femto-st SCIENCES & TECHNOLOGIES

Codes Correcteurs de Hamming

L3 informatique, Sécurité Appliquée

Jean-François Couchot

Université de Franche-Comté, UFR-ST

cnrs UBFC UNIVERSITÉ BOURGOGNE-FRANCHE-COMTÉ UNIVERSITÉ DE FRANCHE-COMTÉ SUP MICRO TECH ENSMM utbm université de technologie Belfort-Montbéliard

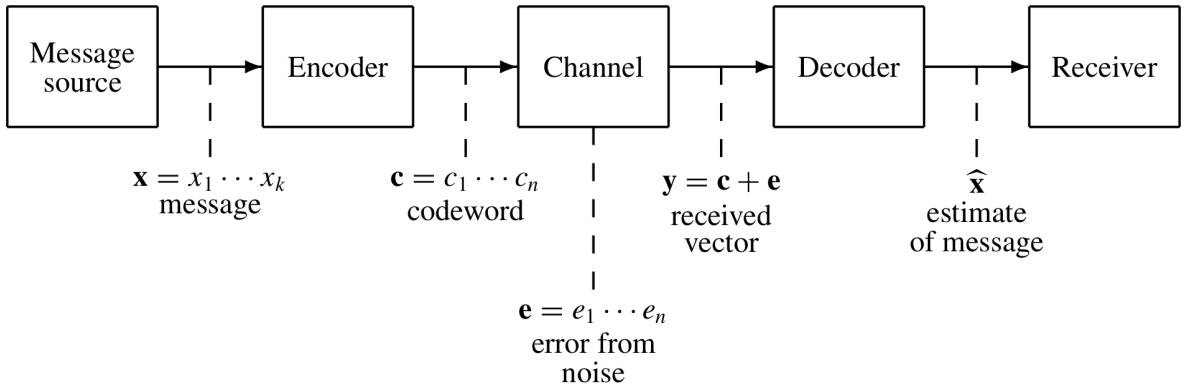
Plan

Plan

Plan

Communication bruitée

Schéma théorique de communication avec correction [1]



1. A la source : un vecteur x doit être envoyé
   - Si x était transmis tel quel : n'importe quel bruit ajouté rendrait le message irrécupérable
   - Idée principale : ajouter de la redondance au message
2. Mot de code c envoyé sur le canal : vecteur contenant x et redondance
3. Erreur e : modélisée par un vecteur de bruit ajouté au mot de code
4. Estimation $\hat{x}$ de x : construite à partir du vecteur reçu y

1. Shannon, C. E. (1948). A mathematical theory of communication. The Bell system technical journal, 27(3), 379-423.

Des erreurs partout

Taux d'erreur

Le taux d'erreur (BER pour Bit Error Ratio) est le rapport entre le nombre de bits erronés reçus par rapport au nombre total de bits transmis.

Ordres de grandeur [2] de BER

- Disques optique : 10^{-5}
- Ligne téléphonique : 10^{-6}
- Communication par fibres optiques : 10^{-9}

2. https ://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Publications/IntroductionAuxCodesCorrecteurs.pdf

Détecter, corriger : des exemples de codes

Au temps des transmissions analogiques[3] de mauvaise qualité

Remplacer chaque lettre par un mot dont la première lettre coïncide avec la lettre à épeler. Sens de « Écho, Roméo, Roméo, Écho, Uniforme, Roméo » ?

Code détecteur : bit de parité

- Codage d'un caractère : nombre décimal entre 0 et 127 (? bits)
- Ajout d'un $8^{\text{ème}}$ bit de parité : la somme des 8 bits est paire
- Corriger 1 erreur ? Détecter 2 erreurs ?

Car.	Dec.	Bin.	Bin+Parité
B	65	1000001	1000001**0**
C	66	1000010	1000010**0**
⋮			
a	97	1100001	1100001**1**

Code correcteur : duplication

- Répéter la totalité du message suffisamment ($\geq 3\times$) de fois (penser à « ââgmee »)
- $011010 \rightarrow 000.111.111.000.111.000$
- Si au plus une erreur, message original associé à $100.111.110.001.110.000$?

3. Rousseau, C., & Saint-Aubin, Y. (2009). Mathématiques et technologie. Springer Science & Business Media.

Efficacité de la détection/correction ?

Définition du rendement ρ

ρ : rapport $\dfrac{\text{nombre de bits de message}}{\text{nombre de bits transmis}}$ toujours inférieur ou égal à 1.

Rendements des codes précédents

- Parité : $\rho_{\text{parite}} = 7/8 = 87.5\%$, mais détection seulement
- Duplication : $\rho_{\text{dupl}_3} = 1/3 \approx 33.3\%$, avec correction

Autres exemples

Formule de Luhn [4]

1. Doubler un chiffre sur deux mod. 9, depuis l'avant dernier, de dr. à gche.
2. Somme de tous les chiffres multiple de 10 $\rightsquigarrow$ validité du nombre original.
3. Exemples : validité de "972-487-086" et "927-487-086" ?
4. Rendement $\rho_{\text{Luhn}_{\text{CB}}} = 15/16 \approx 93.8\%$, mais détection uniquement

Numéro de SS [5]

1. NIR : numéro de 13 chiffres (Genre, deux derniers chiffres de l'année de naissance, mois de naiss...)
2. Clef sur 2 chiffres : NIR mod. 97 (après gestion ev. des corses)
3. Rendement $\rho_{\text{NSS}} = 13/15 \approx 86.7\%$, mais détection uniquement

En vrac

Dans les QR codes [6], dans la DRAM [7], dans les OS,...

4. https://fr.wikipedia.org/wiki/Formule_de_Luhn pour les CB, les SIRET
5. https://fr.wikipedia.org/wiki/Num%C3%A9ro_de_s%C3%A9curit%C3%A9_sociale_en_France#ancrage_C
6. https://fr.wikipedia.org/wiki/Code_QR
7. https://en.wikipedia.org/wiki/ECC_memory

Plan

Rappels d'algèbre de Bool

Somme et produit

- La somme $+$ et le produit $.$ sont définis dans les booléens $\mathbb{B} = \{0.1\}$
- $+$: "OU exclusif"
- $.$: "ET"

$+$	0	1
0	0	1
1	1	0

$.$	0	1
0	0	0
1	0	1

Formalisation

Contraintes pour corriger au plus 1 erreur

- Mot à transmettre de 4 bits : $u = (u_1, u_2, u_3, u_4) \in \mathbb{B}^4$
- Mot de code de 7 bits transmis : $v = (v_1, v_2, v_3, v_4, v_5, v_6, v_7) \in \mathbb{B}^7$

Construction du mot de code $v = (u_1, u_2, u_3, u_4, v_5, v_6, v_7)$

- $v_5 = u_1 + u_2 + u_4$, $v_6 = u_1 + u_3 + u_4$, $v_7 = u_2 + u_3 + u_4$.
- Bits redondants : v_5, v_6 et $v_7 \rightsquigarrow \rho_{H_{(7,4)}} = 4/7 \approx 57.1\%$

A réception de $w = (w_1, w_2, w_3, w_4, w_5, w_6, w_7) \in \mathbb{B}^7$

- $W_5 = w_1 + w_2 + w_4$
- $W_6 = w_1 + w_3 + w_4$
- $W_7 = w_2 + w_3 + w_4$
- Utilisation de la table $\rightarrow$

$w_5 = W_5$	$w_6 = W_6$	$w_7 = W_7$	postion de l'erreur
T	T	T	Tout est OK
T	T	F	inverser w_7
T	F	T	inverser w_6
T	F	F	inverser w_3
F	T	T	inverser w_5
F	T	F	inverser w_2
F	F	T	inverser w_1
F	F	F	inverser w_4

- Demo : mq. si l'unique erreur est $w_1 = \overline{u_1}$, alors $(W_5, W_6, W_7) = (F, F, T)$.

Exemple transmission de $u = (1, 0, 1, 1)$

Construction du mot de code

- Mot de code transmis : $(1, 0, 1, 1, v_5, v_6, v_7)$ avec
  $v_5 = u_1 + u_2 + u_4 = 1 + 0 + 1 = 0$, $v_6 = u_1 + u_3 + u_4 = 1 + 1 + 1 = 1$,
  $v_7 = u_2 + u_3 + u_4 = 0 + 1 + 1 = 0$

A réception de $w = (w_1, w_2, w_3, w_4, w_5, w_6, w_7) = (1, 1, 1, 1, 0, 1, 0)$

$$\begin{aligned} W_5 &= w_1 + w_2 + w_4 = 1 + 1 + 1 = 1 \neq w_5, \\ W_6 &= w_1 + w_3 + w_4 = 1 + 1 + 1 = 1 = w_6, \\ W_7 &= w_2 + w_3 + w_4 = 1 + 1 + 1 = 1 \neq w_7. \end{aligned}$$

- En supposant qu'il n'y ait qu'une erreur et par analyse du tableau précédent : il faut inverser le bit w_2.
- Message corrigé : $(1, 0, 1, 1)$

Plan

Plan

Hamming$(2^k - 1, 2^k - k - 1)$

Remarques

- $2^k - 1$: taille du mot de code
- $2^k - k - 1$: taille du mot u à transmettre
- Pour $k = 3$, on retrouve Hamming$(7, 4)$
- Ne corrige au plus qu'une seule erreur par mot de $2^k - 1$ bits
- Code systématique : « le mot u est complété avec des bits de redondance »
- Dans tout ce qui suit dans le chapitre : que des codes systématiques

Points clés

- Deux matrices G_k et H_k à valeur dans $\mathbb{B}$:
  - G_k : pour générer le mot de code v à partir du mot à transmettre u
  - H_k : pour contrôler w et le corriger éventuellement
- Le tout avec des produits matriciels

Plan

Matrices de contrôle H_k

Définition

$$H_k = \left(\frac{P_k}{I_k}\right) \quad (1)$$

- I_k : matrice identité $k \times k$
- P_k : en ligne, tous les vecteurs non nuls de $\mathbb{B}^k$ qui ne sont pas dans I_k
- $\rightsquigarrow H_k$: contient tous les vecteurs non nuls de $\mathbb{B}^k$.
- $\rightsquigarrow H_k$: $2^k - 1$ lignes et k colonnes

Exemple avec H_3

$$H_3 = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ \hline 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \text{ ou bien } H_3' = \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \text{ ou encore } H_3'' = \left(\begin{array}{ccc} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \ldots$$

Matrices de génération G_k

Définition

$$G_k = \left(I_{2^k-k-1} \mid P_k\right) \quad (2)$$

- P_k : même matrice que dans H_k
- I_{2^k-k-1} : matrice identité $(2^k - k - 1) \times (2^k - k - 1)$
- $\rightsquigarrow$ G_k : $2^k - k - 1$ lignes et $2^k - 1$ colonnes

Exemple avec G_3

$$\text{si } H_3 = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \text{ alors } G_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

Mot de code et syndrome

Mot de code pour $(u_1, \ldots, u_{2^k-k-1}) \in \mathbb{B}^{2^k-k-1}$

- Mot de code associé : $v = uG_k \in \mathbb{B}^{2^k-1}$
- $G_k = (I_{2^k-k-1} \mid P_k)$: les $2^k - k - 1$ premiers bits de v sont ceux de u
- Rendement $\rho_{H_k} = (2^k - k - 1)/(2^k - 1)$: croissant pour $k > 3$

Syndrome de $w \in \mathbb{B}^{2^k-1}$

- Soit $w = (w_1, \ldots, w_{2^k-1})$ le mot à décoder.
- Le mot $\sigma(w) = wH_k \in \mathbb{B}^k$: appelé syndrome de w

Exemple avec $u = (1, 0, 1, 1)$

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right), H = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

- $v = uG = (1, 0, 1, 1, 0, 1, 0)$
- $\sigma(v) = vH = (0, 0, 0)$
- si $w = (1, 0, 0, 1, 0, 1, 0)$
- $\sigma(w) = wH = (0, 1, 1)$

Plan

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc} 1{+}1 & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}\right)$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc} 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}\right)$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 1+1 & . \\ . & . & . \\ . & . & . \\ . & . & . \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & . \\ . & . & . \\ . & . & . \\ . & . & . \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & 0 \\ . & . & . \\ . & . & . \\ . & . & . \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc} 0 & 0 & 0 \\ 1+1 & . & . \\ . & . & . \\ . & . & . \end{array}\right)$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & . & . \\ . & . & . \\ . & . & . \end{array}\right)$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & . \\ . & . & . \\ . & . & . \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1+1 \\ . & . & . \\ . & . & . \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ . & . & . \\ . & . & . \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1+1 & 1+1 & 1+1 \\ 1+1 & 1+1 & 1+1 \end{array}\right)$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Produit $G_k \times H_k$: vecteur nul

Exemple avec $G_3 \times H_3$

$$G_3 \times H_3 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \times \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Montrons que $(G_k \times H_k)_{i,j} = 0$ pour pour toute ligne i et colonne j

- $(G_k \times H_k)_{i,j} = P_{i,j} + P_{i,j} = 0$

Détection d'une erreur

Mot de code et Syndrome nul

Pour un code de Hamming$(2^k - 1, 2^k - k - 1)$, un mot w est un mot de code si et seulement si son syndrome $\sigma(w) = wH$ est nul

Preuve

- $\Rightarrow$: v est un mot de code $\rightsquigarrow v = uG \rightsquigarrow \sigma(v) = vH = uGH = (0)$
- $\Leftarrow$: Soit $w = (w_1, \ldots, w_{2^k-k-1}, w_{2^k-k-1+1}, \ldots, w_{2^k-k-1+k})$

$$\begin{aligned}\sigma(w) = wH = (&\\ &\sum_{i=1}^{2^k-k-1} w_i P_{i,1} + w_{2^k-k-1+1},\\ &\sum_{i=1}^{2^k-k-1} w_i P_{i,2} + w_{2^k-k-1+2},\\ &\ldots,\\ &\sum_{i=1}^{2^k-k-1} w_i P_{i,k} + w_{2^k-k-1+k})\end{aligned}$$

$\sigma(w) = 0 \rightsquigarrow w_{2^k-k-1+j} = \sum_{i=1}^{2^k-k-1} w_i P_{i,j}$ pour tout j, $1 \leq j \leq k$

Ainsi $w = (w_1, \ldots, w_{2^k-k-1})G \rightsquigarrow w$ est un mot de code.

Correction d'une erreur

Correction lorsque le syndrome $\sigma(w)$ n'est pas nul

Soit un code de Hamming$(2^k - 1, 2^k - k - 1)$ et w tel que $\sigma(w)$ n'est pas nul :

- il existe une ligne i de H qui lui est égale et
- le vecteur $w' = (w_1, \ldots, w_{i-1}, \overline{w_i}, \ldots, w_{2^k-1})$ est un mot de code.

Preuve : montrons que $\sigma(w')_c = 0$ pour $1 \leq c \leq k$

$$\sigma(w')_c = \sum_{l=1, l\neq i}^{2^k-1} w_l.H_{l,c} + \overline{w_i}.H_{i,c} \quad (3)$$

$$\sigma(w)_c = \sum_{l=1, l\neq i}^{2^k-1} w_l.H_{l,c} + w_i.H_{i,c} = H_{i,c} \quad (4)$$

- Si $w_i = 1$, de (4), on déduit que $\sum_{l=1, l\neq i}^{2^k-1} w_l.H_{l,c} = 0$ et donc $\sigma(w')_c = 0$.
- Si $w_i = 0$, de (4), on déduit que $H_{i,c} = \sum_{l=1, l\neq i}^{2^k-1} w_l.H_{l,c}$ et donc $\sigma(w')_c = \sum_{l=1, l\neq i}^{2^k-1} w_l.H_{l,c} + \left(\sum_{l=1, l\neq i} w_l.H_{l,c}\right) = 0$

Retour à l'exemple avec $u = (1, 0, 1, 1)$

Rappels

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right), H = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

- $v = uG = (1, 0, 1, 1, 0, 1, 0)$
- $\sigma(v) = vH = (0, 0, 0)$
- si $w = (1, 0, 0, 1, 0, 1, 0)$
- $\sigma(w) = wH = (0, 1, 1)$

Détection de l'erreur et correction

- $v = (1, 0, 1, 1, 0, 1, 0)$ et $\sigma(v) = (0, 0, 0)$: v est un mot de code et le mot original était donc $(1, 0, 1, 1)$
- $w = (1, 0, 0, 1, 0, 1, 0)$ et $\sigma(w) = wH = (0, 1, 1) = H_3$: le mot de code associé à w est $w' = (1, 0, 1, 1, 0, 1, 0)$; le mot original était donc $(1, 0, 1, 1)$

Pour aller plus loin

- les codes de redondance cyclique (CRC) : Hamming, BCH [8], Reed-Solomon [9]
- les codes convolutifs [10]
- les turbo-codes [11] :
  - standards 3G et 4G
  - la NASA lors de Mars reconnaissance Orbiter (1999 . . .2017)
  - la norme IEEE 802.16 (WiMAX)
- les codes de parité à faible densité (LDPC) [12] :
  - standard 5G
  - télévision numérique terrestre
  - Norme Wifi 802.11
  - disques SSD

8. https://en.wikipedia.org/wiki/BCH_code
9. https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon_error_correction
10. https://en.wikipedia.org/wiki/Convolutional_code
11. https://en.wikipedia.org/wiki/Turbo_code
12. https://en.wikipedia.org/wiki/Low-density_parity-check_code