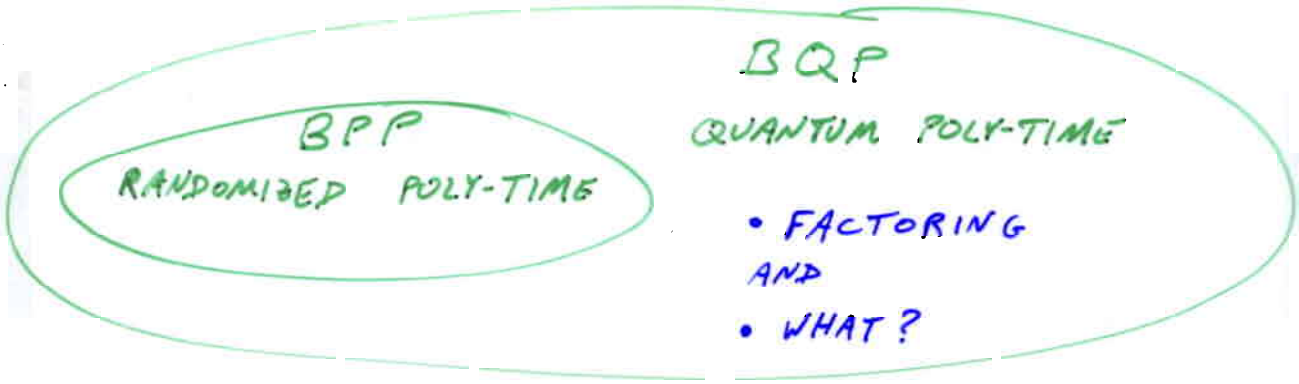
GROUP REPRESENTATIONS & QUANTUM ALGORITHMS

LEONARD J. SCHULMAN

CALTECH


BQP
QUANTUM POLY-TIME
• FACTORING
AND
• WHAT ?
BPP
RANDOMIZED POLY-TIME

PRINCIPAL METHOD:

1. INITIALIZE A QUANTUM MECHANICAL WAVE WHOSE "STRUCTURE" IMPLICITLY CONTAINS DESIRED INFORMATION.

2. APPLY A LINEAR FILTER TO THIS WAVE.

3. MEASURE OUTCOME TO DETECT "LARGE COMPONENTS".

..... REPEAT 1-3 AS NEEDED.

TYPE OF STRUCTURE:	EFFICIENTLY DETECTABLE (BQP)?
1. WAVES WITH ABELIAN GROUP STRUCTURE	YES
2. UNSTRUCTURED WAVES	NO
3. WAVES WITH NONABELIAN GROUP STRUCTURE	?

WAVES WITH ABELIAN GROUP STRUCTURE

BERNSTEIN-VAZIRANI '93
SIMON '94
SHOR '94

EXAMPLE: "ORDER-FINDING". GIVEN PRIME p, $1 \leq g \leq p-1$.

COMPUTE $\quad ord(g) = \min\{ r \geq 1 : g^r = 1 \mod p \}$.

EQUIVALENT FORMULATION:

LET $\quad f: \{0, \ldots, p-2\} \to \{1, \ldots, p-1\}$

$$f(i) = g^i \mod p$$

COMPUTE $\quad$ BLOCKSIZE(f) = COMMON VALUE OF $|f^{-1}(f(i))|$

$$= (p-1)/ord(g).$$

ALGORITHM:

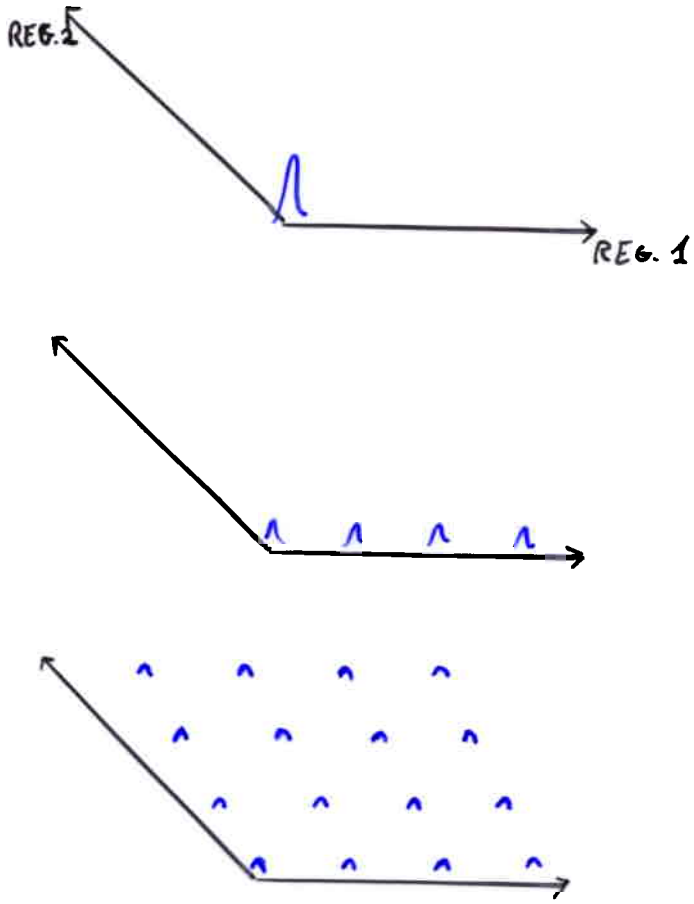
1. INITIALIZE

REGISTER 1 REGISTER 2

$$|0, 0\rangle$$

$$\frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} |i, 0\rangle$$

$$\frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} |i, g^i \bmod p\rangle$$

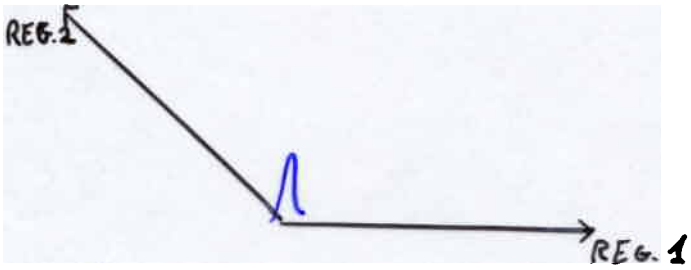


ALGORITHM:

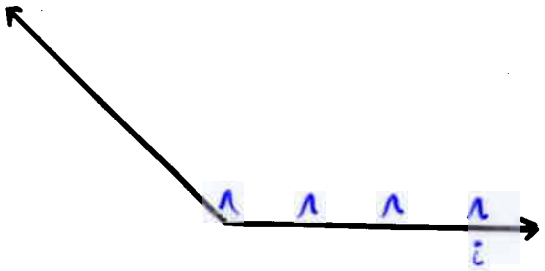
1. INITIALIZE

REGISTER 1 REGISTER 2

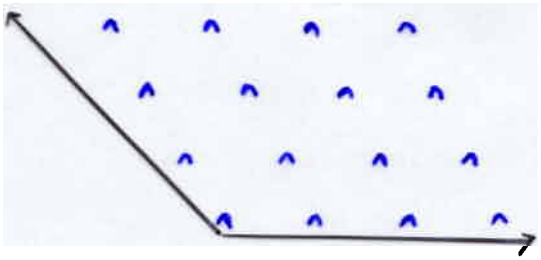
$$|0, 0\rangle$$



$$\frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} |i, 0\rangle$$



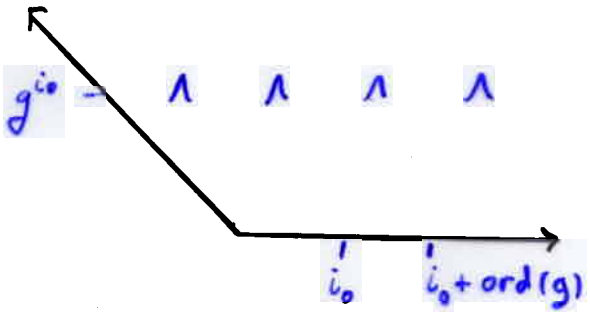
$$\frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} |i, g^i \bmod p\rangle$$



MEASURE REGISTER 2.

STATE IS: FOR UNIFORMLY RANDOM i_0,

$$\sqrt{\frac{ord(g)}{p-1}} \sum_{0 \le j < \frac{p-1}{ord(g)}} |i_0 + j\, ord(g), g^{i_0} \bmod p\rangle$$



2. LINEAR FILTER

FOURIER TRANSFORM OVER $\mathbb{Z}/(p-1)$ IN REGISTER 1.

SPECIAL CASE $i_0 = 0$: SUBGROUP SUPERPOSITION

$$\frac{1}{\sqrt{\dots}} \sum_{j=0}^{(p-1)/\mathrm{ord}(g)} |\, j\ \mathrm{ord}(g) \rangle$$

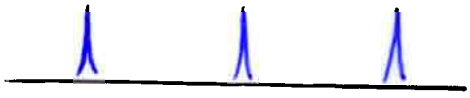
REGISTER 1

↓ FOURIER TRANSFORM

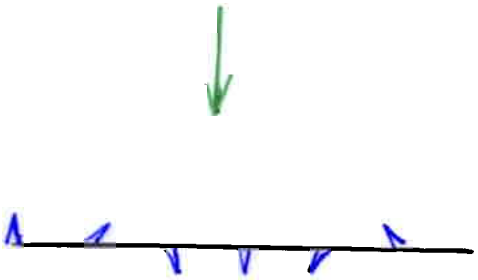
$$\frac{1}{\sqrt{\dots}} \sum_{\ell=0}^{\mathrm{ord}(g)} |\, \ell\ \tfrac{p-1}{\mathrm{ord}(g)} \rangle$$

GENERAL CASE: ARBITRARY i_0. COSET SUPERPOSITION

$$\frac{1}{\sqrt{\dots}} \sum_{j=0}^{(p-1)/\mathrm{ord}(g)} |\, i_0 + j\ \mathrm{ord}(g) \rangle$$



↓ FOURIER TRANSFORM



$$\frac{1}{\sqrt{\dots}} \sum_{\ell=0}^{\mathrm{ord}(g)} \omega^{i_0 \ell} |\, \ell\ \tfrac{p-1}{\mathrm{ord}(g)} \rangle$$

PHASE. * CARRIES COSET IDENTITY

* IS LOST IN MEASUREMENT

2. LINEAR FILTER

FOURIER TRANSFORM OVER $\mathbb{Z}/(p-1)$ IN REGISTER 1.

SPECIAL CASE $i_0 = 0$: SUBGROUP SUPERPOSITION

$$\frac{1}{\sqrt{\dots}} \sum_{j=0}^{(p-1)/\mathrm{ord}(g)} |\, j\ \mathrm{ord}(g)\rangle$$

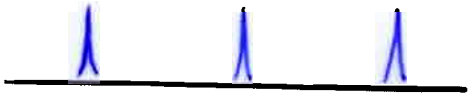
REGISTER 1

↓ FOURIER TRANSFORM

$$\frac{1}{\sqrt{\dots}} \sum_{l=0}^{\mathrm{ord}(g)} |\, l\ \tfrac{p-1}{\mathrm{ord}(g)}\,\rangle$$

GENERAL CASE: ARBITRARY i_0. COSET SUPERPOSITION

$$\frac{1}{\sqrt{\dots}} \sum_{j=0}^{(p-1)/\mathrm{ord}(g)} |\, i_0 + j\ \mathrm{ord}(g)\rangle$$



↓ FOURIER TRANSFORM

$$\frac{1}{\sqrt{\dots}} \sum_{l=0}^{\mathrm{ord}(g)} \omega^{i_0 l} |\, l\ \tfrac{p-1}{\mathrm{ord}(g)}\,\rangle$$

PHASE. * CARRIES COSET IDENTITY

* IS LOST IN MEASUREMENT

3. MEASURE. OUTCOME PROBABILITY = $|\mathrm{AMPLITUDE}|^2$.

⇒ OBTAIN RANDOM MULTIPLE OF $(p-1)/\mathrm{ord}(g)$.

4. SEVERAL REPETITIONS OF STEPS 1-3:

gcd(OUTCOMES) IS PROBABLY $(p-1)/\mathrm{ord}(g)$.

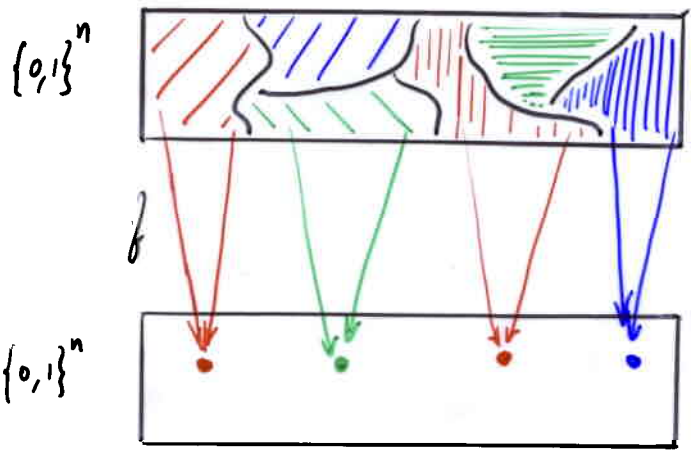
⇒ HAVE A GOOD GUESS OF $\mathrm{ord}(g)$

UNSTRUCTURED SEARCH

GIVEN: A COMPUTER PROGRAM (: "ORACLE" = "BLACK BOX")

COMPUTING A FUNCTION $f: \{0,1\}^n \to \{0,1\}^n$

HAVING A "BLOCKSIZE" = COMMON VALUE OF $|f^{-1}(f(x))|$



COMPUTE BLOCKSIZE(f).

CANNOT BE DONE IN QUANTUM POLY-TIME.

$$\text{TIME} \geq 2^{n/4}$$

AARONSON '01

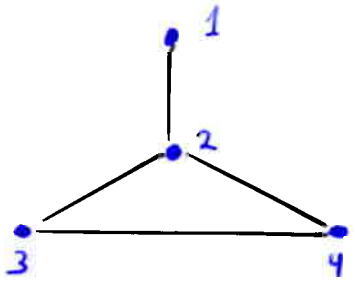
SHI '01

"POLYNOMIAL METHOD:" BEALS, BUHRMAN, CLEVE, MOSCA, DE WOLF '98

WAVES WITH NONABELIAN GROUP STRUCTURE

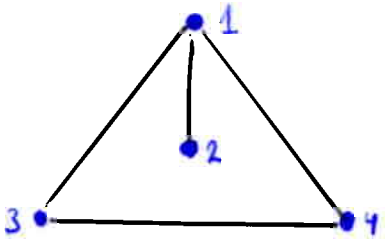
EXAMPLE: "GRAPH AUTOMORPHISM PROBLEM" GIVEN: LABELLED GRAPH ON n NODES

$G =$



SYMMETRIC GROUP S_n acts on G:

$(12)\,G =$



$$AUT(G) = \{ \sigma : \sigma(G) = G \}$$

EXAMPLE: $AUT(G) = \{ id, (34) \}$.

$f : S^n \to$ LABELLED GRAPHS

$f(\sigma) = \sigma(G)$

PROBLEM: GIVEN G, COMPUTE $\text{BLOCKSIZE}(f) = |AUT(G)|$.

NO SUBEXPONENTIAL-TIME ALGORITHM (CLASSICAL OR QUANTUM) KNOWN.

FOLLOW ABELIAN APPROACH

1. INITIALIZE WAVE IN COSET SUPERPOSITION

$$|0 \quad 0\rangle$$

$$\downarrow$$

$$\frac{1}{\sqrt{\cdots}} \sum_{\sigma \in S_n} |\sigma \quad 0\rangle$$

$$\downarrow$$

$$\frac{1}{\sqrt{\cdots}} \sum_{\sigma \in S_n} |\sigma, \quad \sigma(G)\rangle$$

MEASURE REGISTER 2. STATE IS: FOR UNIFORMLY RANDOM σ_0,

$$\frac{1}{\sqrt{|AUT(G)|}} \sum_{\tau \in AUT(G)} |\sigma_0 \tau, \quad \sigma_0(G)\rangle$$

2. LINEAR FILTER : FOURIER TRANSFORM OVER S_n IN REGISTER 1.

WHAT IS THE FOURIER TRANSFORM ?

WHAT IS A REPRESENTATION ?

REPRESENTATION ρ : HOMOMORPHISM $\rho : G \to \mathcal{U}(V)$

UNITARY GROUP $\mathcal{U}_V \cong \mathbb{C}^d$

"EXTEND BY LINEARITY."

LHS: $\mathbb{C}[G]$ = "GROUP ALGEBRA"

= WAVES ON G.

$\mathbb{C}[G]$ IS A $|G|$-DIMENSIONAL VECTOR SPACE (BASIS $\{e_g\}$)

WITH GROUP COMPOSITION $e_g \, e_h = e_{gh}$

(CALLED "CONVOLUTION")

RHS: $\mathrm{End}(V)$ = LINEAR MAPS $V \to V$

$$\rho : \sum_{g \in G} \alpha_g |g\rangle \longrightarrow \sum_{g \in G} \alpha_g \rho(g)$$

$\rho: G \to \mathcal{U}(V)$ IS AN **IRREDUCIBLE REPRESENTATION** (**IRREP**) IF V HAS NO INVARIANT SUBSPACES.

FROBENIUS, SCHUR:

1. FINITE GROUP G HAS A FINITE LIST OF INEQUIVALENT IRREPS $\rho_1, \dots, \rho_k$.

2. ALGEBRA ISOMORPHISM

$$|g\rangle \longrightarrow (\rho_1(g), \dots, \rho_k(g))$$

$$\mathbb{C}[G] \longrightarrow (\mathrm{End}(V_1), \dots, \mathrm{End}(V_k))$$

$\rho: G \to \mathcal{U}(V)$ IS AN IRREDUCIBLE REPRESENTATION (IRREP) IF V HAS NO INVARIANT SUBSPACES.

FROBENIUS, SCHUR:

1. FINITE GROUP G HAS A FINITE LIST OF INEQUIVALENT IRREPS $\rho_1, \dots, \rho_k$.

2. ALGEBRA ISOMORPHISM

$$|g\rangle \xrightarrow[\text{TRANSFORM}]{\text{FOURIER}} (\rho_1(g), \dots, \rho_k(g))$$

$$\mathbb{C}[G] \xrightarrow[\text{TRANSFORM}]{\text{FOURIER}} (\text{End}(V_1), \dots, \text{End}(V_k))$$

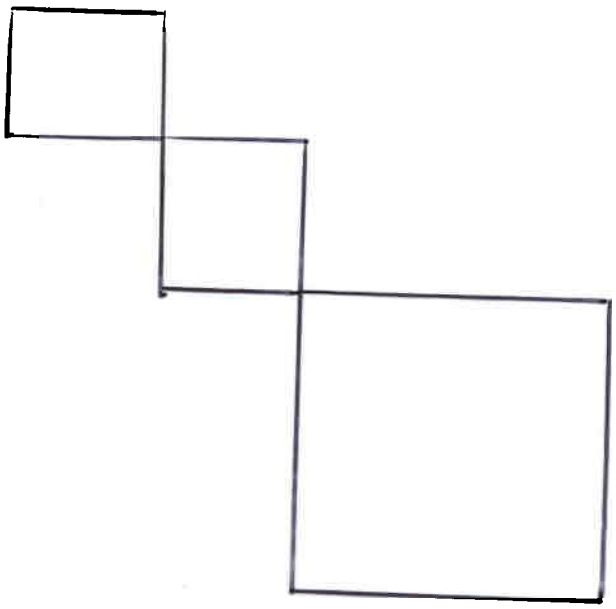
NOTE $|G| = \sum d_i^2$.

3. FOURIER TRANSFORM IS <u>UNITARY</u>

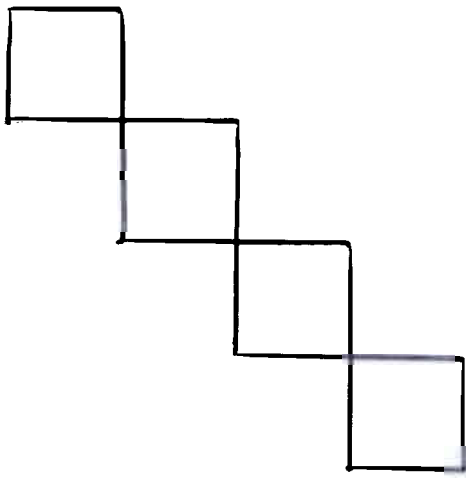
(WITH PROPER CHOICE OF INNER PRODUCT ON RHS)

$$|g\rangle \longrightarrow \left(\sqrt{\frac{d_1}{|G|}}\,\rho_1(g), \dots, \sqrt{\frac{d_k}{|G|}}\,\rho_k(g)\right)$$

EXAMPLE: S_3

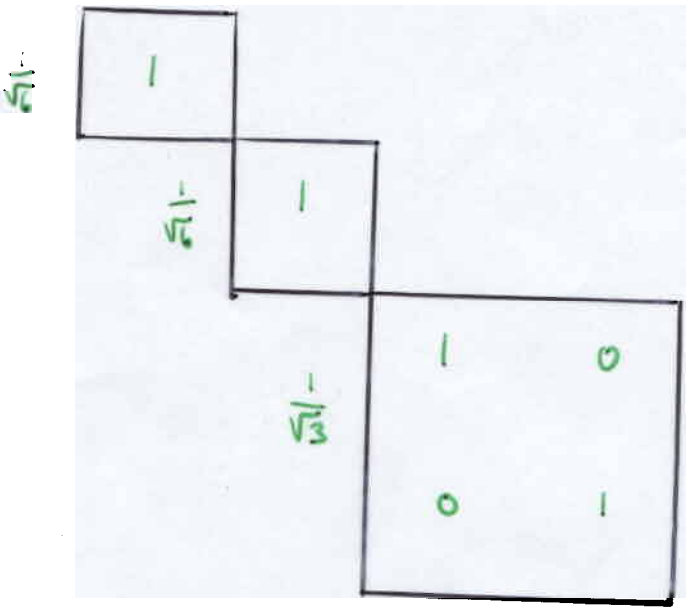


EXAMPLE: C_n

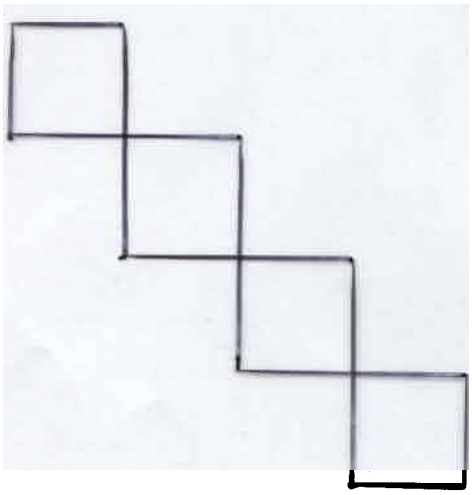


EXAMPLE: S_3

$|id\rangle \rightarrow$

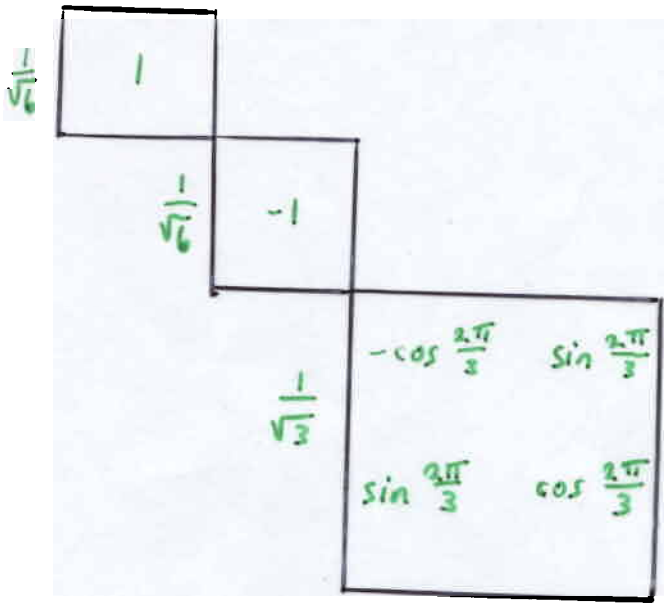


EXAMPLE: C_n

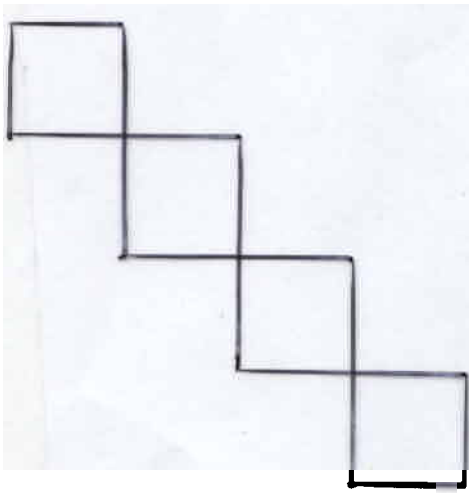


EXAMPLE: S_3

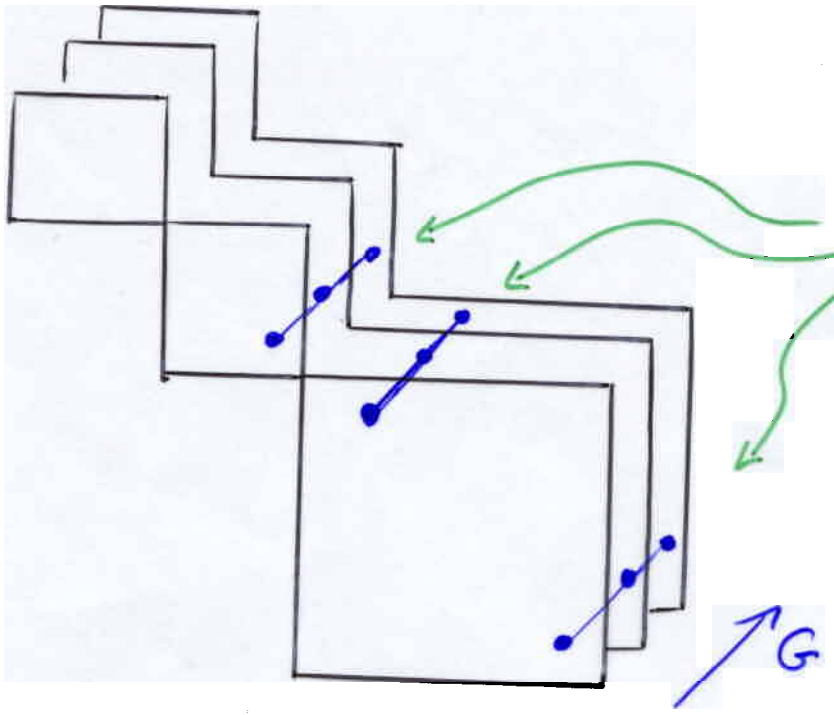
$|(12)(3)\rangle \longrightarrow$



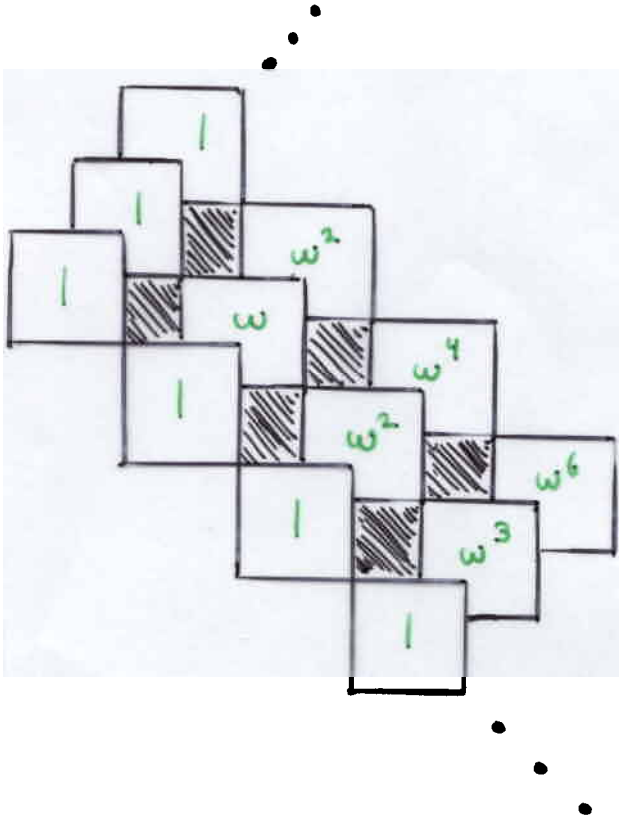
EXAMPLE: C_n



EXAMPLE: S_3



EXAMPLE: C_n



FOR $G = S_n$, FOURIER TRANSFORM IS

EFFICIENTLY COMPUTABLE.

CLAUSEN '89
DIACONIS-ROCKMORE '90
QUANTUM: BEALS '97.

COMPUTATIONAL POWER OF THIS METHOD ?

HALLGREN, RUSSELL, TA-SHMA '00
GRIGNI, SCHULMAN, U. VAZIRANI, M. VAZIRANI '01

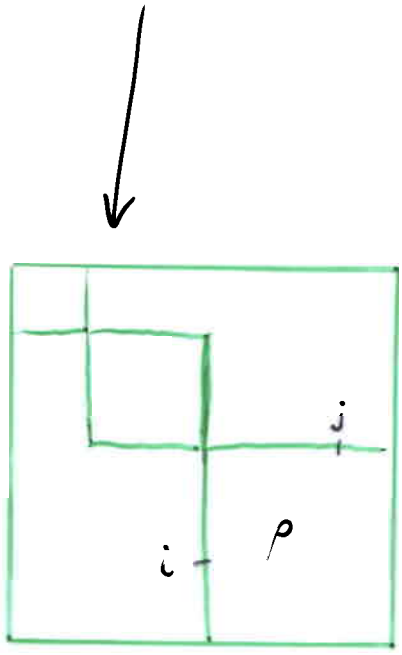
METHOD:

1. PREPARE RANDOM COSET SUPERPOSITION

E.G. FOR GRAPH AUTOMORPHISM: $\frac{1}{\sqrt{|AUT(G)|}} \sum_{\tau \in AUT(G)} |G_0 \tau\rangle$

MORE GENERALLY FOR "HIDDEN SUBGROUP" $H \subseteq G$:

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



2. THEN FOURIER TRANSFORM:

3. MEASURE $|\rho, i, j\rangle$.

* FOR ANY IRREP ρ,

$$\rho(|H\rangle) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \rho(h)$$

IS A SCALAR MULTIPLE OF A PROJECTION MATRIX.

* IF H IS <u>NORMAL</u> IN G, $\rho(|H\rangle)$ IS A SCALAR MULTIPLE OF THE IDENTITY. NONZERO IFF $H \subseteq \ker \rho$.

⇒ (1) FOR NORMAL H, WE'LL ONLY OBSERVE ρ S.T. $H \subseteq \ker \rho$.
(2) FOR NORMAL H, $|\rho\rangle$ IS A "SUFFICIENT STATISTIC" FOR H: i, j BEAR NO FURTHER INFORMATION.

ALGORITHM: REPEAT STEPS 1-3 $\ell = \log|G|$ TIMES, OBSERVING IRREPS $\rho_1, \ldots, \rho_\ell$.

THEOREM: WITH HIGH PROBABILITY $\ker \rho_1 \cap \ldots \cap \ker \rho_\ell$ = LARGEST NORMAL $N \subseteq H$.

EFFICIENT ALGORITHM ALSO FOR "ALMOST ABELIAN" GROUPS.

NORMALIZER OF $H \subseteq G$:

$$N(H) = \{ g \in G : \quad g^{-1} H g = H \} .$$

"MIDDLE" OF G:

$$M(G) = \bigcap_{H \subsetneq G} N(H)$$

G IS "ALMOST ABELIAN" IF $[G : M(G)]$ IS SMALL.

(ABELIAN $\Rightarrow$ $M(G) = G$)

IF H IS NOT NORMAL, $|\rho\rangle$ IS NOT A SUFFICIENT STATISTIC.

HOW MUCH INFORMATION IN i, j ABOUT H?

DEPENDS ON BASIS CHOICE WITHIN ρ.

NOTE: IF ρ IS AN IRREP, SO IS $A^{-1}\rho A$ FOR ANY A.

HIDDEN SUBGROUPS H, $g^{-1}Hg$ HAVE IDENTICAL DISTRIBUTIONS ON $\rho_1, \ldots, \rho_k$. CAN ONLY BE TOLD APART BY BASIS-DEPENDENT INFORMATION.

LOWER BOUNDS

QUESTION 1: CAN FULL MEASUREMENT TELL H, $g^{-1}Hg$ APART?

ANSWER 1: WITH HIGH PROBABILITY OVER CHOICE OF

RANDOM BASES FOR $\rho_1, \ldots, \rho_k$,

$$\text{VARIATION DISTANCE} \leq \frac{|H|^{1/3} \, c(G)^{1/6}}{|G|^{1/6}}$$

WHERE $c(G)$ = # CONJUGACY CLASSES IN G.

... "NO"

QUESTION 2: CAN MEASUREMENT OF $|\rho\rangle$ EFFECTIVELY

DISTINGUISH A SUBGROUP $H = \{id, g\}$ from $H = \{id\}$?

(REMEMBER: ALL WE NEED FOR GRAPH AUTOMORPHISM)

LET $C(g)$ = CONJUGACY CLASS OF g.

ANSWER 2:

$$\text{VARIATION DISTANCE ON IRREPS} \leq \frac{1}{\sqrt{|C(g)|}}$$

... "NO"

COMBINING: THE QUANTUM ALGORITHM, USING RANDOM BASES

IN THE IRREPS, REQUIRES EXPONENTIAL TIME [redacted] TO

DISTINGUISH $|AUT(G)| = 1$ FROM $|AUT(G)| = 2$.

QUESTIONS

1. OTHER METHODS ?

ETTINGER, HOYER, KNILL : TENSORED COSET SUPERPOSITION

$$|g_1 H\rangle \otimes \ldots \otimes |g_t H\rangle$$

FOR $t = 4 \log |G|$, "CONTAINS ENOUGH INFORMATION" ABOUT H.

2. STRONGER LOWER BOUNDS ?

SHOW METHOD FAILS IN EVERY BASIS.

("LAW OF LARGE NUMBERS" FOR IRREPS)

In these days the angel of ~~topology~~ computer science
and the devil of abstract algebra
fight for the soul of every individual
discipline of mathematics

— HERMANN WEYL