Institut Joseph Fourier
Master II C.S.C.I
2004-2005 - semaine 47

TP - Manipulation du corps $\mathbb{F}_{256}$

Addition-soustraction-multiplication-division

Sébastien Varrette Sebastien.Varrette@imag.fr
Jean-Louis Roch Jean-Louis.Roch@imag.fr

1 Rappels : construction d'un corps fini à p^m éléments (p premier, $m \geq 1$)

On considère le corps fini à p éléments $\mathbb{F}_p$ (ou p est premier).
Dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, les opérations sont réalisées modulo p. Soit m un entier positif. On souhaite construire le corps $\mathbb{F}_{p^m}$ possédant p^m éléments. Pour cela, on considère g un polynôme unitaire irréductible de $\mathbb{F}_p[X]$ de degré m. Soit ω une racine[1] de g : $g(\omega) = 0$. On pose alors :

$$\mathbb{F}_{p^m} = \left\{a_0 + a_1.\omega + a_2.\omega^2 + \ldots + a_{m-1}.\omega^{m-1} | a_i \in \mathbb{F}_p\right\} \xrightarrow{\sim} \mathbb{F}_p[X]/(g(X))$$

$\mathbb{F}_{p^m}$ correspond à l'ensemble de tous les polynômes en ω de degrés $\leq m$ et à coefficients dans $\mathbb{F}_p$. On munit $\mathbb{F}_{p^m}$ d'une addition $+$ (correspondant à l'addition de polynômes dans $\mathbb{F}_p[X]$). et une multiplication . (correspondant à la multiplication de polynômes de $\mathbb{F}_p[X]$ modulo $g(X)$). On peut montrer qu'alors $(\mathbb{F}_{p^m}, +, .)$ est un corps de p^m éléments ($\mathbb{F}_{p^m}$ est une extention finie de $\mathbb{F}_p$)
Pour de plus amples informations, se référer au cours de mathématiques sur les corps finis.
Voici les points importants à retenir :

- deux polynômes irreductibles de même degré m sur $\mathbb{F}_p$ fournissent deux corps isomorphes. Il n'est toutefois pas toujours facile d'expliciter cet isomorphisme.
- tout élément de $\mathbb{F}_{p^m}$ s'écrit donc de manière unique :

$$a_0 + a_1.\omega + a_2.\omega^2 + \ldots + a_{m-1}.\omega^{m-1}, \text{ avec } a_i \in \mathbb{F}_p \text{ et } \omega \text{ racine de g}$$

.

- Si $g(X) = \sum_{i=0}^{m-1} \lambda_i X^i + X^m$, alors on a la formule :

$$\omega^m = -\sum_{i=0}^{m-1} \lambda_i \omega^i$$

  Cette formule permet de calculer facilement le produit. La base $1, \omega, \ldots, \omega^{m-1}$ est dite *polynômiale*.
  Soit x un élément de $\mathbb{F}_{p^m}$. x admettra donc deux représentations :

[1]On peut montrer que l'ensemble des racines de g est $\left\{\omega, \omega^p, \omega^{p^2}, \ldots; \omega^{p^{m-1}}\right\}$

– *représentation exponentielle* : soit $x = 0$, soit $\exists i \in [0, p^m - 2]/x = \omega^i$. On représentera alors x par la valeur de l'exposant i (avec par convention $i = p^m - 1$ si $x = 0$).
– *représentation polynômiale* : $\exists \{a_0, \ldots, a_{m-1}\} \in \mathbb{F}_p/x = \sum_{i=0}^{m-1} a_i \omega^i$. Dans ce cas, on représentera x par la séquence $a_{m-1} \ldots a_1 a_0$.

2 Le corps $\mathbb{F}_{256}$

Dans ce TP, on considère le cas du corps $\mathbb{F}_{256}$ ($p = 2$ et $m = 8$). Ce corps est isomorphe a $\mathbb{F}_2[X]/(g(X))$ où
– $\mathbb{F}_2$ est le corps à 2 éléments.
– $g(X)$ est un polynôme (unitaire) irréductible de $\mathbb{F}_2[X]$, de degré 8.
On considèrera pour cela le polynôme $g(X) = X^8 + X^7 + X^2 + X + 1$. Comme on l'a vu dans la section précédente, on disposera de deux représentations des éléments du corps en machine :

1. la représentation exponentielle : le monome ω^i sera représenté par l'entier i. On représentera $\mathbb{F}_{256}$ par
$$\mathbb{F}_{256} = \{0, 1 = \omega^0, \omega, \omega^2, \ldots, \omega^{254}\}$$
On représentera par convention l'élément 0 par 255 (ou -1). Dans cette représentation, la multiplication est facile à implémenter. En effet, pour $i, j \in [0, 254]$,
$$\omega^i \times \omega^j = \omega^{i+j \mod 255}$$
Par contre il n'y a pas de solution simple pour l'addition.
2. la représentation polynômiale : dans ce cas, un octet $a_7 a_6 \ldots a_1 a_0$ représentera le polynôme $\sum_{i=0}^{7} a_i \omega^i$ et on représentera $\mathbb{F}_{256}$ par
$$\mathbb{F}_{256} = \{a_0 + a_1.\omega + a_2.\omega^2 + \ldots + a_7.\omega^7 | a_i \in \mathbb{F}_p\}$$
Dans cette représentation, c'est l'addition qui est facile à implémenter. En effet, elle correspond à une simple addition de polynôme dans $\mathbb{F}_2[X]$ et donc si $x, y \in \mathbb{F}_{256}$ dans cette représentation, alors
$$x + y = x \oplus y$$
Ou $\oplus$ désigne le ou exclusif donc voici la table :

$\oplus$	0	1
0	0	1
1	1	0

3 Travail à réaliser

Ce TP est à réaliser en C et devra permettre la manipulation du corps $\mathbb{F}_{256}$, en particulier l'addition, la soustraction, la multiplication et la division d'éléments de $\mathbb{F}_{256}$.

Il faudra d'abord choisir quelle représentation (exponentielle ou polynômiale) est privilégiée et sera utilisée par défaut. Il s'agira ensuite d'implémenter le passage d'une représentation à l'autre, On pourra alors implémenter facilement chaque type d'opération (en passant éventuellement à l'autre représentation pour faciliter l'opération difficile).
On trouvera en annexe le début de la table de correspondance entre les deux représentations.
A noter que ce travail servira de base au projet à réaliser dans le cadre du cours sur les codes correcteurs. C'est pourquoi on spécifiera dans un fichier header (`f256.h` par exemple) le prototype des fonctions implémentées pouvant être utilisées dans un module extérieur.

A Annexe : début de la table de correspondance entre les deux représentations

Elément de $\mathbb{F}_{256}$		Représentation machine	
rep. exponentielle	rep. polynômiale	rep. exponentielle	rep. polynômiale
0	0	255	0
1	1	0	1
ω	ω	1	2
ω^2	ω^2	2	4
ω^3	ω^3	3	8
ω^4	ω^4	4	16
ω^5	ω^5	5	32
ω^6	ω^6	6	64
ω^7	ω^7	7	128
ω^8	$\omega^7+\omega^2+\omega+1$	8	135
ω^9	$\omega^7+\omega^3+1$	9	137
ω^{10}	$\omega^7+\omega^4+\omega^2+1$	10	149
...	...	...	...

Références

[Can03] Anne Canteaut. "Programmation en Langage C". INRIA - projet CODES, 2003.

[Cas98] Bernard Cassagne. "Introduction au Langage C". Laboratoire CLIPS UJF/CNRS, 1997-1998.

[KR88] B.W. Kernighan and D.M. Ritchie. *The C Programming Language*. Prentice-Hall, Englewood Cliffs, New Jersey, USA, 1988. 2nd edition.

[Sen02] Nicolas Sendrier. Calculs dans F_{256}, 2002. `http://www.enseignement.polytechnique.fr/profs/informatique/Nicolas.Sen%drier/X02/IF/PROJET/f256.html`.