Cours I33 / 30-10-2020

Corps finis (suite et fin)

- Rappels:

- Soit $p \geq 2$ un nbre premier. On identifie l'ens. des corps finis à p éléments à l'ens. $\mathbb{Z}/p\mathbb{Z}$.
On note $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \times)$. (i.e. $\mathbb{F}_{p^r} = GF(p^r)$)

- Pour construire un corps fini à p^r, avec $r \geq 1$ un entier, on choisit un polynôme $P(X)$ irréductible, et à coefficients dans $\mathbb{F}_p$ et de degré r.
Soit α un racine ("imaginaire") de $P(X)$,
(i.e. $P(\alpha) = 0$).
Alors le corps fini à p^r éléments est défini comme suit:

$$\mathbb{F}_{p^r} = \{ a_0 + a_1\alpha + \dots + a_{r-1}\alpha^{r-1} \;/\; a_i \in \mathbb{F}_p \}.$$

- Donc, pour construire un corps fini à 2^r éléments, on choisit un polynôme $Q(X) \in \mathbb{F}_2[X]$ irréductible tel que : $Q(X) = q_0 + q_1 X + \cdots + q_{r-1} X^{r-1} + X^r$

avec $q_0 \in \{0, 1\}$.

On pose α une racine ("imaginaire") de Q.

(Donc, $Q(\alpha) = q_0 + q_1 \alpha + \cdots + q_{r-1} \alpha^{r-1} + \alpha^r = 0$)

On a alors :

$$\mathbb{F}_{2^r} = \left\{ a_0 + a_1 \alpha + \cdots + a_{r-1} \alpha^{r-1} \;/\; a_i \in \{0, 1\} \right\}$$

- Convention de représentation des éléments de $\mathbb{F}_{2^r}$:

Soit $x \in \mathbb{F}_{2^r}$, alors $\exists\, x_0, \ldots, x_{r-1} \in \{0, 1\}$ tel que : $x = x_0 + x_1 \alpha + \cdots + x_{r-1} \alpha^{r-1}$

À l'élément x, on associe l'entier $\tilde{x}$ tel que : $\tilde{x} = \overline{x_{r-1} x_{r-2} \cdots x_0}^{2}$.

On dira que $\tilde{x}$ (l'entier) est la représentation de l'élément x.

- Addition dans $\mathbb{F}_{2^r}$:

Soit $x, y \in \mathbb{F}_{2^r}$ tq :

$$\begin{cases} x = x_0 + x_1\alpha + \dots + x_{r-1}\alpha^{r-1} \\ y = y_0 + y_1\alpha + \dots + y_{r-1}\alpha^{r-1} \end{cases}$$

Alors :

$$x + y = (x_0 + y_0) + (x_1 + y_1)\alpha + \dots + (x_{r-1} + y_{r-1})\alpha^{r-1}$$

⚠ L'opération $x_i + y_i$ est faite dans $\mathbb{F}_2$, donc opération modulo 2. Ainsi, $x_i + y_i = x_i \wedge y_i$

Donc, $\widetilde{x+y} = \tilde{x} \wedge \tilde{y}$.

Algo d'addition, à partir des représentations :

```
add(a, b) :
    retourner a ∧ b
```

- Multiplication par α dans $\mathbb{F}_{2^r}$:

Soit $x \in \mathbb{F}_{2^r}$ tq $x = x_0 + x_1\alpha + \cdots + x_{r-1}\alpha^{r-1}$

Alors : $\alpha . x = x_0\alpha + x_1\alpha^2 + \cdots + x_{r-2}\alpha^{r-1} + x_{r-1}\alpha^r$

Pour rappel, on a construit $\mathbb{F}_{2^r}$ avec un polynôme

$Q(X) = q_0 + q_1 X + \cdots + q_{r-1}X^{r-1} + X^r \in \mathbb{F}_2[X]$

irréductible tel que $Q(\alpha) = 0$

Donc, $\alpha^r = q_0 + q_1\alpha + \cdots + q_{r-1}\alpha^{r-1}$

(car $-1 = 1$ dans $(\mathbb{F}_2, +, \times)$, car c'est anneau de Boole)

D'où $\alpha x = x_0\alpha + \cdots + x_{r-2}\alpha^{r-1} + x_{r-1}(q_0 + q_1\alpha + \cdots + q_{r-1}\alpha^{r-1})$

$= x_{r-1}q_0 + (x_0 + x_{r-1}q_1)\alpha + \cdots + (x_{r-2} + x_{r-1}q_{r-1})\alpha^{r-1}$

On peut remarquer que :

- Si $x_{r-1} = 0$, alors $\widetilde{\alpha x} = \tilde{x} \times 2 = \tilde{x} \ll 1$
- Sinon (i.e. $x_{r-1} = 1$),

$$\widetilde{\alpha x} = (\tilde{x} \ll 1) \wedge \tilde{Q}$$

où $\tilde{Q} = \overline{1\, q_{r-1}\, q_{r-2} \cdots q_0}^{\,2}$ un entier.

On en déduit l'algo suivant de multiplication par α dans $\mathbb{F}_{2^r}$, à partir de représentations :

~~multByAlpha ($\tilde{x}$, $\tilde{\alpha}$, r)~~ :

multByAlpha ($\tilde{x}$, $\tilde{\alpha}$, r) :

$a = \tilde{x} \ll 1$

si $(a \,\&\, (1 \ll r)) == 1$:

~~$\tilde{a}$~~ $a = a \wedge \tilde{\alpha}$

retourner a # $a = \alpha \tilde{x}$

- Multiplication générale dans $\mathbb{F}_{2^r}$:

Soit $x, y \in \mathbb{F}_{2^r}$

$$\begin{cases} x = x_0 + x_1 \alpha + \dots + x_{r-1} \alpha^{r-1} \\ y = y_0 + y_1 \alpha + \dots + y_{r-1} \alpha^{r-1} \end{cases}$$

On a :

$$\begin{aligned} x \times y &= x (y_0 + y_1 \alpha + \dots + y_{r-1} \alpha^{r-1}) \\ &= y_0 x + y_1 (\alpha x) + y_2 (\alpha^2 x) + \dots + y_{r-1} (\alpha^{r-1} x) \end{aligned}$$

On en déduit une fonction suivant de multiplication générale dans $\mathbb{F}_{2^r}$, à partir de représentations multiplication $(\tilde{x}, \tilde{y}, \tilde{Q}, r)$:

```
a = x̃
b = ỹ
s = 0
tant que b != 0 :
    si (b & 1) == 1 :
        s = s ^ a
    a = multByAlpha(a, Q̃, r)
    b = b >> 1
retourner s
```

- Table de $\log_{\alpha}$ en base α dans $\mathbb{F}_{2^r}$:

On suppose ici que le polynôme Q utilisé pour construire $\mathbb{F}_{2^r}$ est primitif.

Donc α est un élément primitif de $\mathbb{F}_{2^r}$ i.e. α est un générateur du groupe cyclique $(\mathbb{F}_{2^r}^*, \times)$.

Donc, $\mathbb{F}_{2^r}^* = \{\alpha^0, \alpha^1, \ldots, \alpha^{2^r-2}\}$

On peut donc construire la table des Log en base α de $\mathbb{F}_{2^r}^*$, i.e.

$\forall x \in \mathbb{F}_{2^r}^*$, l'entier j tel que $\alpha^j = x$

avec $j \in \{0, \dots, 2^r - 2\}$.

Exple 1 : On considère le corps $\mathbb{F}_{2^3}$ qui construit avec le polynôme primitif $P(X) = X^3 + X + 1$.

Construire la table des Log en base α de $\mathbb{F}_{2^3}$ où α est une racine de $P(X)$.

(i.e. Construire la table Log telle que $\forall x \in \mathbb{F}_{2^3}^*$, $\text{Log}[x] = j$ si $x = \alpha^j$

Table des antilog (en base α) de $\mathbb{F}_{2^r}$:

On se met dans les mêmes conditions que celles pour la table des log.

On peut donc construire la table des antilog de $\mathbb{F}_{2^r}$ définie comme suit :

~~i.e. Soit x~~

Soit $x \in \mathbb{F}_{2^r}^*$ tq $x = \alpha^j$ avec $j \in \{0, \dots, 2^r - 2\}$

Alors : ~~antilog~~ $\log_\alpha(x) = j$

$$\text{antilog}_\alpha(j) = x$$

Exple 2 : On reprend les éléments de l'exple 1. Construire la table des antilog de $\mathbb{F}_{2^3}$. (i.e.

Construire la table Antilog telle que

$\forall j \in \{0, \dots, 2^3 - 2\}$, $\text{Antilog}(j) = x$ si $x = \alpha^j$.

- Algo. de multiplication gf8 avec les tables Log et AntiLog :

On suppose qu'on dispose des deux tables Log et AntiLog.

On en déduit l'algo suivant (à partir des reps)

multiplication $(\tilde{x}, \tilde{y}, r)$:

si $\tilde{x} == 0$ ou $\tilde{y} == 0$:

retourner 0

sinon :

$u = Log[\tilde{x}]$

$v = Log[\tilde{y}]$

$s = (u+v) \% (2^r - 1)$

retourner $AntiLog[s]$