^m - m - 1 \end{aligned}$$

1. Quel est le rendement du code de Hamming ?
2. Pour $k = 4$, on a $n = 7$ et la matrice génératrice de code Hamming $(7, 4)$ est donnée par :

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}_{4,7}$$

   (a) Le code défini par $\mathbf{G}$ est-il sous forme systématique ?
   (b) Donner sa matrice de contrôle de parité.
3. Quels sont les mots du code ?
4. Quelle est la distance minimale de ce code ?
5. Quelle est sa capacité de détection, quelle est sa capacité de correction ?
6. En supposant qu'un mot de code subit une unique erreur, comment trouver la position de cette erreur et comment la corriger ?

---

1. Dans ce contexte, on utilise plutôt un code de Hamming étendu doté d'un bit de parité supplémentaire et d'une distance minimale 4, permettant 1 correction et 2 détections.

$$\mathbf{H} = \left(\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right)_{4,8} \text{ et } \mathbf{G} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)_{4,8}.$$