

bénéfice gaffer

CRYPTANISTES Kullback et Leibler

$p(x) \rightarrow q(x)$ $D(p||q) \geq 0$ quand $p=q \Rightarrow D(p||q)=0$

$p(x) \rightarrow \neq q(x)$ $D(p||q)$ augmente

$p(x)$ réalité réalisée

$q(x)$ théorie

exemple 1.1.2

log utilise pour multiplier $\log_2(a \cdot b) = \log_2(a) + \log_2(b)$

quantité d'information $I(x) = \log_2(1/p)$

1.1.3 entropy

maximum $p(a)=0.5 \rightarrow H(x)=1$

probabilité équitable probé

entropy mesure la désordre d'un système

1.2

1.2.1 probabilité alternative densité ; probabilité jointe normalisé

$p(X=x_i)$ a priori $p(X=x_i, Y=y_j)$ a posteriori vraisemblance

$H(X, Y)$ conjointe

$H(X|Y)$ conditionnelle

$p(x_i, y_j) = p(x_i) \cdot p(y_j)$ indépendants aucun information mutuelle $H(X|Y)=H(X) ; T(X, Y)=0$

1.2.2 $I(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \geq 0 \rightarrow$ conditionnel réduit l'entropie

désordre Venn propriétés variables alternées

1.3 rms continue

mesure plus discriminante

2 degrés Keckhoffs

normalisé fréquence

$C = X+K$ ou exclusive

exercices introduction à la théorie de l'information

exercice 1.

$$\ln(\pi\sqrt{2\pi e})$$

entropie différentielle: $H(x) = F(h(x)) = \int_{\mathbb{R}} p(x) \cdot \log_2(1/p(x)) dx$

variable aléatoire gaussienne: $f(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2} \cdot \frac{(x-\mu)^2}{\sigma^2}}$

$$H(x) = E(h(x)) = \int_{\mathbb{R}} p(x) \log_2 (1/p(x)) dx ; p(x) = \frac{1}{T\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2}$$

$$= \int_{\mathbb{R}} \frac{1}{T\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \cdot \log_2 (\frac{1}{T\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2}) dx$$

Propriété $\frac{d}{dx} \log_b x = \frac{1}{\ln(b)} \frac{1}{x}$

$$\frac{d}{dx} \log_2 (1/p(x)) = \frac{1}{\ln(2)} \frac{d}{dx} \ln(1/p(x)) = \frac{1}{\ln(2)} \frac{p'(x)}{p(x)} = \frac{1}{\ln(2)} \cdot p(x) \cdot p'(x) \dots$$

$$\int_a b' = ab - \int_a b$$

2.2

2.2.1 échantillonnage frequency d'informations $\geq x f_{\max}$

quantité exponentielle

longeur moyenne augmente avec l'inverse de la taille du chemin

shannon func

huffman essai?

$$= \frac{1}{T\sqrt{2\pi}} \int_{\mathbb{R}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \cdot \left(\ln \left(\frac{1}{T\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \right) + \frac{1}{2}(\frac{x-\mu}{\sigma})^2 \right) \frac{1}{\ln(2)} dx$$

$$= \frac{1}{T\sqrt{2\pi}} \int_{\mathbb{R}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \cdot \left(\ln \left(\frac{1}{T\sqrt{2\pi}} \right) + \frac{1}{2}(\frac{x-\mu}{\sigma})^2 \right) \frac{1}{\ln(2)} dx$$

$$= \frac{1}{T\sqrt{2\pi} \ln(2)} \int_{\mathbb{R}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \cdot \ln \left(\frac{1}{T\sqrt{2\pi}} \right) + \frac{1}{2}(\frac{x-\mu}{\sigma})^2 \cdot e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} dx$$

$$= + \frac{1}{T\sqrt{2\pi} \ln(2)} \cdot \frac{1}{4} e^{-\frac{1}{2}}$$

exercice 3.

spiral

- a) 1/2 b) 1/4 c) 1/8 d) 1/16 e) 1/16

gauusse plus de l'entropie de discord

photo 13/09/2023

$$H_4 = \frac{1}{4} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{4} \cdot 3 + \frac{1}{4} \cdot 4 = 9$$

$$H_4 = 0.5 \cdot 1 + 0.25 \cdot 2 + 0.125 \cdot 3 + 0.0625 \cdot 4 = 2$$

exercice 3: $H_4 = 1.875$ prouve équivalence entre $H(x)$, entropy, et la longueur moyenne
démonstration gauusse le plus entropicie

$$0 \leq \int p(x) \cdot \log_2 p(x) dx \rightarrow \text{gauusse}$$

$$0 \leq \int p(x) \cdot \log_2 p(x) dx + \int p(x) \cdot \log_2 \frac{1}{q(x)} dx$$

$$-\int p(x) \cdot \log_2 p(x) dx \leq \int p(x) \cdot \log_2 \frac{1}{q(x)} dx$$

$$H(x) \leq \int p(x) \cdot \log_2 \frac{1}{q(x)} dx$$

$$H(x) \leq \int p(x) \cdot \log_2 \left[\left(\frac{1}{\sqrt{2\pi\sigma^2}} \right) \exp \frac{-(x-\mu)^2}{2\sigma^2} \right] dx$$

$$\begin{aligned} H(x) &\leq -\log_2 \left(\frac{1}{\sqrt{2\pi\sigma^2}} \right) \left(\int p(x) dx + \frac{1}{2\sigma^2} \int p(x) \cdot (x-\mu)^2 dx \right) \\ &\leq -\log_2 \frac{1}{\sqrt{2\pi\sigma^2}} + 1 \cdot 1 \cdot 1 \cdot \sigma^2 \end{aligned}$$

$$H(x) \leq \log_2 (2\pi\sigma^2)^{1/2} + 1/2 \log_2 (\sigma^2) - \log_2 (2\pi\sigma^2)/2$$

maximum d'incertitude est quand est enjupable

graphe x et y sont indépendantes probabilité conditionnelle est nulle

théorie de l'information et énergie

$$H(x) \leq H(a)$$

$$d_1 = H(K)/R \rightarrow \text{capacité de transmission}$$

s'un bit est perdu il faut le répéter après, sauf si on
nous complique pour faire de l'information

Caract. Binaire symétrique CBS

stratégie de décodage

/ / Réglage :

visez majoritairement la majorité FFA toward error correction

fonctionnement si n'est pas atteint on disperse ARQ comme rapport réciproque

capacité de perte $K = a_1 \cdot n - b$; répétition de façon continue

- + Rapide, théorique plus précis
- décodage complexe, protocole d'accès

Capacité : théorème de Shannondistance Hammingmot pour substituer des mots et éviter redondance (d_{min})dimension $\lfloor \frac{d}{d_{min}-1} \rfloor$ capacité $(d_{min}-1)/2$ distance de codage HammingTout appareil $T(x,y) = 0$, tout parfait $T(x,y) = H(x)$ théorème de Shannon

$$\begin{aligned} H(y|x) &= H(x+B|x) \xrightarrow{\text{gaussien}} \\ &= H(x|x) + H(B|x) \\ &= H(B) \\ &= \frac{1}{2} \log(2\pi e\sigma^2) \end{aligned}$$

$$C = w \log \left(1 + \frac{S}{N} \right) \xrightarrow{\text{signal}} \text{signaux}$$

\hookrightarrow bruit

\hookrightarrow quantité d'informations

les codes linéairesmatrice génératriceexemples

$$G = \begin{pmatrix} 100101 \\ 111021 \\ 110110 \end{pmatrix} \quad \left. \begin{array}{l} \text{K=3} \\ \text{trouvez quantité de vecteurs dans} \end{array} \right.$$

$$(010)G = (011101)$$

$$(110)G = (000010)$$

$$(001)G = (110110)$$

$$(101)G = (011011)$$

$$(111)G = (111000)$$

$$C = (000)(011101) = (000000)$$

$$spire G = (100101)$$

orthogonalisé $x \perp y \Leftrightarrow x \cdot y = 0$

binaire utilisé module de 2

$$s = rx^T h$$

Get H chose inverse matrix
exercice 1

14/07/2022

chapitre 1 exercice 1.

équation différentielle; variable aléatoire suffisante \rightarrow pour quoi ce signe ne change pas?

$$H(x) = \int_{-\infty}^x \frac{1}{\sqrt{B + \frac{x-y}{2\pi}}} \cdot \exp\left(-\frac{(x-y)^2}{2\pi}\right) \log\left(\frac{\sqrt{B + \frac{x-y}{2\pi}} \cdot \exp\left(-\frac{(x-y)^2}{2\pi}\right)}{\sqrt{2}}\right) dx$$

$$\frac{1}{e^a} = (e^a)^{-1} = e^{-1a}$$

$$= \int_{-\infty}^x \frac{1}{\sqrt{B + \frac{x-y}{2\pi}}} \cdot \exp\left(-\frac{(x-y)^2}{2\pi}\right) \cdot \log\left(\sqrt{B + \frac{x-y}{2\pi}}\right) dx +$$

$$\int_{-\infty}^x \frac{1}{\sqrt{B + \frac{x-y}{2\pi}}} \cdot \exp\left(-\frac{(x-y)^2}{2\pi}\right) \cdot \log\left(\exp\left(-\frac{(x-y)^2}{2\pi}\right)\right) dx$$

$$= \log\left(\sqrt{B + \frac{x-y}{2\pi}}\right) \cdot \int_{-\infty}^x \frac{1}{\sqrt{B + \frac{x-y}{2\pi}}} \exp\left(-\frac{(x-y)^2}{2\pi}\right) dx +$$

$$\int_{-\infty}^x \frac{1}{\sqrt{B + \frac{x-y}{2\pi}}} \cdot \exp\left(-\frac{(x-y)^2}{2\pi}\right) \cdot \ln\left(\exp\left(-\frac{(x-y)^2}{2\pi}\right)\right) / \ln(2) dx$$

$$= \log\left(\sqrt{B + \frac{x-y}{2\pi}}\right) \cdot 1 + \frac{1}{2\pi^2 \ln(2)} \cdot \int_{-\infty}^x -\frac{(x-y)^2}{2\pi} \cdot \exp\left(-\frac{(x-y)^2}{2\pi}\right) dx$$

$$= \log\left(\sqrt{B + \frac{x-y}{2\pi}}\right) + \frac{1}{2\pi^2 \ln(2)} \cdot \pi^2$$

$$= \log\left(\sqrt{B + \frac{x-y}{2\pi}}\right) + \frac{1}{2\pi^2 \ln(2)}$$

IC202 Théorie de l'information

mercredi 14/03/2022

chapitre 1 exercice 1

$$H(x) = \log_2 \left(\frac{1}{2\sqrt{\pi}} \right) + \frac{1}{2\ln(2)} = \log_2 \left(\frac{1}{2\sqrt{\pi}} \right) + \frac{\ln(e)}{2\ln(2)}$$

$$= \log_2 \left(\frac{1}{2\sqrt{\pi}} \right) + \frac{1}{2} \log_2(e) = \log_2 \left(\frac{1}{2\sqrt{\pi}} e \right) \text{ donc}$$

$$H(x) = \log_2 \left(\sqrt{2\pi e \tau^2} \right)$$

Remarque:

$$(I): \int_{\mathbb{R}} \frac{1}{\sqrt{2\pi\tau^2}} \exp\left(-\frac{(x-\mu)^2}{2\tau^2}\right) dx = 1; \text{ définition de distribution}$$

$$(II): \int_{\mathbb{R}} \frac{-(x-\mu)^2}{2\tau^2} \exp\left(-\frac{(x-\mu)^2}{2\tau^2}\right) dx = \tau^2; \text{ définition de variance}$$

chapitre 1 exercice 2

$$H(x) = \int p(x) \log_2 \left(\frac{p(x)}{q(x)} \right) dx = \int p(x) \log_2 p(x) dx + \int p(x) \log_2 \left(\frac{1}{q(x)} \right) dx$$

$$= \int p(x) \cdot \log_2 p(x) dx \leq \int p(x) \cdot \log_2 \left(\frac{1}{\sqrt{2\pi\tau^2}} \exp\left(-\frac{(x-\mu)^2}{2\tau^2}\right) \right) dx$$

$$(I) \quad (II) \quad H(x) \leq \log_2 (\sqrt{2\pi\tau^2} e) \text{ donc la gaussienne à l'entropie maximale}$$

Remarque:

$$(I): H(x) := \int_D p(x) \log_2 \left(\frac{1}{p(x)} \right) dx = \int_D p(x) \log_2 1 dx - \int_D p(x) \log_2 p(x) dx$$

(II) résolution chapitre 1 exercice 1

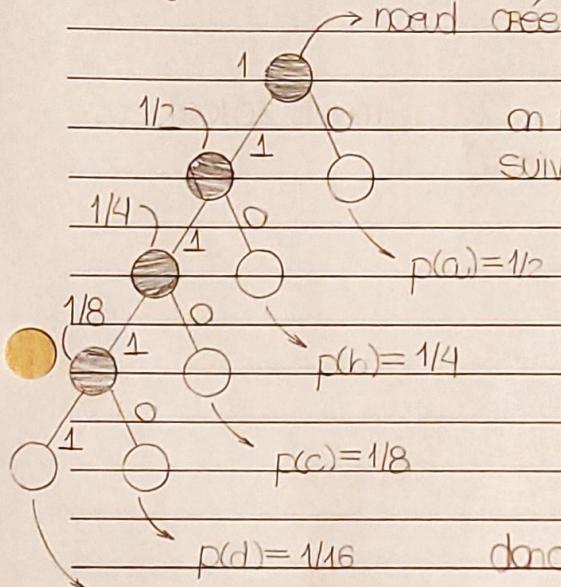
IC202 Théorie de l'information

mardi 14/07/2022

chapitre 1 exercice 3.

on organise selon la méthode de huffman

jeudi 15/07/2022



on note que chaque symbole aura les codes suivantes:

	code	longueur	probabilité
a	0	1	1/2
b	10	2	1/4
c	110	3	1/8
d	1110	4	1/16
e	1111	4	1/16

donc la longueur moyenne, l_m , sera

$$l_m = \sum_{i=1}^n l_i \cdot p_i = 1,875$$

maintenant on calcule l'entropie discrète

$$\begin{aligned} H(x) &= \sum_{i=1}^{N_x} p(x_i) \log_2(1/p(x_i)) \\ &= 1/2 \cdot \log_2(2) + 1/4 \cdot \log_2(4) + 1/8 \cdot \log_2(8) + 2 \cdot 1/16 \cdot \log_2(1/16) \end{aligned}$$

$$H(x) = 1,875$$

on note que c'est le même valeur qui la longueur moyenne c'est possible de le montrer mais c'est difficile

Remarques

la entropie du codage de Huffman est égale à la longueur moyenne car le codage de Huffman est le plus efficace

I2002 Théorie de l'information

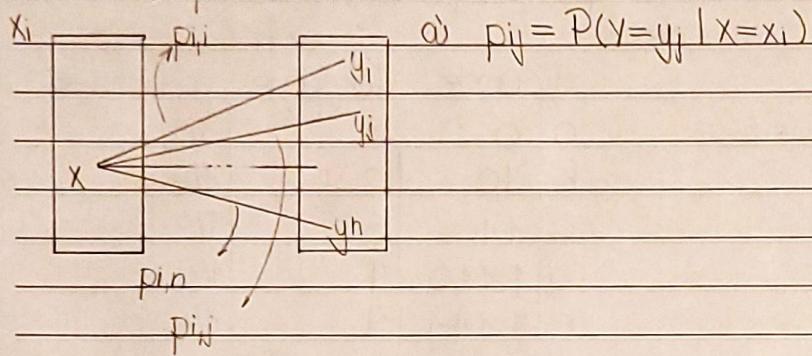
jeudi 15/09/2022

pour être un codage d'Huffman il faut que le mot le plus grand a un "jumeau"; codé avec la même taille

→ page annexe

exercice 1 chapitre 2.

mardi 20/09/2022



Cas casuel binaire symétrique

Référance

10202 Théorie d'information

mardi 20/09/2022

vecteur génératrice

matrice génératrice

exercice 1) page 23

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

dans la grille

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

forme systématique : faire apparaître une identité avec des opérations linéaires, changer lignes et colonnes

attention manipuler adresses change la grille

exemple page 23 au moins explanation fantomatique
pour corriger 1 erreur il faut 3 adresses supplémentaires
$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \quad d_{\text{rect}} = d_{\min} - 1, \quad d_{\text{corrige}} = \frac{d_{\min} - 1}{2}$$

→ erreurs non nulles

Remarquer le moins carte pour confirmer qu'il y a suffisamment de zéros

$$\begin{array}{r}
 \begin{array}{c|ccccc}
 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & & & & & G \\
 1 & 1 & & & & & \\
 \hline
 0 & & & & & &
 \end{array} \\
 \hline
 \end{array} =
 \begin{array}{c|cccc}
 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 1 & 0 \\
 \hline
 1 & 0 & 1 & 1 & 1 \\
 0 & 0 & 1 & 0 & 1 \\
 \hline
 0 & & & &
 \end{array}$$

par $T_{(n-r) \times (n-k)}$ → lignes

exercice 1 page 34

pas peso

$$\begin{array}{r}
 \begin{array}{c|ccccc}
 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
 \hline
 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
 \hline
 \end{array} \\
 \hline
 \end{array} \quad G_1 \leftrightarrow G_2 \quad \rightarrow G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \quad \text{forme systématique}$$

$n=7$ $k=3$

IN202 théorie information
donc:

	1	0	1	1	0	0	0
H =	1	1	1	0	1	0	0
	1	1	0	0	0	1	0
	0	1	1	0	0	0	1

pour découvrir les mots du code on fait la
Combination possible de 2^k (numéros binaires)
et G

mots du code

0 0 0	0 0 0 0 0 0 0
0 0 1	0 0 1 1 1 0 1
0 1 0	0 1 0 0 1 1 1
0 1 1	0 1 1 1 0 0 0
1 0 0	1 0 0 1 1 1 0
1 0 1	1 0 1 0 0 1 1
1 1 0	1 1 0 1 0 0 1
1 1 1	1 1 1 0 1 0 0

refaire exercice

IN202 Théorie Information

mardi 20/09/2022

exemples page 54 $K[x]$ ensemble à 16 éléments avec définition fermeuse par rapport au

$$x^0 = 1 \quad \text{tableau}$$

$$x^1 = x$$

$$x^2 = x^2$$

$$x^3 = x^3$$

$$x^4 = x+1; \text{ modulo } \pi$$

part i $(1+x+x^3)(1+x) \Rightarrow x^7 \cdot x^4 = x^{11} = x^3 + x^2 + x$

$$1+x+x^3+x+x^2+x^4 = 1+2x+x^2+x^3+x^4 = 2+3x+x^2+x^3 \\ \leftarrow = x+x^2+x^3 \quad (I)$$

Remarqué coefficient binôme modulo ordé $= x^{11} = 1110$ v) pourquoi 1 et 2x sont annulés?pas binôme, cette loi puissance présente $(1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0 \cdot 1)$

part ii inverse $x+x^2+x^3$

$$x^3+x^2+x \Rightarrow x^{11} \Rightarrow 1110$$

Comment on travail avec binôme

Remarqué

n%2 est 0 si pair et 1 si imp

(I) comment faire le critère? $m \cdot m^{-1} = 1$ inverse

part iii $x^4 + x^5 = x^4(x+1) = (x+1)(x+1) = x^2 + 2x + 1 \\ = x^2 + 1$

page 53

mardi 27/09/2022

forme polynôme utiliser somme soustraction

forme fraction utiliser multiplication division

page 54Remarqué $T+T=S_1 \rightarrow$ quand $f: I \rightarrow aT+b$ option linéaire
 $f(T)+f(T)=S_3$

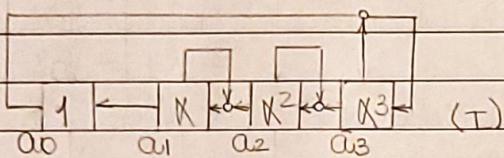
Il y a des photos avec la réponse finale il faut chercher la décaison

/ / IN202 Théorie de l'informationen traine

$$S_2 = f(I) + f(J) = (aI + b) + (aJ + b) = a(I + J) + 2b = aS_1 \quad (I) \quad (II)$$

Remarqué

(I) pourquoi c'est un problème ?

(II) pourquoi $2b$ a disparu modulo de 2exercices introduction aux arêtes algébriquesexercice 1Réaliser un circuit multipliant dans $K_3[X]$ par l'élément X^3 pas nécessaire de faire le reste du circuit

$$X^3 a_1 = X^3(a_0 + Xa_1 + X^2a_2 + X^3a_3)$$

$$= X^3a_0 + X^4a_1 + X^5a_2 + X^6a_3$$

$$= X^3a_0 + (X+1)a_1 + (X^2+X)a_2 + (X^3+X^2)a_3$$

$$X^3a_1 = a_1 + (a_1+a_0)X + (a_2+a_3)X^2 + (a_0+a_3)X^3$$

$$\overline{a_0} + \overline{a_1}X + \overline{a_2}X^2 + \overline{a_3}X^3$$

↳ valeur après clock cycle

Remarqué

(I) qu'est ce que la boîte représenté ?

IN202 Théorie information

mardi 27/09/2022

exercices introduction aux codes algébriquesexercice 2le décodeur présenté au paragraphe 4.4 reçoit $r = (r_0 \ r_1 \ r_2 \ r_3 \ r_4)$

retrouver le mot émis le plus probable

$$S = r^T H$$

$$= (\kappa^5 + \kappa^{10} \quad 1+1)$$

$$= (\kappa^2 + \kappa + \kappa^2 + \kappa + 1 \quad 1+1) \rightarrow \text{modulo } 2 \quad (T)$$

$$= (1 \quad 0)$$

on note que $S_1 \neq 0$ et $S_3 \neq S_1^3$ donc on peut utiliser l'équation
 $x^2 + S_1 x + (S_3/S_1 + S_1^2)^2 = x^2 + x + 1 \quad (\text{II})$

→ chaque valeur du tableau appliquée à l'équation

$$1: 1+1+1=1 \neq 0 \quad \text{inexacte}$$

$$\kappa: \kappa^2 + \kappa + 1 \neq 0$$

:

modèle de?

$$\kappa^5 \kappa^{10} + \kappa^5 + 1 = 1+1=0 \quad \text{donc } T=\kappa^5$$

donc il faut corriger la position 6 et 11 du vecteur
 comme en 0

on note que

$$I \cdot J = 1 \rightarrow (\kappa^5)^{-1} = \kappa^{10} \quad \text{donc } T=\kappa^{10}$$

$$I+J=1$$

→ corrige → dépend de S_1 et S_3 (III)

$$r' = (0000 \ 0000 \ 0000 \ 0000)$$

↑ 6m ↑ 11th

$$I \cdot J = S_3/S_1 - S_1^2 \quad \text{quand on utilise l'équation}$$

$$I+J=S_1$$

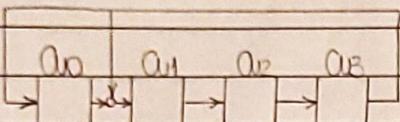
Rémarks

IN200 théorie de l'information

mardi 27/09/2022

exercices du chapitre introduction aux codes algébriques

exercice 3.

→ même processus pour $K^i \dots (T)$ on considère le circuit dans $K_2[X]$ par X 

Séquence: 1000 1001 1010 111, période 15

après on fait la correspondance à des symboles produits

$$+--- +--+ ++-+ +++ \rightarrow \begin{array}{l} \text{produit scalaire } S \text{ et} \\ S \text{ décalé de } T \end{array}$$

on peut donner la loi : $\text{OSS}(T) = \sum_{i=1}^{n=15} S(i) \cdot S(i+5)$

$$\text{OSS}(0) = \sum_{i=1}^{n=15} i^2 = 15$$

$$\text{OSS}(T) = A - D = 7 - 8 = -1$$

\downarrow désaccord quand la séquence est
accord, décalé de 2

pour valider l'équation \rightarrow Relation orale

décalé: séquence

$$0: +--- +--+ ++-+ +++ \quad \text{OSS}(0) = 15$$

$$1: ++---+--++-++-++ \quad \text{OSS}(1) = -1$$

$$2: +++---+--++-++-+ \quad \text{OSS}(2) = -1$$

Remarques

IN200 Théorie de l'information

mardi 27/09/2022

Théorie page 59 importantéchelle de grischasse d'équivalence ne sert à rienThéorème de Fermatexerciceon cherche le mps $G(7)$ et la multiplication modulo 7définitionpart 1 quel est l'ordre de $6[7]$ Réolution

$$6^2 = 36 = 1[7] \text{ donc ordre } 2$$

part 2 vérifier le petit théorème de Fermat pour $y=5[7]$ y est il premierRéolution

$$5^2 = 25 = 1[7]$$

$$5^3 = 5 \cdot 25 = 20[7] = 6[7]$$

$$5^6 = 5^3 \cdot 5^3 = 6[7] \cdot 6[7] = 36[7] = 1[7]$$

s. divide 6: 1, 2, 3 ou 6 sont des premiers

IN202 théorie de l'information
analogie

mercredi 27/09/2022

rem (\mathbb{C}, \mathbb{R}) ($\mathbb{G}[\mathbb{P}]$, $\mathbb{Z}/p\mathbb{Z}$)

$$\begin{aligned} 1^{\circ} z &= a + jb \\ &= r \exp(j\phi) \end{aligned}$$

$$\gamma = \sum_{i=1}^r a_i x^i$$

$$\begin{aligned} 2^{\circ} \bar{z} &\text{ conjugué de } z \\ (z_1 + z_2) &= \bar{z}_1 + \bar{z}_2 \\ (z_1 \cdot z_2) &= \bar{z}_1 \cdot \bar{z}_2 \end{aligned}$$

$$\begin{aligned} \gamma^p &\text{ conjugué de } \gamma \\ (\gamma_1 + \gamma_2)^p &= \gamma_1^p + \gamma_2^p \\ (\gamma_1 \cdot \gamma_2)^p &= \gamma_1^p \cdot \gamma_2^p \end{aligned}$$

$$\begin{aligned} 3^{\circ} \mathbb{R} &\subset \mathbb{C} \\ z \in \mathbb{R} &\Leftrightarrow z = \bar{z} \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\subset \mathbb{G}[\mathbb{P}] \\ \gamma \in \mathbb{Z}/p\mathbb{Z} &\Leftrightarrow \gamma^p = \gamma \end{aligned}$$

$$\begin{aligned} 4^{\circ} f \text{ polynôme à coefficients} \\ \text{réels} \text{ admet } z \text{ comme racine} \Rightarrow \\ z \text{ est laire} \\ \text{racine} \end{aligned}$$

si γ racine de f polynôme à coefficients dans \mathbb{Z}

$(x - z_0)(x - \bar{z}_0)$ est un polynôme
à coefficients réels

Récrire dans $\mathbb{G}[16] = K_2(\mathbb{X})$ exemple

$$\mathbb{X}^3 x + \mathbb{X}^5 = 1$$

$$\mathbb{X}^3 x + \mathbb{X}^2 + \mathbb{X} = 1$$

$$\mathbb{X}^3 x = 1 + \mathbb{X} + \mathbb{X}^2$$

$$\mathbb{X}^3 x = \mathbb{X}^{10}$$

$$x = \mathbb{X}^7$$

INCO2 Théorie d'information

mardi 04/10/2022

question chapitre

$$\mathbb{F}_2[x] = K_2(\mathbb{K})$$

$$\left| \begin{array}{l} x + x^{11}y = x^8 \\ x + x^6y = x^2 \end{array} \right. \rightarrow x + x^{10}y = x^7 \rightarrow x = x^7 + x^{10}y$$

$$x^3(x^7 + x^{10}y) + x^6y = x^2 \rightarrow x^{10} + x^{13}y + x^6y = x^2$$

$$y(x^6 + x^{13}) = x^2 + x^{10} \rightarrow y(x^3 + x^2 + x^3 + x^2 + 1) = x^2 + x^2 + x + 1$$

$$y = x+1 \mid \text{donc, } x = x^7 + x^{11} + x^{10} = x^3 + x + 1 + x^8 + x^2 + x + x^2 + x + 1$$

$$x = x$$

ordres et conjugués de $\beta = x^6$

$$\beta^5 = 1 \quad \beta^3 = x^{18} = x^3 \quad \text{l'ordre est } s=5$$

$$\beta^2 = x^{12}$$

$$\beta^5 = x^{15} = 1$$

$$\beta^{2^1} \quad \beta^4 = x^9 ; (\beta^2)^2 = (x^{12})^2 = x^{24} = x^{15+9} = x^{15} \cdot x^9 = 1 \cdot x^9 = x^9$$

$$\beta^8 = x^3 ; (\beta^4)^2 = (x^9)^2 = x^{18} = x^{15+3} = x^3$$

$$\beta^{16} = \beta = x^6 \quad (\beta^8)^2 = (x^3)^2 = x^6$$

Remarque

(I) Réviser concept

(II) Réviser l'équation ✓

IN202 Théorie d'information

mardi 04/10/2022

α^1	15	1 2 4 8	$x^4 + x + 1$	-
α^2	15	2 4 8 1	$x^4 + x + 1$	-
α^3	5	3 6 12 9	$x^4 + x^3 + x^2 + x + 1$	-
α^4	15	4 8 1 2	$x^4 + x + 1$	-
α^5	3	5 10	$x^2 + x + 1$	-
α^6	5	6 12 9 3	$x^4 + x^3 + x^2 + x + 1$	-
α^7	15	7 14 13 11	$x^4 + x^3 + 1$	-
α^8	15	8 1 2 4	$x^4 + x + 1$	-
α^9	5	9 3 6 12	$x^4 + x^3 + x^2 + x + 1$	-
α^{10}	3	10 5	$x^2 + x + 1$	-
α^{11}	15	11 7 14 13	$x^4 + x^3 + 1$	-
α^{12}	5	12 9 3 6	$x^4 + x^3 + x^2 + x + 1$	-
α^{13}	15	13 11 7 14	$x^4 + x^3 + 1$	-
α^{14}	15	14 13 11 7	$x^4 + x^3 + 1$	-
α^{15}	1	15	$x + 1$	-

ordre conjugués

polynôme

→ conjugués

$$\beta^{2^1} = \beta^{-0} = \beta^1 \rightarrow 2^0 \cdot 15 = 1$$

$$\beta^{2^2} = \beta^2 \quad 2^1 \cdot 15 = 2$$

$$\beta^{2^3} = \beta^4 \quad 2^2 \cdot 15 = 4$$

$$\beta^{2^4} = \beta^8 \quad 2^3 \cdot 15 = 8$$

$$\beta^{2^5} = \beta^{16} \quad 2^4 \cdot 15 = 1$$

$$\beta^{2^6} = \beta^{32} \quad 2^5 \cdot 15 = 2$$

$$\beta^{2^7} = \beta^{64} \quad 2^6 \cdot 15 = 4$$

$$\beta^{2^8} = \beta^{128} \quad 2^7 \cdot 15 = 8$$

$$\beta^{2^9} = \beta^{256} \quad 2^8 \cdot 15 = 16$$

$$\beta^{2^{10}} = \beta^{512} \quad 2^9 \cdot 15 = 32$$

$$\beta^{2^{11}} = \beta^{1024} \quad 2^{10} \cdot 15 = 64$$

$$\beta^{2^{12}} = \beta^{2048} \quad 2^{11} \cdot 15 = 128$$

$$\beta^{2^{13}} = \beta^{4096} \quad 2^{12} \cdot 15 = 256$$

$$\beta^{2^{14}} = \beta^{8192} \quad 2^{13} \cdot 15 = 512$$

$$\beta^{2^{15}} = \beta^{16384} \quad 2^{14} \cdot 15 = 1024$$

$$\beta^{2^{16}} = \beta^{32768} \quad 2^{15} \cdot 15 = 2048$$

$$\beta^{2^{17}} = \beta^{65536} \quad 2^{16} \cdot 15 = 4096$$

$$\beta^{2^{18}} = \beta^{131072} \quad 2^{17} \cdot 15 = 8192$$

$$\beta^{2^{19}} = \beta^{262144} \quad 2^{18} \cdot 15 = 16384$$

$$\beta^{2^{20}} = \beta^{524288} \quad 2^{19} \cdot 15 = 32768$$

$$\beta^{2^{21}} = \beta^{1048576} \quad 2^{20} \cdot 15 = 65536$$

$$\beta^{2^{22}} = \beta^{2097152} \quad 2^{21} \cdot 15 = 131072$$

$$\beta^{2^{23}} = \beta^{4194304} \quad 2^{22} \cdot 15 = 262144$$

$$\beta^{2^{24}} = \beta^{8388608} \quad 2^{23} \cdot 15 = 524288$$

$$\beta^{2^{25}} = \beta^{16777216} \quad 2^{24} \cdot 15 = 1048576$$

$$\beta^{2^{26}} = \beta^{33554432} \quad 2^{25} \cdot 15 = 2097152$$

$$\beta^{2^{27}} = \beta^{67108864} \quad 2^{26} \cdot 15 = 4194304$$

$$\beta^{2^{28}} = \beta^{134217728} \quad 2^{27} \cdot 15 = 8388608$$

$$\beta^{2^{29}} = \beta^{268435456} \quad 2^{28} \cdot 15 = 16777216$$

$$\beta^{2^{30}} = \beta^{536870912} \quad 2^{29} \cdot 15 = 33554432$$

$$\beta^{2^{31}} = \beta^{1073741824} \quad 2^{30} \cdot 15 = 67108864$$

$$\beta^{2^{32}} = \beta^{2147483648} \quad 2^{31} \cdot 15 = 134217728$$

$$\beta^{2^{33}} = \beta^{4294967296} \quad 2^{32} \cdot 15 = 268435456$$

$$\beta^{2^{34}} = \beta^{8589934592} \quad 2^{33} \cdot 15 = 536870912$$

$$\beta^{2^{35}} = \beta^{17179869184} \quad 2^{34} \cdot 15 = 1073741824$$

$$\beta^{2^{36}} = \beta^{34359738368} \quad 2^{35} \cdot 15 = 2147483648$$

$$\beta^{2^{37}} = \beta^{68719476736} \quad 2^{36} \cdot 15 = 4294967296$$

$$\beta^{2^{38}} = \beta^{137438953472} \quad 2^{37} \cdot 15 = 8589934592$$

$$\beta^{2^{39}} = \beta^{274877856944} \quad 2^{38} \cdot 15 = 17179869184$$

$$\beta^{2^{40}} = \beta^{549755713888} \quad 2^{39} \cdot 15 = 34359738368$$

$$\beta^{2^{41}} = \beta^{1099511427776} \quad 2^{40} \cdot 15 = 68719476736$$

$$\beta^{2^{42}} = \beta^{2199022855552} \quad 2^{41} \cdot 15 = 137438953472$$

$$\beta^{2^{43}} = \beta^{4398045711104} \quad 2^{42} \cdot 15 = 274877856944$$

$$\beta^{2^{44}} = \beta^{8796091422208} \quad 2^{43} \cdot 15 = 549755713888$$

$$\beta^{2^{45}} = \beta^{17592182844416} \quad 2^{44} \cdot 15 = 1099511427776$$

$$\beta^{2^{46}} = \beta^{35184365688832} \quad 2^{45} \cdot 15 = 2199022855552$$

$$\beta^{2^{47}} = \beta^{70368731377664} \quad 2^{46} \cdot 15 = 4398045711104$$

$$\beta^{2^{48}} = \beta^{140737462755328} \quad 2^{47} \cdot 15 = 8796091422208$$

$$\beta^{2^{49}} = \beta^{281474925510656} \quad 2^{48} \cdot 15 = 17592182844416$$

$$\beta^{2^{50}} = \beta^{562949851021312} \quad 2^{49} \cdot 15 = 35184365688832$$

$$\beta^{2^{51}} = \beta^{1125899702042624} \quad 2^{50} \cdot 15 = 70368731377664$$

$$\beta^{2^{52}} = \beta^{2251799404085248} \quad 2^{51} \cdot 15 = 140737462755328$$

$$\beta^{2^{53}} = \beta^{4503598808170496} \quad 2^{52} \cdot 15 = 281474925510656$$

$$\beta^{2^{54}} = \beta^{9007197616340992} \quad 2^{53} \cdot 15 = 562949851021312$$

$$\beta^{2^{55}} = \beta^{18014395232681984} \quad 2^{54} \cdot 15 = 1125899702042624$$

$$\beta^{2^{56}} = \beta^{36028790465363968} \quad 2^{55} \cdot 15 = 2251799404085248$$

$$\beta^{2^{57}} = \beta^{72057580930727936} \quad 2^{56} \cdot 15 = 4503598808170496$$

$$\beta^{2^{58}} = \beta^{144115161861455872} \quad 2^{57} \cdot 15 = 9007197616340992$$

$$\beta^{2^{59}} = \beta^{288230323722911744} \quad 2^{58} \cdot 15 = 18014395232681984$$

$$\beta^{2^{60}} = \beta^{576460647445823488} \quad 2^{59} \cdot 15 = 36028790465363968$$

$$\beta^{2^{61}} = \beta^{1152921294891646976} \quad 2^{60} \cdot 15 = 72057580930727936$$

$$\beta^{2^{62}} = \beta^{2305842589783293952} \quad 2^{61} \cdot 15 = 144115161861455872$$

$$\beta^{2^{63}} = \beta^{4611685179566597904} \quad 2^{62} \cdot 15 = 288230323722911744$$

$$\beta^{2^{64}} = \beta^{9223370359133195808} \quad 2^{63} \cdot 15 = 576460647445823488$$

$$\beta^{2^{65}} = \beta^{18446740718266391616} \quad 2^{64} \cdot 15 = 1152921294891646976$$

$$\beta^{2^{66}} = \beta^{36893481436532783232} \quad 2^{65} \cdot 15 = 2305842589783293952$$

$$\beta^{2^{67}} = \beta^{73786962873065566464} \quad 2^{66} \cdot 15 = 4611685179566597904$$

$$\beta^{2^{68}} = \beta{147573925746131132928} \quad 2^{67} \cdot 15 = 9223370359133195808$$

$$\beta^{2^{69}} = \beta{295147851492262265856} \quad 2^{68} \cdot 15 = 18446740718266391616$$

$$\beta^{2^{70}} = \beta{590295702984524531712} \quad 2^{69} \cdot 15 = 36893481436532783232$$

$$\beta^{2^{71}} = \beta{1180591405969049063424} \quad 2^{70} \cdot 15 = 73786962873065566464$$

$$\beta^{2^{72}} = \beta{2361182811938098126848} \quad 2^{71} \cdot 15 = 147573925746131132928$$

$$\beta^{2^{73}} = \beta{4722365623876196253696} \quad 2^{72} \cdot 15 = 295147851492262265856$$

$$\beta^{2^{74}} = \beta{9444731247752392507392} \quad 2^{73} \cdot 15 = 590295702984524531712$$

$$\beta^{2^{75}} = \beta{18889462495504785014784} \quad 2^{74} \cdot 15 = 1180591405969049063424$$

$$\beta^{2^{76}} = \beta{37778924991009570029568} \quad 2^{75} \cdot 15 = 2361182811938098126848$$

$$\beta^{2^{77}} = \beta{75557849982019140059136} \quad 2^{76} \cdot 15 = 4722365623876196253696$$

$$\beta^{2^{78}} = \beta{151115699964038280188272} \quad 2^{77} \cdot 15 = 9444731247752392507392$$

$$\beta^{2^{79}} = \beta{302231399928076560376544} \quad 2^{78} \cdot 15 = 18889462495504785014784$$

$$\beta^{2^{80}} = \beta{604462799856153120753088} \quad 2^{79} \cdot 15 = 37778924991009570029568$$

$$\beta^{2^{81}} = \beta{1208925599712306241506176} \quad 2^{80} \cdot 15 = 75557849982019140059136$$

$$\beta^{2^{82}} = \beta{2417851199424612483012352} \quad 2^{81} \cdot 15 = 151115699964038280188272$$

$$\beta^{2^{83}} = \beta{4835702398849224966024704} \quad 2^{82} \cdot 15 = 302231399928076560376544$$

$$\beta^{2^{84}} = \beta{9671404797698449932049408} \quad 2^{83} \cdot 15 = 604462799856153120753088$$

$$\beta^{2^{85}} = \beta{19342809595396899864098816} \quad 2^{84} \cdot 15 = 1208925599712306241506176$$

$$\beta^{2^{86}} = \beta{38685619190793799728197632} \quad 2^{85} \cdot 15 = 2417851199424612483012352$$

$$\beta^{2^{87}} = \beta{77371238381587599456395264} \quad 2^{86} \cdot 15 = 4835702398849224966024704$$

$$\beta^{2^{88}} = \beta{154742476763175198912780128} \quad 2^{87} \cdot 15 = 9671404797698449932049408$$

$$\beta^{2^{89}} = \beta{309484953526350397825560256} \quad 2^{88} \cdot 15 = 19342809595396899864098816$$

$$\beta^{2^{90}} = \beta{618969907052700795651120512} \quad 2^{89} \cdot 15 = 38685619190793799728197632$$

$$\beta^{2^{91}} = \beta{1237939814105401591302241024} \quad 2^{90} \cdot 15 = 77371238381587599456395264$$

$$\beta^{2^{92}} = \beta{2475879628210803182604482048} \quad 2^{91} \cdot 15 = 154742476763175198912780128$$

$$\beta^{2^{93}} = \beta{4951759256421606365208964096} \quad 2^{92} \cdot 15 = 309484953526350397825560256$$

$$\beta^{2^{94}} = \beta{9903518512843212730417928192} \quad 2^{93} \cdot 15 = 618969907052700795651120512$$

$$\beta^{2^{95}} = \beta{19807037025686425460835856384} \quad 2^{94} \cdot 15 = 1237939814105401591302241024$$

$$\beta^{2^{96}} = \beta{39614074051372850921671712768} \quad 2^{95} \cdot 15 = 2475879628210803182604482048$$

$$\beta^{2^{97}} = \beta{79228148102745701843343425536} \quad 2^{96} \cdot 15 = 4951759256421606365208964096$$

$$\beta^{2^{98}} = \beta{158456296205491403686686851072} \quad 2^{97} \cdot 15 = 9903518512843212730417928192$$

$$\beta^{2^{99}} = \beta{316912592410982807373373702144} \quad 2^{98} \cdot 15 = 19807037025686425460835856384$$

$$\beta^{2^{100}} = \beta{633825184821965614746747404288} \quad 2^{99} \cdot 15 = 39614074051372850921671712768$$

$$\beta^{2^{101}} = \beta{1267650369643931229493494808576} \quad 2^{100} \cdot 15 = 79228148102745701843343425536$$

$$\beta^{2^{102}} = \beta{2535300739287862458986989617152} \quad 2^{101} \cdot 15 = 158456296205491403686686851072$$

$$\beta^{2^{103}} = \beta{5070601478575724917973979234304} \quad 2^{102} \cdot 15 = 316912592410982807373373702144$$

$$\beta^{2^{104}} = \beta{1014120295715144983594795846864} \quad 2^{103} \cdot 15 = 633825184821965614746747404288$$

$$\beta^{2^{105}} = \beta{2028240591430289967189591693728} \quad 2^{104} \cdot 15 = 1267650369643931229493494808576$$

$$\beta^{2^{106}} = \beta{4056481182860579934379183387456} \quad 2^{105} \cdot 15 = 2535300739287862458986989617152$$

$$\beta^{2^{107}} = \beta{8112962365721159868758366774912} \quad 2^{106} \cdot 15 = 5070601478575724917973979234304$$

$$\beta^{2^{108}} = \beta{1622592473144231973751673354984} \quad 2^{107} \cdot 15 = 1014120295715144983594795846864$$
</

IN202 théorie d'information

mercredi 05/10/2022

Révisiondissimilité (divergence de KL) (discrete)définition

$$D(p||q) = \mathbb{E}_p \log_2 \left(\frac{p(x)}{q(x)} \right) = \sum_{i=1}^{N_x} p(x_i) \log_2 \left(\frac{p(x_i)}{q(x_i)} \right) \text{ a)$$

$p(X)$ et $q(X)$ sont des lois de probabilité définies sur la même variable aléatoire X

propriété $D(p||q) \geq 0$ et $D(p||q) = 0 \Leftrightarrow p(x) = q(x)$

quantité d'information (incertitude) (discrete)

1er postulat de Shannon

$$h(X=x) = h(x) = \log_2 \left(\frac{1}{p(x)} \right)$$

2^e de

1^{er} incertitude est inversement proportionnelle

à simplification

de la situation

p(x=x)

2^e incertitude de la réalisation de deux événements indépendants est la somme d'incertitude

entropie (discrete)

$$H(X) = \mathbb{E}_p h(x=x) = \sum_{i=1}^{N_x} p(x=x_i) \cdot h(x=x_i) = \sum_{i=1}^{N_x} p(x_i) \log_2 \left(\frac{1}{p(x_i)} \right)$$

incertitude moyenne portée par les éléments

propriété l'entropie d'une somme discrète est maximum lorsque les probabilités sont équiprobables

$$H(X, Y) = H(X) + H(Y) \quad \text{quand variables indépendantes}$$

$$H(X|Y) = H(X) \quad \text{démonstration avec propriété de probabilité}$$

/ / IN202 Théorie d'information

mercredi 05/10/2022

RévisionProbabilités

$$p(x=x_i | y=y_j) = p(x=x_i, y=y_j) / p(y=y_j)$$

→ x_i, y_j indépendants

probabilité conjointe $p(x_i, y_j) = p(x_i) \cdot p(y_j)$

probabilité conditionnelle, probabilité a posteriori

Information mutuelle (discrete)

$$I(X, Y) = \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} p(x_i, y_j) \cdot I(x_i, y_j) \quad \text{et} \quad I(x_i, y_j) = \log_2 \left(p(x_i, y_j) / p(x_i) \cdot p(y_j) \right)$$

$$I(X, Y) = I(Y, X) \text{ symétrique et } \geq 0 \text{ par définition}$$

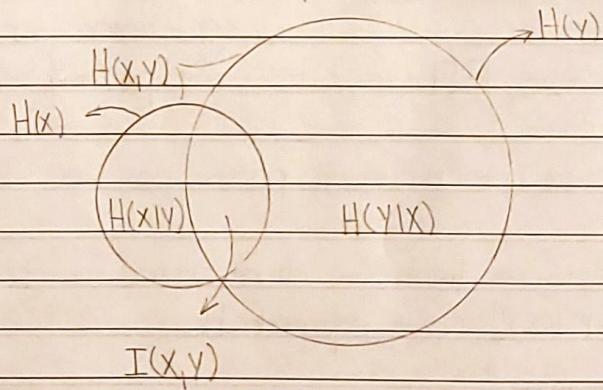
$$I(X, Y) = 0 \Leftrightarrow X \text{ et } Y \text{ indépendants}$$

$$I(X, Y) = \mathbb{E}[\log_2(p(x_i, y_j) / p(x_i) \cdot p(y_j))] = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

→ définition avec espérance

$$H(X, Y) = H(X) + H(Y) - I(X, Y) \text{ démonstration avec l'espérance}$$

$$H(X, Y) = H(X) + H(Y|X)$$

Interprétation visuelle

INFO: théorie de l'information

jeudi 09/10/2022

divergence de KL (continue)

$$D(p||q) = \mathbb{E}[\log_2(p(x)/q(x))] = \int_{\mathcal{D}x} p(x) \cdot \log_2(p(x)/q(x)) dx$$

entropie (continue)

$$H(x) = \mathbb{E}[h(x)] = \int_{\mathcal{D}x} p(x) \cdot \log_2(1/p(x)) dx$$

$$H(x,y) = \mathbb{E}[h(x,y)] = \int_{\mathcal{D}x} \int_{\mathcal{D}y} p(x,y) \cdot \log_2(1/p(x,y)) dx dy$$

$$H(x|y) = \mathbb{E}[h(x|y)] = \int_{\mathcal{D}x} \int_{\mathcal{D}y} p(x,y) \cdot \log_2(1/p(x|y)) dx dy$$

information mutuelle (continue)

$$I(X,Y) = \mathbb{E}[i(x,y)] = \int_{\mathcal{D}x} \int_{\mathcal{D}y} p(x,y) \cdot \log_2(p(x,y)/(p(x) \cdot p(y))) dx dy$$

les mêmes propriétés sont valides

$$p(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \exp(-(x-\mu)^2/2\sigma^2)$$

exercices du chapitre: codes correcteurs algébriques

mardi 11/10/2022

exercice 1

$$x^5 + x^2 + 1$$

IC202 Théorie d'information

mardi 11/10/2022

exercice du chapitre : codes correcteurs algébriques

mard. bimise	Réprésentation polynomiale	x^i	i
1		0	
x	c'est à cause du polynôme	1	
x^2	IRREDUCTIBLE donne	2	
x^3	$x^5 + x^2 + 1 = 0$ dm.	3	
x^4	$x^5 = x^2 + 1$	4	
$x^2 + 1$	plus info page 50	5	
$x^3 + x$		6	
$x^4 + x^2$		7	
$x^3 + x^2 + 1$		8	
$x^4 + x^3 + x$		9	
$x^4 + 1$ ($(x^4 + x^2 + x^2 + 1)$)		10	
$x^2 + x + 1$		11	
$x^3 + x^2 + x$		12	
$x^4 + x^3 + x^2$		13	
$x^4 + x^3 + x^2 + 1$		14	
$x^4 + x^3 + x^2 + x + 1$		15	
$x^4 + x^3 + x + 1$		16	
$x^4 + x + 1$		17	
$x + 1$		18	
$x^2 + x$		19	
$x^3 + x^2$		20	
$x^4 + x^3$		21	
$x^4 + x^2 + 1$		22	
$x^3 + x^2 + x + 1$		23	
$x^4 + x^3 + x^2 + x$		24	
$x^4 + x^3 + 1$		25	
$x^4 + x^2 + x + 1$		26	
$x^3 + x + 1$		27	
$x^4 + x^2 + x$		28	
$x^3 + 1$		29	
$x^4 + x$		30	
1		31	

10202 théorie d'unicarac.

mardi 11/10/2011

exercice du chapitre: corps caractéres algébriques

exercice 1:

calculer le polynôme irréductible

on a donné $x^5+x^2+1=0$ et donc $x^5=x^2+1$

compléter le tableau de division euclidien pour le corps de galois

après la trouille, si dans ce cas, il devrait rentrer à 1

pour corriger 2 erreurs $\rho = (n-1)/2 \rightarrow n=7\rho+1=51$

après on fait l'égalité avec les polynômes

 $(x, x^2, x^4, x^8, x^{16})$ chaque polynôme est élevé au carré $(x^3, x^6, x^{12}, x^{24}, x^{48})$ (1) comment choisir le premier $(x^5, x^{10}, x^{20}, x^9, x^{18})$ (1) choisir le deuxième élément différencié à partir $(x^7, x^{14}, x^{28}, x^{25}, x^{50})$ de la liste $(x^{11}, x^{22}, x^{13}, x^{26}, x^{21})$ (2) le premier sera le carré du précédent (carré) $(x^{15}, x^{30}, x^{29}, x^{27}, x^{23})$ il y a n puissances où $2^n=31$ dans ce cas
l'écriture 16/10/2011puissances de x

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ...

 $x^2; x^4; x^8; x^{16}$ puissances de x restant

3 5 6 7 9 10 11 12 13 14 15 17 18 19 20 21

 $x^3; x^6; x^{12}; x^{24}; x^{48}$ puissances de x restant

5 7 9 10 11 13 14 15 16 18 19 20 21 22 23 25

IC202 Théorie information

exercices du chapitre introduction aux codes algébriques
après il faut déterminer les polynômes pour chaque groupe

2/ 7 2

$$\text{ordre de } G \quad \text{et } n = 6 = 1$$

En 1, l'ordre est un diviseur de $6 = p-1$

6

$$q = p^2$$

2

$$G^1 = 6 \neq 1$$

$$p-1 = 6$$

$$6^2 - 36 = 36 + 1 = 1 [7]$$

7x5 : ordre 2

 $(1, 2, 3, 6)$

$$S^1 = S \neq S$$

$$S^2 = 2S = 4 [7] \neq 1$$

$$S^3 = 12S = 6 \neq 1$$

$$S^2 \times S = 4 \times S = 20 = 6 [7]$$

$$S^4 = S^3 \quad S^3 = 6 \times 6 - 36 = 1 [7]$$

ICP02 Théorie d'Information

Vendredi 21/10/2022

exercices du chapitreexercice 2.

$(x^1, x^2, x^4, x^8, x^{15})$ c'est quoi les polynômes génératrices ?

$(x^3, x^6, x^{12}, x^{24}, x^{17})$

$(x^5, x^{10}, x^{20}, x^9, x^{18})$

$(x^7, x^{14}, x^{28}, x^{25}, x^{19})$

$(x^{11}, x^{22}, x^{13}, x^{26}, x^{21})$

$(x^{15}, x^{30}, x^{29}, x^{27}, x^{23})$

$$f_1(x) = (x - x^1)(x - x^2)(x - x^4)(x - x^8)(x - x^{15}) \Rightarrow$$

$$f_2(x) = (x - x^3)(x - x^6)(x - x^{12})(x - x^{24})(x - x^{17}) \Rightarrow$$

$$f_3(x) = (x - x^5)(x - x^{10})(x - x^{20})(x - x^9)(x - x^{18}) \Rightarrow$$

$$f_4(x) = (x - x^7)(x - x^{14})(x - x^{22})(x - x^{25})(x - x^{19}) \Rightarrow$$

$$f_5(x) = (x - x^{11})(x - x^{22})(x - x^{13})(x - x^{26})(x - x^{21}) \Rightarrow$$

$$f_6(x) = (x - x^{15})(x - x^{20})(x - x^{29})(x - x^{27})(x - x^{23}) \Rightarrow$$

Il faut développer les polynômes : (ensuite)

$f_1(x) :$

$$(x^2 - x^2x - x^3x + x^9)(x^2 - x^8x - x^4x + x^{12})(x - x^{15})$$

$$(x^4 - x^8x^3 - x^4x^3 + x^{12}x^2 - x^2x^3 + x^{10}x^2 + x^6x^2 - x^{14}x - x^3x^3 + x^{11}x^2 + x^7x^2 - x^{15}x + x^9x^2 - x^{17}x - x^{13}x + x^{21})(x - x^{15})$$

$$(x^4 + (x^8 + x^4 + x^2 + x^3)x^3 + (x^{12} + x^{10} + x^6 + x^{11} + x^7 + x^9)x^2 + (x^{14} + x^{15} + x^{13} + x^{17})x + x^{21})(x - x^{15})$$

$$(x^4 + (x^4 + 1)x^3 + (x^4 + x^3 + x^2)x^2 + (x^3 + x^2 + 1)x + x^{-1})(x - x^{15})$$

$$x + x^2 + x^4 + x^8 + x^9 + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20}$$

$$x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20}$$

IC200 Théorie de l'information

lundi 24/10/2022

exercices du chapitre: codes algébriquesexercice 1.

les éléments du corps de Galois engendré pour le polynôme $x^5 + x^2 + 1$ sont représentés dans le livre il faut développer les binaires comme décrit:

$\rightarrow K=5$, puissance du K
d'abord on note que $x^2 + 1 = x^5 \Rightarrow K^5 = K^2 + 1$ condition du cycle
après on développe les $n=2^K - 1$ équations, $n=31$.

i) équation K code binaire

0	1	10000	16	$x^4 + x^3 + x + 1$	11011
1	x	01000	17	$x^4 + x + 1$	11001
2	x^2	00100	18	$x + 1$	11000
3	x^3	00010	19	$x^2 + x$	01100
4	x^4	00001	20	$x^3 + x^2$	00110
5	$x^2 + 1$	10100	21	$x^4 + x^3$	00011
6	$x^3 + x$	01010	22	$x^4 + x^2 + 1$	10101
7	$x^4 + x^2$	00101	23	$x^3 + x^2 + x + 1$	11110
8	$x^3 + x^2 + 1$	10110	24	$x^4 + x^3 + x^2 + x$	01111
9	$x^4 + x^3 + x$	01011	25	$x^4 + x^3 + 1$	10011
10	$x^4 + 1$	10001	26	$x^4 + x^2 + x + 1$	11101
11	$x^2 + x + 1$	11100	27	$x^3 + x + 1$	11010
12	$x^3 + x^2 + x$	01110	28	$x^4 + x^2 + x$	01101
13	$x^4 + x^3 + x^2$	00111	29	$x^3 + 1$	10010
14	$x^4 + x^3 + x^2 + 1$	10111	30	$x^4 + x$	01001
15	$x^4 + x^3 + x^2 + x + 1$	11111	31	1	1000

↓
Lsb MSB

exercice 1

on désire corriger 2 erreurs donc $e=2$

$$e = (d_{\min} - 1)/2 \Rightarrow d_{\min} \geq 5 \text{ (nombre de mots ronds)}$$

de cette façon la $T=2$ donc $(x^2)^T = x^4$ sera la puissance maximale de ce code.

montaremos

spiral Seleccionaremos polinomios cuyo grado do primero for menor ou igual a $(x^2)^T$

Propriétés de l'infinité

lundi 24/10/2022

exercices du chapitre : codes algébriques

exercice 1

les conjugués sont les puissances de alpha (α^j) avec le 10, ($k-11$) et on commence avec α^2

$$(\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16})$$

après on choisit la prochaine puissance de alpha que n'a pas apparaître, la plus petit, que dans ce cas sera α^3

$$(\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} \xrightarrow{\text{Rappeler du module}} \alpha^{17})$$

on répète jusqu'à les puissances de α sont finis

$$\begin{array}{|c|c|c|c|c|} \hline & \alpha^5 & \alpha^{10} & \alpha^{20} & \alpha^9 & \alpha^{18} \\ \hline & \alpha^7 & \alpha^{14} & \alpha^{28} & \alpha^{25} & \alpha^{19} \\ \hline & \alpha^{11} & \alpha^{22} & \alpha^{13} & \alpha^{26} & \alpha^{21} \\ \hline & \alpha^{15} & \alpha^{30} & \alpha^{29} & \alpha^{27} & \alpha^{23} \\ \hline \end{array}$$

pour chaque séquence de conjugués on aura une polynôme minimale à une variable définie comme

$$P_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})$$

on pourraient multiplier avec l'expansion du corde mais c'est pénible. on peut le décomposer avec le codage binaire

la puissance 1e du ensemble de conjugués

$$P_1(x) = x^5 + bx^4 + cx^3 + dx^2 + ex + 1$$

$$P_1(\alpha) = \alpha^5 + b\alpha^4 + c\alpha^3 + d\alpha^2 + e\alpha + 1$$

MSB →	[0]	[1]	[0]	[0]	[0]	[0]	[b]	donc
	0	0	1	0	0	0	c	$b=0$
	1	+b	0	+c	0	+d	1	$c=0$
	0	0	0	0	1	0	e	$d=1$
LSB →	1	0	0	0	0	1	0	$e=1$

10202 Théorie d'information

lundi 24/10/2022

exercices du chapitre: codes algébriques

exercice 1

de la façon là, on a $P_1(x) = x^5 + 1x^2 + 1$ après on repete avec le deuxième ensemble de conjugués
la puissance

$$P_3(x) = (x - \alpha^5)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{17})$$

$$P_3(x) = x^5 + bx^4 + cx^3 + dx^2 + ex + 1$$

$$P_3(\alpha^3) = \alpha^{15} + b\alpha^{12} + c\alpha^9 + d\alpha^6 + e\alpha^3 + 1$$

MSB	1	0	1	0	0	0	1+c
	1	1	1	1	1	0	1+b+c+d+e
	1+b	1+c	0+d	0+e	0+	0	= 1+b
	1	1	1	1	0	0	1+b+c+d
LSB	1	0	0	0	0	1	0

donc $c=1$; $b=1$; $d=1$; $e=0$ donc $P_3(x) = x^5 + 1x^4 + 1x^3 + 1x^2 + 1$ → décoder como $(\alpha^2)^4 = \alpha^8$ operar oaprès il faut découvrir $g(x) = P_1(x) \cdot P_3(x)$ grupo de conjugués de α e α^3
foi selecionado, onto contrário o

$$\begin{aligned} g(x) &= (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1) \quad \text{decoder possuiria mais primôrios} \\ &= x^{10} + x^9 + x^8 + x^7 + x^5 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \\ &= x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1 \end{aligned}$$

degree de g avec $g(x)$ on peut découvrir l'ensemble de comment codage
de corps de Galois: $\hookrightarrow \neq \rightarrow$ (problème de définition)

$$d^o g = n - K \Rightarrow 10 = (2^k - 1) - K = 31 - K \Rightarrow K = 21 \quad \text{donc}$$

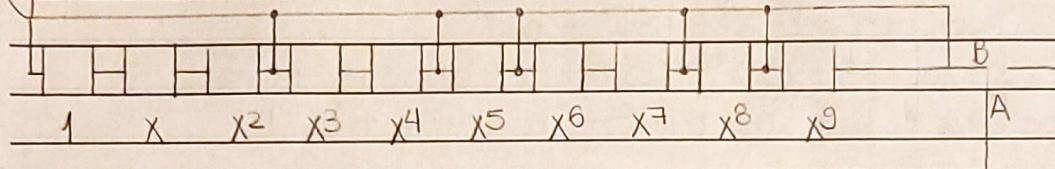
 $K=21$ longueur avant codage $n=31$ longueur après codage

IC202 Théorie d'information

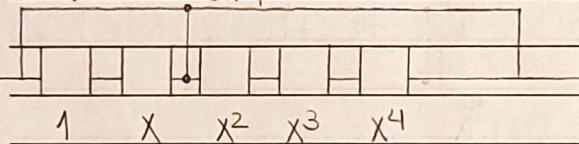
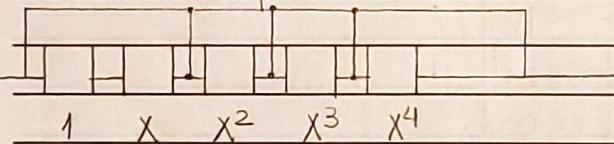
lundi 24/10/2022

exercices du chapitre: codes algébriques

exercice 1

 $g(x)$ 

Requ

 $P_1(x)$ diviseur pour $x^5 + x^2 + 1$  $P_3(x)$ diviseur pour $x^5 + x^4 + x^3 + x^2 + 1$ on note que $g(x) = P_1(x) \cdot P_3(x) = (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1)$ $P_1(x)$ représente les conjugués $x^1, x^2, x^4, x^8, x^{16}$

utilisés pour construire le circuit de détection d'erreurs

 $P_3(x)$ représente les conjugués $x^3, x^6, x^{12}, x^{24}, x^{17}$ on note que $d^\circ P_1(x) = d^\circ P_3(x) = 5$ donc les syndromes auront la forme suivanteSi: $x \rightarrow w^i = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 \quad \forall i = \{1, 2, 4, 8, 16\}$ degrés des conjugués de $P_1(x)$ Si: $x \rightarrow w^j = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 \quad \forall j = \{3, 6, 12, 24, 17\}$ degrés des conjugués de $P_3(x)$
dans ce cas Si = Sj parce que $d^\circ P_1(x) = d^\circ P_3(x)$
mais on separe pour bi généralisation

IC202 Théorie d'information

mardi 25/10/2022

donc

$$S_1: x = x^1 : b_0 + b_1 \cdot x + b_2 x^2 + b_3 x^3 + b_4 x^4$$

$$P_1(x)$$

$$S_2: x = x^2 : b_0 + b_1 x^2 + b_2 x^4 + b_3 x^6 + b_4 x^8$$

$$P_2(x) \quad b_0 + b_1 x^2 + b_2 x^4 + b_3 (x^3 + x) + b_4 (x^3 + x^2 + 1)$$

$$(b_0 + b_4) + b_3 x + (b_1 + b_4) x^2 + (b_3 + b_4) x^3 + b_2 x^4$$

$$S_3: x = x^3 : b_0 + b_1 x^3 + b_2 x^6 + b_3 x^9 + b_4 x^{12}$$

$$P_3(x) \quad b_0 + b_1 x^3 + b_2 (x^3 + x) + b_3 (x^4 + x^3 + x) + b_4 (x^3 + x^2 + x)$$

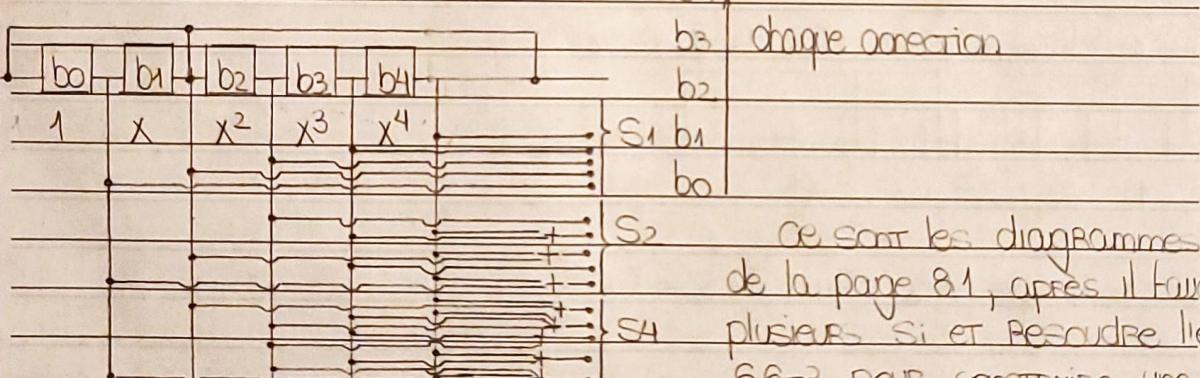
$$b_0 + (b_2 + b_3 + b_4) x + (b_4) x^2 + (b_1 + b_2 + b_3 + b_4) x^3 + b_3 x^4$$

$$S_4: x = x^4 : b_0 + b_1 x^4 + b_2 x^8 + b_3 x^{12} + b_4 x^{16}$$

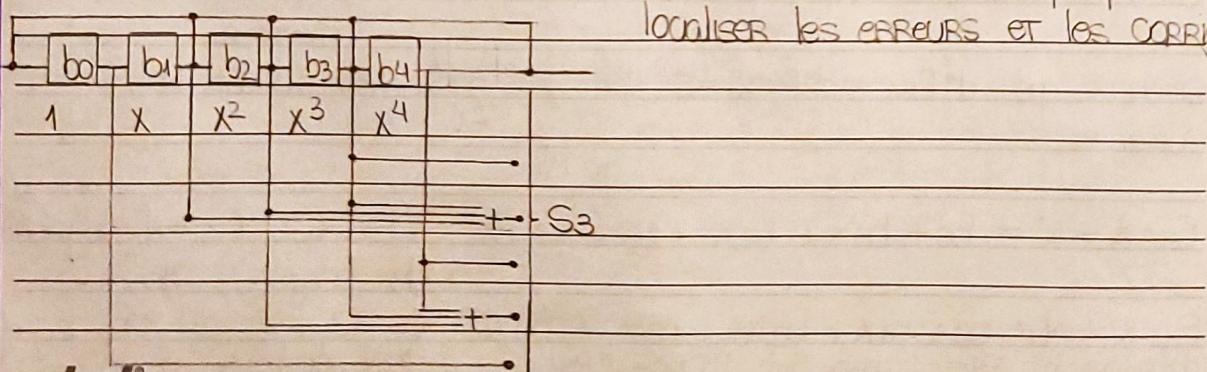
$$P_4(x) \quad b_0 + b_1 x^4 + b_2 (x^3 + x^2 + 1) + b_3 (x^3 + x^2 + x) + b_4 (x^4 + x^3 + x + 1)$$

$$(b_0 + b_2 + b_4) + (b_3 + b_4) x + (b_2 + b_3) x^2 + (b_2 + b_3 + b_4) x^3 + (b_1 + b_4)$$

$$P_1(x)$$



$$P_2(x)$$



IC202 Théorie d'information

mardi 25/10/2022

exercices du chapitre: codes correcteurs algébriquesexercice 2

G(8): corps de Galois à 8 éléments, pour ça il faut trouver les polynomes minimales nécessaires pour construire le corps

du tableau après BCH de la page 86 on a
 $(n, k, t) = (7, 4, 1)$ code par $g(x) \equiv 13 = (001)(011) = (x+1)$
 $= 01101 = x^3 + x^2 + 1$

du exemple de la page 70

$$x^7 - 1 = (x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

$$x^4 x^3 x^2 x^1$$

donc $x^3 + x^2 + 1$ sera l'élément minimal

$$x^3 + x^2 + 1 \Rightarrow x^3 + x^2 + 1 = 0 \Rightarrow x^3 = x^2 + 1$$

LSB MSB

0	1	1	100	dans le code considéré le code corrigé $r=1$
1	x	x	010	erreurs dans, $e = (d_{\min} - 1)b \Rightarrow d_{\min} \geq 3$
2	x^2	x^2	001	
3	x^3	$x^2 + 1$	101	de cette façon $t=1$ donc $(x^2)^T = x^2$ c'est
4	x^4	$x^2 + x + 1$	111	la puissance maximale de la charge
5	x^5	$x + 1$	110	
6	x^6	$x^2 + x$	011	dans, $g(x) = P_1(x) = x^3 + x^2 + 1$
7	x^7	1	100	$d_{\text{cor}} = n - k \Rightarrow k = 4$ longueur avant codage $n = 7$ longueur après codage

contenus: $i \in \{0, (k-1)\} = \{0, 2\}$

(x, x^2, x^4) modulo 7

(x^3, x^6, x^5)

polynomes associés

$$P_1(x) = (x-0)(x-x^2)(x-x^4)$$

$$P_2(x) = (x-x^3)(x-x^6)(x-x^5)$$

1G202 Théorie d'information

mardi 25/10/2022

$$P_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) \Rightarrow P_1(x) = x^3 + x^2 + 1$$

$$P_1(x) = x^3 + b_2 x^2 + b_1 x + 1$$

$$P_1(\alpha) = \alpha^3 + b_2 \alpha^2 + b_1 \alpha + 1$$

$$\begin{array}{c|cccc} \text{MSB} & [1] & [1] & [0] & [0] \\ & = [0+b_2] & [0+b_1] & [1+] & [0] \\ \text{LSB} & [1] & [0] & [0] & [1] \\ & & & & [0] \end{array} = 0 \Rightarrow b_1 = 0, b_2 = 1$$

$$P_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) \Rightarrow P_2(x) = x^3 + x + 1$$

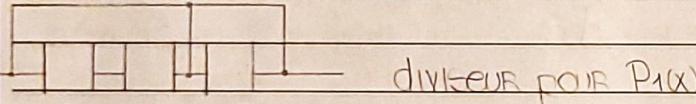
$$P_2(x) = x^3 + b_2 x^2 + b_1 x + 1$$

$$P_2(\alpha^3) = \alpha^9 + b_2 \alpha^6 + b_1 \alpha^3 + 1$$

$$\begin{array}{c|cccc} \text{MSB} & [1] & [1] & [1] & [0] \\ & = [0+b_2] & [1+b_1] & [0+] & [0] \\ \text{LSB} & [0] & [0] & [1] & [1] \\ & & & & [b_1+1] \end{array} = 0 \Rightarrow b_1 = 1, b_2 = 0$$

 $\hookrightarrow i \in \{1, 2, 4\}$

$$\text{Si } x = \alpha^i : b_0 + b_1 x + b_2 x^2$$



$$1 \quad x \quad x^2$$

$$\alpha^1: b_0 + b_1 \alpha + b_2 \alpha^2$$

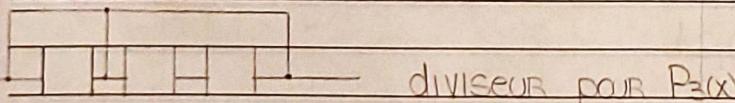
$$\alpha^2: b_0 + b_1 \alpha^2 + b_2 \alpha^4$$

$$\alpha^3: b_0 + b_1 \alpha^3 + b_2 (\alpha^2 + \alpha + 1)$$

$$(b_0 + b_2) + b_2 \alpha + (b_1 + b_2) \alpha^2$$

 $\hookrightarrow j \in \{3, 6, 5\}$

$$\text{Si } x = \alpha^j : b_0 + b_1 x + b_2 x^2$$



$$1 \quad x \quad x^2$$

$$\alpha^3: b_0 + b_1 \alpha^3 + b_2 \alpha^6$$

$$\alpha^4: b_0 + b_1 (\alpha^2 + 1) + b_2 (\alpha^2 + \alpha)$$

$$(b_0 + b_1) + b_2 \alpha + (b_1 + b_2) \alpha^2$$