Notions de code

Table des matières

Exemple : signaux de télévision numérique MPEG

Tension	Niveau quantifié	Équivalent binaire
-0,5 $[V]$	16	00010000
0 $[V]$	128	10000000
+0,5 $[V]$	240	11110000

TABLE 6: Liens entre 3 valeurs analogiques de chrominance et les niveaux quantifiés.

Chaque ligne active de la composante de luminance est encadrée d'un délimiteur qui comporte un octet XY tel que

$$X = (1, F, V, H)$$

$Y = P_1 P_2 P_3 P_4$ est défini comme suit

$$\begin{aligned} P_1 &= V \oplus F \oplus H \\ P_2 &= V \oplus F \\ P_3 &= F \oplus H \\ P_4 &= V \oplus H \end{aligned}$$

où le OU exclusif (XOR), noté $\oplus$, correspond à une addition modulo 2, comme indiqué dans la table ci-après :

V	H	$P_4 = V \oplus H$
0	0	0
0	1	1
1	0	1
1	1	0

Terminologie

- Mot message $m = (F, V, H)$, de longueur $k = 3$ bits
- Mot parité $p = (P_1, P_2, P_3, P_4)$, de longueur $r = 4$ bits
- Message+parité = mot de code par blocs ou mot codé par bloc $c = (P_1, P_2, P_3, P_4 \,|\, F, V, H)$, de longueur $n = 7$ bits.

Modèle

Modèle de canal

Définition 36. *Un canal discret sans mémoire est caractérisé par un alphabet d'entrée, un alphabet de sortie et un jeu de probabilités conditionnelles, $p(j|i)$, où $1 \leq i \leq M$ représente l'indice du caractère d'entrée, $1 \leq j \leq Q$ représente l'indice du caractère de sortie, et $p(j|i)$ la probabilité d'avoir j en réception alors que i a été émis.*

$$\begin{aligned} p(0|1) &= p(1|0) = p \\ p(1|1) &= p(0|0) = 1-p \end{aligned}$$

Probabilité d'erreur P_e vaut

$$P_e = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{229}$$

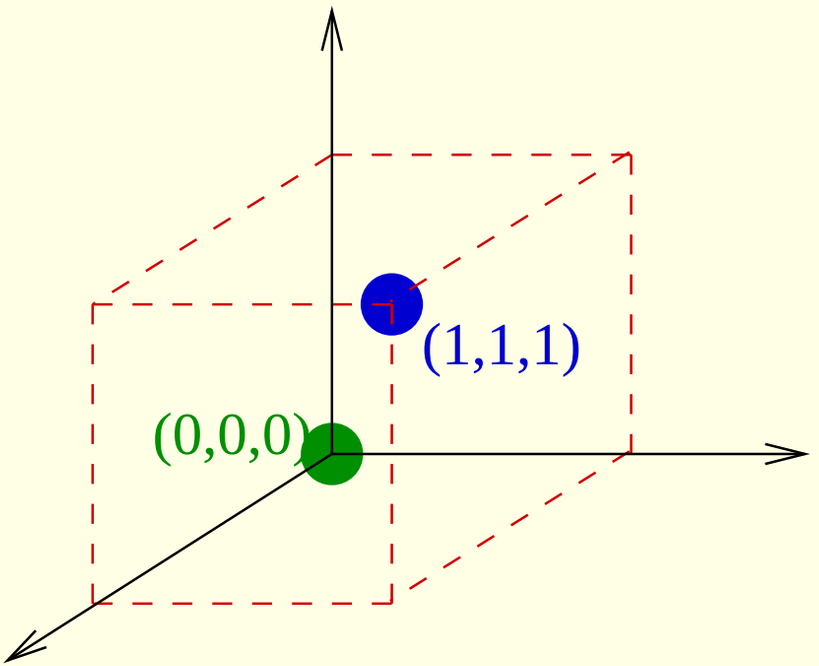
Définition 37. *Le taux de redondance d'un code est défini par le rapport*

$$\frac{n-k}{n} \tag{230}$$

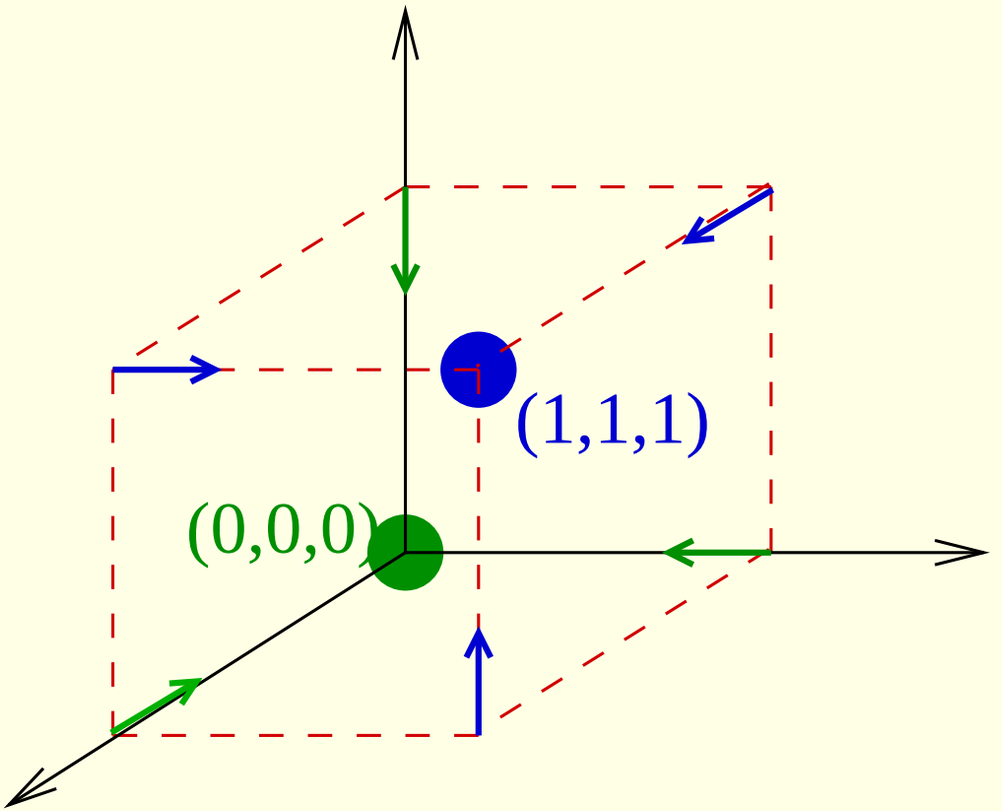
Exemple de code redondant

devient

0	$\longrightarrow$	000
1	$\longrightarrow$	111
Espace 1-D		Espace 3-D



Correction par vote majoritaire



OK pour une erreur simple

Pas OK pour des erreurs doubles ou triples

Codes linéaires

Dans le cas du code utilisé pour MPEG

$$
\begin{aligned}
c_1 &= \alpha_{11} m_1 \oplus \alpha_{21} m_2 \oplus \alpha_{31} m_3 \\
c_2 &= \alpha_{12} m_1 \oplus \alpha_{22} m_2 \oplus \alpha_{32} m_3 \\
c_3 &= \alpha_{13} m_1 \oplus \alpha_{23} m_2 \oplus \alpha_{33} m_3 \\
c_4 &= \alpha_{14} m_1 \oplus \alpha_{24} m_2 \oplus \alpha_{34} m_3 \\
c_5 &= m_1 \\
c_6 &= m_2 \\
c_7 &= m_3
\end{aligned}
$$

Notations

- Message de départ $\overrightarrow{m} = (m_1, m_2, \ldots, m_k)$
- Vecteur de parité $\overrightarrow{p} = (p_1, p_2, \ldots, p_r)$
- Mot codé $\overrightarrow{c} = (c_1, c_2, \ldots, c_n)$

Matrice génératrice

$$\vec{c} = \vec{m}G \tag{231}$$

La matrice G est appelée matrice génératrice. Elle a pour expression générale

$$G = \begin{bmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \cdots \\ \vec{v}_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & & & \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix} \tag{232}$$

Dans le cas des signaux MPEG, la matrice génératrice se ramène à

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{233}$$

Codes à parité

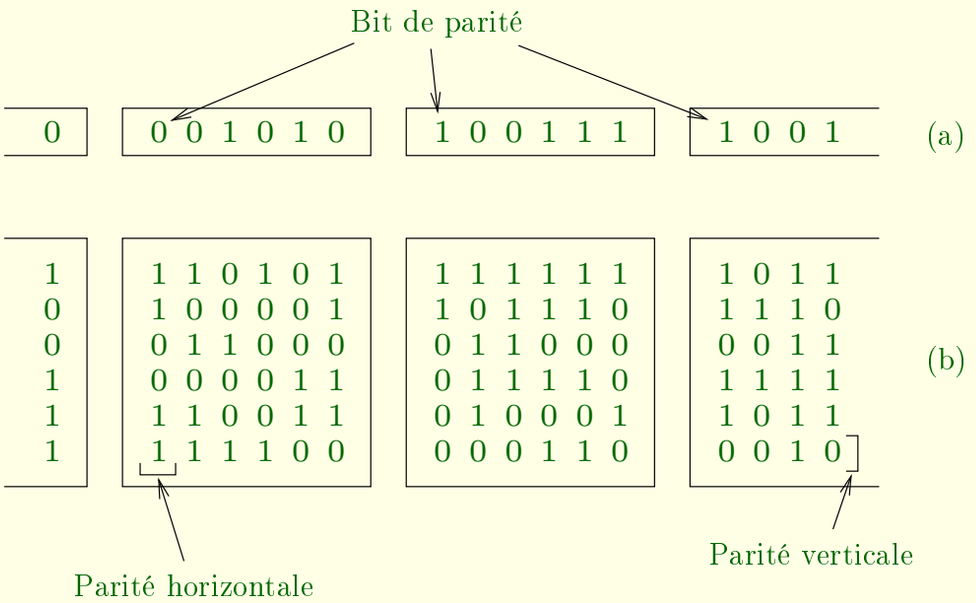


FIGURE 62: Codes de parité paire pour (a) connexion série ou (b) parallèle.

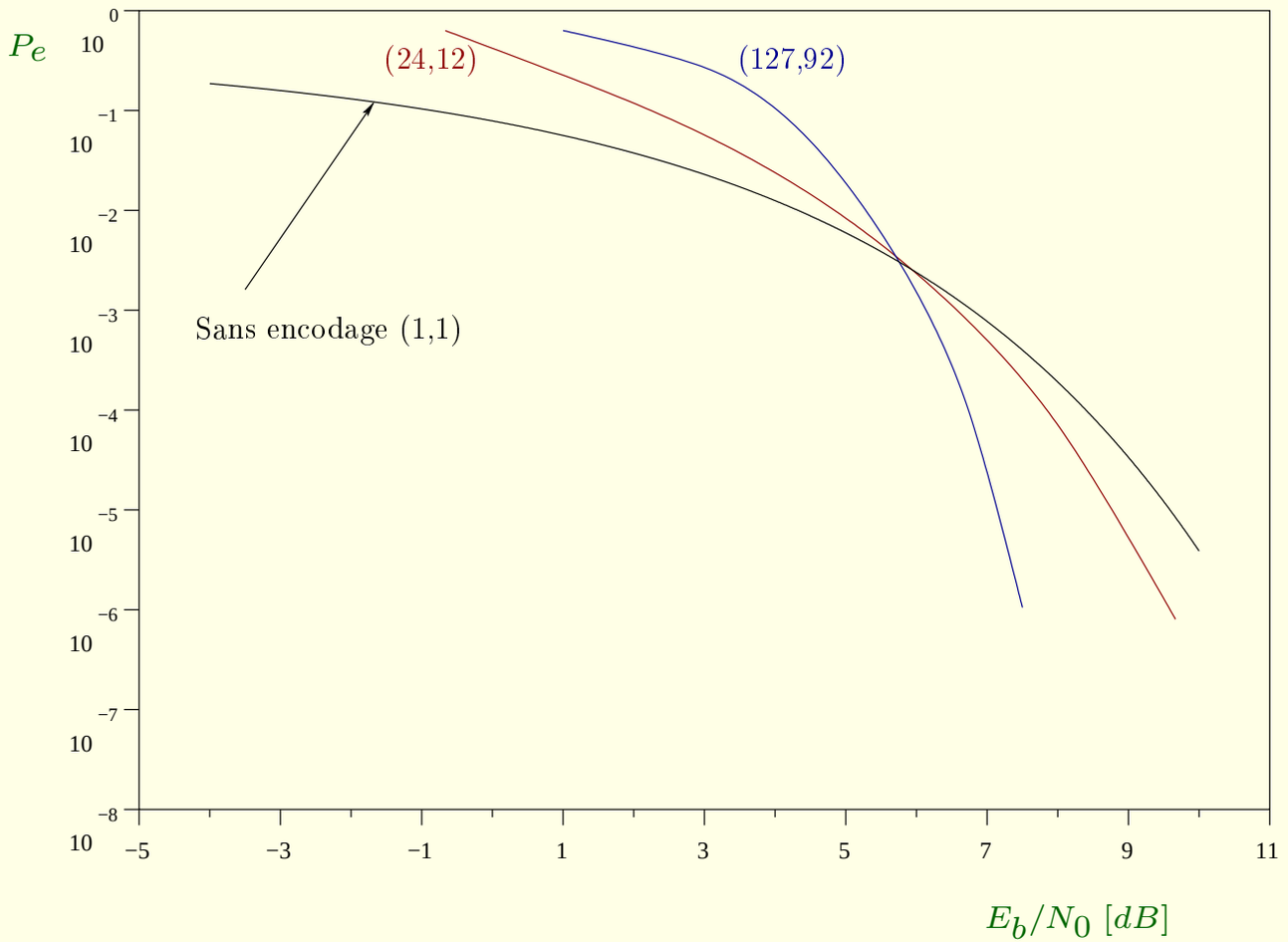


FIGURE 63: Performance d'une détection PSK après codage.

En-tête du protocole IP : IP header

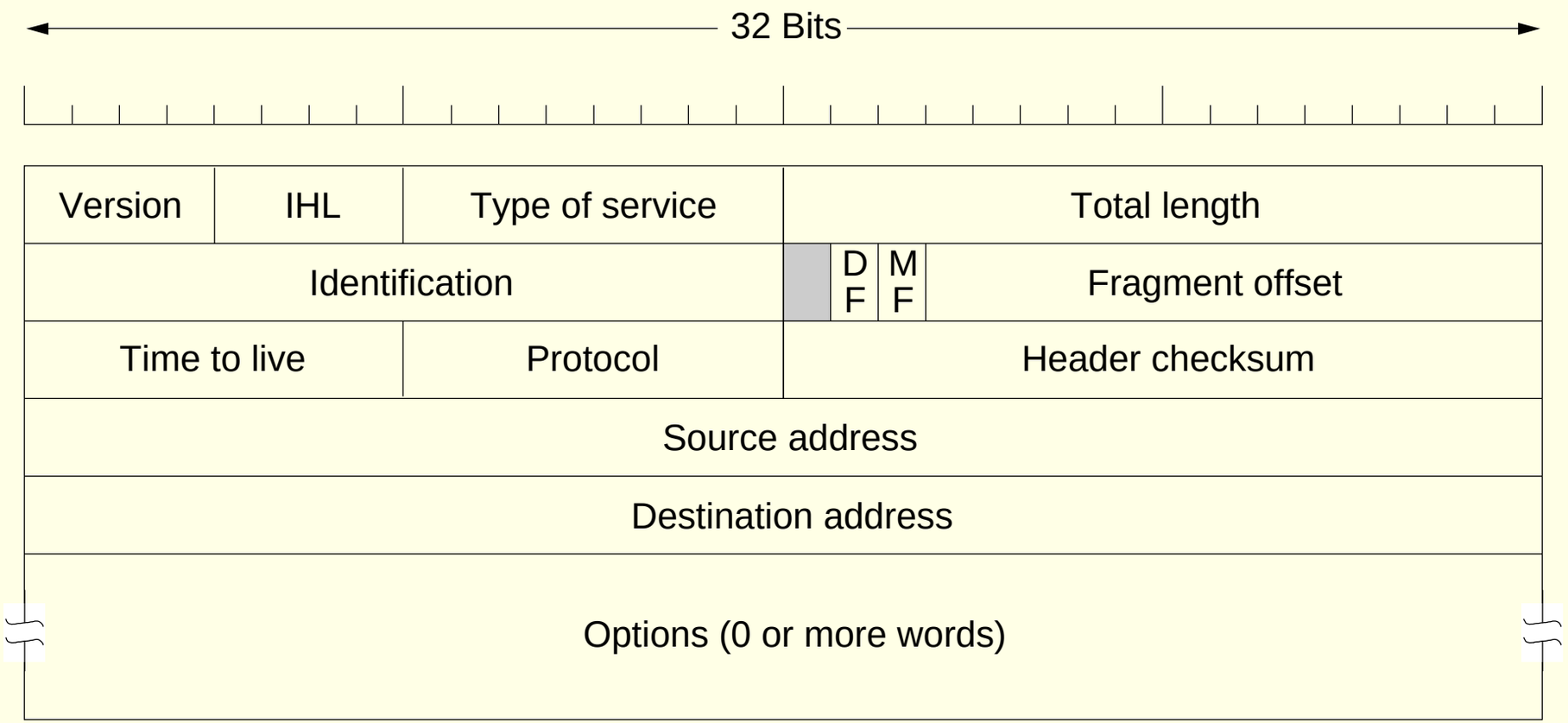


FIGURE 64: En-tête du protocole IP.

Code systématique

Définition 38. *Un code est dit systématique si une partie du mot codé coïncide avec le message.*

$$G = [P \,|\, I_k] \tag{234}$$

$$= \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1(n-k)} & 1 & 0 & \ldots & 0 \\ p_{21} & p_{22} & \cdots & p_{2(n-k)} & 0 & 1 & \ldots & 0 \\ \vdots & & & & & & \vdots & 0 \\ p_{k1} & p_{k2} & \cdots & p_{k(n-k)} & 0 & 0 & \ldots & 1 \end{bmatrix}$$

Et donc

$$\vec{c} = (m_1, m_2, ..., m_k)$$

$$\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1(n-k)} & 1 & 0 & \ldots & 0 \\ p_{21} & p_{22} & \cdots & p_{2(n-k)} & 0 & 1 & \ldots & 0 \\ \vdots & & & & & & \vdots & 0 \\ p_{k1} & p_{k2} & \cdots & p_{k(n-k)} & 0 & 0 & \ldots & 1 \end{bmatrix}$$

Matrice de contrôle de parité

$$GH^T = \underline{0} \tag{235}$$

$$H^T = \left[\frac{I_{n-k}}{P} \right] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & 1 \\ p_{11} & p_{12} & \cdots & p_{1(n-k)} \\ p_{21} & p_{22} & \cdots & p_{2(n-k)} \\ \vdots & & & \\ p_{k1} & p_{k2} & \cdots & p_{k(n-k)} \end{bmatrix}$$

On vérifie que tout produit $\overrightarrow{c}H^T$ pour tout $\overrightarrow{m}$ généré au moyen de la matrice génératrice G fournit un vecteur nul :

$$\overrightarrow{c}H^T = (p_1 + p_1,\ p_2 + p_2,\ \dots,\ p_{n-k} + p_{n-k}) = 0 \tag{236}$$

À la réception

Vecteur à la réception

$$\vec{r} = \vec{c} + \vec{e} \tag{237}$$

Définition 39. *Le vecteur $\vec{s} = \vec{r} H^T$ est appelé vecteur syndrome d'erreur ou plus simplement syndrome.*

$$\vec{s} = \vec{r} H^T \tag{238}$$

En développant l'expression du syndrome,

$$\begin{aligned} \vec{s} &= (\vec{c} + \vec{e})\, H^T && (239)\\ &= \vec{c} H^T + \vec{e} H^T && (240)\\ &= \vec{e} H^T && (241) \end{aligned}$$

Correction d'erreur

$$
\begin{array}{cccc}
 & \overrightarrow{c}_1 & \ldots & \overrightarrow{c}_{2^k} \\
\overrightarrow{e}_1 & \overrightarrow{c}_1 + \overrightarrow{e}_1 & \ldots & \overrightarrow{c}_{2^k} + \overrightarrow{e}_1 \\
\overrightarrow{e}_2 & \overrightarrow{c}_1 + \overrightarrow{e}_2 & \ldots & \overrightarrow{c}_{2^k} + \overrightarrow{e}_2 \\
\vdots & \vdots & & \vdots \\
\overrightarrow{e}_j & \overrightarrow{c}_1 + \overrightarrow{e}_j & \ldots & \overrightarrow{c}_{2^k} + \overrightarrow{e}_j \\
\vdots & \vdots & & \vdots \\
\overrightarrow{e}_{2^{n-k}} & \overrightarrow{c}_1 + \overrightarrow{e}_{2^{n-k}} & \ldots & \overrightarrow{c}_{2^k} + \overrightarrow{e}_{2^{n-k}}
\end{array}
$$

Algorithme de correction d'erreur suivant :

1. Calcul du syndrome $\overrightarrow{s} = \overrightarrow{r} H^T$ sur base du signal reçu.
2. Détermination du vecteur d'erreur $\overrightarrow{e}_j$ correspondant.
3. Estimation du mot codé réel au moyen de $\overrightarrow{c} = \overrightarrow{r} \oplus \overrightarrow{e}_j$.

Efficacité du codage ?

Distance et poids de Hamming

Définition 40. *Le poids de* HAMMING $w(\overrightarrow{c})$ *du vecteur* $\overrightarrow{c}$ *est le nombre de* 1 *qu'il contient.*

Définition 41. *Soient deux vecteurs binaires* $\overrightarrow{c}_1$, $\overrightarrow{c}_2$, *la distance de* HAMMING $d(\overrightarrow{c}_1, \overrightarrow{c}_2)$ *est le nombre de bits qui diffèrent.*

Capacité de correction

Détection, correction d'erreurs et distance minimale

On choisit le vecteur $\overrightarrow{c}_i$ qui vérifie la relation

$$p(\overrightarrow{r}|\overrightarrow{c}_i) = \max_{\overrightarrow{c}_j} p(\overrightarrow{r}|\overrightarrow{c}_j) \tag{242}$$

Dans le cas le plus simple, le vecteur $\overrightarrow{c}_i$ est choisi tel que

$$d(\overrightarrow{r}, \overrightarrow{c}_i) = \min_{\overrightarrow{c}_j} d(\overrightarrow{r}, \overrightarrow{c}_j) \tag{243}$$

Définition 42. *Capacité de correction (=nombre maximum de bits que l'on peut corriger) :*

$$t = \mathit{arrondi\_}\frac{d_{\min} - 1}{2} \tag{244}$$

Codes cycliques

$\overrightarrow{c}$	$\overrightarrow{p}$				$\overrightarrow{m}$		
0	0	0	0	0	0	0	0
1	1	1	0	1	0	0	1
2	0	1	1	1	0	1	0
3	1	0	1	0	0	1	1
4	1	1	1	0	1	0	0
5	0	0	1	1	1	0	1
6	1	0	0	1	1	1	0
7	0	1	0	0	1	1	1

TABLE 7: Éléments d'un code linéaire $(7, 3)$.

Définition 43. *D'une manière générale, on appelle code cyclique un code linéaire (n, k) tel que toute permutation cyclique des bits sur un mot codé génère un autre mot codé.*

Autres codes

Codes de Hamming

Les codes de HAMMING constituent un sous-ensemble des codes en blocs pour lesquels (n, k) valent

$$(n, k) = (2^m - 1,\, 2^m - 1 - m) \tag{245}$$

pour $m = 2, 3, \ldots$

La probabilité d'erreur s'écrit

$$P_B \simeq p - p(1-p)^{n-1} \tag{246}$$

Code de Golay étendu

Codes Bose-Chadhuri-Hocquenghem (BCH)

Codes de Reed-Solomon

Turbo-codes