L 28
6/3/2020

Deciding finiteness

Igor Pak

Problem: $G = GL(n, \mathbb{Z})$, $H = \langle S \rangle$, $S = \{s_1, \dots s_k\} \subset G$

Is H - infinite or finite?

Th [Babai-Beals-Rockmore, 1993]

Finiteness problem is in ZPP

Proof idea: construct two algorithms

Alg1: Probab (Monte Carlo) testing in expected poly time s.t. Yes ← True
No ← w/ Prob $> 1-\varepsilon$

Alg2: Same but Yes ← w/ Prob $> 1-\varepsilon$
No ← True

Now: Run Alg1 & Alg2 in parallel. ▨ (1)

Norms of matrices

Th! [Minkowski, Feit] (Burnside+)

$H \subset GL(n, \mathbb{Z})$ finite $\Rightarrow$ $|H| \le (2n)!$ [Burnside, Minkowski]

u/o CFSG

$\Rightarrow$ $|H| \le 2^n n!$, $n \ge 10$ [Feit 1996]

using CFSG

L [BBR] $H \subset GL(n, \mathbb{Z})$ finite

$M := \max \{ \|s_i\|, i = 1..k \}$

then $\|h\| \le M^{n^2} e^{O(n^2 \log n)}$ / $\leftarrow n^{2n^2+3}$ more precisely

---

Alg! Use Babai or Cooperman-Dixon Alg to obtain elts $h \in H$ outside of larger & larger ε-R cubes.

STOP when $\|h\| > M^{n^2} n^{(2n^2+3)}$

Analysis of Alg 1

$s_1 \dots s_k \; h_1, h_2 \dots h_e$, $e = O(\log(2n)!) = O(n \log n)$

⟨C-D⟩ $h_{i+1} = s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k} h_1^{\alpha_1} \dots h_i^{\alpha_i}$ $\alpha_j, \varepsilon_j \in \{0,1\}$ random

(Babai) $h_{i+1} =$ RW on $\{ s_1 \dots s_k \; h_1 \dots h_i \}$ for $L = O(n \log n)^3$ steps $= O(n^3 \log^3 n)$

For Alg 1 $X \subset GL(m, \mathbb{Z})$, $X := \{ \|X\| \le M^{n^2} n^{2n^2+3} \}$

$|X| = O\left((M^{n^2} n^{2n^2+3})^{n^2} \right) = O(M^{n^4} n^{2n^4+3n^2})$

$e \leftarrow O(\log |X|) = O(n^4 (\underbrace{\log M}_{\text{input}} + \log n))$

$L \leftarrow e^3$

$C_e^{-1} C_e \neq H$

If STOP $\Rightarrow$ $h_e \notin X \Rightarrow_L$ H inj.

If NOT $\Rightarrow$ $H \subset X$ uhp. ▨

Invariant Matrices

Th [Burnside] $H \subset GL(n, \mathbb{Z})$ is finite
if and only if $\exists B \subset Mat(n, \mathbb{R})$ s.t.
B - positive definite, symmetric $B^T = B$
and $h^T B h = B \quad \forall h \in H$

Exc $\Rightarrow$ follows from $B := \frac{1}{|H|} \sum_{h \in H} h^T h$

Alg2 [Use REO (Babai, C-D or PRA) to obtain
ε-uniform $h \in H$.
Do this ℓ times to obtain $h_1 .. h_\ell$

For $i = 1 \ldots \ell$
$B_{i+1} \leftarrow \frac{1}{2}\left[h_i^T B_i h_i + B_i\right]$ | $B_0 \leftarrow I$, $\ell = poly(n)$

STOP if $B \approx$ Burnside matrix

Analysis of Alg 2

$$B_e = \sum_{\bar{I}=(d_1 \cdots d_e)} (h^T h)^{\frac{1}{2^e}}, \quad h = h_1^{d_1} \cdots h_e^{d_e}$$

$d_i \in \{0,1\}$ uniform

$$= \mathbb{E}[h^T h]$$

By ε-R Thm $\forall$ $h_i \in \varepsilon$-unif, $\ell > 2\log|H| + \log\frac{1}{\varepsilon} + 2\log\frac{1}{\delta} + \log\frac{1}{\gamma}$

$$\boxed{\sup(B_e, B) < \gamma \text{ w/ Pr} > 1-\delta}$$

where $B = \sum_{h \in H} h^T h / |H|$

Take $\gamma \leq \frac{1}{2(2n)!}$ / to be precise $\frac{1}{2n M^2 (2n)!}$ /

so the rounding over $\mathbb{Z}$ gives exact B, note: $\log(\frac{1}{\gamma}) = \text{poly}(n, \log n)$

Testing $B_e \stackrel{?}{=} B$: check $s_i^T B s_i = B$ $\forall$ $i = 1 \cdots k$.

$\Rightarrow h^T B h = B$ $\forall h \in H$ ▨

Putting Alg 1 + Alg 2 together

Fix $\varepsilon = \frac{1}{2}$. After $\text{poly}(n + \log M)$ we have:

If $\lvert H\rvert < \infty$	Alg 2 stops w/ $Pr > 1-\varepsilon$	}	proves result
$\lvert H\rvert = \infty$	Alg 1 stops w/ $Pr > 1-\varepsilon$	}	↑ outputs inf/fin certificates

Repeat $O(1)$ times. Done.

Generalizations: [BBR]

1) $G = GL(n, \mathbb{Q})$, $GL(n, F)$, $F \in$ algebraic number field

2) deterministic alg using ellipsoid method

Q: Why is this astonishing?

A: Many problems for inf groups are undecidable

Th [Adian-Rabin, 1955, 1958] $G := \langle x_1 - x_n \rangle / R$

$G \simeq 1$, G-fin, $G \simeq F_2$, — ← all undecidable.

Th [Mihailova, 1958] $n \geq 4$

$G = SL(n, \mathbb{Z})$, $H = \langle S \rangle$, $S = \{s_1, \dots s_k\}$, $g \in G$

Then $g \in ?\ H$ is undecidable

L $M_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $M_1, M_2 \in SL(2, \mathbb{Z})$

Then $\langle M_1^{\pm 1}, M_2^{\pm 1} \rangle = F_2$ / Sanov subgroup /

Exc $\langle M_1^{\pm 1}, M_2^{\pm 1} \rangle$ is a subgroup of $SL(2, \mathbb{Z})$ of index 12

Proof idea of L: $X = \mathbb{Z}^2$,

$\mathcal{A} = \{(p, q) \in \mathbb{Z}^2 \mid |p| > |q|\}$

$\mathcal{B} = \{(p, q) \in \mathbb{Z}^2, |q| > |p|\}$

check that $\boxed{M_2^n \mathcal{A} \in \mathcal{B}, \ M_2^n \mathcal{B} \in \mathcal{A}}$

$\Rightarrow$ result follows by ping-pong lemma

Proof idea of Mihailova Thm $n=4$

$\left(\begin{array}{c|c} F_2 & 0 \\ \hline 0 & F_2 \end{array}\right) \subset SL(4,\mathbb{Z})$ Consider $S_i = \left(\begin{array}{c|c} u_i & 0 \\ \hline 0 & v_i \end{array}\right)$ $u_i, v_i \in F_2$, $i = 1 \ldots k$

$$word(s_1 \ldots s_k) = word(u_1 \ldots u_k) * word(v_1 \ldots v_k)$$

Th [PCP = Post correspondence problem, E. Post '46]

$\alpha_1 \ldots \alpha_N$ ∈ words over $X = \{x_1 \ldots x_k\}$
$\beta_1 \ldots \beta_N$

Then ∃? word ∈ alphabet $\{y_1 \ldots y_N\}$ s.t. $word(\alpha_1 \ldots \alpha_N) = word(\beta_1 \ldots \beta_N)$
is undecidable

Exc Prove PCP Thm via reduction to halting problem

D(Mih) idea: take any $x_1 \ldots x_k \in F_2$, $u_i \in \alpha_i$, $v_i \in \beta_i$
→ include in S extra "parity" gen's.

Exc Take $y = \left(\begin{array}{cc} x_1^2 & \\ & x_1^2 \end{array}\right)$