8.371 p. 1/6
3/21/06

Lecture 12: The Hidden Subgroup Problem

Lecturer: Sean Hallgren
Scribe: Kayla Jacobs

Def: <u>The Hidden Subgp Problem</u>

Given $f: G \to S$ (G = group, S = set)

$\exists$ (unknown) subgp $\mathcal{H} \leq G$ s.t.

f is constant on cosets of $\mathcal{H}$

f is distinct on different cosets

Def: <u>Group</u>: set w/ operation (usually called add. or mult.)

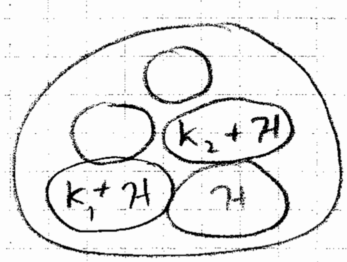
Op associative. $\exists$ identity. Every elt has inverse

e.g. $\mathbb{Z}_m = \{0, \dots, m-1\}$ with $+$

Def: <u>Coset</u> $k + \mathcal{H} = \{ k + h \mid h \in \mathcal{H} \}$ (abelian notation) op commutative

$g\mathcal{H} = \{ gh \mid h \in \mathcal{H} \}$ (non-abelian notation)

Picture rep of problem: f:



f const in each circle, diff in diff circles

Find $\mathcal{H}$.

Examples of problems which reduce to $\mathcal{HSP}$:

(Recall: A reduces to B $(A \le B)$ if
an effective alg. for B gives
an effective alg. for A too)

- **Abelian gp examples** (i.e. $a+b = b+a$)

Ex 1) Discrete log (mod p) $\le$ $\mathcal{HSP} / \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ (Shor)

Given prime p, $g, g^s \in \mathbb{Z}_p$
Find s

$$f: \underbrace{\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}}_{\text{group under } +} \longrightarrow \underbrace{\mathbb{Z}_p}_{\text{group under } *}$$

$$f(a,b) = g^{a-bs} \pmod p$$

$$\mathcal{H} = \{ (a,b) \mid a - bs \equiv 0 \pmod{p-1} \}$$

Ex 2) Factoring $N \le \mathcal{HSP} / \mathbb{Z}$ (Shor)

Recall: This reduces to computing the order of
a random elt a (mod N)

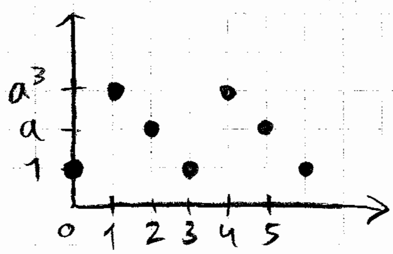
Recall: $\text{Ord}(a) = \min m$ s.t. $a^m \equiv 1 \pmod N$

Define $f: \mathbb{Z} \to \mathbb{Z}_N$ by

$$f(i) = a^i \pmod N$$

$\mathcal{H} = \mathrm{ord}(a)\,\mathbb{Z} = \{ \mathrm{ord}(a) \cdot k \mid k \in \mathbb{Z} \}$

Can verify f is an $\mathcal{H}$SP instance



$a^3 \equiv 1 \pmod N$

Ex 3) <u>Class group of an imaginary number field $\leq \mathcal{H}SP / \mathbb{Z}^n$</u>

Given generators $g_1, \dots, g_n$ of group G

Decompose $G = \bigtimes_i \mathbb{Z}_{e_i}$ $\quad e_i \mid e_{i+1}$

Define $f: \mathbb{Z}^n \to G$ by

$$f(a_1, \dots, a_n) = \sum a_i g_i$$

$\mathcal{H} = \{ (a_1, \dots, a_n) \mid \sum a_i g_i = e \}$

Then compute Smith Normal Form.

Ex 4) <u>Pell's Equation "$\leq$" $\mathcal{H}SP / \mathbb{R}$</u>

4a) Unit group of a constant degree number field "$\leq$" $\mathcal{H}SP / \mathbb{R}^c$ (c const)

Ex 5) <u>Principal ideal problem "$\leq$" $\mathcal{H}SP$ / $\mathbb{R}^c$</u>

Given an ideal $\alpha I \subseteq \Theta \subseteq F$

Approximate $\log \alpha$

Ex 6) <u>Class group of a real number field "$\leq$" $\mathcal{H}SP$ instance where S is quantum states</u>

- **Non-abelian gp examples**

Ex 7) <u>Graph isomorphism $\leq$ $\mathcal{H}SP$ / S_n</u>

Given graphs G_0, G_1 $\qquad G = (V, E)$

G_0

$\exists$ permutation $\pi \in S_n$ which preserves edge set

Define $f: S_{2n} \longrightarrow \{$graphs on $2n$ vertices$\}$ by

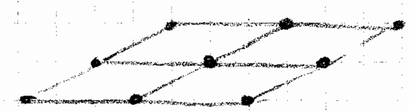
$$f(\pi) = \pi(G_0 \cup G_1)$$

$\mathcal{H} = \{\pi \in S_{2n}$ preserving the edge set$\}$

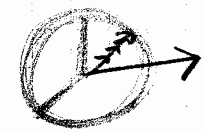
Ex 8) Unique shortest lattice vector problem "$\subseteq$" HSP / D_n

Def: Lattice L given by a basis $b_{1 \ldots n} \in \mathbb{R}^n$

$$L := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in \mathbb{Z} \right\}$$



Given shortest lattice $b_1, \ldots, b_n$ s.t.
any vector not parallel to the shortest vector v_0
has length at least $n^c \cdot \|v_0\|$



Find v_0.

Examples' Status:

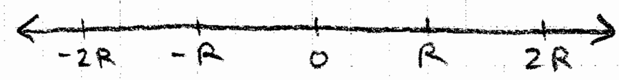
Examples #1–6 have efficient quantum algs.
#7 & 8 are still open

Def: Dual lattice L^* of lattice L is

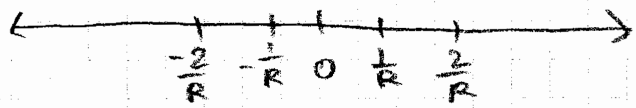
$$L^* := \{ x \in \mathbb{R}^n \mid v \cdot x \in \mathbb{Z} \;\; \forall v \in L \}$$

$\exists$ classical poly-time algs to compute
L from L^* & L^* from L

Example: $L = \langle R \rangle$



$L^* = \langle \frac{1}{R} \rangle$



Two Problems Over lattices

1) Given some description of a lattice L, compute a basis for L. (i.e. examples #1-6)

2) Given a lattice (by a basis), compute the shortest vector. ⟸ NP-complete

   2a) Same but lattice has a unique shortest vector (i.e. example #8)

Algorithm for the $\mathcal{H}$SP ("The Standard Method")

Repeat k times:

1) Create "coset state:"

   Compute f in superpos & measure f

$$\sum_g |g, f(g)\rangle \xrightarrow{\text{measure } f} \sum_{h \in \mathcal{H}} |k+h\rangle\,|f(k)\rangle \qquad k \in_R G$$

$$\approx \sum_{h \in \mathcal{H}} |k+h\rangle$$

2) Fourier-sample

Compute the FT / G & measure

$$\sum_{h\in H} |k+h\rangle \xrightarrow{FT/G} \sum_{\rho,i,j} \alpha_{\rho,i,j} |\rho,i,j\rangle$$

$$\downarrow \text{measure}$$

$$|\rho,i,j\rangle \quad \text{w/ prob } |\alpha_{\rho,i,j}|^2$$

Then, classically compute H from the samples $\{(\rho, i, j)\}$

---

2 issues:

1) abelian: How does it work when $G = \mathbb{R}$ or even $\mathbb{Z}$?
2) non-abelian: FT/G not uniquely defined

Fact: Poly many coset states have enough info to distinguish diff subgps

Example: Case $G = \mathbb{Z}$

Given $f: \mathbb{Z} \to S$

$\mathcal{H} = \langle r \rangle$, $r \in \mathbb{Z}$

a) Choose large $q \in \mathbb{Z}$

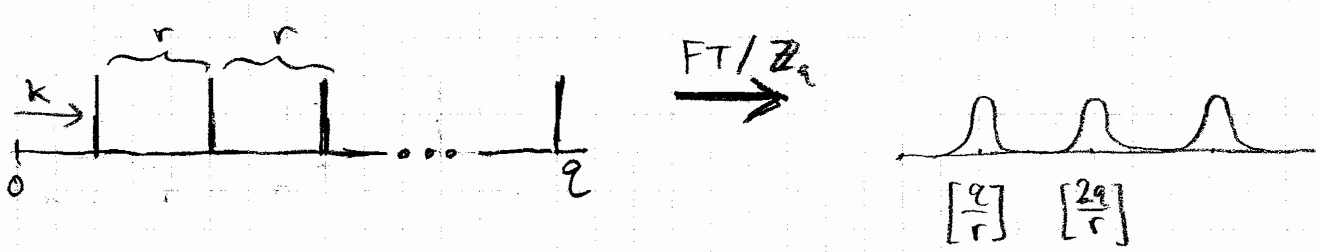
& run standard method w/ f over $\mathbb{Z}_q$

(essentially Shor's alg)

$$\sum_{i=0}^{q-1} |k + ir\rangle \xrightarrow{FT} \sum_{c=0}^{q-1} \sum_{i=0}^{q-1} \omega_q^{c(k+ir)} |c\rangle$$

b) Measure c

Compute continued fraction expansion of c/q



$$|i\rangle \to \sum_c \omega_q^{ic} |c\rangle$$

$$Pr(c) = \left| \sum_{i=0}^{q-1} \omega_q^{c(k+ir)} \right|^2$$

Claim: W/ high prob, measure c s.t. $\left| \frac{c}{q} - \frac{l}{r} \right| \leq \frac{1}{2r^2}$

This means $\frac{l}{r}$ appears in the CF expansion

Pell's Equation

Given positive, non-square integer d
Find integer sol^{n}s x, y s.t. $x^2 - dy^2 = 1$

Note $x^2 - dy^2 = (x + \sqrt{d}\,y)(x - \sqrt{d}\,y) = 1$

<u>Thm</u>: $\exists\, x_1, y_1$ s.t. all sol^{n}s x_n, y_n have form:

$$(x_1 + \sqrt{d}\,y_1)^n = x_n + \sqrt{d}\,y_n$$

In general, x_1, y_1 have exponentially many bits

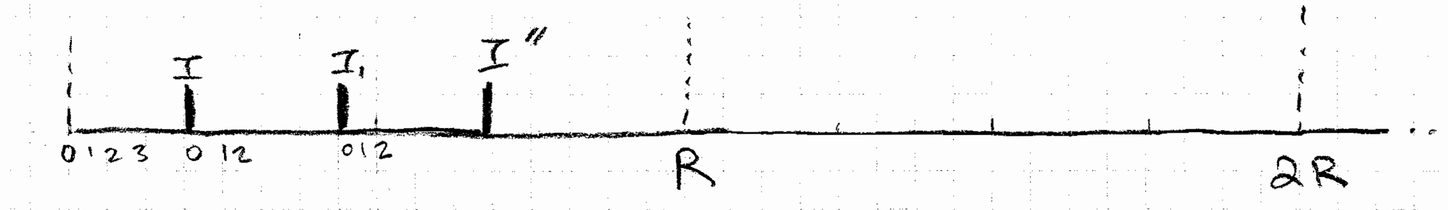
<u>Def</u>: The <u>regulator</u> $R := \log(x_1 + \sqrt{d}\,y_1)$

So solving Pell's Eq $\longleftrightarrow$ approximating R

Practically, don't need a lot of accuracy
— getting to within a polynomial is good enough

<u>Thm</u>: Given d, $\exists f: \mathbb{R} \rightarrow (\text{Ideals} \times \mathbb{R})$
s.t. f is an HSP instance over $\mathbb{R}$, $\mathcal{H} = \langle R \rangle$

Discretizing f:

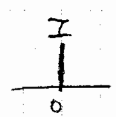


let $f_N : \mathbb{Z} \to (\text{Ideal} \times \mathbb{Z})$

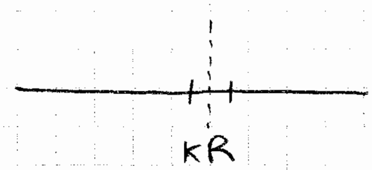
$f_N(i) = (\text{Ideal to left of } i/N, \text{ closest int to the left})$

Properties of f_N:

1) Can verify that int M is s.t.
   M/N is within $1/N$ of a multiple of R



$f_N(0) = cI$



$f_N(M)$ & $f_N(M+1)$ & check if I

2) For most $k \le RN$,

$$f_N(k) = f_N(k + [iRN]) \quad \forall i \in \mathbb{Z}$$

$[x] = \lceil x \rceil$ or $\lfloor x \rfloor$, $x \in \mathbb{R}$

Alg for approximating R given f_N:

a) $\sum_{i=0}^{q/R-1} |k + [iRN]\rangle \longrightarrow \sum_c \sum_i W_q^{c(k+[iRN])} |c\rangle$

b) Measure c & $d \leq q/\log R$

Compute the continued fraction expansion of

$c/d \rightarrow k/l$

Compute $(c/qk)^{-1} \approx R$ & verify

With high prob, show $\left|\frac{c}{d} - \frac{k}{l}\right| \leq \frac{1}{2l^2}$