Projet de Recherche . 2020-2021

Faculté des Sciences et Techniques
Master 1 - Maths. CRYPTIS

Polynômes de Permutations

A l'attention de :
M. NECER

Rédigé par :
PIARD A.
JACQUET R.
CARVAILLO T.

Table des matières

Introduction **2**

1 Construction des Corps Finis **3**
1.1 Existence et unicité 3
1.2 Construction 4

2 Polynômes de permutations **6**
2.1 Quelques généralités 6
2.2 Histoire de groupes... 7
2.2.1 Préliminaires, l'interpolation de Lagrange 7
2.2.2 Un groupe, enfin ! 8

3 Premiers critères d'identifications avec implémentations **12**
3.1 Considérations triviales 12
3.2 Le critère d'Hermite-Dickson 12
3.3 Implémentations 13

4 Classes de polynômes **14**
4.1 Polynômes exceptionnels 14
4.2 Polynômes linéarisés 16

Conclusion **17**

Références **18**

Introduction

1 Construction des Corps Finis

1.1 Existence et unicité

Soit $\mathbb{K}$ un corps quelconque et soit φ le morphisme suivant :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array} \right.$$

Définition 1. Soit $\mathbb{K}$ un corps quelconque. Toute partie $\mathcal{P}$ de $\mathbb{K}$ vérifiant :

- $\mathcal{P}$ est non vide et est une partie stable pour $+$ et $\times$ de $\mathbb{K}$ et $\mathcal{P}$ muni des lois induites par celles de $\mathbb{K}$ est lui-même un corps.
- $\mathcal{P}$ est un sous anneau de $\mathbb{K}$, $1 \in \mathcal{P}$ et $(p \in \mathcal{P}^* = \mathcal{P} - \{0\} \Rightarrow p^{-1} \in \mathcal{P}^*)$.
- $\mathcal{P}$ est un sous groupe de $(\mathbb{K}, +)$ et $\mathcal{P}^*$ muni de la loi $\times$ est un sous groupe multiplicatif $(\mathbb{K}^*, \times)$.

est appelée sous-corps de $\mathbb{K}$.

Définition 2. Soit $\mathbb{K}$ un corps quelconque.

- $\mathbb{K}$ est dit premier s'il ne contient aucun sous-corps strict.
- Si $\mathbb{K}$ est un corps, le sous-corps de $\mathbb{K}$ engendré par 1_K est un corps premier, c'est le sous-corps premier de $\mathbb{K}$.

Le noyau du morphisme φ est un idéal de $\mathbb{Z}$ et donc de la forme $k\mathbb{Z}$ pour $k \in \mathbb{Z}$. Par le premier théorème d'isomorphisme on a $\mathrm{Im}(\varphi) \cong \mathbb{Z}/n\mathbb{Z}$. Par intégrité de $\mathbb{Z}/n\mathbb{Z}$, $n = 0$ où n est un nombre premier. Si $n = 0$ alors φ est injective et donc le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$. Si $n \neq 0$ alors le sous-corps premier est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et n s'appelle la **caractéristique** de $\mathbb{K}$.

Définition 3. Soient L et $\mathbb{K}$ deux corps. Si L/K est une extension de corps alors L est un espace vectoriel sur K, où l'addition vectorielle est l'addition dans L et la multiplication par un scalaire $K \times L$ est la restriction à $K \times L$ de la multiplication dans L. La dimension du K-espace vectoriel L est appelée le degré de l'extension et est notée $[L : K]$.

Définition 4. Soit P un polynôme sur un corps K. On appelle corps de décomposition de P sur K une extension L de K telle que :

- dans $L[X]$, P est produit de facteurs de degré 1,
- les racines de P engendrent L.

Proposition 1. *Soit P un polynôme sur un corps K. Alors P admet un corps de décomposition, unique à K-isomorphisme près.*

Proposition 2.

— *Le cardinal de* $\mathbb{K}$ *est une puissance de* p.

— *Réciproquement, pour tout* $n \in \mathbb{N}^*$, *il existe un corps* $\mathbb{K}$ *de cardinal* p^n. *En outre* $\mathbb{K}$ *est unique à isomorphisme près.*

Démonstration.

— Puisque le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ alors $\mathbb{K}$ est naturellement muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. On note $n = [\mathbb{K} : \mathbb{Z}/p\mathbb{Z}]$ alors $\#\mathbb{K} = \#(\mathbb{Z}/p\mathbb{Z})^n = p^n$.

— Soit $n \in \mathbb{N}^*$. Si $\mathbb{K}$ est un corps fini de cardinal p^n alors $\mathbb{K}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$: en effet, puisque pour tout $x \in \mathbb{K}$, x est racine de $X^{p^n} - X$ donc $X^{p^n} - X$ possède ses p^n racines dans $\mathbb{K}$.
Réciproquement, soit K le corps de décomposition de X^{p^n} sur $\mathbb{Z}/p\mathbb{Z}$. Soit $\mathcal{K}$ l'ensemble des éléments de K qui sont racines de $X^{p^n} - X$. On vérifie que $\mathcal{K}$ est un sous-corps de K. Puisque $1_K \in \mathcal{K}$, et si $x, y \in \mathcal{K}$ alors $x^{p^n} = x$ et $y^{p^n} = y$, donc $(x+y)^{p^n} x + y$ et $(xy^{-1})^{p^n} = xy^{-1}$, si bien que $x + y, xy^{-1} \in \mathcal{K}$. Par ailleurs la dérivée formelle, $(X^{p^n} - X)' = -1$ est premier avec $X^{p^n} - X$ donc les racines de $X^{p^n} - X$ sont simples. On en déduit alors que $\#\mathcal{K} = p^n$. Finalement $K = \mathcal{K}$ est un corps à p^n éléments et il est unique à isomorphisme près en vertu de l'unicité du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

□

On notera dorénavant $\mathbb{F}_q$ **le** corps fini à $q = p^n$ éléments.

1.2 Construction

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible sur $\mathbb{F}_p$. On note $n = \deg(P)$. Puisque P est irréductible, l'idéal (P) est donc maximal. Le quotient $\mathbb{F}_p[X]/(P)$ est le corps de rupture de P sur $\mathbb{F}_p$ de cardinal p^n. Afin de montrer que l'on peut toujours construire les corps finis nous allons montrer que pour tout $n \in \mathbb{N}^*$ il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.

Proposition 3. *Soit* $n \in \mathbb{N}^*$, *on définit par*

$$\mathcal{P}(n,p) = \{P \in \mathbb{F}_p[X],\ P \text{ unitaire , irréductible de degré } n\}.$$

alors pour tout $n \in \mathbb{N}^*$ *on a,*

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}(n,p)} P.$$

Démonstration.

— Soit P un facteur irréductible de $X^{p^n} - X$ sur $\mathbb{F}_p$ de degré d. Le corps de rupture de P sur $\mathbb{F}_p$ est de cardinal p^d du corps de décomposition $X^{p^n} - X$ sur $\mathbb{F}_p$, c'est-à-dire F_{p^n}, donc d divise n.

— Réciproquement, on suppose que d divise n et soit $P \in \mathcal{P}(n,p)$. Soit α une racine de P dans le corps de rupture de P sur $\mathbb{F}_p$. Alors par le théorème ? on a $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$. D'où α est racine de $X^{p^n} - X$. Or puisque P est irréductible,

alors P est le polynôme minimal de α sur $\mathbb{F}_p$ donc P divise $X^{p^n} - X$. En outre les facteurs irréductible de$X^{p^n} - X$ sur $\mathbb{F}_p$ sont simple puisque P étant le polynôme minimal de α et que P divise $X^{p^n} - X$.

□

Corollaire 1. Soit $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n.

Démonstration. En conservant les notations de la proposition précédente, il s'agit de montrer que $\#\mathcal{P}(n,p) > 0$. Pour ce faire on évalue le degré de l'égalité

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}(n,p)} P.$$

on a alors

$$p^n = \sum_{d|n} d \cdot \#\mathcal{P}(n,p)$$

On en déduit alors que pour tout $d \in \mathbb{N}^*$ on a $p^d \geq d \cdot \#\mathcal{P}(n,p)$, puis,

$$\begin{aligned} n \cdot \#\mathcal{P}(n,p) &= p^n - \sum_{d|n, d \neq n} d \cdot \#\mathcal{P}(n,p) \\ &\geq p^n - \sum_{d|n, d \neq n} p^d \\ &\geq p^n - \sum_{d=1}^{n-1} p^d \\ &\geq p^n - p\frac{p^{n-1} - 1}{p-1} > 0 \end{aligned}$$

Puisque n est positif alors $\mathcal{P}(n,p) > 0$. □

2 Polynômes de permutations

2.1 Quelques généralités

Rappelons d'abord ce qu'est un polynôme dans le cas général.

Définition 5. Soit K un ensemble non vide. On appelle polynôme en l'indéterminée X, toute application

$$P : \left| \begin{array}{ccc} K & \longrightarrow & K \\ X & \longmapsto & \sum_{i=0}^{n} a_i X^i, a_i \in K. \end{array} \right.$$

Définition 6. Soit K un ensemble fini de cardinal $n \in \mathbb{N}^*$. Une permutation de K est une bijection de K dans K.

Définition 7. Soit P un polynôme de $\mathbb{F}_q[X]$. P est appelé **polynôme de permutation** de $\mathbb{F}_q$ si et seulement si la fonction associée

$$P : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & P(x) \end{array} \right.$$

est une permutation, c'est-à-dire est bijective.

Exemples. On se place dans $\mathbb{F}_5$.

1. Le polynôme X^3 est un polynôme de permutation. En effet, l'application

$$P : \left| \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ X & \longmapsto & X^3 \end{array} \right.$$

est clairement bijective.

2. Le polynôme X^2 n'est pas un polynôme de permutation. Considérons l'application

$$P : \left| \begin{array}{ccc} \mathbb{F}_5 & \longrightarrow & \mathbb{F}_5 \\ X & \longmapsto & X^2 \end{array} \right.$$

En effet cette application n'est pas injective. Soient $(X, Y) \in (\mathbb{F}_5 \times \mathbb{F}_5)$. On a $P(X) = P(Y)$ si et seulement si $X^2 = Y^2$. En prenant $X = 2$ et $Y = 3$ on fausse l'injectivité.

De manière plus générale, nous avons pour $k \in \mathbb{N}$

Proposition 4. *X^k est un polynôme de permutation de $\mathbb{F}_q$ si et seulement si $pgcd(k, q-1) = 1$.*

Démonstration. $\Leftarrow$ Supposons que $pcgd(k, q-1) = 1$. Soit

$$P : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & P(x) \end{array} \right.$$

Si $pcgd(k, q-1)$, i.e. si $k \nmid q-1$ ou $q-1 \nmid k$, il est évident que $x^k \neq 0 \ \forall x \in \mathbb{F}_q \backslash \{0\}$. Donc 0 est le seul antécédent de 0. $\mathbb{F}_q$ étant un corps, on a $\mathbb{F}_q^* = \mathbb{F}_q^\times$, donc $|\mathbb{F}_q^*| = q-1$. Soit α un générateur de $\mathbb{F}_q^*$. La théorie élémentaire des groupes nous donne $| < \alpha^k > | = \frac{q-1}{pcgd(k,q-1)}$. Et donc par hypothèse, $| < \alpha^k > | = q-1$. Donc $P(\alpha)$ engendre $P(\mathbb{F}_q^*)$ et par cardinalité nous obtenons la conclusion voulue.
$\Rightarrow$ Nous allons raisonner par contraposée, i.e. montrer que $pcgd(k, q-1) \neq 1 \Rightarrow X^k$ n'est pas un polynôme de permutation.
Supposons donc $pcgd(k, q-1) = m$, où $m \in \mathbb{N}$, on obtient donc

$$\left\{ \begin{array}{l} k = k'.m \\ q-1 = q'.m \end{array} \right.$$

Et par suite, $k = k'.\frac{q-1}{q}$.
Donc, $X^k = X^{k'.\frac{q-1}{q}} = (X^{(q-1)})^{\frac{k'}{q'}} = 1$. Donc, $\forall x \in \mathbb{F}_q^\times$, $P(x) = 1$, l'application associé n'est donc pas bijective, par suite P n'est pas un polynôme de permutation. On obtient donc l'équivalence souhaitée. □

2.2 Histoire de groupes...

2.2.1 Préliminaires, l'interpolation de Lagrange

Les motivations et descriptions analytiques détaillées de cette notion n'entrent pas dans le cadre de ce projet. Nous nous contenterons donc de rappeler, dans notre cadre, la définition suivante :

Définition 8. Soit

$$\phi : \left| \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & \phi(x) \end{array} \right.$$

Le problème est de trouver un polynôme P, de degré minimal $\leq q$, tel que

$$P(x) = \phi(x) \ \forall \in x \in \mathbb{F}_q.$$

Proposition 5 (Admise)**.** *L'unique solution au problème présenté ci-dessus est donnée par*

$$P(x) := \sum_{d \in \mathbb{F}_q} \phi(d).\frac{\prod\limits_{c \in \mathbb{F}_q, c \neq d} (x-c)}{\prod\limits_{c \in \mathbb{F}_q, c \neq d} (d-c)}$$

Proposition 6. *De manière plus élégante, nous avons*

$$P(x) := \sum_{d \in \mathbb{F}_q} \phi(d)(1-(x-d)^{q-1})$$

Démonstration. De manière générale, nous avons que $X^q - X = \prod_{c\in\mathbb{F}_q}(X-c)$, donc

$$\begin{aligned}\prod_{c\in\mathbb{F}_q,c\neq d}(x-c) &= \frac{\prod_{c\in\mathbb{F}_q}(x-c)}{x-d}\\ &= \frac{x^q-x}{x-d}\\ &= \frac{x^q-d^q-(x-d)}{x-d}\\ &= (x-d)^{q-1}-1\end{aligned}$$

En appliquant cette égalité pour $x = d$, on obtient que

$$\prod_{c\in\mathbb{F}_q,c\neq d}(d-c) = -1$$

Finalement, on obtient que

$$\sum_{d\in\mathbb{F}_q}\phi(d).\frac{\prod_{c\in\mathbb{F}_q,c\neq d}(x-c)}{\prod_{c\in\mathbb{F}_q,c\neq d}(d-c)} = \sum_{d\in\mathbb{F}_q}\phi(d)(1-(x-d)^{q-1})$$

et la proposition est ainsi prouvée. □

Remarque 1. Il est facile de voir que si ϕ est un polynôme, alors l'interpolation de Lagrange est une simple application du lemme chinois des restes.
Il suffit de considérer la solution P du système

$$\begin{cases}\phi \equiv 1 \pmod{X-c_1}\\ \phi \equiv 1 \pmod{X-c_2}\\ \ldots\\ \phi \equiv 1 \pmod{X-c_q}\end{cases}$$

pour s'en convaincre.

De cette remarque découle le fait que pour travailler sur des polynômes de permutation, il suffit de les regarder modulo $X^q - X$. Nous allons dès lors obtenir une structure intéressante, celle de groupe.

2.2.2 Un groupe, enfin !

Proposition 7. *L'ensemble* $\mathbb{P}\mathrm{ol}\mathbb{y}$ *des polynômes de permutation à coefficient dans* $\mathbb{F}_q$ *et de degré inférieur à* q *muni de la loi de composition* $\circ$ *est un groupe, i.e,* $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ)$ *est un groupe.*

Démonstration. Soient $P = \sum_{i\in[\![0,q]\!]} A_i X^i$, $Q = \sum_{j\in[\![0,q]\!]} B_j X^j$ et $R = \sum_{k\in[\![0,q]\!]} C_k X^k$ des polynômes à coefficients dans $\mathbb{F}_q$.

- ♣ La composée de deux polynômes est encore un polynôme. Il est de plus facile de remarquer que si l'on permute un ensemble deux foix, cela reste un ensemble permuté. La composition de deux polynômes de permutation est donc un polynôme de permutation. Nous avons donc notre loi interne.
- ♣ Montrons son associativité :
  D'une part, on a

$$(P\circ Q)\circ R$$

$$= \sum_{i\in[\![0,q]\!]} A_i \left(\sum_{j\in[\![0,q]\!]} B_j X^j\right)^i \circ \left(\sum_{k\in[\![0,q]\!]} C_k X^k\right)$$

$$= \sum_{i\in[\![0,q]\!]} A_i \left(\sum_{j\in[\![0,q]\!]} B_j \left(\left(\sum_{k\in[\![0,q]\!]} C_k X^k\right)\right)^j\right)^i$$

  puis,

$$P\circ(Q\circ R)$$

$$= \left(\sum_{i\in[\![0,q]\!]} A_i X^i\right) \circ \left(\sum_{j\in[\![0,q]\!]} B_j \left(\left(\sum_{k\in[\![0,q]\!]} C_k X^k\right)\right)^j\right)$$

$$= \sum_{i\in[\![0,q]\!]} A_i \left(\sum_{j\in[\![0,q]\!]} B_j \left(\left(\sum_{k\in[\![0,q]\!]} C_k X^k\right)\right)^j\right)^i$$

  donc la loi $\circ$ est associative.
- ♣ Le neutre est évidemment le polynôme constant égal à 1.
- ♣ Rappelons que, par définition, un polynôme de permutation est une application bijective de $\mathbb{F}_q$. Il suffit donc de considérer son application récipoque P^{-1} pour obtenir Q tel que $P\circ Q = 1$. Ceci nous donne l'élément neutre. Ceci marche toujours modulo $X^q - X$ car

$$\Pi : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]\backslash(X^q - X) \\ P & \longmapsto & [P]_{X^q-X} \end{array} \right.$$

  est un morphisme d'anneaux.

Il s'ensuit que $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ)$ est un groupe. □

Proposition 8. *On a l'isomorphisme suivant,* $(\mathbb{P}\mathrm{ol}\mathbb{y}, \circ) \cong \mathbb{S}_q$*, où* $\mathbb{S}_q$ *est le groupe des permutations de l'ensemble* $[\![1, ..., q]\!]$.

Démonstration. La difficulté de cette preuve réside dans le fait qu'un polynôme de $\mathbb{F}_q$ peut être représenté par une permutation très complexe et inversement. On rappelle que dans $\mathbb{S}_q$, toute permutation τ peut être représentée comme produit de transpositions. Dans notre cas il est suffisant de considérer les transpositions échangeant uniquement les éléments 0 et $a \in \mathbb{F}_q$ que l'on note $\tau_{0,a}$. Il vient alors que pour toutes transpositions de $\mathbb{S}_q$ échangeant deux éléments a et b de $\mathbb{F}_q$ on a,

$$\tau_{0,a} \cdot \tau_{0,b} \cdot \tau_{0,a} = \tau_{a,b}$$

si bien que l'on exhibe le polynôme associé à la transposition

$$\tau_{0,a} : \mathbb{t}(x) = -a^2 \left[\left((x-a)^{q-2} + a^{-1} \right)^{q-2} - a \right]^{q-2}$$

Il est facile de le vérifier dans le cas où $a = 1$. On considère le corps $\mathbb{F}_p$. On remarque que

$$\mathbb{g}_1(x) - x = \begin{cases} 1 & \text{si } x = 0 \\ -1 & \text{si } x = 1 \\ 0 & \text{sinon.} \end{cases}$$

On en déduit alors que $\mathbb{g}_0(x) - x = (ax + b) + \prod_{k=2}^{p-1}(x-k)$

En appliquant notre égalité pour $x = 1$ et $x = 0$ on obtient le système suivant,

$$\begin{cases} 1 & = -b(p-1)! \\ -1 & = -(a+b)(p-2)! \end{cases}$$

Or puisque dans $\mathbb{F}_p$ on a $(p-1)! = -1$ et $(p-2)! = 1$ alors on en déduit que $(a, b) = (0, 1)$ et donc $\mathbb{g}_1(x) = x + \prod_{k=2}^{p-1}(x-k)$. □

Proposition 9. *Soit α un élément primitif de $\mathbb{F}_q$, alors $(\mathbb{Poly}, \circ)$ est engendré par $\{\alpha X, X+1, X^{q-2}\}$*

Démonstration. Remarquons tout d'abord que, pour $a, b \in \mathbb{F}_q$,

- $< aX > = < \alpha^m X > = < \alpha X >^m$ (cette dernière égalité découle de la loi de composition)
- $< \alpha X >^{m-n} < X+1 > < \alpha X >^n$
  $= < \alpha X >^{m-n} < \alpha^n X + 1 >$
  $= < \alpha^{m-n} X > < \alpha^n X + 1 >$
  $= < \alpha^{m-n}(\alpha^n X + 1) >$
  $= < \alpha^m X + \alpha^{m-n} >$, ce qui nous donne un générateur de la forme $< aX + b >$

Il suffit ensuite de considérer la forme générale du polynôme correspond à la transposition $\tau_{0,a}$, en remarquant que

$$\tau_{0,a} =< -a^2X >< X^{q-2} >< X-a >< X^{q-2} >< X+a^{q-2} >< X^{q-2} >< X-a >$$

Il est ensuite aisé de construire n'importe quel polynôme de permutation en sachant que $\tau_{0,a} \cdot \tau_{0,b} \cdot \tau_{0,a} = \tau_{a,b}$ □

3 Premiers critères d'identifications avec implémentations

Nous venons de voir les premières définitions et propriétés sur les polynômes de permutation. Il est plus que nécessaire, avant de se lancer dans la tâche ardue qu'est l'étude des polynômes de permutations, de se donner les moyens de les identifier, ou tout du moins de savoir les reconnaître. Dans cette partie, nous verrons trois premiers critères triviaux, qui seront implémentés en *Python* via *Sagemath*.

3.1 Considérations triviales

Une manière bien simple de reconnaitre un polynôme de permutation consiste à en calculer toute les images, puis de les comparer une à une. Si une image est égale à une autre, i.e. l'application n'est pas injective, alors le polynôme ne sera pas de permutation. On obtient dès lors le critère suivant :

Critère 1. Un polynôme $P \in \mathbb{F}_q[X]$ est une permutation de $\mathbb{F}_q$ si et seulement si

$$\prod_{c \in \mathbb{F}_q} (X - P(c)) = X^q - X$$

En plus d'être très peu élégante, cette méthode requiert une puissance de calcul, croissante et en le degré du polynôme et en le cardinal du corps dans lequel on se place.

A l'attention des bg, question 1. Inclut-on les raisonnement sur la complexité du calcul ?

Il est également possible de faire la démarche en sens inverse, et de considérer les antécédents.

Critère 2. P est un polynôme de permutation si et seulement si $\forall \alpha \in \mathbb{F}_q$,

$$deg((X^q - X) \wedge (P(X) - \alpha)) = 1$$

Démonstration. En effet, le fait que $deg((X^q - X) \wedge (P(X) - a)) \neq 1$ signifie que $X^q - X$ et $P(X) - a$ ont comme facteur commun $\prod_{c \in \mathbb{F}_q, P(c) = a} (X - c)$, donc $P(X) - a$ s'annule en plusieurs points et finalement P n'est pas une bijection.
Réciproquement, si $deg((X^q - X) \wedge (P(X) - a)) = 1$, alors le seul facteur commun à $X^q - X$ et $P(X) - a$ est $X - c$, où c est tel que $P(c) = a$. La conclusion s'ensuit. □

3.2 Le critère d'Hermite-Dickson

Soit $q = p^n$ une puissance d'un nombre premier quelconque. On rappelle que la fonction

$$\Pi : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X] \backslash (X^q - X) \\ P & \longmapsto & [P]_{X^q - X} \end{array} \right.$$

définit un morphisme d'anneaux, de sorte que, $\overline{(P(X))^k} = \overline{P(X)}^k \pmod{X^q - X}$. On se donne également un polynôme P à coefficients dans $\mathbb{F}_q$, et l'ensemble

$$A_{p,q} := \{k \in [\![1, q-2]\!] \text{ tels que } p \nmid k\}$$

Enonçons maintenant le

Critère 3 (Hermite-Dickson)**.** P est un polynôme de permutation si et seulement si les deux conditions suivantes ont lieu

1. pour tout $k \in A_{p,q}$, $deg(\overline{(P(X))^k}) < q-1$
2. $deg(\overline{(P(X))^{q-1}}) = q-1$

A l'attention des bg, question 2. Possiblement implémentable ?
Si oui,

Nous implémenterons ce critère dans un prochain rendu.

3.3 Implémentations

4 Classes de polynômes

Les méthodes d'identifications que nous venons de voir sont, fonctionnelles certes, mais non raffinées. Elles sont extrêmement couteuses en terme de puissance de calcul. Il est donc primordial d'établir une liste de critères permettant d'accélérer le processus. Cette partie y sera entièrement consacrée. Pour ce faire, nous travaillons sur des "familles" de polynômes. Nous n'aurons pas la prétention d'en donner une liste exhaustive ; cependant dans ce premier rendu nous donnerons les plus élémentaires. Une étude plus approfondie sera faite au second semestre.

4.1 Polynômes exceptionnels

Avant de commencer, rappelons la

Proposition 10. *L'ensemble $\mathbb{F}_q[X,Y]$ des polynômes en les indéterminées X et Y à coefficients dans $\mathbb{F}_q$ est muni d'une structure d'anneau, et est construit comme suit :*

$$\mathbb{F}_q[X,Y] = (\mathbb{F}_q[X])[Y] = (\mathbb{F}_q[Y])[X]$$

Définition 9. Un polynôme en les deux indéterminées X et Y est dit absolument irréductible s'il est irréductible sur toute extension de $\mathbb{F}_q$. En d'autres termes, s'il est sur la clôture algébrique $\bar{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Remarque 2. On rappelle que toute extension de $\mathbb{F}_q$ est algébrique, il en va de même de sa clôture.

A l'attention des bg, question 3. On rappelle ce qu'est $\bar{\mathbb{F}}_q$?

Définition 10. On dit qu'un polynôme en l'indéterminée X est exceptionnel sur $\mathbb{F}_q$ si aucun facteurs irréductibles du polynôme en les indéterminées X et Y

$$\Psi(X,Y) := \frac{P(X) - P(Y)}{X - Y}$$

n'est absolument irréductible. En d'autres terme, si les facteurs irréductibles admettent une décomposition sur une extension de $\mathbb{F}_q$.

Avant de nous aventurer dans l'énoncé de critères, voyons un premier exemple de polynôme exceptionnel.

Exemple 1. Considérons le polynôme $P(X) := X^3 + 3X^2 + 3X \in \mathbb{F}_q$, où q est choisit tel qu'il soit la puissance d'un nombre premier impair.

Construisons le fameux polynôme $\Psi(X,Y)$ à partir de P

$$\begin{aligned}\Psi(X,Y) &= \frac{P(X)-P(Y)}{X-Y}\\ &= \frac{X^3+3X^2+3X-Y^3-3Y^2-3Y}{X-Y}\\ &= \frac{X^3-Y^3+3X^2-3Y^2+3X-3Y}{X-Y}\\ &= \frac{(X-Y)(X^2+Y^2)-XY^2+YX^2+3(X+Y)(X-Y)+3X-3Y}{X-Y}\\ &= \frac{(X-Y)(X^2+Y^2)+XY(X-Y)+3(X+Y)(X-Y)+3X-3Y}{X-Y}\\ &= X^2+Y^2+XY+3(X+Y)+3\\ &= X^2+(3+Y)X+Y^2+3Y+3\end{aligned}$$

Nous avons donc un polynôme de degré 2 en l'indéterminée X, faisons une étude de discrimant.
$\Delta_{\Psi(X,Y)} = (3+Y)^2-4(Y^2+3Y+3) = -3(Y+1)^2$
Nous pouvons dès à présent distinguer deux cas :

— -3 est un carré dans $\mathbb{F}_q$, i.e. $\exists c \in \mathbb{F}_q$ tel que $c^2=-3$. Les racines Ψ existent donc ; et

$$\Psi(X,Y) = (X-\frac{-Y-3+c(Y+1)}{2})(X-\frac{-Y-3-c(Y+1)}{2})$$

Ces facteurs étant de degré 1, il est clair qu'ils sont irréductibles sur toute extension de $\mathbb{F}_q$, Ψ présente donc des facteurs absolument irréductibles, il n'est donc pas un polynôme exceptionel.

— dans le cas contraire, $\Psi(X,Y)$ est irréductible dans $\mathbb{F}_q[X,Y]$. Cependant, -3 sera, par définition, un carré dans la clôture algébrique de $\mathbb{F}_q$. (Il suffit de considérer le polynôme X^2-3...) Nous sommes donc dans la même situation que dans le premier cas, à la subtilité près que, cette fois-ci, Ψ admet des facteurs irréductibles dans une extension de $\mathbb{F}_q$ et non dans $\mathbb{F}_q$, donc peu nous importe la réductibilité de ces dit facteurs ! Il s'ensuit que, par définition, Ψ est un polynôme exceptionnel.

Enonçons maintenant un critère fondamental :

Critère 4. Tout polynôme exceptionel à coefficients dans $\mathbb{F}_q[X]$ est un polynôme de permutation.

Exemple 2. De l'exemple précédent, il découle que $P := X^3+3X^2+3X$ est un polynôme de permutation si -3 n'est pas un carré dans $\mathbb{F}_q$.
Dans $F_5 \simeq \mathbb{Z}/5\mathbb{Z}$, $-3 = 2$ qui n'est pas un carré, donc P est un polynôme de permutation. En revanche, dans $F_3 \simeq \mathbb{Z}/3\mathbb{Z}$, $-3 = 0 = 9 = 3^2$, donc P n'est pas un polynôme de permutation.

Remarque 3. La réciproque de ce théorème est fausse. Même s'il existe des conditions sous lesquelles elle a lieu, nous nous contenterons de donner un contre exemple.

Exemple 3. Soit $q = p^n$ une puissance d'un nombre premier quelconque. Soit $P := X^p$, nous avons clairement $pgcd(q-1, p) = 1)$ la *Proposition 4* nous assure donc que P est un polynôme de permutation. Calculons une nouvelle fois le fameux polynôme $\Psi(X, Y)$ à partir de P :

$$\begin{aligned}\Psi(X,Y) &= \frac{P(X)-P(Y)}{X-Y} \\ &= \frac{X^p - Y^p}{X-Y} \\ &= \frac{(X-Y)^p}{X-Y} \text{(on travaille sur un corps de caracteristique } p) \\ &= (X-Y)^{p-1}\end{aligned}$$

Or, les $(X - Y)$ sont évidemment irréductibles sur toute extension de $\mathbb{F}_q$, donc P n'est pas un polynôme exceptionnel.

Nous allons maintenant énoncé un non-critère fort, qui sera admis pour le moment. Sa démonstration s'appuie sur des éléments complexes de la théorie de *Galois* ; nous nous laissons l'opportunité de le démontrer en ce second semestre.

Critère 5 (non-critère)**.** Soit $q = p^n$ une puissance d'un nombre premier quelconque. Soit $k \in \mathbb{N}$, tel que $pgcd(k, q-1) > 1$. Alors, il n'existe pas de polynôme exceptionnel à coefficients dans $\mathbb{F}_q$ de degré k.

4.2 Polynômes linéarisés

Conclusion

Références