Quantum Algorithms for Group Theoretic Problems

François Le Gall

The University of Tokyo

work done during the period 2006-2009 while affiliated with the ERATO-SORST Quantum Computation and Information project (JST)

• Introduction

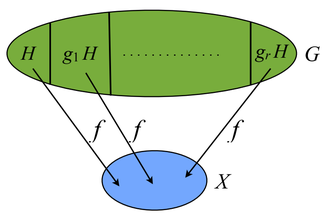
Most of the computational problems for which quantum computers offer an exponential speed-up with respect to the best known classical algorithms possess a nice algebraic structure (or, informally speaking, a lot of symmetries). This research aims at further investigating these aspects of quantum computation by focussing on the construction of quantum algorithms for group-theoretic problems.

• The Hidden Subgroup Problem

The Hidden Subgroup Problem (HSP) is a generalization of Shor's order-finding problem to an arbitrary group G.

Hidden Subgroup Problem

input: a group G and a map $f: G \to X$ constant on the cosets of a hidden subgroup H
output: a set of generators of H



An efficient quantum algorithm solving the HSP over the dihedral group would solve problems over lattices (such as the shortest vector problem) believed to be hard in the classical setting and related to the security of cryptosystems.

$G = \mathbb{Z}_n \rtimes \mathbb{Z}_2$

We have showed (Reference [1]) that the HSP can be solved in polynomial time on a quantum computer over a closely related class of semidirect product groups.

$G = \mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$
(p: odd prime)

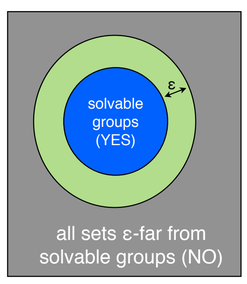
• Quantum Property Testing

One of the main open problems in the area of algebraic property testing is to understand the complexity of testing whether a given set is "close to a group".

Since closeness to an *abelian group* can be checked efficiently on a classical computer, we considered the case of *solvable groups* (note that any abelian group is solvable but the class of solvable groups includes many non-abelian groups).

Property Testing of Group Solvability

input: a set S and a operator $*: S \times S \to S$
output: YES if $(S,*)$ is a solvable group
NO if $(S,*)$ is ε-far from any solvable group



We have constructed (Reference [2]) a quantum algorithm that solves this problem using a polynomial number of queries, which is exponentially better than the best known classical algorithm. The algorithm relies on the ability of quantum computers to handle solvable groups efficiently.

• The Group Isomorphism Problem

The group isomorphism problem is a fundamental problem in computational group theory that is believed to be hard (for example, there are 49,487,365,422 non-isomorphic groups of size 1024).

Group Isomorphism Problem

input: two finite groups G and H of size $|G|=|H|=n$
question: are G and H isomorphic?

The best known classical algorithm for the group isomorphism problem has time complexity $n^{\log n + o(1)}$, which is exponential in the input size. On the other hand, it is known that the group isomorphism problem is not harder than the graph isomorphism problem.

We have showed (Reference [4]) that there exists a quantum algorithm with complexity polynomial in $\log n$ solving the group isomorphism problem over the following class of groups.

our class of groups

$A \rtimes \mathbb{Z}_m$

A: abelian group
m: integer coprime with $|A|$
$\rtimes$: semidirect product

examples: all abelian groups
the dihedral groups of odd order
many other constructions (e.g., 9 non-isomorphic groups of the form $A = \mathbb{Z}_3^4 \rtimes \mathbb{Z}_4$)

This is the first quantum algorithm that solves instances of the non-abelian group isomorphism problem in time polynomial in $\log n$ (such complexity was previously achieved only for abelian groups).

We also proved (Reference [3]) that there exists a *classical* algorithm solving the same problem in time polynomial in n, by replacing the quantum part of the algorithm by classical techniques. This is one of the very few classes of non-abelian groups for which isomorphism testing can be done in polynomial-time classically.

• Related Publications

[1] Yoshifumi Inui and François Le Gall. **Efficient Quantum Algorithms for the Hidden Subgroup Problem over a Class of Semi-direct Product Groups.** Quantum Information and Computation, Vol.7 No.5&6, pp. 559-570, 2007.

[2] Yoshifumi Inui and François Le Gall. **Quantum Property Testing of Group Solvability.** Algorithmica, published online on July 11, 2009.

[3] François Le Gall. **Efficient Isomorphism Testing for a Class of Group Extensions**. Proceedings of STACS'09, pp. 625-636, 2009.

[4] François Le Gall. **An Efficient Quantum Algorithm for some Instances of the Group Isomorphism Problem.** Proceedings of STACS'10, pp. 549-560, 2010.