CIR$_2$

CORPS FINIS

I/ Corps de Galois $\mathbb{F}_q = GF(q)$ où $q = p^r$, p premier et $r \in \mathbb{N}^*$

On se limitera ici au cas $p = 2$. On appelle $\mathbb{F}_2$ le corps des nombres binaires $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$

1. Anneau $\mathcal{K} = \mathbb{F}_2[X]/(P)$

Soit P un polynôme de degré r dans $\mathbb{F}_2[X]$.

On considère les classes modulo P des polynômes de $\mathbb{F}_2[X]$.

Exemples

	modulo X^2+X+1	modulo X^3+X^2+1
1	1	1
X	X	X
X^2	$X+1$	X^2
X^3	1	X^2+1
X^4	X	X^2+X+1
X^5		
$1+X^2+X^4+X^5$		

Pour calculer $Q = X^7+X^5+X^3+1$ par $P = X^4+X+1$, on pose la division de Q par P :

$$X^7+X^5+X^3+1 = (X^4+X+1)(X^3+X+1)+X^2 \text{ donc } Q = X^2 \text{ modulo } P$$

On appelle $\mathcal{K}$ l'ensemble de ces classes : $\mathcal{K} = \mathbb{F}_2[X]/(P)$

En notant $\overline{A}$ la classe de A, on pose $\overline{A}+\overline{B} = \overline{A+B}$, $\lambda\,\overline{A} = \overline{\lambda A}$ et $\overline{A}.\overline{B} = \overline{A\,B}$

L'ensemble des classes $\mathcal{K}$, muni de ces opérations, est un anneau commutatif.

Si $\deg(P) = r$, $\mathcal{K}$ est isomorphe à l'anneau des polynômes de degré $< r$ à coefficients dans $\mathbb{F}_2$

Tout $\xi \in \mathcal{K}$ s'écrit de manière unique $\xi = \overline{R}$ avec degré(R) $< r$

On identifie alors R et $\overline{R}$ pour tout R tel que degré(R) $< r$.

Exemple avec $P = X^2+X+1$, $\mathcal{K} = \{0,1,X,1+X\}$ avec les tables :

+	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

×	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

2. Espace vectoriel $\mathcal{K} = \mathbb{F}_2[X]/(P)$

En notant $\overline{A}$ la classe de A, on pose $\overline{A} + \overline{B} = \overline{A + B}$, $0\ \overline{A} = \overline{0}$, $1\ \overline{A} = \overline{A}$

Tout $\xi \in \mathcal{K}$ s'écrit de manière unique $\xi = a_0 + a_1 X + ... + a_{r-1} X^{r-1}$, où $a_0, a_1, ..., a_{r-1}$ sont des éléments de $\mathbb{F}_2$

donc $\mathcal{K}$ est également un espace vectoriel sur $\mathbb{F}_2$, de base $(1, X, X^2, ..., X^{r-1})$, de dimension r.

On peut aussi identifier $\xi = a_0 + a_1 X + ... + a_{r-1} X^{r-1}$ à $v = (a_0, a_1, ..., a_{r-1}) \in (\mathbb{F}_2)^r$

3. Corps $\mathcal{K} = \mathbb{F}_2[X]/(P)$

Soit maintenant P un polynôme **irréductible** de degré r dans $\mathbb{F}_2[X]$.

Exemples $P = X^2 + X + 1$

$P = X^3 + X^2 + 1$

$P = X^4 + X + 1$

Contre exemples $P = X^2 + 1$

$P = X^5 + X^4 + 1 = (X^2 + X + 1)(X^3 + X + 1)$

P étant irréductible, l'anneau $\mathcal{K} = \mathbb{F}_2[X]/(P)$ est **intègre**.

Comme il est fini (il a 2^r éléments) c'est donc un **corps**.

On le note $\mathbb{F}_{2^r}$ ou $GF(2^r)$: corps de Galois à 2^r éléments

(on démontre qu'il n'y en a qu'un à isomorphisme près)

Remarque : puisque $P(X) = 0$ modulo P le polynôme P a une racine dans $\mathbb{F}_{2^r}$ (la classe de X)

alors qu'il n'a pas de racine dans $\mathbb{F}_2$, puisqu'il est irréductible dans $\mathbb{F}_2$.

$\mathbb{F}_{2^r}$ apparaît donc comme le corps obtenu à partir de $\mathbb{F}_2$ en adjoignant un élément α vérifiant $P(\alpha) = 0$.

Pour tout $\alpha \in \mathbb{F}_{2^r}$ non nul, $\langle \alpha \rangle = \{..., \alpha^{-n}, ..., \alpha^{-2}, \alpha^{-1}, 1, \alpha, \alpha^2, ..., \alpha^n, ...\}$ est un sous-groupe du groupe multiplicatif de $\mathbb{F}_{2^r}$ (sous-groupe engendré par α).

Il est donc fini et son ordre k divise $2^r - 1$. On a alors $\langle \alpha \rangle = \{1, \alpha, \alpha^2, ..., \alpha^{k-1}\}$.

Si l'ordre de α est égal à $2^r - 1$, alors on dit que α est **primitif** et $\mathbb{F}_{2^r} = \{0, 1, \alpha, \alpha^2, ..., \alpha^{2^r - 1}\}$

Exemples : Dans $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$, $\alpha = X$ est primitif : $\alpha^2 = \alpha + 1$ donc $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$.

Dans $\mathbb{F}_8 = \mathbb{F}_3[X]/(X^3 + X + 1)$, tout élément non nul est primitif puisque 7 est premier.

Dans $\mathbb{F}_{256} = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)$, étudions l'élément $\alpha = X$. On a $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$.

Puisque $255 = 3 \times 5 \times 17$, l'ordre de α ne peut être que 1, 3, 5, 17, $15 = 3 \times 5$, $51 = 3 \times 17$, $85 = 5 \times 17$, ou 255

On calcule $\alpha^{16} = (\alpha^4 + \alpha^3 + \alpha + 1)^2 = \alpha^8 + \alpha^6 + \alpha^2 + 1 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$

donc $\alpha^{15} = \alpha^5 + \alpha^3 + \alpha^2 + \alpha^1 + 1 \neq 1$ et et $\alpha^{17} = \alpha^7 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 \neq 1$

puis $\alpha^{32} = ... = \alpha^7 + \alpha^6 + \alpha^5 + \alpha^2$ et $\alpha^{51} = \alpha^{32} \alpha^{16} \alpha^2 \alpha = ... = 1$! : α n'est donc pas primitif.

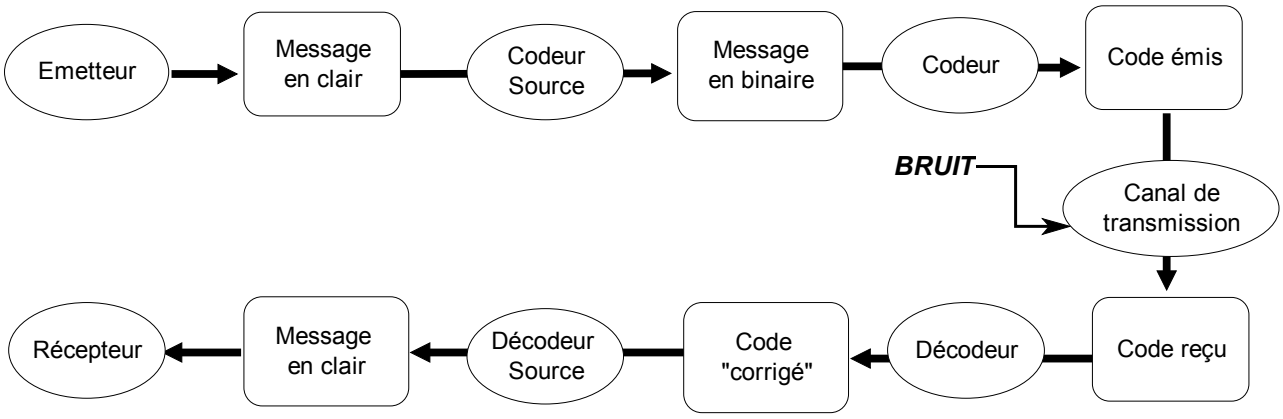
On peut montrer que $\beta = \alpha + 1$ est primitif.

Le corps à 256 éléments apparaît notamment dans l'algorithme de chiffrement symétrique le plus répandu, l'Advanced Encryption Standard, et dans les codes de Reed-Solomon utilisés pour la correction d'erreurs pour le stockage optique (CD/DVD/Blue-Ray) et les communications satellitaires.

II/ Codes correcteurs

1/ Introduction

Schéma de communication avec bruit



2/ Code de Hamming (7,4)

On veut détecter et corriger une erreur quand il n'y en a qu'une au plus par message
On ajoute des bits de contrôle au message.
On cherche à calculer un syndrome qui permette de localiser l'erreur, s'il y en a au plus une, de manière que $s_2 s_1 s_0$ donne en binaire le numéro du digit erroné

Message *m* :

d_1	d_2	d_3	d_4

Code *c* :

d_1	d_2	d_3	d_4	d_5	d_6	d_7

Code reçu *c'*:

d'_1	d'_2	d'_3	d'_4	d'_5	d'_6	d'_7

Syndrome :

s_1	s_2	s_3

Erreur sur :	s_3	s_2	s_1
aucun	0	0	0
d_1	0	0	1
d_2	0	1	0
d_3	0	1	1
d_4	1	0	0
d_5	1	0	1
d_6	1	1	0
d_7	1	1	1

Posons $e_i = d_i + d'_i$. si on envisage au plus une erreur, on a alors $(1)\begin{cases} s_1 = e_1 + e_3 + e_5 + e_7 \\ s_2 = e_2 + e_3 + e_6 + e_7 \\ s_3 = e_4 + e_5 + e_6 + e_7 \end{cases}$

Mais on ne connaît pas les d_i seulement les d'_i On va donc s'arranger pour que $(2)\begin{cases} 0 = d_1 + d_3 + d_5 + d_7 \\ 0 = d_2 + d_3 + d_6 + d_7 \\ 0 = d_4 + d_5 + d_6 + d_7 \end{cases}$.

Dès lors le système (1) devient $(3)\begin{cases} s_1 = d'_1 + d'_3 + d'_5 + d'_7 \\ s_2 = d'_2 + d'_3 + d'_6 + d'_7 \\ s_3 = d'_4 + d'_5 + d'_6 + d'_7 \end{cases}$ et on peut calculer s_1, s_2, s_3 à l'aide du code reçu.

(2) est un système de 3 équations à 3 inconnues d_5, d_6, d_7 qui donne: $\begin{cases} d_5 = d_2 + d_3 + d_4 \\ d_6 = d_1 + d_3 + d_4 \\ d_7 = d_1 + d_2 + d_4 \end{cases}$

remarque : dans la pratique, les digits $d_1 .. d_7$ ne sont pas dans cet ordre.

On écrit sous forme matricielle :

$$\begin{pmatrix} d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 \end{pmatrix} = \begin{pmatrix} d_1 & d_2 & d_3 & d_4 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$ soit $c = m.G$. G est la **matrice génératrice**

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} d'_1 \\ d'_2 \\ d'_3 \\ d'_4 \\ d'_5 \\ d'_6 \\ d'_7 \end{pmatrix}$$ soit $s^{\mathsf{T}} = H.c'^{\mathsf{T}}$. H est la **matrice de test**