Scribe: Igor Sylvester

Quantum Information Science II: 3/23/2006

Projects website: https://scripts-cert.mit.edu/~ichuang/wiki:8371

Lecturer: Sean Hallgren

Last time

Efficient algorithms for number theory problems

factoring $\leq$ Pell's eqn $\leq$ principal ideal problem (PIP)

$\leq$ class group $\longleftarrow$ constant degree # fields

Class group is a finite abelian group

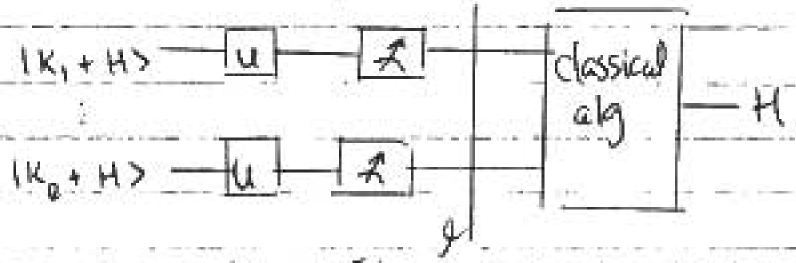
Cryptosystem RSA assumes factoring is hard

Buchmann - Williams - key exchange assumes PIP is hard

History: Lenstra - Pell

Open problem: arbitrary degree number of fields.

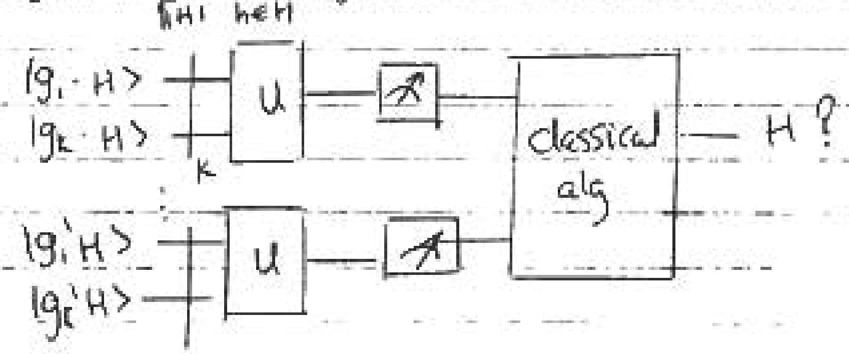
*For Abelian Groups



G abelian $U = FT/G$ $\ell = \log|G|$

Today: Non-abelian Groups

$$|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$



Main question: do entangled measurements help?

1) D_N $k = 1$ $\ell = \text{poly}$ 3) H_p $k = 2$ $\ell = 1$

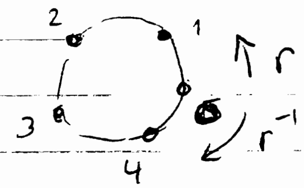
2) D_N $k = 8^{\sqrt{n}}$ $\ell = 1$

The dihedral group D_N

Cyclic group $\mathbb{Z}_N = \langle r : r^N = 1 \rangle$

$r^a \cdot r^b = r^{a+b \pmod N}$

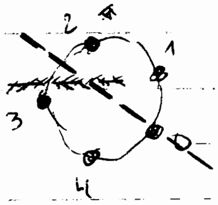
$\mathbb{Z}_5$:



Dihedral group D_N

$D_N = \langle r, s : r^N = 1, s^2 = 1, rs = sr^{-1} \rangle$

D_5 :



$|D_N| = 2|\mathbb{Z}_N|, \quad \mathbb{Z}_N \subseteq D_N$

N order 2 subgroups $H = \{e, r^i s\}$

$$r^i s r^i s = r^{i-i} \cdot s \cdot s = \underset{\overset{\uparrow}{\text{identity}}}{e} \quad \forall i$$

*The Fourier Transform over group G : FT/G

Def A homomorphism $\rho : G \to A$, G, A groups s.t. $\rho(g_1)\rho(g_2) = \rho(g_1 g_2) \quad \forall g_1, g_2 \in G$.

Def An irreducible representation (irrep) is a homomorphism $\rho : G \to M_{d\rho \times d\rho} = \{$ invertible unitary $d\rho \times d\rho$ matrices with no fixed subspace $\}$

$\hat{G}$:= irreps of G

Fact: $\sum_{\rho \in \hat{G}} d\rho^2 = |G|$

An arbitrary rep. $\tilde{\rho}$ can be written

$$\tilde{\rho} = \bigoplus_{\rho \in \hat{G}} a_\rho \, \rho.$$

$$\mathbb{C}[G] = \{ \sum_{g \in G} \alpha_g |g\rangle : \alpha \in \mathbb{C} \}$$

$$\bigoplus_{\rho \in \hat{G}} M_{d\rho \times d\rho} = \text{vector space of dim } \sum d\rho^2 = |G|$$

Thm The FT/G is an isomorphism between these two algebras.

In many groups (eg. abelian, S_n, D_n) $\exists$ eff. quant alg. to compute it.

$$\sum \alpha_g |g\rangle \xrightarrow{FT/G} \sum_{\rho \in \hat{G}} \sum_{i,J=1}^{d_\rho} \alpha_{\rho,i,J} |\rho, i, J\rangle$$

Example of irreps

(1) $\mathbb{Z}_N = \langle r \rangle$

$$\chi_c(r^i) = \omega_N^{ic} \qquad c = 0, \dots, N-1$$

$$|r^i\rangle \xrightarrow{FT} \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} \chi_c(r^i) |c\rangle$$

(2) $D_N = \langle r, s \rangle$

Two or four one-dim irreps for N even/odd.

There are $N/2-1$ 2x2 irreps:

$$\rho_c(r^i) = \begin{bmatrix} \omega_N^{ic} & \\ & \omega_N^{-ic} \end{bmatrix}, \quad \rho_c(s) = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \text{ for } c = 1 \dots \tfrac{N}{2}-1.$$

$$|r^i s^b\rangle \xrightarrow{FT} \frac{1}{\sqrt{N}} \sum_{c=1}^{N/2-1} \sum_{c,J=1}^{2} \left(\rho_c(r^i s^b)\right)_{iJ} |c, i, J\rangle \underbrace{+ \frac{1}{\sqrt{2N}} |\chi_0\rangle + \frac{(-1)^b}{\sqrt{2N}} |\chi_1\rangle}_{\text{ignore this because prob. of sampling these is exp. small.}}$$

The HSP/DN

Proposition: HSP/D_N w/subgrp

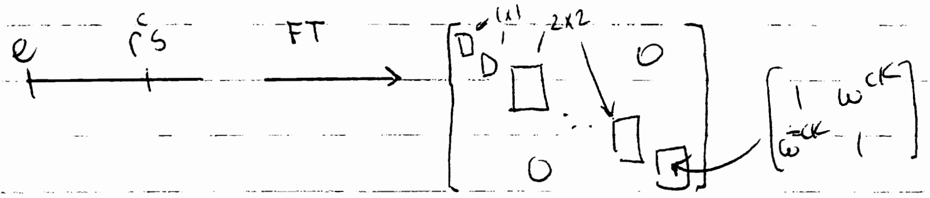
$H \subseteq$ HSP/D_N w/subgrp H' s.t.
$H = \{e\}$ or $H = \{e, r^i s\}$.

Pf sketch: restrict f to $\mathbb{Z}_N \subseteq D_N$ and solve the HSP $\rightarrow A$. Work in D_N / A.

Let $H = \{e, r^k, s\}$

$$|e\rangle + |r^k s\rangle \xrightarrow{FT} \sum_{\rho \in \hat{D}_N} \sum_{i,J=1}^{2} \left(\rho_c(e) + \rho_c(r^k s)\right)_{iJ} |c, i, J\rangle$$

$$\rho_c(e) + \rho_c(r^k s) = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} + \begin{bmatrix} & \omega^{ck} \\ \omega^{-ck} & \end{bmatrix} = \begin{bmatrix} 1 & \omega^{ck} \\ \omega^{-ck} & 1 \end{bmatrix} \Leftarrow \text{the FT at } \rho_c$$


e
$r^c s$
FT
1x1
2x2
0
0
$\begin{bmatrix} 1 & \omega^{ck} \\ \omega^{-ck} & 1 \end{bmatrix}$

<u>Thm</u> Use the basis $\underbrace{H \rho_c(H) H}_{\text{hadamard}}$, $\rho_c(H) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \rho_c(h)$

measure irrep : $Pr(\text{measuring col } 0) \simeq \frac{1}{4N} \sin^2\left(\pi \frac{kc}{N}\right)$

=> poly many samples + exp. post processing => find H.

Some general facts about coset states:

(1) $\rho_c(H)$ is a projection

(2) $Pr(\text{measure irrep } \rho) = \frac{|H|}{|G|} d_\rho \, \text{rank}(\rho(H))$

(3) The density matrix $\frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH|$ is block diagonal in the Fourier basis with respect to irreps $\hat{G}$, because ρ has $\rho(H)$

(4) Therefore info theoretically can compute FT and measure ρ.

(5) Also, can discard row index

<u>Two observations</u>

(1) If could always measure the same irrep, say $c = 1$ or $c = 2^{n-1}$ $(N = 2^n)$ then could compute a block of K.

(2) Working tensor products of two coset states gives more freedom in basis choice.

$$|r^{l_1} H\rangle \otimes |r^{l_2} H\rangle \xrightarrow{FT} \underbrace{\begin{bmatrix} \omega^{l_1 c_1} & \omega^{l_1 + kc_1} \\ \omega^{-l c_1 - kc_1} & \omega^{-l_1 c_1} \end{bmatrix} \otimes \begin{bmatrix} \omega^{l_2 c_2} & \omega^{l_2 c_2 + kc_2} \\ \omega & \omega^{-l_2 c_2} \end{bmatrix}}_{\text{choose a basis for this space}}$$

measure irreps c_1, c_2

measure row → $\alpha_1 \cdot \alpha_2 [1 \ \omega^{kc_1}] \otimes [1 \ \omega^{kc_2}]$

$\alpha_1 = \omega^{l_i c_i}$ <u>or</u> $\omega^{-l_i c_i - k c_i}$

Kuperberg's sub exp. time alg for D_N

Subroutine

Input: two coset states projected onto irreps c_1 and c_2. and discard row.

Output: – w.p. 1/2 the state is projected onto $c_1 - c_2$ irrep.

– w.p. 1/2 "fail"

Steps

(0) Input: $(|0\rangle + \omega^{kc_1}|1\rangle) \otimes (|0\rangle + \omega^{kc_2}|1\rangle)$

(1) CNOT into second bit

$$|0,0\rangle + \omega^{k(c_1+c_2)}|1,0\rangle + \omega^{kc_2}(|0,1\rangle + \omega^{k(c_1-c_2)}|1,1\rangle)$$

(2) Measure rt bit

Algorithm: for least significant bit of k.

(1) Create $8^{\sqrt{n}}$ coset states, project onto irrep, discard row.

(2) Repeat $O(\sqrt{n})$ times:

(1) Sort by irrep: $\ldots \otimes [1 \ \omega^{c_1 k}] \otimes [1 \ \omega^{c_2 k}] \otimes \cdots \quad c_1 \leq c_2$

(2) Run subroutine on pair c_{2i-1}, c_{2i} discard "fail".

(3) w.h.p. a copy of $[1 \ \omega_{2^n}^{2^{n-1}k}]$ $\quad N = 2^n$.

$\Rightarrow$ Compute LSB of k from $\uparrow$

Heisenberg group H_p

$$H_p = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : \overset{p \text{ prime}}{x, y, z \in \mathbb{Z}} \right\} \qquad |H_p| = p^3$$

Interesting: $H_{r,s} := \left\langle \begin{pmatrix} 1 & 1 & s \\ 0 & 1 & r \\ 0 & 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & x & \binom{x}{2} r + xs \\ 0 & 1 & xr \\ 0 & 0 & 1 \end{pmatrix}, x \in \mathbb{Z}_p \right\}$

Irreps: p^2 1-dim irreps

$(p-1)$ p-dim irreps.

$$\rho_c \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \omega^{cz} \sum_{a \in \mathbb{Z}_p} \omega^{cya} |a\rangle\langle a+x|, \quad c = 1, \ldots, p-1.$$

The FT of $H_{r,s}$ at ρ_c:

$$\sum_{x \in \mathbb{Z}_p} \rho_c \begin{pmatrix} 1 & x & \binom{x}{2} r + xs \\ 0 & 1 & xr \\ 0 & 0 & 1 \end{pmatrix} = |v_{c,r,s}\rangle\langle v_{c,r,s}|$$

↑ one-dim projector

where $|v_{c,r,s}\rangle = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{Z}_p} \omega^{-c(\binom{x}{2} r + xs)} |x\rangle$

Algorithm for finding r and s

(1) create two cosets, proj onto irreps c_1, c_2, discard row

$|v_{c_1,r,s}\rangle |v_{c_2,r,s}\rangle$

$$= \frac{1}{p} \sum_{x,y \in \mathbb{Z}_c} \omega^{c_1(\binom{x}{2} r + xs) + c_2(\binom{y}{2} r + ys)} |x,y\rangle$$

Change variables: $r' = 2r \pmod p$ $\quad s' = ~~s~~ \; s - 2r \pmod p$

$$= \frac{1}{p} \sum_{x,y \in \mathbb{Z}_p} \omega^{r'(c_1 x^2 + c_2 y^2) + s'(c_1 x + c_2 y)} |x,y\rangle$$

Note: $|r,s\rangle \rightarrow \frac{1}{p} \sum_{x,y \in \mathbb{Z}_p} \omega^{rx+sy} |x,y\rangle$

(2) $|x,y\rangle \longrightarrow |c_1 x^2 + c_2 y^2, c_1 x + c_2 y, 0\rangle$ if alg. returns x, y

$|x,y\rangle \longrightarrow |-,-,z\rangle \quad z \neq c.$

(3) Compute FT^{-1} and measure r', s' w.p. $\geq 1/2$

Recap: Positive and Negative Results

+ (1) D_N

(2) Heisenberg

(3) Orbit coset alg solve $\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$ uses poly amount of ent.

− (4) $k = \log |G|$ always suffices, information theoretically.

(5) There are groups where $k = \log |G|$ is necessary

(a) S_n

(b) $S_4^n \rightarrow$

(6) PGM approach

Non-HSP exp. speed up

(1) Recursive FS - not in NP

(2) Approx. Jones poly - BQP-complete

(3) Hidden shifts problems

(4) Rnd walk

1,3,4 are oracle problems