Explicit Formulas for Coppersmith's Method (Asymptotic Bounds)

Coppersmith's method.

Def: (Small roots) Given bound X_j $_{1\le j\le k}$ and $f \in \mathbb{Z}[x_1, \dots, x_k]$. modulus M. Find root $\vec{u} = (u_1, \dots, u_k)$

Integer with $u_j < X_j$ and $f(\vec{u}) \equiv 0 \bmod M$

Alg: Coppersmith method. [Motivation: if the coefficient of $f(x)$ are small enough. one might have $\underline{f(\vec{u}) = 0 \text{ over } \mathbb{Z}}$]

Easier

View Coppersmith's method as a black box

$f = x_1x_2 + C_1x_1 + C_2 \longrightarrow \boxed{\text{Black Box Coppersmith}} \longrightarrow$ Find all (x_1, x_2) with $x_i < \cancel{X_i}$ ~~& $X_1^2 X_2 < M$~~

$|x_i| < M^{\frac{1}{3}}$ ~~$X < M^{\frac{1}{3}}$~~

JM basic Strategy

Explicit formulas for constraint X_j

Application (Commutative Isogeny Hidden Number Problem) CI-HNP

Two public curves E_A, E_B. Given some of MSBs of CDH of two curves. The goal is to compute E_{AB}

CI-HNP (CSURF)

Solving the following polynomial equation. $\begin{cases} f = x^2 + xy^2 + xy + x + y^2 + y + 1 \\ g = z^2 + x^2z + xz + z + x^2 + x + 1 \end{cases}$ with $x, y, z < X$

[MN23] $X < M^{10/41} \approx M^{0.244}$ [Ours] $X < M^{8/31} \approx M^{0.25806}$

+ New heuristic

Coppersmith's method. Step 1. Fix m construct $G = \{g_j\}$ share the same root of f when mod M^m, eg. $M^{m-j} f^j = g_j$

$$\boxed{\begin{array}{l} J_\ell = \{x_1^{i_1} \cdots x_k^{i_k} \mid x_1^{i_1} \cdots x_k^{i_k} \in \operatorname{supp}\{f^m\} \text{ and } \frac{\lambda}{LM(f)^\ell} \in \operatorname{supp}\{f^{m-\ell}\}\} \\ \text{For } \ell = 0, 1, \dots, m. \quad x_1^{i_1} \cdots x_k^{i_k} \in J_\ell \setminus J_{\ell+1} \\ g_{[i_1, \dots, i_k]}(x_1, \dots, x_k) = \frac{x_1^{i_1} \cdots x_k^{i_k}}{LM(f)^\ell} f^\ell M^{m-\ell} \end{array}}$$

Step 2. Construct linear combination of $G = \{g_j\}$ as h with small norm. s.t. $h(\vec{u}) = 0 \bmod M^m$ / over $\mathbb{Z}$

① Using the coefficient vector of $g(x_1X_1, \dots, x_kX_k)$ construct $\mathcal{L}$

② Using Lattice basis reduction to find shorter vector v_h, which is related to h.

the leading coefficient of $g_{[i_1, \dots, i_k]}(x_1X_1, \dots, x_kX_k)$ is $LC(g_{[i_1, \dots, i_k]}(x_1X_1, \dots, x_kX_k)) = X_1^{i_1} \cdots X_k^{i_k} M^{m-\ell}$

$\mathcal{L}$: diagonal $\quad \det(\mathcal{L}) = \prod_{g_{[i_1, \dots, i_k]} \in G} LC\, g(x_1X_1, \dots, x_kX_k) = X_1^{P_1(m)} \cdots X_k^{P_k(m)} M^{P_F(m)}$

$$\dim(\mathcal{L}) = \left|\bigcup_{\ell=0}^{m} J_\ell\right| = |J_0| = |\operatorname{supp}\{f^m\}|$$

We Need $\det(\mathcal{L}) < \cancel{\dim^m} M^{m \dim(\mathcal{L})}$

Tools from Additive Combinatorics

Def. $A(f) = \{(v_1,\dots,v_k) \mid x_1^{v_1}\cdots x_k^{v_k}$ is a monomial of $f\}$, its convex hull $N(A)$ is called Newton polytope of f

Prop1. $A(f^m) = mA$

Prop2. (Khovanskii 92). $\exists N$. when $m>N$. $\exists f_k(m)$ s.t. $|mA(f)| = f_k(m)$ and $LC(f_k(m)) = V(N)$.

$$J_\ell = \{x_1^{i_1}\cdots x_k^{i_k} \mid (i_1,\dots,i_k)\in mA \ \& \ (i_1,\dots,i_k)\in(m-\ell)A+\ell\underset{LM(f)}{\underset{\downarrow}{\alpha}}\}$$

$$\dim(\mathcal{L}) = \left|\bigcup_{\ell=0}^{m} J_\ell\right| = |J_0| = |mA(f)| \xrightarrow{\text{Khovanskii 92}} V(N(f))\,m^k + o(m^k)$$

$$\det(\mathcal{L}) = X_1^{P_1(m)}\cdots X_k^{P_k(m)} M^{P_F(m)} = X_1^{\int_{N(f)} x_1\,dV\,m^{k+1}} \cdots X_k^{\int_{N(f)} x_k\,dV\,m^{k+1}} M^{\frac{k}{k+1}V(N(f))m^{k+1}+o(m^{k+1})}$$

$$P_j:\ \sum_{(i_1,\dots,i_k)\in mA} i_j \xrightarrow{?} |mA_j|$$

$$\boxed{\begin{tikzcd} A \arrow[r, "\times m"] \arrow[d, "\psi_j"'] & mA \arrow[d, "\psi_j"] \\ \psi_j(A) \arrow[r, "\times m"] & m\psi_j(A) \end{tikzcd}}$$

Commutative diagram.

$$\psi_j: \mathbb{Z}^k \to \mathbb{Z}^{k+1}$$

$$(i_1,\dots,i_k) \mapsto (i_1,\dots,i_k,0),\ \dots,\ (i_1,\dots,i_k,i_j).$$

$$\sum_{(i_1,\dots,i_k)\in mA} i_j = \sum_{(i_1,\dots,i_k,i_{k+1})\in\psi_j(mA)} 1 = \sum_{(i_1,\dots,i_{k+1})\in m\psi_j(A)} 1$$

P_F: Construct $\tilde{A}\in\mathbb{Z}^{k+1}$, $\sum_{\ell=0}^{m}(m-\ell)|J_\ell\setminus J_{\ell+1}| \overset{?}{=} |m\tilde{A}|$

$$\sum_{\ell=0}^{m}(m-\ell)|J_\ell\setminus J_{\ell+1}| = \sum_{\ell=0}^{m}(m-\ell)(|J_\ell|-|J_{\ell+1}|) \xrightarrow{\text{Abel's summation Formula}} \underset{m|mA|}{\underset{\downarrow}{m|J_0|}} - \underset{???}{\underline{\sum_{\ell=0}^{m}|J_\ell|}}$$

$$\tilde{A} = (A,1)\cup(\alpha,0).\quad \sum_{\ell=0}^{m}|(m-\ell)A+\ell\alpha| = |m\tilde{A}| \cancel{=\tfrac{1}{k+1}},\ V(N(\tilde{A})) = \frac{1}{k+1}V(N(A))$$

Generalized to a system of polynomial system

$$\mathcal{F} = \{f_1,\dots,f_n\} \quad A(\mathcal{F}) = \bigcup_{j=1}^{n} A(f_j) \quad S_\ell = \{x_1^{i_1}\cdots x_k^{i_k} \mid (i_1,\dots,i_k)\in \overbrace{(m-\ell)A(\mathcal{F}) + \bigcup_{\substack{\ell_1+\dots+\ell_n=\ell \\ 0\le\ell_j\le m}} \sum \ell_j\alpha_j}^{(m-\ell)A(F)+\ell B}\}$$

$$g_{[i_1,\dots,i_k]}(x_1,\dots,x_k) = \frac{x_1^{i_1}\cdots x_k^{i_k}}{\prod_{j=1}^{n} LM(f_j)^{\ell_j}}\prod f_j^{\ell_j} M^{m-\ell}$$

Add. t-shift $\quad J_\ell = \bigcup_{0\le j\le t}\{x_i^j\lambda \mid \lambda/LM(f)^\ell \in \operatorname{supp}\{f^{m-\ell}\}\} \quad \dim(L) = |mA+tE|$

$$\text{CJURF}: X < M^{\frac{51-3\sqrt{29}}{45}} \approx M^{0.25812}$$