Polynômes de permutation

CARVAILLO T. - PIARD A. - JACQUET R.

Université de Limoges

Sommaire

- Qu'est-ce qu'un polynôme de permutation ?
- Structure de groupe
- Premiers critères et algorithmes
- Un exemple de famille de polynômes
- Applications en cryptographie

Qu'est-ce qu'un polynôme de permutation ?

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.

Structure de groupe

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

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

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

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

On a l'isomorphisme $(\mathbb{Poly}, \circ) \cong \mathbb{S}_q$

Premiers critères

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

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

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    temp = t - f(R(0)) # R(0) désigne le premier élément du corps F_q
    for i in R:
        if R(0) == i:
            continue
        temp = temp * (t - f(i))
    if temp == t**q - t:
        return (True)
    return (False)
```

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

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

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    a = t**q - t
    for element in R:
        if (a.gcd(f - element)).degree() != 1:
            return (False)
    return(True)
```

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

1. pour tout $k \in A_{p,q}$, $deg(\overline{(P(X))^k}) < q - 1$ $\quad A_{p,q} := \{k \in [\![1, q-2]\!] \text{ tels que } p \nmid k\}$
2. $deg(\overline{(P(X))^{q-1}}) = q - 1$

```
def estDePermutation(f, q):
    R.<x> = GF(q) # Corps fini à q éléments
    S.<t> = PolynomialRing(R) # Anneau de polynômes sur F_q en l'indéterminée t
    f = S(f)
    a_pk = []
    for i in range(0, q-2):
        if p % k != 0:
            a_pk.append(i)
    for j in a_pk:
        if (f(t)**j % (t**q - t)).degree() > q - 1:
            return (False)
    if (f(t)**(q-1) % (t**q - t)).degree() == q - 1:
        return (True)
    return (False)
```

Un autre critère dépendant des caractères

Définition 9. Soit G un groupe abélien fini d'ordre n. On appelle caractère additif de G tout homomorphisme χ de G dans le groupe W_n des racines n-ièmes de l'unité.

Critère 4. Soit P un polynôme à coefficients dans $\mathbb{F}_q$, alors P est de permutation si et seulement si $\displaystyle\sum_{\alpha \in \mathbb{F}_q} \chi(P(\alpha)) = 0$ pour tout caractère additif non-trivial.

Un exemple de famille de polynômes

Les polynômes exceptionnels

Polynôme absolument irréductible : Irréductible sur toute extension du corps où il est défini.

Définition 14. On dit qu'un polynôme en l'indéterminée X est exceptionnel sur $\mathbb{F}_q$ si aucun facteur irréductible 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 $\mathbb{F}_q$.

Critère 5. Tout polynôme exceptionnel à coefficients dans $\mathbb{F}_q[X]$ est un polynôme de permutation.

Exemple $P(X) := X^3 + 3X^2 + 3X \in \mathbb{F}_q$

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

Applications en cryptographie

RSA

Polynôme de permutation : X^e, où *e* est l'exposant de chiffrement.

Avantages

- $X^e \mod n \Longrightarrow X$ impossible en temps raisonnable.
- Simple exponentiation modulaire.

LUC

$$\mathbb{D}_0(X,\alpha) = 2 \ , \ \mathbb{E}_0(X,\alpha) = 1$$

$$\mathbb{D}_n(X,\alpha) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} (-\alpha)^k X^{n-2k} \ , \ \textbf{si } n \textbf{ est positif}$$

$$\mathbb{E}_n(X,\alpha) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} (-\alpha)^k X^{n-2k} \ , \ \textbf{si } n \textbf{ est positif}$$

On obtient alors les relations de récurrences suivante,

$$\mathbb{D}_n(X,\alpha) = X\mathbb{D}_{n-1}(X,\alpha) - \alpha\mathbb{D}_{n-2}(X,\alpha)$$
$$\mathbb{E}_n(X,\alpha) = X\mathbb{E}_{n-1}(X,\alpha) - \alpha\mathbb{E}_{n-2}(X,\alpha)$$

Proposition 19. Soit $a \in \mathbb{F}_q^*$, le polynôme $\mathbb{D}_n(X,a)$ est de permutation sur $\mathbb{F}_q$ si et seulement si $\text{pgcd}(n, q^2-1) = 1$.