Détection d'erreur de transmission

M. Combacau - combacau@laas.fr

Université Paul Sabatier
LAAS-CNRS

14 novembre 2024

Objectif

Transmission d'information en informatique
Détection d'erreur par test de redondance cyclique (CRC)

Outils mathématiques (1)

Le corps F_2 est constitué par

- Ensemble $F = \{0, 1\} \sim$ ensemble des booléens (mise en œuvre 🙂)
- une lci addition $(+)$, définie par

x	y	$x + y$
0	0	0
0	1	1
1	0	1
1	1	0

  - commutative $(0 + 1 = 1 + 0)$
  - associative (à démontrer par induction)
  - élément neutre 0 (voir définition)
  - symétrique (opposé) $0 + 0 = 0$ et $1 + 1 = 0$

Cette structure $(F, +)$ est un groupe abélien (commutatif)

Outils mathématiques (2)

- Ici multiplication (.) définie ainsi

x	y	$x.y$
0	0	0
0	1	0
1	0	0
1	1	1

  - la définition montre la commutativité
  - l'associativité est aussi démontrable par induction (à faire)
  - élement neutre : 1 ; élement absorbant 0
  - inverse de 1 : 1, pas de symétrique pour 0 (absorbant)
  - multiplication distributive sur $+$ (par induction)
- Structure $(F, +, .)$: **corps**.
- Plus petit corps existant nommé **corps de Galois** et noté F_2.

Intérêt de la structure F_2 : proximité avec logique booléenne

1. addition dans $F_2 \leftrightarrow$ XOR dans B_2 (booléens)
2. multiplication dans $F_2 \leftrightarrow$ ET dans B_2 (booléens)

La réalisation sur circuit électronique très simple

Outils mathématiques (3)

Espace vectoriel sur le corps de Galois

- Soit l'ensemble $F_2^n = \{[x_{n-1}, \dots, x_0]$ avec $\forall i \in [0, n-1], x_i \in F_2\}$
- Ici [1] l'addition $(+)$ définie par $A + B = [a_{n-1} + b_{n-1}, \dots, a_0 + b_0]$
  - commutative et associative (hérite de $\oplus$ dans F)
  - élément neutre $[0, \dots, 0]$
  - M a pour opposé M
- Ice [2] multiplication (.) par un élément de F définie par $\forall a \in F, \forall M \in F_2^n, a * M = [a.m_{n-1}, \dots, a.m_0]$
  - Élément neutre $m = [1, \dots, 1]$
  - distributive à gauche sur $+$ ($+$ définie dans F_2^n)
  - distributive à gauche sur $+$ ($+$ définie dans F)
  - associative mixte avec . (.définie dans F) : $(a.b).M = a.(b.M)$

Structure $(F_2^n, +, .)$: espace vectoriel

1. loi de composition interne
2. loi de composition externe

Outils mathématiques (4)

- Dans F_2, $1+1=0$ et $1-1$=0 (soustraction = addition)
- Dans $(F_2^n, +, .)$, $1.v = v$ et $0.v = 0$ (simple non ?)
- un vecteur de $(F_2^n, +, .)$: coefficients d'un polynôme
  $[10011] \leftrightarrow x^4 + x + 1$
- Addition et soustraction de polynômes possibles

$$\begin{array}{cccccc} & x^4 & & & +x & +1 \\ + & & x^3 & +x^2 & +x & \\ \hline = & x^4 & +x^3 & +x^2 & & +1 \end{array} \quad \text{et} \quad \begin{array}{cccccc} & x^4 & & & +x & +1 \\ - & & x^3 & +x^2 & +x & \\ \hline = & x^4 & +x^3 & +x^2 & & +1 \end{array}$$

Outils mathématiques (5)

- Division de polynômes possible

  Il s'agit d'écrire $P(x)$ sous la forme $Q(x) \times G(x) + R(x)$
  - $Q(x)$ est le quotient
  - $G(x)$ est le générateur (souvent appelé diviseur)
  - $R(x)$ est le reste

$$
\begin{array}{cccccc|c}
 & x^4 & & +x & +1 & & x+1 \\
\cline{7-7}
+ & x^4 & +x^3 & & & & x^3 \\
\hline
= & & x^3 & & & &
\end{array}
$$

Outils mathématiques (5)

- Division de polynômes possible

  Il s'agit d'écrire $P(x)$ sous la forme $Q(x) \times G(x) + R(x)$
  - $Q(x)$ est le quotient
  - $G(x)$ est le générateur (souvent appelé diviseur)
  - $R(x)$ est le reste

$$
\begin{array}{rrrrrr|l}
 & x^4 & & & +x & +1 & x+1 \\
\cline{7-7}
+ & x^4 & +x^3 & & & & x^3+x^2 \\
\cline{1-3}
= & & x^3 & +0 & & & \\
 & + & x^3 & +x^2 & & & \\
\cline{2-4}
 & = & & x^2 & & &
\end{array}
$$

Outils mathématiques (5)

- Division de polynômes possible
  Il s'agit d'écrire $P(x)$ sous la forme $Q(x) \times G(x) + R(x)$
  - $Q(x)$ est le quotient
  - $G(x)$ est le générateur (souvent appelé diviseur)
  - $R(x)$ est le reste

$$
\begin{array}{rrrrrr|l}
 & x^4 & & & +x & +1 & x+1 \\
\cline{7-7}
+ & x^4 & +x^3 & & & & x^3+x^2+x \\
\cline{1-3}
= & & x^3 & +0 & & & \\
 & + & x^3 & +x^2 & & & \\
\cline{2-4}
 & = & & x^2 & +x & & \\
 & & + & x^2 & +x & & \\
\cline{3-5}
 & & = & & & 1 &
\end{array}
$$

- Degré (1) $<$ degré (x+1) $\rightarrow$ fin de la division
  Dans $(F_2^n, +, .)$ $\underbrace{x^4 + x + 1}_{P(x)} = \underbrace{(x^3 + x^2 + x)}_{Q(x)} \times \underbrace{(x+1)}_{G(x)} + \underbrace{1}_{R(x)}$

Principe du CRC

L'utilisation d'un CRC repose sur les données suivantes

- Mot P à n bits à transmettre $\leftrightarrow$ polynôme $P(x)$
- Mot G à (k+1) bits ($k+1<n$) générateur $\leftrightarrow$ $G(x)$ (degré k)

1. L'émetteur calcule R(x) = reste $R(x)$ de la division $\frac{x^k \times P(x)}{G(x)}$ (mot R)
2. L'émetteur transmet $D=[PR] \leftrightarrow$ polynôme
$$D(x)=x^K \times P(x)+R(x)$$
3. Le récepteur calcule le reste $Rr(x)$ de $\frac{D(x)}{G(x)}$
   1. pas d'erreur de transmission $\Rightarrow Rr(x)=0$
   2. nombre d'erreurs $\in [1,k-2], \Rightarrow Rr(x) \neq 0$ (non démontré)
4. Ne fournit pas de mécanisme de correction

CRC nul en l'absence d'erreur

Le récepteur recoit $[PR] \leftrightarrow x^k \times P(x) + R(x)$ (par construction)
Le calcul du reste :

$$Rr(x) = \frac{x^k \times P(x) + R(x)}{G(x)} = \frac{x^k \times P(x)}{G(x)} + \frac{R(x)}{G(x)}$$

Décomposons ceci :

$$\begin{cases} \frac{x^k \times P(x)}{G(x)} & = R(x) \quad \text{même calcul que celui fait par l'émetteur} \\ \frac{R(x)}{G(x)} & = R(x) \quad \text{puisque degré}[R(x)] < \text{degré } [G(x)] \end{cases}$$

D'où

$$Rr(x) = R(x) - R(x) = 0 \quad \text{en l'absence d'erreur de transmission}$$

Exemples d'utilisation

Nous ne citerons que deux exemples :

1. CRC1 G(x) de degré 1 : $x+1$. Reste à 1 bit qui n'est rien d'autre que le bit de parité vu un peu plus tôt !
2. CRC32 Polynôme de degré 32)

   $$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

   utilisé par le réseau Ethernet
3. Très utilisé pour sa simplicité de mise en œuvre électronique et informatique

Exemple applicatif (1)

CRC1 de polynôme $G(x) = x + 1$

- G=[11] $\leftrightarrow$ polynôme générateur $x + 1$ (degré 1)
- $P = [10011011] \leftrightarrow P(x) = x^7 + x^4 + x^3 + x + 1$
- $x.P(x) = x^8 + x^5 + x^3 + x^2 + x$ à diviser par $x + 1$
- seul le reste est calculé ($Q(x)$ n'intervient jamais dans le CRC)

Exemple applicatif (2)

$$
\begin{array}{cccccccccc}
 & \multicolumn{8}{c}{\overbrace{x^8 \qquad\qquad +x^5 \qquad +x^3 \quad +x^2 \quad +x}^{x^k \times P(x)}} & +0 \\
+ & x^8 & +x^7 & & & & & & & \\
\cline{1-3}
= & & x^7 & & +x^5 & & +x^3 & +x^2 & +x & +0 \\
+ & & x^7 & +x^6 & & & & & & \\
\cline{1-4}
= & & & x^6 & +x^5 & & +x^3 & +x^2 & +x & +0 \\
+ & & & x^6 & +x^5 & & & & & \\
\cline{1-5}
= & & & & & & +x^3 & +x^2 & +x & +0 \\
+ & & & & & & x^3 & +x^2 & & \\
\cline{1-8}
= & & & & & & & & x & +0 \\
+ & & & & & & & & x & +1 \\
\cline{1-10}
= & & & & & & & & & 1
\end{array}
$$

Le mot $[PR]$ transmis est donc

$$[PR] = [100110111]$$

Exemple applicatif (3)

Le mot reçu, en l'absence d'erreur est $[PR] = [100110111]$
Le début de la division, jusqu'à ce que le reste entre en jeu est identique à la division faite à l'émission (seul le bit R change)

$$
\begin{array}{rrrrrrrr}
x^8 & & +x^5 & & +x^3 & +x^2 & +x & +1 \\
 & \vdots & & & & & & \\
\cline{3-5}
= & & & & +x^3 & +x^2 & +x & \\
 & & & + & x^3 & +x^2 & & \\
\cline{4-6}
 & & & = & & & x & +1 \\
 & & & & & + & x & +1 \\
\cline{5-8}
 & & & & & = & & 0
\end{array}
$$

Le reste est nul. Mais ce serait le cas si 2xk erreurs avaient eu lieu pendant la transmission (exercice à faire)

Au sujet de la mise en œuvre

- Un mot $\rightarrow$ une valeur de R approche par table + multiplexeur
- Division polynomiale dans $F_s^n \leftrightarrow$ opération xor bit à bits + décalage (Cours S6 DES ?)
- Calcul de R sur les mots plutôt que sur les polynômes (exemple précédent)

$$
\begin{array}{cccccccccc}
 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
\oplus & 1 & 1 & & & & & & & \\
\hline
= & & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
 & \oplus & 1 & 1 & & & & & & \\
\hline
 & = & & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
 & & \oplus & 1 & 1 & & & & & \\
\hline
 & & = & & & & 1 & 1 & 1 & 0 \\
 & & & & & \oplus & 1 & 1 & & \\
\hline
 & & & & & = & & & 1 & +0 \\
 & & & & & & & + & 1 & +1 \\
\hline
 & & & & & & & = & & \color{red}{1}
\end{array}
$$