# Sécurité Appliquée : Codes de Hamming, TD

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

## 1 Application d'un code systématique de Hamming

**Exercice 1.1 (Application directe d'un code systématique de Hamming.).** *1. On considère le code systématique de Hamming dont les deux matrices $G_k$ et $H_k$ sont les suivantes :*

$$G_k = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\ 0&1&0&0&0&0&0&0&0&0&0&1&1&0&0\\ 0&0&1&0&0&0&0&0&0&0&0&1&0&1&1\\ 0&0&0&1&0&0&0&0&0&0&0&0&1&1&1\\ 0&0&0&0&1&0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&1&0&0&0&0&0&1&1&0&1\\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&0\\ 0&0&0&0&0&0&0&0&1&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1&0 \end{pmatrix} \quad H_k = \begin{pmatrix} 0&1&1&0\\ 1&1&0&0\\ 1&0&1&1\\ 0&1&1&1\\ 1&0&0&1\\ 1&1&0&1\\ 0&1&0&1\\ 1&0&1&0\\ 1&1&1&1\\ 0&0&1&1\\ 1&1&1&0\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}$$

*(a) Quelle est la valeur de $k$ ?*

*(b) Parmi la liste de mots suivants lesquels peuvent être encodés ? Lesquels ont la dimension pour être des mots de code ? Lesquels ne sont ni l'un, ni l'autre ?*

*i.* $(1,0,0,0,0,0,0,0,0,0,1,0)$.

*ii.* $(1,0,0,0,0,0,0,0,0,0,1,0,1,0,1,0)$.

*iii.* $(1,0,0,0)$.

2. *Construire le mot de code associé à* $(1,0,0,0,0,0,0,0,0,0,0,1)$.
3. *Vous recevez le vecteur* $w_1 = (1,1,1,0,0,0,0,0,0,0,0,0,0,0,1)$.
   *(a) Calculer son syndrome.*
   *(b) Quel mot a été encodé ?*
4. *Mêmes questions avec* $w_2 = (0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1)$.

## 2 Taux d'erreurs

**Exercice 2.1 (Probabilités, extrait de [1]).** *On considère la probabilité $p = 10^{-3}$ qu'un bit soit inversé lors d'une transmission.*

1. *Quelle est la probabilité d'avoir exactement deux bits erronés lors de la transmission de sept bits, (comme lors de la transmission d'un mot du code de Hamming$(7,4)$) ?*
2. *Quelle est la probabilité d'avoir plus d'une erreur lors de la transmission de sept bits ? Est-il alors sensé d'utiliser le code de Hamming$(7,4)$ ? Quelle est la probabilité $P_{H_74}$ que le code de Hamming décode correctement le message initial ?*
3. *Plutôt que d'exploiter le code de Hamming$(7,4)$, on transmet un bit en le répétant trois fois. On décode à la majorité. Calculer la probabilité qu'on décode correctement le bit envoyé.*
4. *On transmet quatre bits en répétant chacun trois fois. Quelle est la probabilité $P_{\times 3}$ que les quatre bits soient décodés correctement ?*
5. *Comparer les résultats de la question précédente avec ceux de la question 2. Et en terme de rendement ?*

# 3 Rendement

**Exercice 3.1 (Rendement compatible avec le taux d'erreur).** *On désire utiliser le code de Hamming* $(2^k - 1, 2^k - k - 1)$ *pour un certain* $k$*. On voudrait que le rendement soit supérieur à* $\frac{1}{1.05}$.

1. *Trouver la plus petite valeur de* $k$ *qui permet d'assurer ceci. On pourra exploiter la courbe représentative de la fonction* $x \mapsto 0.05 \times 2^x - 1.05x - 0.05$ *représentée à la figure 1.*
2. *Quel est le taux de correction d'une telle instance ? Est-ce compatible avec les valeurs de l'exercice précédent ?*

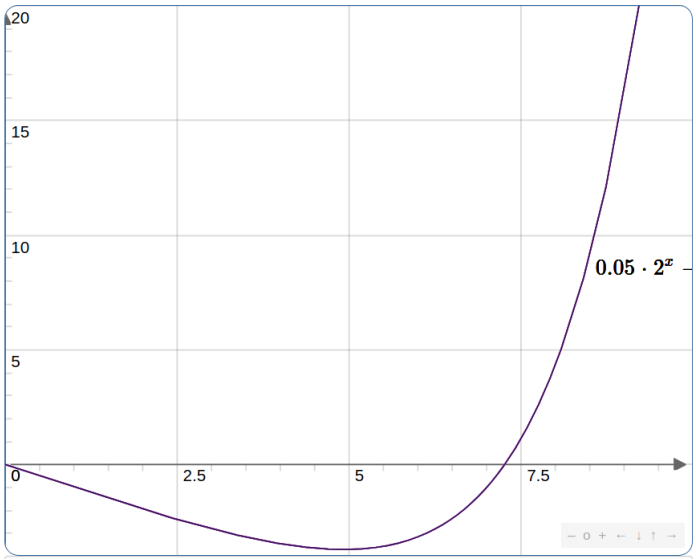


FIGURE 1 – Courbe réprésentative de $x \mapsto 0.05 \times 2^x - 1.05x - 0.05$