Shor's Algorithm & the Hidden Subgroup Problem

Shiang Yong LOOI

Carnegie Mellon University

20th March 2012

Overview

- Motivation
- Formal Definition of HSP
- Recent Results and Open Problems

References

- Wikipedia : Hidden Subgroup Problem.
- A. M. Childs & W. van Dam, Quantum algorithms for algebraic problems, Rev. Mod. Phys. **82**, 1–52 (2010).
- D. Bacon & W. van Dam, Recent Progress in Quantum Algorithms, Comms. ACM **52**, Issue 2 (2010).

Motivation

The most well-known quantum algorithm is arguably Shor's algorithm (1994).

To factor a large number with *n* bits, the fastest classical algorithm is in

$$O\left(\exp(n^{\frac{1}{3}} \times \log^{\frac{2}{3}} n)\right)$$

Shor's algorithm runs in $O(n^3)$.

Motivation

The most well-known quantum algorithm is arguably Shor's algorithm (1994).

To factor a large number with n bits, the fastest classical algorithm is in

$$O\left(\exp(n^{\frac{1}{3}} \times \log^{\frac{2}{3}} n)\right)$$

Not known if there are faster classical algorithms.

Motivation

Fallacy : Quantum computers can solve NP-Complete problems efficiently!

Factoring is not known to be NP-Complete.

Experts do not think quantum computers can solve NP-Complete problems efficiently.

Motivation

Soon after Shor’s algorithm’s significance was recognized, researchers started to ask:

What is the “secret sauce” of Shor’s algorithm? Why can’t classical computers perform just as fast?

Can the core subroutine be generalized to solve other problems?

Motivation

The core of Shor's algorithm (period finding) is a hidden subgroup problem.

For which there is no efficient classical algorithm.

Simon's algorithm is also solving a HSP.

Motivation

What are other problem that can be expressed as HSPs?

Are there generalizations of HSP that are interesting?

Formal Definition

Let G be the cyclic group with 6 elements.

The group operation is addition mod 6.

$G = \{0, 1, 2, 3, 4, 5\}$.

Subgroups of G are $\{0, 3\}$ and $\{0, 2, 4\}$.

Formal Definition

Let us now define group operation on a set of group elements.

We are familiar with $2 \bullet 5 = 1$.

Then define $2 \bullet \{3, 5\} = \{2\bullet 3, 2\bullet 5\}$

Formal Definition

Let us now define group operation on a set of group elements.

We are familiar with 2 • 5 = 1.

Then define 2 • {3, 5} = {2•3, 2•5} = {5, 1}.

Formal Definition

To define cosets, let us focus on the subgroup $H = \{0, 3\}$.

Notice that $0 \bullet H = H$ and $3 \bullet H = H$.

Also $1 \bullet H = \{1, 4\}$ and $4 \bullet H = \{1, 4\}$.

And $2 \bullet H = 5 \bullet H = \{2, 5\}$.

Are there any other cosets?

Observe that $G = H \cup 1H \cup 2H$.

Formal Definition

Here are some facts about cosets:

1) Each element can only belong to a unique coset, hence cosets are all disjoint.
2) Every coset has exactly the same number of elements.
3) The union of every coset is the original group.

Formal Definition

Given a group G, there is an oracle $f : G \mapsto \mathbf{R}$.

There is a "hidden" subgroup H and f has the property that

1) $f(g_1) = f(g_2)$, if $g_1H = g_2H$.
2) $f(g_1) \neq f(g_2)$, if $g_1H \neq g_2H$.

The HSP is to determine subgroup H by querying f with as few queries as possible and as little processing time as possible.

Formal Definition

The period-finding subroutine in Shor's algorithm is an HSP, the group being $Z_N \times Z_N$.

The details are quite technical. Ref : www.math.uwaterloo.ca/~amchilds/teaching/w11/l03.pdf

Formal Definition

Let G be an Abelian group with $|G|$ elements and define $n = \log |G|$.

Then there exists a quantum algorithm that solves the HSP (for any H) in $O(\text{poly}(n))$.

Whereas for some G, the best classical algorithm runs in

$$O\left(\exp(n^{\frac{1}{3}} \times \log^{\frac{2}{3}} n)\right)$$

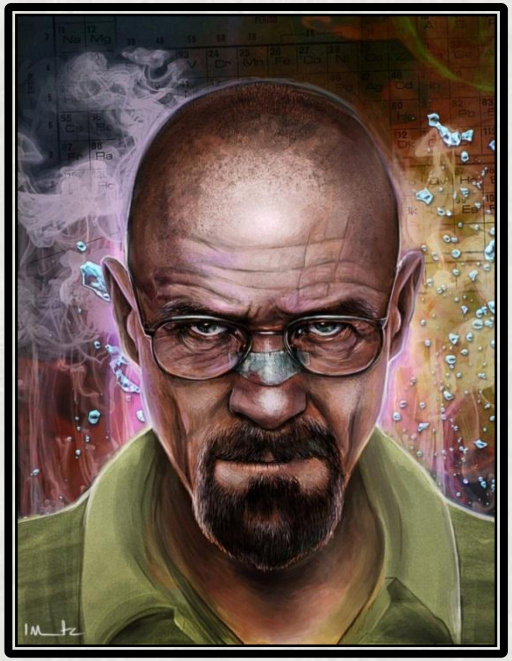
Recent Work

The race was on to find quantum algorithms to solve HSP on non-Abelian groups efficiently.

Recent Work

The following non-Abelian group can be solved efficiently:

- G is a nil-2 group.
- H is a normal subgroup of a solvable group G.
- G is a Weyl-Heisenberg group.



Recent Work

These non-Abelian group can be solved efficiently:

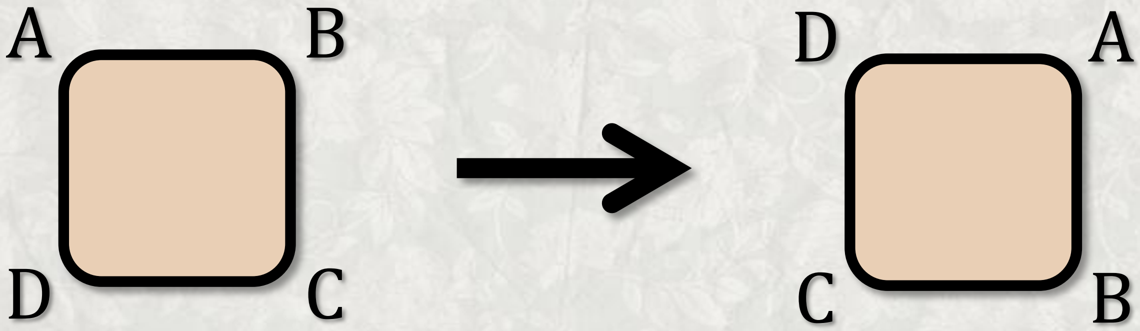
- *G* is a nil-2 group.
- *H* is a normal subgroup of a solvable group *G*.
- *G* is a Weyl-Heisenberg group.

Unfortunately not all groups are interesting.

Dihedral group

Group that preserves regular polygons.
Generalizes the cyclic group.

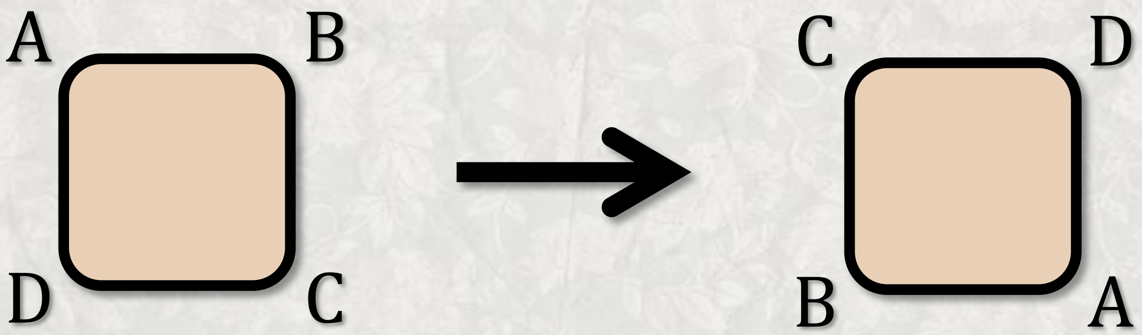
For example consider $\mathbf{Z}_4$.



Dihedral group

Group that preserves regular polygons.
Generalizes the cyclic group.

For example consider $\mathbf{Z}_4$.

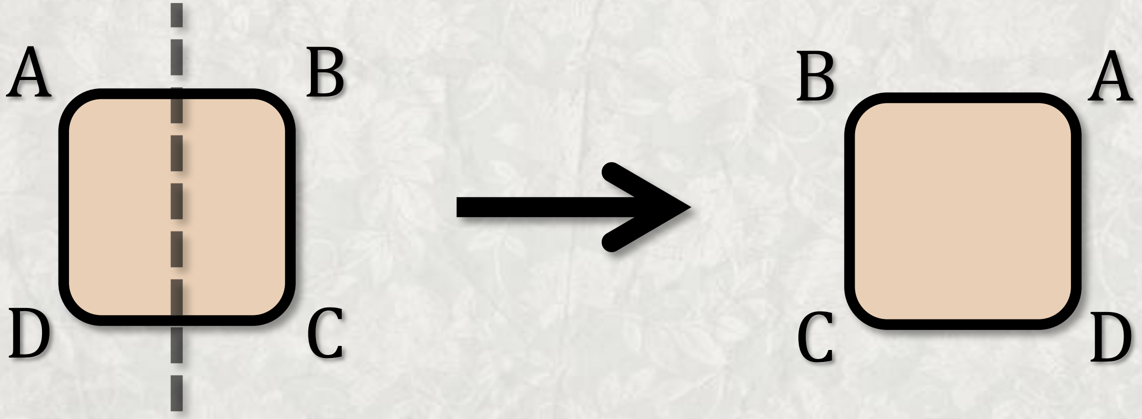


$\mathbf{Z}_4$ has four elements.

Dihedral group

Group that preserves regular polygons.
Generalizes the cyclic group.

Now consider D_4.

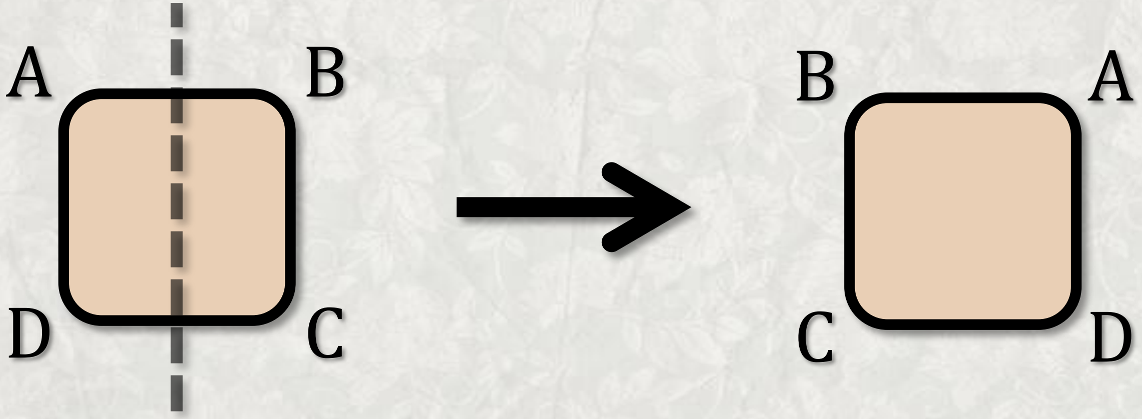


D_4 has 8 elements and Z_4 is a subgroup.

Dihedral group

Group that preserves regular polygons.
Generalizes the cyclic group.

Now consider D_4.



D_4 is non-Abelian.

Dihedral group

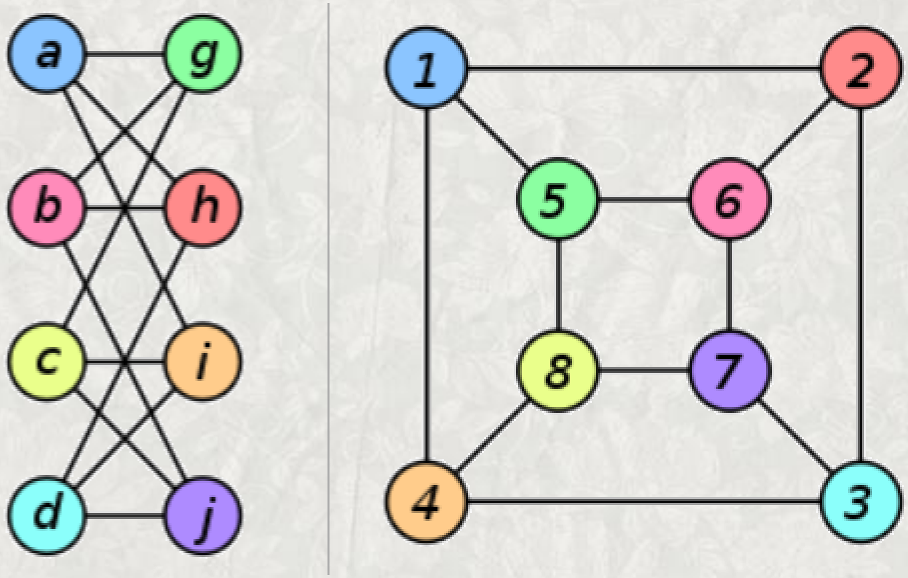
Dihedral groups are interesting:

1) Non-Abelian but "almost" Abelian.
2) Can be used to break lattice-based cryptography.

This group is solved for D_p when p is prime.

Symmetric group

HSP on the symmetric group S_n is equivalent to the graph isomorphism problem.



Generalization

HSP has been generalized to:

1) Hidden Polynomial Problem
2) Hidden Symmetry Subgroup Problem
3) Hidden Translation Problem

References

- Wikipedia : Hidden Subgroup Problem.
- A. M. Childs & W. van Dam, Quantum algorithms for algebraic problems, Rev. Mod. Phys. **82**, 1–52 (2010).
- D. Bacon & W. van Dam, Recent Progress in Quantum Algorithms, Comms. ACM **52**, Issue 2 (2010).