Corps de Galois : aide mémoire

A . Le Glaunec

Un Corps de Galois est un corps contenant un nombre fini d'éléments. Vous en connaissez déjà…

1-Corps de Galois contenant un nombre premier d'éléments

1-1-Définition

Considérons l'ensemble des entiers relatifs Z et un nombre q premier appartenant à N : l'ensemble des entiers relatifs modulo q est un corps : il contient q éléments.

1-2-Exemples

- L'ensemble Z/q est formé des éléments : $\{\bar{0}, \bar{1}, \bar{2} \ldots\ldots\ldots, \overline{q-1}\}$.

Les nombres 0,…..,q-1 sont surmontés d'une barre pour montrer que les éléments du corps sont les classes des nombres 0,…,q-1 modulo q.
Pour tout a appartenant à Z, a peut s'écrire :
a=pq+r r étant le reste de la division de a par q $0 \leq r \leq q-1$.
a appartient à la classe de r, notée $\bar{r}$
Z/q contient q éléments. On peut le noter CG(q), Corps de Galois à q éléments.

- L'ensemble Z/2 ou CG(2) contient les classes 0 et 1 : $CG(2)=\{\bar{0}, \bar{1}\}$.

Les tables d'addition et de multiplication sont :

+	0	1
0	0	1
1	1	0

X	0	1
0	0	0
1	0	1

L'addition modulo 2 se réalise par un « ou exclusif », la multiplication modulo 2 se réalise par un « et ».

Un Corps de Galois défini comme une classe de nombres modulo q ne peut contenir qu'un nombre premier d'éléments. Ceci est restrictif.
Nous allons donc montrer comment on peut étendre la définition d'un Corps de Galois à partir du CG(q) ou définir des extensions de CG(q).
Ces corps contiennent q^m éléments et nous allons en exposer la construction sans justification théorique : vous les trouverez par exemple dans les références citées à la fin du document.

2-Corps de Galois défini comme ensemble de polynômes à coefficients dans Z/q

2-1-Définition

Considérons les polynômes en x dont les coefficients sont dans Z/q ou CG(q) . Soit f(x) un tel polynôme : il s'écrit :

$f(x)=f_{n-1}x^{n-1}+f_{n-2}x^{n-2}+....+f_1x+f_0$

Les coefficients $f_0, f_1, \ldots f_{n-1}$ sont des éléments de Z/q
L'ensemble de ces polynômes est Z/q[X]
Pour construire le $CG(q^m)$ on va procéder de la même façon que pour construire les Z/q mais en raisonnant non plus sur les entiers relatifs mais sur les polynômes de Z/q[X]. Pour

cela on suppose qu'on connaît un polynôme p(x) de Z/q[X] de degré m irréductible.
Irréductible veut dire qui n'est divisible par aucun autre polynôme de degré inférieur.
L'ensemble des polynômes modulo p(x) à coefficients dans CG(q) est un ensemble fini : on peut démontrer que c'est un corps.
Pour trouver à quelle classe de polynômes modulo p(x) appartient un polynôme quelconque f(x) on effectue la division Euclidienne de f(x) par p(x) :
$f(x)=q(x)p(x)+r(x)\quad 0\leq d°r(x)<d°p(x)=m$

Alors f(x) appartient à la classe de $r(x)=\overline{r(x)}$.

L'ensemble Z/q[p(x)]est formé de l'ensemble des classes de polynômes de degré inférieur ou égal à m-1 (puisque ce sont les restes par divisions Euclidiennes par p(x)).
Par abus de langage, on dira que l'ensemble Z/q[p(x)]est formé de l'ensemble de tous les polynômes de degré inférieur ou égal à m-1.
Combien contient-il d'éléments ? Chaque polynôme contient m éléments de Z/q qui peuvent prendre q valeurs : donc le nombre d'élément de Z/q[p(x)] est q^m.
À une condition près sur p(x) que nous verrons dans le paragraphe suivant, cet ensemble est le Corps de Galois à q^m éléments : CG(q^m). De plus la caractéristique du corps est q.

2-2-Exemple

Très, très souvent, le corps de départ est le CG(2) ou Z/2.

- Construction

Sur CG(2), $p(x)=x^3+x+1$ est irréductible.
En effet :

- x+1 ne divise pas p(x) puisque 1 n'est pas racine
- x ne divise pas p(x) puisque 0 n'est pas racine
- aucun polynôme de degré 2 ne divise p(x) sinon p(x) serait le produit d'un polynôme de degré 2 et d'un polynôme de degré 1 ce qui est impossible puisque aucun polynôme de degré 1 ne divise p(x).

Tous les polynômes de degré inférieur à 3 forment une classe de polynômes modulo p(x)
Ils sont :

Polynômes	notation utilisant les valeurs des coefficients en x^2 x x^0
$f_0(x)=0$	0 0 0
$f_1(x)=1$	0 0 1
$f_2(x)=x$	0 1 0
$f_3(x)=x+1$	0 1 1
$f_4(x)=x^2$	1 0 0
$f_5(x)=x^2+1$	1 0 1
$f_6(x)=x^2+x$	1 1 0
$f_7(x)=x^2+x+1$	1 1 1

Cet ensemble contient 2^3éléments : c'est le CG(2^3) ou CG(8).
On voit que les éléments du CG(q^m) définis de cette façon ne sont pas très commodes à écrire. Pour les utiliser, on peut les représenter sous forme de m-uplets du corps de départ soit m bits si celui-ci est CG(2).
Nous avons défini l'ensemble qui n'est pas très original…Pour définir le corps, il faut définir les opérations d'addition et de multiplication.

- Addition

L'addition de 2 éléments du CG(q^m) en général est l'addition des polynômes terme à terme. Il faut se souvenir de la propriété de l'addition dans le corps de départ où sont pris les coefficients.
Dans l'exemple que nous avons pris, dans le CG(2) corps des coefficients : 1+1=0 (+ ou - = même chose…).
Par exemple : $f_4(x)+f_5(x)= x^2+ x^2+1=1=f_1(x)$

- Multiplication

Pour sa définition, on fait enfin appelle à la définition du corps.
Cherchons par exemple : $f_2(x)f_4(x)=x^3$
Pour trouver à quel élément il est « égal », il faut trouver à quelle classe appartient x^3.
On effectue la division de x^3 par $p(x)=x^3+x+1$: on trouve rapidement : $x^3= (x^3+x+1)+x+1$
La classe de x^3est $x+1= f_3(x)$: donc $f_2(x)f_4(x)= f_3(x)$.

Petit truc : pour trouver le reste d'un polynôme par la division par x^3+x+1, donc pour trouver à quelle classe de polynôme il appartient, il faut remplacer x^3+x+1 par 0 dans le polynôme de départ : quelle est la classe de x^3 ? on sait que $x^3+x+1=0$ donc $x^3=x+1$.

2-3-Corps d'extension

Dans l'exemple précédent, le CG(8) est le corps d'extension du corps de départ le CG(2).
Il contient le corps de départ. En effet, toutes les constantes de CG(2)={0,1} sont des éléments du CG(8) puisque ce sont des polynômes de degré 0.
Pourquoi « le corps d'extension » ?
x^3+x+1 est irréductible sur {0,1} mais x^3+x^2+1 l'est aussi. On peut montrer que ces 2 corps sont isomorphes. Donc on considère que c'est le même corps.

Cette représentation sous forme de polynômes est assez limitée pour des développements théoriques : nous allons voir une autre méthode de construction de CG(q^m)

3-Corps de Galois définis à partir d'un élément primitif

3-1-Définition

Pour définir le CG(q^m) première manière, on a trouvé un polynôme irréductible p(x) de degré m, à coefficients dans CG(q). Ce polynôme étant premier n'a pas de racine dans CG(q).Mais on imagine qu'il existe des racines « ailleurs » que dans CG(q), on peut en trouver m : on note α l'une d'elles.
Cette racine est alors l'élément primitif du CG(q^m).
En effet on va trouver les éléments du corps de Galois en considérant toutes les puissances de α : $\{ \alpha^0, \alpha, \ldots \alpha^{q^m-2} \}$.

3-2-Exemple

On va construire le CG(8) avec cette nouvelle définition.
Soit toujours $p(x)=x^3+x+1$ le polynôme irréductible.
On appelle α une de ces racines, et on va exprimer les différentes puissances de α en fonction de $\alpha^0=1, \alpha, \alpha^2$.
En effet dès α^3 on peut exprimer en fonction des puissances inférieures parce que $\alpha^3+\alpha+1=0$, donc $\alpha^3=\alpha+1$. On continue…
$\alpha^4=\alpha^2+\alpha$

$\alpha^5=\alpha^3+\alpha^2=\alpha+1+\alpha^2$
Etc…
De façon générale, si on effectue la division de α^n par $\alpha^3+\alpha+1$, $\alpha^n=q(\alpha)(\alpha^3+\alpha+1)+r(\alpha)$, comme $\alpha^3+\alpha+1=0$, $\alpha^n=r(\alpha)$. Continuons de cette façon :
$\alpha^6=(\alpha^3+\alpha+1)(\alpha^3+\alpha+1)+\alpha^2+1=\alpha^2+1$
$\alpha^7=(\alpha^4+\alpha^2+\alpha)(\alpha^3+\alpha+1)+1=1$
On voit que $\alpha^7=1$, donc $\alpha^7+1=0$.

Ceci est général : si le polynôme p(x) est « correctement » choisi, $\alpha^{2^m-1}+1=0$ ou encore pour un corps de caractéristique q $\alpha^{q^m-1}-1=0$.
Donc on trouve bien 2^m éléments constituant le CG(2^m).

Attention : le polynôme p(x) est « correctement » choisi veut dire qu'il n'existe pas de puissance $j<2^m-1$ (ou q^m-1) telle que $\alpha^j+1=0$ (ou $\alpha^j-1=0$). On dit que le polynôme est **primitif**.
Les correspondances entre la notation des éléments à l'aide de puissance de α et la notation à l'aide de polynômes s'effectue en remplaçant α par x. On obtient le tableau du Corps de Galois.
Dans l'exemple précédent le tableau de CG(8) est :

	α^2	α	1
0	0	0	0
1	0	0	1
α	0	1	0
α^2	1	0	0
α^3	0	1	1
α^4	1	1	0
α^5	1	1	1
α^6	1	0	1

3-3-Opérations

- multiplication : on utilise la notation en puissances de α :
  $\alpha^i\alpha^j=\alpha^{(i+j)\bmod(2^m-1)}$ ou de façon générale $\alpha^i\alpha^j=\alpha^{(i+j)\bmod(q^m-1)}$.
- addition : on utilise la notation en polynômes de α. On fait la somme bit par bit modulo 2 (q)

3-4-Quelques propriétés du Corps de Galois CG(2^m) ou CG(q^m).

- Le Corps de Galois CG(q^m), q étant premier et m entier est l'ensemble des puissances d'un élément primitif α et l'élément 0.

$$\mathbf{CG(q^m)=}\left\{0,1,\alpha,\alpha^2,.....\alpha^{q^m-2}\right\}.$$

Le Corps contient effectivement q^m éléments car $\alpha^{q^m-1}=1$. Il est de caractéristique q.

- α est une racine d'un polynôme p(x) de degré m irréductible dans CG(q). Ce polynôme doit de plus être primitif.

C'est-à-dire qu'on ne trouve pas d'autre puissance j inférieure à q^m-1 telle que $\alpha^j=1$.

- Pour tout j, $\left(\alpha^j\right)^{q^m-1}=1$

Donc : $1,\alpha,\alpha^2,.....\alpha^{q^m-2}$ sont les racines du polynôme $x^{q^m-1}-1=0$.
Comme ce polynôme de degré q^m-1 a q^m-1 racines, on peut écrire que :

$\mathbf{x^{q^m-1}-1=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3).....(x-\alpha^j).....(x-\alpha^{q^m-2})}$.

- On peut démontrer que si un élément β du CG(q^m)est racine d'un polynôme f(x) à coefficients dans CG(q), $\beta^q,\beta^{q^2},.....\beta^{q^j}$ sont aussi racines de f(x).

Cela vient du fait que $f(x^q)=[f(x)]^q$: en effet $(f_0+f_1x)^q=f_0^q+(f_1x)^q+\sum_j C_q^j f_0^{q-j}(f_1x)^j$ or

$C_q^j=\frac{q(q-1)...(q-j+1)}{j!}$, comme q est premier C_q^j est proportionnel à q, donc nul dans CG(q) (modulo q).

$(f_0+f_1x)^q=f_0^q+(f_1x)^q$. De plus dans CG(q), on peut montrer par récurrence que $f_i^q=f_i$. En procédant par induction (!) avec $f(x)=f_0+f_1x+.....f_px^p$, on montre que $f(x^q)=[f(x)]^q$.

En particulier, les racines de p(x) sont : $\alpha,\alpha^q,\alpha^{q^2}.....\alpha^{q^{m-1}}$ (on en a m puisque $\alpha^{q^m}=\alpha$). Donc :

$\mathbf{p(x)=(x-\alpha)(x-\alpha^2).....(x-\alpha^{q^{m-1}})}$.

On voit que p(x) est un diviseur de $\mathbf{x^{q^m-1}-1}$.
On peut démontrer de même que tous les polynômes irréductibles de degré m divisent $x^{q^m-1}-1$.

- Revenons sur le polynôme p(x) irréductible qui doit être primitif pour qu'une de ses racines définisse le Corps de Galois. En général tous les polynômes irréductibles sont primitifs…Sauf…si (considérons les corps de caractéristique 2) 2^m-1 n'est pas premier.

En effet alors soit j un des diviseurs de 2^m-1. x^j-1 divise $x^{2^m-1}-1$.Certains polynômes irréductibles de degré m diviseurs de $x^{2^m-1}-1$ peuvent aussi être diviseurs de x^j-1, alors $x^j=1$, et une racine de p(x) ne définit plus le CG(2^m)

- Le plus petit entier j tel que $\beta^j=1$ est l'ordre de l'élément β.

3-5-Polynôme minimal d'un élément d'un Corps de Galois

Le polynôme minimal d'un élément β du CG(q^m) est le polynôme normalisé à coefficients dans CG(q) qui a pour racine β et de degré minimum.

Ce polynôme a aussi pour racines $\beta,\beta^q,..\beta^{q^j}.....\beta^{q^{r-1}}$, l'exposant étant pris modulo q^m-1 et r est le premier entier tel que $\beta^{q^r}=\beta$.

Ces racines sont les racines conjuguées. **Toutes les racines conjuguées ont le même polynôme minimal.**
Et le polynôme minimal d'un élément est le polynôme qui a pour racines toutes les racines conjuguées de cet élément.

Exemple : reprenons le CG(8) construit à partir de la racine α de $p(x)=x^3+x+1$.

	α^2	α	1		α^2	α	1
0	0	0	0	α^3	0	1	1
1	0	0	1	α^4	1	1	0
α	0	1	0	α^5	1	1	1
α^2	1	0	0	α^6	1	0	1

Le polynôme primitif de 1 est $m_0(x)=x+1$.
Le polynôme primitif de α est $m_1(x)=p(x)= x^3+x+1$.
Le polynôme primitif de α^2 est $m_2(x)= m_1(x)$. (les racines sont conjuguées)
Le polynôme primitif de α^3 est $m_3(x)$, il a pour racines : α^3, α^6, $\alpha^{12 \bmod (7)}= \alpha^5$ (c'est tout puisque $\alpha^{10 \bmod (7)}= \alpha^3$).Donc $m_3(x)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^5)=x^3+x^2+1$.
Le polynôme primitif de α^4 est $m_4(x)=m_1(x)$.
Le polynôme primitif de α^5 est $m_5(x)=m_3(x)$.
Le polynôme primitif de α^6 est $m_6(x)=m_3(x)$.

On peut déduire de ceci que $x^7+1=m_0(x)m_1(x)m_3(x)=(x+1)(x^3+x+1)(x^3+x^2+1)$.

4-Codes cycliques et Corps de Galois

Un polynôme générateur g(x) d'un code cyclique C(n,k) divise x^n-1.
Donc les racines de g(x) sont aussi des racines de x^n-1. Si $n=2^m-1$, elles sont des éléments du $CG(2^m)$.
Comme un mot de code est un multiple de g(x), ses racines sont aussi racines des mots de code.
Si les racines de g(x) sont $\alpha_1,\alpha_2,\alpha_3.....,\alpha_u$, $c(\alpha_j)=0$ pour $j=1...u$. Les α_j sont des puissances de l'élément primitif du $CG(2^m)$.
Ceci peut s'expliciter par : $c_{n-1}\alpha_j^{n-1}+.....+c_1\alpha_j+c_0=0$ pour $j=1...u$.

Ou encore : $\left[\alpha_j^{n-1},\alpha_j^{n-2},.....\alpha_j,1\right]\begin{bmatrix} c_{n-1} \\ c_{n-2} \\ . \\ . \\ c_0 \end{bmatrix}=0$ pour $j=1...u$.

Soit $\begin{bmatrix} \alpha_1^{n-1} & \alpha_1^{n-2} & . & . & \alpha_1 & 1 \\ \alpha_2^{n-1} & \alpha_2^{n-2} & . & . & \alpha_2 & 1 \\ \alpha_3^{n-1} & \alpha_3^{n-2} & . & . & \alpha_3 & 1 \\ . & . & . & . & . & 1 \\ . & . & . & . & . & 1 \\ \alpha_u^{n-1} & \alpha_u^{n-2} & . & . & \alpha_u & 1 \end{bmatrix}\begin{bmatrix} c_{n-1} \\ c_{n-2} \\ . \\ . \\ c_1 \\ c_0 \end{bmatrix}=0$

On peut identifier cette matrice à la matrice de parité ou de contrôle en décomposant verticalement les α_j^i en représentation binaire. Mais le nombre de lignes n'est pas forcément n-k : il le devient si on enlève les lignes nulles ou combinaison linéaires d'autres lignes.

Exemple :

Soit le code C(7,3) engendré par $g(x)=(x^3+x+1)(x+1)=x^4+x^3+x^2+1$.

Ses racines sont : α,α^2,α^4 pour (x^3+x+1)

et 1 pour x+1

La matrice H est : $\begin{bmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

Soit en représentation binaire : $\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$.

Dans la matrice H on n'a pris en compte qu'une des racines correspondant au polynôme minimal.

5-Bibliographie

- Introduction aux codes correcteurs : Pierre Csillag Ed. Ellipses

Le site de Pierre Csillag : http://www.geocities.com/Vienna/5635/

- Codes en bloc détecteurs et correcteurs d'erreurs : Gérard Attal Poly Supélec 05538
- Théorie de l'information – Codage – Communication numérique : Jean-Claude Dany et Marie-Claude Dumas Poly Supélec 11055