

You cannot win in a quantum casino
joint work with Cristopher Moore and Alexander Russell

Piotr Śniady

Polish Academy of Sciences and University of Wrocław

Hidden Subgroup Problem

G is a known group (usually finite);

$H \subset G$ is a hidden subgroup;

$f : G \rightarrow S$ is the oracle,

we are promised that $f(a) = f(b) \iff Ha = Hb \iff ab^{-1} \in H$;

Problem: $H = ?$

Examples

- Schor's algorithm: $G = \mathbb{Z}$,
- Simon's algorithm: $G = (\mathbb{Z}_2)^n$,
- Kuperberg's algorithm: $G = D_n$ the dihedral group,
- Graph Isomorphism Problem: $G = (S_n \times S_n) \rtimes \mathbb{Z}_2$,

Hidden Subgroup Problem, simplified

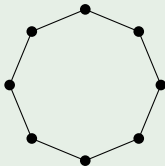
assume $N \subset G$ is a subgroup, $[G : N] = 2$,

we are promised that either

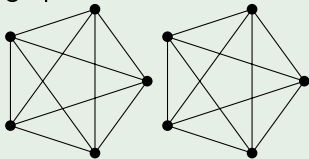
- $H = \{e\}$ is trivial, or
- $H = \{e, s\}$ with $s \notin N$

Examples

Kuperberg's algorithm:
 G is the dihedral group,



Graph Isomorphism Problem:
 G is the automorphism group of two copies of the complete graph



Representations

V is a (finite dimensional) vector space,

$\phi : G \rightarrow \text{End } V$ is a group homomorphism:

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for any } a, b \in G;$$

we say that V is a **representation** of a group G

representation V is **irreducible** if it cannot be written as a sum of smaller representations: $V \neq V_1 \oplus V_2$.

Example 1: discrete Fourier transform

$$G = \mathbb{Z}_n = \{0, 1, \dots, n-1\},$$

irreducible representations are indexed by $k \in \mathbb{Z}_n$,

$V_k = \mathbb{C}$ is one-dimensional,

$$\phi_k(l) = e^{\frac{2\pi ikl}{n}}$$

$$\phi_k(a+b) = \phi_k(a)\phi_k(b) \quad \text{for any } a, b \in \mathbb{Z}_n.$$

Representations

V is a (finite dimensional) vector space,

$\phi : G \rightarrow \text{End } V$ is a group homomorphism:

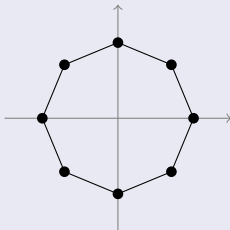
$$\phi(ab) = \phi(a)\phi(b) \quad \text{for any } a, b \in G;$$

we say that V is a **representation** of a group G

representation V is **irreducible** if it cannot be written as a sum of smaller representations: $V \neq V_1 \oplus V_2$.

Example 2

irreducible representation of the dihedral group as symmetries of a polygon on the plane



Representations

V is a (finite dimensional) vector space,

$\phi : G \rightarrow \text{End } V$ is a group homomorphism:

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for any } a, b \in G;$$

we say that V is a **representation** of a group G

representation V is **irreducible** if it cannot be written as a sum of smaller representations: $V \neq V_1 \oplus V_2$.

Example 3: the left-regular representation

the group G can be represented on the vector space

$$V = \mathcal{H} = \ell^2(G)$$

orthonormal basis: $|a\rangle_{a \in G}$

$$\phi(g)|a\rangle = |ga\rangle$$

Characters

if V is an irreducible representation of G , we consider its **character**

$$\chi_V(g) = \text{Tr } \phi(g)$$

if $N \subset G$ is a fixed subgroup and $[G : N] = 2$,
we say that an irreducible representation V of G is **unlucky** if

$$\chi_V(g) = 0 \quad \text{for all } g \notin N$$

Notations

if V is a representation of G

and $H \subset G$ is a subgroup

we denote by

$$V^H = \{v \in V : \phi(h)v = v \text{ for all } h \in H\}$$

the set of **H -invariant vectors**

if $W \subseteq \mathcal{H}$ is a vector space, we denote by

$$\rho_W = \frac{1}{\dim W} (\text{projection on } W)$$

the uniform mixed state on W

Coset state

Notations

we will use Hilbert space $\mathcal{H} = \ell^2(G)$ with basis $|a\rangle$, $a \in G$;
for $X \subset G$ we denote the pure state $|X\rangle = \frac{1}{\sqrt{|X|}} \sum_{a \in X} |a\rangle$

1 start with pure state $|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{a \in G} |a\rangle$,

2 compute the oracle function $f : G \rightarrow S$

$$\frac{1}{\sqrt{|G|}} \sum_{a \in G} |a, f(a)\rangle \in \ell^2(G) \otimes \ell^2(S)$$

3 measure the second coordinate, forget the output

$$\rho_{H \setminus G} = \frac{1}{|G|} \sum_{a \in G} |Ha\rangle \langle Ha| = \rho_{\ell^2(G)^H}$$

the coset state

Burnside decomposition 1

$$\ell^2(G) = \bigoplus_{\substack{V \text{ - irreducible} \\ \text{representation of } G}} V \otimes V^* = \bigoplus_V V \oplus \dots \oplus V$$

this decomposition can be used for a quantum measurement;

$$\rho_{G \setminus H} = \rho_{\ell^2(G)^H} = \bigoplus_V \rho_{V^H} \otimes \rho_{V^*}$$

the measurement gives us:

- the name of the irreducible representation V ,
let us hope it is lucky!
- state ρ_{V^H} (useful, but encrypted quantum information),
- state ρ_{V^*} (useless!)

Burnside decomposition 2

$$\rho_{G \setminus H} = \rho_{\ell^2(G)^H} = \bigoplus_V \rho_{V^H} \otimes \rho_{V^*}$$

Probability distribution:

- if $H = \{e\}$

$$P(V) = \frac{(\dim V)^2}{|G|}, \quad \text{Plancherel measure}$$

- if $H = \{e, s\}$

$$P(V) = \frac{(\dim V)(\dim V + \chi_V(s))}{|G|},$$

if V is unlucky, there is no difference

if we are unlucky we should do something more...

Quantum poker

unlucky? we can iterate this procedure: $(V_1, \rho_{V_1^H}), (V_2, \rho_{V_2^H}), \dots$

tensor product of representations:

$$V_1 \otimes V_2 = \bigoplus_V V \oplus \dots \oplus V$$

state:

$$\rho_{V_1^H} \otimes \rho_{V_2^H} = \rho_{V_1^H \otimes V_2^H} = \bigoplus_V \rho_{(\text{some subspace of } V^H)}$$

measurement gives us:

- the name of the irreducible representation V ,
let us hope it is lucky!
- state $\rho_{(\text{some subspace of } V^H)}$,

and if we are unlucky...

Quantum poker, simplified

- whenever you like, you can ask the dealer for a random irreducible representation V of G ,
- whenever you like, you can also...
 - 1 take two irreducible representations V_1, V_2 from your deck of cards, give them to the dealer,
 - 2 the dealer gives you back the random irreducible representation from the tensor product $V_1 \otimes V_2$,
- if you have a **lucky** irreducible representation, you **WON!**; otherwise you have to keep playing

Quantum poker

Theorem (Kuperberg)

if G is the *dihedral group*, there is an *explicit strategy to win* in a quantum poker quickly with high probability

Theorem (Moore, Russell, Śniady)

if G is the *automorphism group of two copies of the complete graph*, there is *no strategy to win* in a quantum poker quickly with high probability

proof: very strong estimates on the characters of the symmetric groups

Bibliography



Cristopher Moore, Alexander Russell, and Piotr Śniady.

On the impossibility of a quantum sieve algorithm for graph isomorphism.

In *STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 536–545. ACM, New York, 2007.



Cristopher Moore, Alexander Russell, and Piotr Śniady.

On the impossibility of a quantum sieve algorithm for graph isomorphism.

SIAM J. Comput., 39(6):2377–2396, 2010.



Valentin Féray and Piotr Śniady.

Asymptotics of characters of symmetric groups related to Stanley character formula.

Ann. of Math. (2), 173(2):887–906, 2011.