TP4 : Factorisation partielle de polynômes univariés sur un corps fini

Résumé du TP

Bertrand Meyer

4 décembre 2019

Ingrédient principal

On souhaite factoriser un polynôme $f \in \mathbb{F}_q[x]$.

Outil unique :
Calculer des pgcd entre f et des polynômes *intelligemment choisis*.

Démarche en trois étapes.

1. Découpage par exposant
2. Découpage par degré
3. Découpage final

L’algorithme de Yun

La factorisation sans facteurs carrés

Soit un polynôme à factoriser

$$g = \prod_{1 \leq i \leq k} f_i^{e_i} \in \mathbb{Q}[X]$$

et $(f_i)_{i \leq k}$ ses facteurs irréductibles distincts.

Étape 1 : Regrouper par exposant : i.e. trouver

$$g_j = \prod_{i \text{ t.q. } e_i = j} f_i.$$

Calcul de g_1 en caractéristique 0

$$g' \text{ est } \begin{cases} \text{divisible par} & f_i^{e_i-1} \\ \text{non-divisible par} & f_i^{e_i} \end{cases}$$

Calcul de g_1 en caractéristique 0

$$g' \text{ est } \begin{cases} \text{divisible par} & f_i^{e_i-1} \\ \text{non-divisible par} & f_i^{e_i} \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{1 \le i \le k} f_i^{e_i-1}$$

Calcul de g_1 en caractéristique 0

$$g' \text{ est } \begin{cases} \text{divisible par} & f_i^{e_i-1} \\ \text{non-divisible par} & f_i^{e_i} \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{1 \leq i \leq k} f_i^{e_i-1} \quad \text{et} \quad u = \frac{g}{t} = \prod_{1 \leq i \leq k} f_i$$

Calcul de g_1 en caractéristique 0

$$g' \text{ est } \begin{cases} \text{divisible par} & f_i^{e_i-1} \\ \text{non-divisible par} & f_i^{e_i} \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{1 \leq i \leq k} f_i^{e_i-1} \quad \text{et} \quad u = \frac{g}{t} = \prod_{1 \leq i \leq k} f_i$$

Finalement, on obtient

$$g_1 = \prod_{i \text{ t.q. } e_i=1} f_i = \frac{u}{u \wedge t}.$$

Calcul de g_1 en caractéristique 0

$$g' \text{ est } \begin{cases} \text{divisible par} & f_i^{e_i-1} \\ \text{non-divisible par} & f_i^{e_i} \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{1\leq i\leq k} f_i^{e_i-1} \quad \text{et} \quad u = \frac{g}{t} = \prod_{1\leq i\leq k} f_i$$

Finalement, on obtient

$$g_1 = \prod_{i \text{ t.q. } e_i=1} f_i = \frac{u}{u \wedge t}.$$

Récursion sur t pour trouver g_j avec $j \geq 2$.

Calcul de g_1 en caractéristique p

$$g' \text{ est } \begin{cases} \text{exactement divisible par} & f_i^{e_i - 1} & \text{si} & i \text{ non-multiple de } p \\ \text{exactement divisible par} & f_i^{e_i} & \text{si} & i \text{ multiple de } p \end{cases}$$

Calcul de g_1 en caractéristique p

$$g' \text{ est } \begin{cases} \text{exactement divisible par} \quad f_i^{e_i-1} \quad \text{si} \quad i \text{ non-multiple de } p \\ \text{exactement divisible par} \quad f_i^{e_i} \quad \text{si} \quad i \text{ multiple de } p \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{\substack{1 \leq i \leq k, \\ i \text{ non multiple} \\ \text{de } p}} f_i^{e_i-1} \prod_{\substack{1 \leq i \leq k, \\ i \text{ multiple de } p}} f_i^{e_i} \quad \text{et} \quad u = \frac{g}{t} = \prod_{\substack{1 \leq i \leq k, \\ i \text{ non multiple} \\ \text{de } p}} f_i$$

Calcul de g_1 en caractéristique p

$$g' \text{ est } \begin{cases} \text{exactement divisible par } & f_i^{e_i-1} & \text{si} & i \text{ non-multiple de } p \\ \text{exactement divisible par } & f_i^{e_i} & \text{si} & i \text{ multiple de } p \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{\substack{1 \leq i \leq k, \\ i \text{ non multiple} \\ \text{de } p}} f_i^{e_i-1} \prod_{\substack{1 \leq i \leq k, \\ i \text{ multiple de } p}} f_i^{e_i} \quad \text{et} \quad u = \frac{g}{t} = \prod_{\substack{1 \leq i \leq k, \\ i \text{ non multiple} \\ \text{de } p}} f_i$$

Finalement, on obtient

$$g_1 = \prod_{i \text{ t.q. } e_i = 1} f_i = \frac{u}{u \wedge t}.$$

Récursion sur t pour trouver g_j avec $j \geq 2$ et j non-multiple de p.

Calcul de g_1 en caractéristique p

$$g' \text{ est } \begin{cases} \text{exactement divisible par } & f_i^{e_i-1} & \text{si} & i \text{ non-multiple de } p \\ \text{exactement divisible par } & f_i^{e_i} & \text{si} & i \text{ multiple de } p \end{cases}$$

Donc

$$t = g \wedge g' = \prod_{\substack{1 \le i \le k, \\ i \text{ non multiple} \\ \text{de } p}} f_i^{e_i - 1} \prod_{\substack{1 \le i \le k, \\ i \text{ multiple de } p}} f_i^{e_i} \quad \text{et} \quad u = \frac{g}{t} = \prod_{\substack{1 \le i \le k, \\ i \text{ non multiple} \\ \text{de } p}} f_i$$

Finalement, on obtient

$$g_1 = \prod_{i \text{ t.q. } e_i = 1} f_i = \frac{u}{u \wedge t}.$$

Récursion sur t pour trouver g_j avec $j \geq 2$ et j non-multiple de p.

Reste finalement $t = \prod_{\substack{j \text{ multiple} \\ \text{de } p}} g_j^{e_j}$

Racine p-ième d'un polynôme en caractéristique p

Un polynôme $f \in \mathbb{F}_q[x]$ est de la forme u^p ssi $f' = 0$.

$$\left(u_d x^d + \cdots + u_1 x + u_0\right)^p = (u_d)^p x^{pd} + \cdots + (u_1)^p x^p + (u_0)^p.$$

Exemple

$$3x^{125} + 2x^{30} + 4x^5 + 2 = (3x^{25} + 2x^6 + 4x + 2)^5 \in \mathbb{F}_5[x].$$

Factorisation étagée en degrés distincts

Factorisation étagée en degrés distincts

Soit un polynôme à factoriser

$$g_j = \prod_{1 \leq i \leq k} f_i \in \mathbb{Q}[X]$$

et $(f_i)_{i \leq k}$ ses facteurs irréductibles distincts.

Étape 2 : Regrouper par degrés : i.e. trouver

$$g_{j,d} = \prod_{i \text{ t.q. } \deg f_i = d} f_i.$$

Critère de Rabin

Théorème

Le polynôme $x^{q^n} - x \in \mathbb{F}_q[x]$ est le produit des irréductibles unitaires de degré divisant n.

Algorithme de factorisation en degré distincts

Entrée : $f \in \mathbb{F}_q[x]$ sans facteur carré.

Pour d de 1 à ∞ :

- $g_d \leftarrow f \wedge (x^{q^d} - x)$
- $f \leftarrow f / g_d$.

Fin de la factorisation

Factorisation étagée en degrés distincts

Soit un polynôme à factoriser

$$g_{j,d} = \prod_{1 \leq i \leq k} f_i \in \mathbb{Q}[X]$$

et $(f_i)_{i \leq k}$ ses facteurs irréductibles distincts tous de même degré d.

Étape 3 : Trouver les facteurs, c'est-à-dire les

$$f_i.$$

Cantor-Zassenhauss

Théorème
Si f produit d'irréductibles distincts de degré d, pour tout polynôme $u(x)$,

$$f = (f \wedge u) \cdot \left(f \wedge (u^{(q^d-1)/2} - 1)\right) \cdot \left(f \wedge (u^{(q^d-1)/2} + 1)\right).$$

Algorithme de factorisation en degré distincts
Entrée : $f \in \mathbb{F}_q[x]$ produit d'irréductibles distincts de degré d.
Répéter jusqu'à factorisation complète

- Tirer u au hasard
- Calculer $t \leftarrow f \wedge (u^{(q^d-1)/2} - 1)$
- Répéter sur t et sur f/t.