Exercice 8: Soit $p = \frac{1}{1000}$ la probabilité qu'un bit soit transmis érronément.

(a) Quelle est la probabilité d'avoir exactement deux bits fautifs lors de la transmission de sept bits,

comme lors de la transmission d'un mot de code de Hamming $C(7,4)$?

(b) Quelle est la probabilité d'avoir plus d'une erreur lors de la transmission de sept bits ?

(c) Plutôt que le code de Hamming, on transmet un code en le répétant trois fois. On décode à la majorité. Calculer la probabilité qu'on décode correctement le bit envoyé.

(d) On transmet quatre bits en répétant chacun trois fois. Quelle est la probabilité que les quatre bits soient décodés correctement ?

Sol : (a) $\mathbb{P}(\{\text{exactement deux erreurs}\})$

$$= \binom{7}{2}\left(\frac{1}{1000}\right)^2\left(1-\frac{1}{1000}\right)^5$$

(b) $\mathbb{P}(\{\text{Aucune erreur}\}) = \left(1-\frac{1}{1000}\right)^7$

$$\mathbb{P}(\{\text{exactement une erreur}\}) = \binom{7}{1}\left(\frac{1}{1000}\right)^1\left(1-\frac{1}{1000}\right)^6$$

$$\Rightarrow \mathbb{P}(\{\text{plus d'une erreur}\}) = 1-\left(1-\frac{1}{1000}\right)^7-\binom{7}{1}\left(\frac{1}{1000}\right)^1\left(1-\frac{1}{1000}\right)^6$$

(c) On le décode correctement s'il y a 0 ou exact une erreur, donc $\mathbb{P}(\{\text{bien décoder}\})$

$$= \mathbb{P}(\{\text{aucune erreur}\}) + \mathbb{P}(\{\text{exactement une erreur}\})$$

$$= \left(1 - \frac{1}{1000}\right)^3 + \binom{3}{1}\left(\frac{1}{1000}\right)^1 \left(1 - \frac{1}{1000}\right)^2$$

(d) $\mathbb{P}(\{\text{bien décoder}\}) = \left(\left(1 - \frac{1}{1000}\right)^3 + \binom{3}{1}\left(\frac{1}{1000}\right)^1 \left(1 - \frac{1}{1000}\right)^2\right)^4$

TP9 28 mars 2025

Section 8.6

Exercice 1: Montrer que, si on génère une suite de bits indépendants et si on les regroupe par blocs de longueur r, lesquels représentent l'expression binaires (de gauche à droite) de nombres entiers de $S = \{0, 1, \dots, 2^{r-1}\}$, alors chaque entier apparaît en moyenne un fois sur 2^r.

Sol: Soit $a \in S$ et X la variable aléatoire représentant le nombre de blocs de longueur r à faire avant que a soit formé.

Comme $\mathbb{P}(\{a \text{ est formé}\}) = \frac{1}{2^r}$, on a que $X \sim \text{Géo}(\frac{1}{2^r})$.

On a donc $E[X] = 2^r$, ce qui veut dire qu'il faut, en moyenne, former 2^r blocs de longueur r pour que a apparaisse, donc a apparait en moyenne une fois sur 2^r.

Exercice 2: Le générateur linéaire congruentiel génère des nombres de $E = \{1, \dots, p-1\}$ par la règle $x_n = a x_{n-1} \pmod p$, où p est premier et a est tel que $\begin{cases} a^k \not\equiv 1 \pmod p, \ 0 < k < p-1 \\ a^{p-1} \equiv 1 \pmod p \end{cases}$

(a) Soit $p = 11$. Trouver les racines primitives de $\mathbb{F}_{11}$. (Il y en a 4)

Sol(a): Rappel: Théorème de Lagrange: Pour tout groupe fini G et tout sous-groupe H de G, l'ordre de H divise l'ordre de G: $|H|/|G|$.

Une racine primitive est un nombre $r \in E$ qui respecte les contraintes du nombre a de l'énoncé. On veut donc que r génère tous les éléments de E lorsqu'on le multiplie par lui-même. Comme $|E| = 10$, on doit seulement vérifier que $r^2, r^5 \not\equiv 1 \pmod{11}$ pour dire que r est une racine primitive de $\mathbb{F}_{11}$, par le

théorème de Lagrange.

On teste tous les éléments de E (sauf 1).

$2^2 = 4 \not\equiv 1 \pmod{11}$, $2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11}$

$\Rightarrow$ 2 est une racine primitive

$3^2 = 9 \not\equiv 1 \pmod{11}$, $3^5 = (3^2)^2 \cdot 3 = 9^2 \cdot 3 \equiv (-2)^2 \cdot 3 \pmod{11}$

$\equiv 4 \cdot 3 \pmod{11}$

$\equiv 1 \pmod{11}$

$\Rightarrow$ 3 n'est pas une racine primitive

$4^2 = 16 \equiv 5 \pmod{11}$, $4^5 = 4^2 \cdot 4^2 \cdot 4 \equiv 5 \cdot 5 \cdot 4 \pmod{11}$

$\not\equiv 1 \pmod{11}$ $\equiv 1 \pmod{11}$

$\Rightarrow$ 4 n'est pas une racine primitive

$5^2 = 25 \equiv 3 \pmod{11}$, $5^5 = 5^2 5^2 5 \equiv 3 \cdot 3 \cdot 5 \pmod{11}$

$\not\equiv 1 \pmod{11}$ $\equiv 1 \pmod{11}$

$\Rightarrow$ 5 n'est pas une racine primitive

$6^2 = 36 \equiv 3 \pmod{11}$, $6^5 = 6^2 6^2 6 \equiv 3 \cdot 3 \cdot 6 \pmod{11}$

$\not\equiv 1 \pmod{11}$ $\equiv 3 \cdot 3 \cdot (-5) \pmod{11}$

$\equiv -1 \pmod{11}$

$\not\equiv 1 \pmod{11}$

$\Rightarrow$ 6 est une racine primitive

$7^2 = 49 \equiv 5 \pmod{11}$, $7^5 = 7^2 \cdot 7^2 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \pmod{11}$

$\not\equiv 1 \pmod{11}$ $\equiv 3 \cdot 7 \pmod{11}$

$\equiv 10 \pmod{11}$

$\not\equiv 1 \pmod{11}$

$\Rightarrow$ 7 est une racine primitive

$8^2 = 64 \equiv 9 \pmod{11}$, $8^5 = 8^2 \cdot 8^2 \cdot 8 \equiv 9 \cdot 9 \cdot 8 \pmod{11}$

$\not\equiv 1 \pmod{11}$ $\equiv 32 \pmod{11}$

$\equiv 10 \pmod{11}$

$\not\equiv 1 \pmod{11}$

$\Rightarrow$ 8 est une racine primitive

$\Rightarrow$ 2, 6, 7, 8 sont les 4 racines primitives de $\mathbb{F}_{11}$.

(b) Montrer que, quel que soit $x_0 \in E$, ce générateur produit une suite périodique de période exactement $p-1$.

Sol (b) : Soit a une racine primitive et $x_0 \in E$.

Comme a est une racine primitive de $\mathbb{F}_p$, on a que $\exists n \in \{1,2,\dots,p-1\}$ tel que $a^n \equiv x_0 \pmod p$

Ainsi, on a $x_1 = a \cdot x_0 \equiv a^{n+1} \pmod p$

Comme $|a| = p-1$, ce générateur produit une suite périodique de période exactement $p-1$.

Exercice 5 : On considère un registre à décalage (c-à-d un générateur $\mathbb{F}_2$-linéaire) de coefficients $(q_0, q_1, q_2, q_3) = (1,0,0,1)$ et les conditions initiales $(a_0, a_1, a_2, a_3) = (0,0,0,1)$. Vérifier que la suite générée est périodique de période 15, mais qu'elle n'est pas celle de l'exemple 8.4.

Sol : On obtient la suite

000111101011001000111 10...

qui est de période 15 et différente de celle de l'exemple. (Si vous n'arrivez pas à générer la suite, venez me voir durant mes dispos ou écrivez-moi un courriel ☺)

Exercice 6: Montrer que le polynôme $x^4+x^3+x^2+x+1$ est irréductible (pas besoin de le montrer), mais n'est pas primitif sur $\mathbb{F}_2$. Vérifier d'autre part que, si on prend $(q_0, q_1, q_2, q_3) = (1,1,1,1)$ comme coefficients d'un registre à décalage, alors aucune suite générée par le registre à décalage n'est de période 15.

Sol: Montrons que $x^4+x^3+x^2+x+1 = Q(x)$ n'est pas primitif sur $\mathbb{F}_2$.

Comme le polynôme $Q(x)$ est de degré 4, on considère les éléments non nuls de $\mathbb{F}_{2^4}$ qui sont

$$1, x, x^2, x^3, 1+x, 1+x^2, 1+x^3, x+x^2, x+x^3, x^2+x^3, 1+x+x^2,$$
$$1+x+x^3, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3$$

On veut montrer qu'un de ces polynômes ne peut pas s'écrire comme une puissance de x modulo $Q(x)$, i.e. $\mathbb{F}_{p^r} \setminus \{0\} = \{x^i \mid i = 0, 1, \dots, 2^4-2\}$ où on prend x^i modulo $Q(x)$.

On a $Q(x)=0 \iff x^4 = x^3+x^2+x+1$

$\Rightarrow x^5 = x^4+x^3+x^2+x = 1$

$\Rightarrow x^6 = x$

$\Rightarrow x^7 = x^2$

$\Rightarrow x^8 = x^3$

$\Rightarrow x^9 = x^4$

On voit donc que les puissances de x modulo $Q(x)$ ne génère que $1, x, x^2, x^3, x^4$ et x^3+x^2+x+1

Ainsi, $Q(x)$ n'est pas primitif.

Vérifions que si on prend $(a_0, a_1, a_2, a_3) = (1,1,1,1)$ aucune suite générée par le registre à décalage n'est de période 15.

Avec $(a_0, a_1, a_2, a_3) = (0,0,0,1)$, on obtient 000110001 1...

Avec $(a_0, a_1, a_2, a_3) = (0,0,1,0)$, on obtient 001010010100...

Avec $(a_0, a_1, a_2, a_3) = (1,0,1,0)$, on obtient 101001010010 10...

On vérifie comme ça pour les $2^4 - 1 = 15$ choix de (a_0, a_1, a_2, a_3) (le -1 vient du fait qu'il est

inutile de vérifier pour $(a_0, a_1, a_2, a_3) = (0,0,0,0)$).