Plaisir Géométrie Diophantienne et polynômes lacunaires

1. Racines et facteurs de petit degré

$f(t) = \sum_{i=1}^{N} c_i t^{a_i} \in \mathbb{Z}[X]$ $\quad d = \deg f = \max a_i$

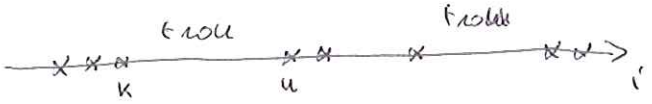
$\ell(f)$ = taille de l'entrée $\approx \max_i(\log|c_i|, \log a_i) \approx \max(h(f), \log d, N)$

Remarque : exponentiel en $\ell(f)$

Cucker-Koiran-Smale '98 : $\xi \in \mathbb{Z}$ donné. $f(\xi)=0$?

Remarque si $\xi \neq 0, \pm 1 \Rightarrow$ taille de $f(\xi)$ exponentiel en $\ell(f)$

Mais on a



des gros trous !

$$f(X) = r(X) + X^u q(t)$$

$\deg r = k < u$, $k-u$ « grand »

Supposons $f(\xi) \neq 0$ et $q(\xi) \neq 0$

Alors (← norme ℓ_1 du vecteur des coeffs)

$$|r(\xi)| \leq \|f\|_1 \cdot |\xi|^k$$

$$|\xi^u q(\xi)| = |\xi|^u \cdot |q(\xi)| \overset{\text{Dio}}{\geq} |\xi|^u \quad (q(\xi) \in \mathbb{N}_{\geq 1})$$

$$\Rightarrow \quad \|f\|_1 \geq |\xi|^{u-k} \overset{\text{Dio}}{\geq} 2^{u-k}$$

$$\Rightarrow \quad u-k \leq \frac{\log \|f\|_1}{\log 2} \quad , \text{« extrapolation »}$$

Il suffit donc de sauvegarder f en morceaux assez → espacés de $f_1, \dots, f_m$ et tester par chaque morceau si $f(\xi)=0$.

$$\rightarrow \quad f = \sum \alpha^{n_j} f(t)$$

↑
petit signé

Et si $\xi \in \mathbb{Q}^*$? $\xi = a/b$, $(a,b)=1$

$$(*) \qquad u - \kappa \geq \frac{\log \|f\|_1}{h(\xi)} \qquad h(\xi) = \max(\log|a|, \log|b|)$$

Pareil.

Et si $\xi \in \overline{\mathbb{Q}}^*$? Supposons pour simplifier ξ entier algébrique : l'équation minimale unitaire de ξ sur $\mathbb{Q}$ est à coefficients entiers. On définit (« hauteur de Weil ») :

$$h(\xi) = \frac{1}{n} \sum_{i=1}^{n} \log \max(|\xi_i|, 1) \qquad \geq 0$$

($n = \deg \xi$, ξ_i racines du polynôme minimale)

Kronecker : $\xi \neq$ racine de $1 \iff h(\xi) = 0$

Lehmer conj : $\xi \neq$ racine de $1 \implies h(\xi) \geq C_\varepsilon n^{-1-\varepsilon}$ ← Dobrowolski

On a encore $(*)$! Et on sait évaluer rapidement dans les racine de 1.

Th (Lenstra '99)
On peut calculer les facteurs irréductibles de f de degré $\leq n$ en temps $(\ell(f) + n)^{O(1)}$

(Factorisation dense pour chaque morceau)

Ex $f(X) = X^p - 1$ $\qquad \ell(f) \approx \log p$

$= (t-1)\, h(X)$ $\qquad h(X) = 1 + t + \cdots + t^{p-1}$ $\qquad \ell(h) \geq p$

groupe algébrique

[2] En plusieurs (deux) variables $(\overline{\mathbb{Q}}^*)^2 = \mathbb{G}_m^2(\overline{\mathbb{Q}})$

$\overline{\mathbb{Q}}^*$

1

sous-tores $T: 1$, $x^a y^b - 1 = 0$, $\mathbb{G}_m^2$
$(a,b)=1$

ξ racine de 1

variété de torsion : $T\xi$

sous-tore — point de torsion

$h(\xi)$

$\mathcal{P}_{\infty}(\mathcal{C}) = \inf\{h > 0 \mid \exists \infty\, \alpha \in \mathcal{C}$
$h(\alpha) \leq h\}$

courbe

~~torsion~~ torsion $\iff$ $\mathcal{P}_{\infty}(\mathcal{C}) = 0$ (Lehmer Manford)

$\mathcal{C} \neq$ torsion $\implies$ $\mathcal{P}_{\infty}(\mathcal{C}) \geq \ldots$ $**$

$\rightsquigarrow$ On généralise davantage CKS ~~aux facteurs~~
à la recherche des facteurs im. de degré d borné
d'un polynôme recherché en plusieurs variables :

Avendano - Kwek - Sombre 05 ($**$: A - David 03)
Kaltofen - Koiran 05 ($**$: A - Zannier 00)

[2] gcd (moins existé ...)

f lacunaire $\Leftrightarrow$ on fixe le squelette de f

$$f_{\underline{a}}(t) = F(x_1^{a_1} \cdots x_N^{a_N})$$

où $F \in \mathbb{Z}[x_1, \ldots, x_N]$ est fixé

et $a_1, \ldots, a_N \in \mathbb{Z}$ varient

(f est la restriction d'une fonction régulière sur $\mathbb{G}_m^n$

– Un polynôme de Laurent – c'est un sous-groupe à 1 paramètre qui varie)

$\rightarrow$ $d = \deg f << \max |a_i|$

f, g lacunaires $\rightsquigarrow$ $\gcd(f, g) = ?$

F G

Remarques

· Euclide : exponentiel (polynômiale en d $\rightarrow$ exp dans la taille des données !)

· Plaisted : le calcul du degré du gcd en codage lacunaire $=$ NP-hard

(i.e. tout problème NP peut se réduire en temps polynomiale à celui ci) $\longrightarrow$

Filaseta, Granville, Schinzel (2008)

Soit $f, g \in \mathbb{Z}[X]$ sans facteurs cyclotomiques. Alors on peut calculer $\gcd(f, g)$ en $\tilde{O}_{F,G}(\log d)$ opérations $\deg f, \deg g \leq d$

Compliment : A., Lecerf, Sombra (19) – Même résultat pour calculer $p \mid \gcd(f, g)$ et l.q. $\gcd(f, g)/p$ = produit de cyclotomiques $\longrightarrow$

Exemple a, b premiers entre eux

$$\gcd\left(X^{ab} - 1, (t^a - 1)(t^b - 1)\right) = \frac{(t^a - 1)(t^b - 1)}{t - 1}$$ pas lacunaire !

On peut également calculer les racines cyclotomiques de $b = g = 0$ -

→ <u>En particulier</u> : on peut décider si b et g sont premiers entre eux avec complexité quasi-linéaire

Rm/ Plaisted : décider $\gcd(b, g) = 1$ NP-hard

Donc $P \neq NP \Rightarrow$ décider $\gcd(b, g) = 1$ pas polynomial en h, # coeff, log coeff

L'outil diophantien

Conjecture (Schinzel '65)

$F, G \in \mathbb{Z}[X_1, \dots, X_N]$ premiers entre eux.

$\xi \neq$ racine de 1, $F(\xi^{a_1}, \dots, \xi^{a_N}) = G(\xi^{a_1}, \dots, \xi^{a_N}) = 0$.

Alors $\exists\, \underline{b} \in \mathbb{Z}^N \setminus \{0\}$, $\|\underline{b}\|_1 \leq C(F,G)$, $\underline{b} \perp \underline{a}$

Prouvé par Bombieri et Zannier ('95) : géométrie des nombres + minoration de la hauteur en $\mathbb{G}_m^n$ (A.-David '95)

Conjecture $\rightarrow$ FGS

Si $(F,G) \neq 1$, tant mieux ! Sinon, $\forall \xi$ racine commune de $F(t^{\underline{a}})$, $G(t^{\underline{a}})$, il existe $\underline{b} \in \mathbb{Z}^N \setminus \{0\}$ dans un ensemble fini t.q. $\underline{b} \perp \underline{a}$ — le plus petit élément de valuable on peut supposer $\underline{b} = (0, \dots, 0, 1)$, i.e. ξ racine de $F(t^{\underline{a}}) = \tilde{F}(t^{a_1}, \dots, t^{a_{N-1}})$ et de $G(t^{\underline{a}}) = \tilde{G}(t^{a_1}, \dots, t^{a_{N-1}})$ — On continue ...

Plus précisément, cela donne un ensemble fini de matrices $\mathcal{A}$ de $\mathbb{Z}^{N \times N}$ t.q. $\forall\, \underline{a} \in \mathbb{Z}^N \setminus \{0\}$, $\exists\, A \in \mathcal{A}$, $\underline{a} = A\underline{a}'$ et on obtient la (la partie non-cyclotomique du) pgcd de $F(t^{\underline{a}})$ et $G(t^{\underline{a}})$ du pgcd de $F(\underline{x}^A)$ et $G(\underline{x}^A)$ par spécialisation $\underline{x} \rightarrow t^{\underline{a}'}$

Dépendence dans les coefficients

$$F(x,y) = x - p \qquad G(x,y) = y - p^q$$

$$F(p, p^q) = G(p, p^q) = 0 \quad \not\Rightarrow \quad C(F,G) \geq q$$

Cela suggère une dépendence logarithmique dans la hauteur des coefft

Une version plus uniforme de la ex-conj. de Schinzel permet de traiter le cas des racines multiples :

$$\gcd\left(b_0 + b_1 t^{q_1} + \dots + b_N t^{q_N},\ a_1 b_1 t^{q_1 - 1} + \dots + q_N b_N t^{q_N - 1}\right)$$

(ASZ 11)

Et en plusieurs variables ?

Conj Schinzel : cas particulier d'une conjecture de Zilber :

$X \subseteq \mathbb{G}_m^N$ irr

$T \subseteq \mathbb{G}_m^N$ variété de torsion

Y composante « exceptionnel » de $X \cap T$:

$$\dim Y > \dim T - \operatorname{codim} X$$

$\Rightarrow Y \subseteq$ réunion finie de variétés de ~~[illegible]~~ sous-groupes de $\mathbb{G}_m^N$ (dépendant seulement de X)

$\dim T = 0$: Menin-Mumford (Laurent '84)

$\dim T = 1 \Rightarrow$ Conjecture de Schinzel ($\dim X = 2$)

$\dim X = 1$: Manin '08 (BMZ '98)

Application (ALS 19)
On admet une version effective de la conjecture de Zilber.
Alors toute variété définie par des polynômes de courbures
de degré $\leq d$ peut se décomposer en réunion
d'intersection complète en dehors d'un fermé, en
temps $\tilde{O}(\text{lsol})$ opérations élémentaires

3 Retour à la factorisation

Schinzel (65) conjecture un résultat similaire
pour la factorisation :

$$f_0(t) = F(t^{q_1}, \dots, t^{q_N})$$

$\exists A \in \mathbb{Z}^{N \times N}$ dans un ensemble fini qui dépend seulement de F
t.q. $\underline{q} = A\underline{q}'$ et la factorisation de f_0
provient (en dehors de facteurs cyclotomique) de
celle de $F(\underline{X}^A)$ par spécialisation $\underline{X} \to t^{\underline{q}'}$

Hors de la portée des méthodes diophantiennes ...

ABC 17 : analogue pour $F \in \mathbb{C}(z)[\underline{X}]$

Ingrédient principal : une version torique du th.
de Bertini (sous-espace affine $\to$ sous-variété de torsion)

Th Z 19, $F \cap Z$ 17
$F(z, \underline{X})$ in $+(PB) \Rightarrow F(z, t^{\underline{a}})$ in
en dehors d'un nombre fini de 1-dim sous les
$\{t^{\underline{a}} \mid t \in \mathbb{G}_m\}$

$V \subseteq \mathbb{C}^n_m$ defini par des polynômes locaux

$$\rightarrow \quad V = \bigcup_{i=1}^{k} Z(P_{i1}, \dots, P_{il_i}) \setminus Z(Q_i)$$

↑

dont les composantes irr. sont de cotaines l_i

(PB) $F(z, x_1^{m}, \dots, x_N^{m})$ irr $\underline{\forall m \in \mathbb{N}^*}$

(ex : $F(z, x, y) = z^2 - xy^2$ irr

$F(z, x^2, y^2) = (z + xy^2)(z - xy^2)$

et $F(z, t^a, t^b)$ réd si a est pair)

AS : préciser ce qui se passe $\underline{\text{sans}}$ PB ?