Introduction aux corps finis

M. Belkasmi

ENSIAS 2009-2010

Intérêt

- Les opérations sur l'anneau des entiers classiques sont relativement lentes.
- Les calculs dans les corps finis peuvent être fait beaucoup plus vite, surtout sur architectures dédiées.
- Pour cette raison, il existe des cryptogrammes utilisant les corps finis (ex: courbes elliptiques)
- De plus ils sont utilisés dans d'autres domaines des communications (codes en blocs, Reed-Solomon, BCH, codes de Goppa …)

Notion de corps

- Un corps est un anneau où tous les éléments non nuls sont inversibles.

Exemples:

- l'ensemble des réels, des complexes...
- L'ensemble des entiers relatifs est un anneaux mais pas un corps.
- $Z/2Z$ est un corps, $Z/4Z$ n'en est pas un.
- L'ensemble $Q[\sqrt{2}]$ formé des réels de la forme $a+b\sqrt{2}$ avec $a,b \in Q$ est un corps.

Polynômes irréductibles

- On dit qu'un polynôme $P(X)$ est irréductible s'il n'admet pas de factorisation.
- Cette notion dépend de l'ensemble où sont considérés les coefficients de P.
- Exemple:
- Prenons $P(X)=X^2-2$. Si on considère ce polynôme comme un polynôme de $R[X]$, alors il n'est pas irréductible ($P(X)=(X+\sqrt{2})(X-\sqrt{2})$).
- Par contre, si on considère $P(X)$ comme un polynôme de $Q[X]$, P est irréductible.

Théorèmes principaux

- Théorème: Soit p un nombre premier et $I(X)$ un polynôme irréductible de degré $n \geq 1$ dans $Z/pZ[X]$. Alors $(Z/pZ[X])/(I)$ est un corps. Il possède p^n éléments et il ne dépend pas de I (seulement du degré de I).
- Ce corps est appelé corps de Galois à p^n éléments, noté $GF(p^n)$ (GF pour Galois Fields).
- Théorème: Les seuls corps finis qui existent sont les corps de Galois.

Exemples

- Soit $p=2$ et $I(X)=X^2+X+1$. $I(X)$ est bien irréductible dans $Z/2Z[X]$ (on peut vérifier par exemple qu'aucun des polynômes de $Z/2Z[X]$ de degré inférieur ou égal à 1 ne divise $I(X)$).

  → $(Z/2Z[X])/(I)$ est donc un corps (c'est $GF(2^2)$).

- De même si $P(X)= X^3+X+1$ alors $Z/2Z[X]/(P)$ est un corps. Il est formé des restes modulo P des polynômes de $Z/2Z[X]$. C'est le corps $GF(2^3)$.

Deux Questions

- Quels sont les éléments de ces corps :
  - $GF(2^2) \approx (Z/2Z[X])/(I) = (Z/2Z[X])/(X^2+X+1)$
  - $GF(2^3) \approx (Z/2Z[X])/(I) = (Z/2Z[X])/(X^3+X+1)$
- Comment peut on faire les calculs avec?

Calcul dans les corps finis

- La relation d'équivalence est $P \mathcal{R} Q$ ssi $P-Q \in (I)$.
- (I) est l'idéal $\{ R \in K[X] \mid \exists S \in K[X], R(X)=S(X).I(X) \}$.
- Deux polynômes P et Q sont dans la même classe si et seulement si
  $P(X)-Q(X) = S(X).I(X)$ avec $S \in K[X]$
  donc $P(X) = Q(X) \bmod I(X)$.
- Pour faire les calculs, on prend donc n'importe quel élément de la classe et on fait les calculs modulo $I(X)$.

Exemple

- Soit $GF(8) \approx Z/2Z[X]/(X^3+X+1)$.
- L'ensemble des classes d'équivalence est exactement l'ensemble des restes des polynômes de $Z/2Z[X]$ modulo X^3+X+1.
- Il s'agit donc de tous les polynômes de degré strictement inférieur à 3 dans $Z/2Z[X]$ ($=GF(2)[X]$).
- Soit à calculer $(\underline{X^2+X+1}).(\underline{X^2+1})$:
- On prend deux représentants dans l'anneau $GF(2)[X]$ et on les multiplie: $(X^2+X+1).(X^2+1) = X^4+X^3+2X^2+X+1$.
- On réduit ensuite modulo X^3+X+1 : $X^4+2X^2+2X+2 = X^2+X$

Représentation linéaire

- Théorème: $GF(2^n)$ est un espace vectoriel de dimension n sur $GF(2) \approx Z/2Z$.
- ça veut dire que l'on peut représenter les éléments de $GF(2^n)$ comme des n-uplets d'éléments de $GF(2)$.
- $\underline{X^2+X+1} \leftrightarrow (1,1,1)$
- On parle de représentation linéaire du corps $GF(2^n)$.
- Exemple : GF(4)={(00),(01),(10),(11)}

Racines de polynômes

- Théorème: Soit P un polynôme irréductible de $GF(2)[Y]$ de degré égal à n. Alors P est entièrement décomposable dans $GF(2^n)[Y]$.

- Exemple: $P(Y)=Y^3+Y^2+1$ est irréductible dans $GF(2)[Y]$.
- Dans $GF(8)\approx GF(2)[X]/(X^3+X+1)$, P admet trois racines.

Groupe multiplicatif

- Théorème: Soit n un nombre entier $n\geq 1$. Alors $(GF(2^n)-\{0\},*)$ est un groupe. De plus il est monogène i.e. il existe $\alpha\in GF(2^n)-\{0\}$ tel que pour tout $\beta\in GF(2^n)-\{0\}$, $\exists k$ entier compris entre 0 et 2^n-2 tel que $\beta=\alpha^k$.

  On dit que α est un générateur du groupe. On a de plus $\forall\beta\in GF(2^n)-\{0\}$, $\beta^{2^n-1}=1$.

Exemple

- Dans GF(16)=GF(2)[X]/(X^4+X+1) pour un élément quelconque $\beta \neq 0$ on a $\beta^{15}=1$.

- Si α est une racine de X^4+X+1 alors α est un générateur de GF(16)-{0}.
- De même α^7 est un générateur
- Par contre α^3 n'en est pas un.

Racines primitives

- Définition: Soit *I* un polynôme à coefficients dans *GF(2)* et soit α une racine de *I*. Si α est un générateur de *GF(2^n)-{0}*, on dit que α est une racine primitive de *I*.

Exemples:

- Dans *GF(16)≈GF(2)[X]/(X^4+X+1)*, *P* (X)= X^4+X+1 admet α, α^2,α^4 et α^8 comme racines. Toutes ses racines sont primitives.
- L'élément α^3 qui est racine du polynôme $Y^4+Y^3+Y^2+Y+1$. Il n'est pas primitif.

Polynôme primitif

- Définition: Soit *I* un polynôme de degré *n*, irréductible sur *GF(2)[X]*. Le polynôme est dit primitif si ses racines sont primitives dans GF(2^n)

Exemples :

- X^4+X+1 est un polynôme primitif pour GF(2)
- $X^4+X^3+X^2+X+1$ n'est pas primitif.

Exemples

- $I(X)=X^4+X^3+X^2+X+1$ sur *GF(2)*, α racine de I(X)
- On calcule récursivement $u_k=\alpha^k$
- Si *I(X)* est primitif, on doit générer 15 éléments distincts (les éléments du groupe multiplicatif).
- On a $u_0=1$, $u_1=\alpha$, $u_2=\alpha^2$, $u_3=\alpha^3$, $u_4=\alpha^4$, $u_5=\alpha^5=1$.
- On ne génère donc que 5 éléments et donc I n'est pas primitif (Irréductible mais non primitif)

- Par contre ($X^4+1=(X+1).(X^3+X^2+X+1)$) n'est pas primitif parce qu'il n'est pas irréductible.

Représentation exponentielle

- Soit I un polynôme de degré n, irréductible sur GF(2)$[X]$ et α une racine primitive de I dans $GF(2^n)$.

  Alors pour tout élément non nul β de $GF(2^n)$, on a $\beta = \alpha^k$, avec $0 \leq k \leq 2^n-2$.
- k est dit le logarithme discret de β.

Multiplication et division

- Soit α non nul dans $GF(2^n)$, alors $\alpha^{2^n-1}=1$.

- Soit $\beta_1 = \alpha^{k1}$, alors $0.\ \beta_1 = 0$.
- Soit $\beta_2 = \alpha^{k2}$, alors $\beta_1.\beta_2 = \alpha^k$, avec $k=k_1+k_2 \pmod{2^n-1}$.
- De plus, $\beta_1/\beta_2 = \alpha^{k'}$, avec $k'=k_1-k_2 \pmod{2^n-1}$.

Construction de GF(16)

Représentation de $GF(2^4)$ en utilisant $p(z) = z^4 + z + 1$		
Notation Exponentielle	Notation Polynomiale	Notation linéaire
0	0	0000
α^0	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	1100
α^7	$\alpha^3 + \alpha + 1$	1011
α^8	$\alpha^2 + 1$	0101
α^9	$\alpha^3 + \alpha$	1010
α^{10}	$\alpha^2 + \alpha + 1$	0111
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101
α^{14}	$\alpha^3 + 1$	1001

Liste des polynômes primitifs

Degré du polynôme	Polynômes primitifs
2	$X^2 + X + 1$
3	$X^3 + X + 1$
4	$X^4 + X + 1$
5	$X^5 + X^2 + 1$
6	$X^6 + X + 1$
7	$X^7 + X^3 + 1$
8	$X^8 + X^4 + X^3 + X^2 + 1$
9	$X^9 + X^4 + 1$
10	$X^{10} + X^3 + 1$

Quelques applications

- Cryptographie sur courbes elliptiques.
- Construction de fonctions intéressantes pour des opérations de hachage.
- Codes correcteurs: codes BCH, codes RS, codes de Goppa, codes résidus quadratiques.
- Construction de géométries projectives pour les codes LDPC (Low Density Parity Check Codes).
- Etc…