International Journal of Foundations of Computer Science
Vol. 26, No. 2 (2015) 255–268

DOI: 10.1142/S012905411550015X

World Scientific
www.worldscientific.com

# Quantum Algorithms for a Set of Group Theoretic Problems

Stephen Fenner*
*Department of Computer Science and Engineering, University of South Carolina*
*Columbia, SC 29208, USA*
*fenner@cse.sc.edu*

Yong Zhang
*Department of Computer Science, Kutztown University of Pennsylvania*
*Kutztown, PA 19530, USA*
*zhang@kutztown.edu*

Received 5 June 2014
Accepted 20 October 2014
Communicated by Kazuo Iwama

We introduce two decision problems, Stabilizer$_D$ and Translating Coset$_D$, and give quantum reductions from them to the problem Orbit Superposition, as well as quantum reductions to them from two group theoretic problems Group Intersection and Double Coset Membership. Based on these reductions, efficient quantum algorithms are obtained for Group Intersection and Double Coset Membership in the setting of black-box groups. Specifically, for solvable groups, this gives efficient quantum algorithms for Group Intersection if one of the underlying solvable groups has a smoothly solvable commutator subgroup, and for Double Coset Membership if one of the underlying solvable groups is smoothly solvable. We also show that Group Intersection and Double Coset Membership are in the complexity class **SZK**.

*Keywords*: Quantum algorithm; black-box groups; computational complexity.

## 1. Introduction

In 1994 Shor [32] discovered polynomial time quantum algorithms for two problems, Integer Factoring and Discrete Logarithm. The two problems are not known to have polynomial time classical algorithms. They are important problems in public-key cryptography as they are foundations of the RSA cryptosystem and Diffie-Hellman key exchange. After Shor's breakthrough discovery, more problems for which quantum algorithms offer exponential speedup over the best known classical algorithms were discovered. It turns out that many such problems have

*Partially supported by NSF grants CCF-0515269 and CCF-0915948 and by the National Security Agency (NSA) and Advanced Research and Development Agency (ARDA) under Army Research Office (ARO) contract number DAAD 19-02-1-0048.

similar underlying algebraic structures. This insight was later characterized by the framework of HIDDEN SUBGROUP problem. In specific, a large set of problems that exhibit quantum speedup, including Deutsch's problem [15], Simon's XOR problem [10, 33], Shor's FACTORING and DISCRETE LOGARITHM problems [32], Boneh and Lipton's HIDDEN LINEAR FUNCTION problem [9], and Kitaev's ABELIAN STABILIZER problem [27], can be shown to reduce to instances of the HIDDEN SUBGROUP problem.

We define the HIDDEN SUBGROUP problem as follows. Given an finitely generated group $G$ and an efficiently computable function $f$ mapping $G$ into a finite set, $f$ satisfies the promise that there exists a subgroup $H$ of $G$ such that $f$ is constant on each left(right) coset of $H$ and distinct on different left(right) cosets of $H$. The task is to find a generating set for $H$. All the above mentioned problems with quantum speedup reduce to instances of HIDDEN SUBGROUP where the underlying groups $G$ are abelian. Mosca, building on the work of Kitaev, gave a general polynomial time quantum algorithm for the abelian HIDDEN SUBGROUP problem [29]. An interesting question is whether we can obtain similar polynomial time quantum algorithms for the cases when the underlying groups G are non-abelian. The motivation for this research direction is that some well-known problems such as GRAPH ISOMORPHISM reduce to instances of HIDDEN SUBGROUP with non-abelian underlying groups [25]. Several research has been conducted along this line of research, however, only limited progress was reported [13, 16, 17, 22–24, 31]. For a review on quantum algorithms over algebraic problems, see [14].

Friedl *et al.* [19] introduced STABILIZER and TRANSLATING COSET, both of which generalize HIDDEN SUBGROUP, and showed that they can be solved efficiently on quantum computers for a family of smoothly solvable groups. They introduced in the same paper the problem ORBIT SUPERPOSITION as a useful tool. In this paper we further investigate the relationships among STABILIZER, TRANSLATING COSET, and ORBIT SUPERPOSITION. We study the decision versions of STABILIZER and TRANSLATING COSET, denoted as STABILIZER$_D$ and TRANSLATING COSET$_D$. We show that in bounded error quantum polynomial time STABILIZER$_D$ reduces to ORBIT SUPERPOSITION over solvable groups and TRANSLATING COSET$_D$ reduces to ORBIT SUPERPOSITION over any finite groups.

The reductions to ORBIT SUPERPOSITION suggest that the difficulty in STABILIZER$_D$ and TRANSLATING COSET$_D$ resides in the construction of uniform quantum superpositions over orbits (in a group action). This is in general not a surprise. Very often, solving a problem with a quantum algorithm can be reduced to preparing the right quantum superposition. For example, if one can prepare a uniform superposition over all graphs isomorphic to a given graph, then one can solve the GRAPH ISOMORPHISM problem easily via a simple swap test [2, 11]. Our results on STABILIZER$_D$ and TRANSLATING COSET$_D$ help us to obtain efficient quantum algorithms for two well studied problems in computational group theory, GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP. No efficient classical algorithms are known for these two problems. Watrous [36] constructed efficient

quantum algorithms for several group theoretic problems on solvable groups, such as ORDER VERIFICATION and GROUP MEMBERSHIP. Based on an algorithm of Beals and Babai [8], Ivanyos, Magniez, and Santha [24] obtained efficient quantum algorithms for ORDER VERIFICATION as well as several other group theoretic problems. Watrous [36] asked whether there are efficient quantum algorithms for problems such as GROUP INTERSECTION and COSET INTERSECTION. In this paper we study GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP where DOUBLE COSET MEMBERSHIP generalizes COSET INTERSECTION as well as GROUP MEMBERSHIP and GROUP FACTORIZATION. We show that for solvable groups, there are efficient quantum algorithms for GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP under certain conditions. We obtain these results by showing that these two problems reduce to STABILIZER$_D$ and TRANSLATING COSET$_D$, respectively. Our results also imply that for *abelian* groups, GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP are in the complexity class **BQP**. Combined with Fortnow and Rogers' result [18] that any problem in **BQP** is low for the counting class **PP**, we obtain an alternative proof that they are low for the class **PP**, which was first proved in Arvind and Vinodchandran [3].

Finally, motivated by a similar result in Aharonov and Ta-Shma [2], we show that GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP have honest-verifier zero knowledge proof systems, and thus are in **SZK**. This is an improvement of Babai's result [5] that GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP are in $\mathbf{AM} \cap \mathrm{co}\mathbf{AM}$. While Watrous [35] showed that GROUP NONMEMBERSHIP is in the complexity class **QMA**, another implication of our results is that GROUP NONMEMBERSHIP is in **SZK**.

## 2. Preliminaries

Background on general group theory and quantum computation can be found in the standard textbooks [12, 30].

### 2.1. *The black-box group model*

We study the group theoretic problems in the context of black-box groups. The black-box group model was first introduced by Babai and Szemerédi [7]. It was then widely adpoted as a general framework for studying algorithmic problems over finite groups [1, 26, 28, 36]. We will use a similar descriptions of this model as in Arvind and Vinodchandran [3].

Fix the alphabet $\Sigma = \{0, 1\}$. A *group family* is a countable sequence $\mathcal{B} = \{B_m\}_{m \geq 1}$ of finite groups $B_m$, such that there exist a polynomial $p$ satisfying the following conditions. For each $m \geq 1$, elements of $B_m$ are encoded as strings (not necessarily unique) in $\Sigma^{p(m)}$. The group operations (inverse, product and identity testing) of $B_m$ are performed at unit cost by black-boxes (or group oracles). We refer to the groups $B_m$ of a group family and their subgroups (presented by generator sets) as *black-box groups*. Common examples of black-box groups are $\{S_n\}_{n \geq 1}$ where

$S_n$ is the permutation group on $n$ elements, and $\{GL_n(q)\}_{n\geq 1}$ where $GL_n(q)$ is the group of $n \times n$ invertible matrices over the finite field $F_q$. Depending on whether the group elements are uniquely encoded, we have the *unique encoding model* and *non-unique encoding model*, the latter of which enables us to deal with factor groups [7]. In the non-unique encoding model an additional group oracle has to be provided to test if two strings represent the same group element. Our results will apply only to the unique encoding model. In one of our proofs, however, we will use the non-unique encoding model to handle factor groups. For how to implement group oracles in the form of quantum circuits, see Watrous [36].

**Definition 1.** [3] *Let $\mathcal{B} = \{B_m\}_{m\geq 1}$ be a group family. Let $e$ denote the identity element of each $B_m$. Let $k \geq 2$ be any integer. Let $\langle S\rangle$ denote the group generated by a set $S$ of elements of $B_m$. Below, $g$ and $h$ denote elements, and $S_1$ and $S_2$ subsets, of $B_m$:*

$$\begin{aligned}
\textsc{Group Intersection} &:= \{(0^m, S_1, S_2) \mid \langle S_1\rangle \cap \langle S_2\rangle = \langle e\rangle\},\\
\textsc{Multiple Group Intersection} &:= \{(0^m, S_1, \ldots, S_k) \mid \langle S_1\rangle \cap \ldots \cap \langle S_k\rangle = \langle e\rangle\},\\
\textsc{Group Membership} &:= \{(0^m, S_1, g) \mid g \in \langle S_1\rangle\},\\
\textsc{Group Factorization} &:= \{(0^m, S_1, S_2, g) \mid g \in \langle S_1\rangle\langle S_2\rangle\},\\
\textsc{Coset Intersection} &:= \{(0^m, S_1, S_2, g) \mid \langle S_1\rangle g \cap \langle S_2\rangle \neq \emptyset\},\\
\textsc{Double Coset Membership} &:= \{(0^m, S_1, S_2, g, h) \mid g \in \langle S_1\rangle h \langle S_2\rangle\}.
\end{aligned}$$

Multiple Group Intersection is a generalized version of Group Intersection. Also, it is easily seen that Double Coset Membership generalizes Group Membership, Group Factorization, and Coset Intersection. Therefore in this paper we will focus on Double Coset Membership. All our results about Double Coset Membership will also apply to Group Membership, Group Factorization, and Coset Intersection. (Actually, Coset Intersection and Group Factorization are easily seen to be the same problem.)

### 2.2. *Solvable groups*

The *commutator subgroup* $G'$ of a group $G$ is the subgroup generated by elements $g^{-1}h^{-1}gh$ for all $g, h \in G$. We define $G^{(n)}$ such that

$$\begin{aligned}
G^{(0)} &= G,\\
G^{(n)} &= (G^{(n-1)})', \text{ for } n \geq 1.
\end{aligned}$$

$G$ is *solvable* if $G^{(n)}$ is the trivial group $\{e\}$ for some $n$. We call $G = G^{(0)} \triangleright G^{(1)} \triangleright \cdots \triangleright G^{(n)} = \{e\}$ the *derived series* of $G$, of length $n$. Note that all the factor groups $G^{(i)}/G^{(i+1)}$ are abelian. There is a randomized procedure that computes the derived series of a given group $G$ [6].

The *exponent* of a group is the least common multiple of the orders of all elements of the group. The term *smoothly solvable* is first introduced in

Friedl *et al.* [19]. We say that a family of abelian groups is *smoothly abelian* if each group in the family can be expressed as the direct product of a subgroup with bounded exponent and a subgroup of polylogarithmic size in the order of the group. A family of solvable groups is *smoothly solvable* if the length of each derived series is bounded by a constant and the family of all factor groups $G^{(i)}/G^{(i+1)}$ is smoothly abelian.

In designing efficient quantum algorithms for computing the order of a solvable group (Order Verification), Watrous [36] obtained as a byproduct a method to construct approximately uniform quantum superpositions over elements of a given solvable group.

**Theorem 2.** [36] *In the model of black-box groups with unique encoding, there is a quantum algorithm operating as follows (relative to an arbitrary group oracle). Given generators $g_1, \ldots, g_m$ such that $G = \langle g_1, \ldots, g_m \rangle$ is solvable, the algorithm outputs the order of $G$ with probability of error bounded by $\epsilon$ in time polynomial in $mn + \log(1/\epsilon)$ (where $n$ is the length of the strings representing the generators). Moreover, the algorithm produces a quantum state $\rho$ that approximates the state $|G\rangle = |G|^{-1/2} \sum_{g \in G} |g\rangle$ with accuracy $\epsilon$ (in the trace norm metric).*

### 2.3. *A note on quantum reductions*

In Secs. 3 and 4 we describe quantum reductions to various problems. Quantum algorithms for these problems often require several identical copies of a quantum state or unitary gate to work to a desired accuracy. Therefore, we will implicitly assume that our reductions may be repeated $t$ times, where $t$ is some appropriate parameter polynomial in the input size and the logarithm of the desired error bound.

## 3. Stabilizer$_D$ and Translating Coset$_D$

Friedl *et al.* [19] introduced several problems which are closely related to Hidden Subgroup. In particular, they introduced Stabilizer, Hidden Translation, Translating Coset, and Orbit Superposition. Stabilizer generalizes Hidden Subgroup. In fact, the only difference between Stabilizer and Hidden Subgroup is that in the definition of Stabilizer the function $f$ can be a *quantum function* that maps group elements to mutually orthogonal quantum states with unit norm. Translating Coset generalizes Stabilizer and Hidden Translation. Orbit Superposition is a relevant problem, which is also of independent interest. The superpositions Watrous constructed in Theorem 2 can be considered as an instance of Orbit Superposition.

We would like to further characterize the relationship of these problems. First we define and study the decision versions of Stabilizer and Translating Coset, denoted as Stabilizer$_D$ and Translating Coset$_D$. The original definitions of Stabilizer and Translating Coset concern about finding generating sets of certain stabilizer subgroups. In the decision version, we simplify the problems by

only asking whether the stabilizer subgroups are trivial. We also give the definition of the problem Orbit Superposition.

Let $G$ be a finite group. Let $\Gamma$ be a set of mutually orthogonal quantum states. Let $\alpha : G \times \Gamma \to \Gamma$ be a group action of $G$ on $\Gamma$, i.e., for every $x \in G$ the function $\alpha_x : |\phi\rangle \to |\alpha(x, |\phi\rangle)\rangle$ is a permutation over $\Gamma$ and the map $h$ from $G$ to the symmetric group over $\Gamma$ defined by $h(x) = \alpha_x$ is a homomorphism. We use the notation $|x \cdot \phi\rangle$ instead of $|\alpha(x, |\phi\rangle)\rangle$, when $\alpha$ is clear from the context. We let $G(|\phi\rangle)$ denote the set $\{|x \cdot \phi\rangle : x \in G\}$, and we let $G_{|\phi\rangle}$ denote the stabilizer subgroup of $|\phi\rangle$ in $G$, i.e., $\{x \in G : |x \cdot \phi\rangle = |\phi\rangle\}$. Given any positive integer $t$, let $\alpha^t$ denote the group action of $G$ on $\Gamma^t = \{|\phi\rangle^{\otimes t} : |\phi\rangle \in \Gamma\}$ defined by $\alpha^t(x, |\phi\rangle^{\otimes t}) = |x \cdot \phi\rangle^{\otimes t}$. We need $\alpha^t$ because the input superpositions cannot be cloned in general.

**Definition 3.** *Let $G$ be a finite group and $\Gamma$ be a set of pairwise orthogonal quantum states. Fix the group action $\alpha : G \times \Gamma \to \Gamma$.*

- *Given generators for $G$ and a quantum state $|\phi\rangle \in \Gamma$,* Stabilizer$_D$ *is to check if the subgroup $G_{|\phi\rangle}$ is the trivial subgroup $\{e\}$.*
- *Given generators for $G$ and two quantum states $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$,* Translating Coset$_D$ *is to either reject the input if $G(|\phi_0\rangle) \cap G(|\phi_1\rangle) = \emptyset$ or accept the input if $G(|\phi_0\rangle) = G(|\phi_1\rangle)$.*
- *Given generators for $G$ and a quantum state $|\phi\rangle \in \Gamma$,* Orbit Superposition *is to construct the uniform superposition*

$$|G \cdot \phi\rangle = \frac{1}{\sqrt{|G(|\phi\rangle)|}} \sum_{|\phi'\rangle \in G(|\phi\rangle)} |\phi'\rangle.$$

Note that with two quantum states $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$, $G(|\phi_0\rangle)$ and $G(|\phi_1\rangle$ are either identical or disjoint, therefore the problem Translating Coset$_D$ is well defined.

Next we show that the difficulty of Stabilizer$_D$ and Translating Coset$_D$ may reside in constructions of certain uniform quantum superpositions, which can be achieved by the problem Orbit Superposition.

We will use the following result which is easily derivable from Theorem 6 in Ivanyos, Magniez, and Santha [24]:

**Theorem 4.** [24] *Assume that $G$ is a solvable black-box group given by generators with not necessarily unique encoding. Suppose that $N$ is a normal subgroup given as a hidden subgroup of $G$ via a function. Then the order of the factor group $G/N$ can be computed by quantum algorithms in time polynomial in the input size.*

Note that we can apply Theorem 4 when $G$ is a factor group since it uses the non-unique encoding black-box groups model.

**Theorem 5.** *Over solvable groups,* Stabilizer$_D$ *reduces to* Orbit Superposition *in bounded-error quantum polynomial time.*

**Proof.** Let the solvable group $G$ and quantum state $|\phi\rangle$ be the input for the problem STABILIZER$_D$. We can find in classical polynomial time generators for each element in the derived series of $G$ [6], namely, $\{e\} = G_1 \triangleleft \cdots \triangleleft G_n = G$. For $1 \leq i \leq n$ let $S_i = (G_i)_{|\phi\rangle}$, the stabilizer of $|\phi\rangle$ in $G_i$. By Theorem 2 we can compute efficiently the orders of $G_1, \ldots, G_n$ and thus the order of $G_{i+1}/G_i$ for any $1 \leq i < n$. We will proceed in steps. Suppose that before step $i+1$, we know that $S_i = \{e\}$. We want to find out if $S_{i+1} = \{e\}$ in the $(i+1)$st step. Since $G_i \triangleleft G_{i+1}$, by the Second Isomorphism Theorem, $G_i S_{i+1}/G_i \cong S_{i+1}$. Consider the factor group $G_{i+1}/G_i$, we define a function $f$ such that $f$ is constant on $G_i S_{i+1}/G_i$ and distinct on left cosets of $G_i S_{i+1}/G_i$ in $G_{i+1}/G_i$. Then by Theorem 4 we can compute the order of the factor group $G_{i+1}/G_i$ over $G_i S_{i+1}/G_i$. The group oracle needed in the non-unique encoding model to test if two strings $s_1$ and $s_2$ represent the same group elements can be implemented using the quantum algorithm for GROUP MEMBERSHIP, namely, testing if $s_1^{-1} s_2$ is a member of $G_i$. The order of this group is equal to the order of $G_{i+1}/G_i$ if and only if $S_{i+1}$ is trivial.

Here is how we define the function $f$. Using $G_i$ and $|\phi\rangle$ as the input for ORBIT SUPERPOSITION, we can construct the uniform superposition $|G_i \cdot \phi\rangle$. Let $\Gamma$ be the set $\{|gG_i \cdot \phi\rangle | g \in G_{i+1}\}$. Define $f : G_{i+1}/G_i \to \Gamma$ to be $f(gG_i) = |gG_i \cdot \phi\rangle$. What is left is to verify that $f$ hides the subgroup $G_i S_{i+1}/G_i$ in the group $G_{i+1}/G_i$. For any $g \in G_i S_{i+1}$, it is straightforward to see that $|gG_i \cdot \phi\rangle = |G_i \cdot \phi\rangle$. If $g_1$ and $g_2$ are in the same left coset of $G_i S_{i+1}$, then $g_1 = g_2 g$ for some $g \in G_i S_{i+1}$ and thus $|g_1 G_i \cdot \phi\rangle = |g_2 G_i \cdot \phi\rangle$. If $g_1$ and $g_2$ are not in the same left coset of $G_i S_{i+1}$, we will show that $|g_1 G_i \phi\rangle$ and $|g_2 G_i \phi\rangle$ are orthogonal quantum states. Suppose there exists $x_1, x_2 \in G_i$ such that $|g_1 x_1 \cdot \phi\rangle = |g_2 x_2 \cdot \phi\rangle$, then $x_1^{-1} g_1^{-1} g_2 x_2 \in S_{i+1}$. But $x_1^{-1} g_1^{-1} g_2 x_2 = x_1^{-1} x_2' g_1^{-1} g_2$ for some $x_2' \in G_i$. Thus $g_1^{-1} g_2 \in G_i S_{i+1}$. This contradicts the assumption that $g_1$ and $g_2$ are not in the same coset of $G_i S_{i+1}$.

We need to repeat the above procedure at most $\Theta(\log |G|)$ times. For each step the running time is polynomial in $\log |G| + \log(1/\epsilon)$, for error bound $\epsilon$. So the total running time is still polynomial in the input size. □

We can also easily reduce TRANSLATING COSET$_D$ to ORBIT SUPERPOSITION in quantum polynomial time. In this reduction, we do not require the underlying groups to be solvable. The proof uses similar techniques that Watrous [35] and Buhrman *et al.* [11] used to differentiate two quantum states.

**Theorem 6.** TRANSLATING COSET$_D$ *reduces to* ORBIT SUPERPOSITION *in bounded-error quantum polynomial time.*

**Proof.** Let the finite group $G$ and two quantum states $|\phi_1\rangle$, $|\phi_2\rangle$ be the inputs of TRANSLATING COSET$_D$. Remember that the orbit coset of $|\phi_1\rangle$ and $|\phi_2\rangle$ are either identical or disjoint, which implies the two quantum states $|G \cdot \phi_1\rangle$ and $|G \cdot \phi_2\rangle$ are either identical or orthogonal. We may then tell which is the case using a version of the swap test of Buhrman *et al.* [11]. □

## 4. Quantum Algorithms for Group Intersection and Double Coset Membership

In this section we use results in the previous section to make progress in finding quantum algorithms for Group Intersection and Double Coset Membership.

We will need the following results which are easily derivable from Friedl *et al.* [19].

**Theorem 7.** [19] *Let $G$ be a finite solvable group having a smoothly solvable commutator subgroup. Let $\alpha$ be a group action of $G$.* Stabilizer$_D$ *can be solved in $G$ for $\alpha^t$ in quantum time poly$(\log|G|)\log(1/\epsilon)$ with error $\epsilon$ when $t = (\log^{\Omega(1)}|G|)\log(1/\epsilon)$,*

**Theorem 8.** [19] *Let $G$ be a smoothly solvable group and let $\alpha$ be a group action of $G$. When $t = (\log^{\Omega(1)}|G|)\log(1/\epsilon)$,* Translating Coset$_D$ *can be solved in $G$ for $\alpha^t$ in quantum time poly$(\log|G|)\log(1/\epsilon)$ with error $\epsilon$.*

First we show that with the help of certain uniform quantum superpositions over group elements, Group Intersection can be reduced to Stabilizer$_D$.

**Theorem 9.** Group Intersection *reduces to* Stabilizer$_D$ *in bounded-error quantum polynomial time if one of the underlying groups is solvable.*

**Proof.** Given an input $(0^m, S_1, S_2)$ for Group Intersection, without loss of generality, suppose that $G = \langle S_1\rangle$ is an arbitrary finite group and $H = \langle S_2\rangle$ is solvable. By Theorem 2 we can construct an approximately uniform superposition $|H\rangle = |H|^{-1/2}\sum_{h\in H}|h\rangle$. For any $g \in G$, let $|gH\rangle$ denote the uniform superposition over left coset $gH$, i.e., $|gH\rangle = |H|^{-1/2}\sum_{h\in gH}|h\rangle$. Let $\Gamma = \{|gH\rangle | g \in G\}$. Note that the quantum states in $\Gamma$ are (approximately) pairwise orthogonal. Define the group action $\alpha : G\times\Gamma \to \Gamma$ to be that for every $g \in G$ and every $|\phi\rangle \in \Gamma$, $\alpha(g, |\phi\rangle) = |g\phi\rangle$. Then the intersection of $G$ and $H$ is exactly the subgroup of $G$ that stabilizes the quantum state $|H\rangle$. □

**Corollary 10.** Group Intersection *over solvable groups can be solved within error $\epsilon$ by a quantum algorithm that runs in time polynomial in $m+\log(1/\epsilon)$, where $m$ is the size of the input, provided one of the underlying solvable groups has a smoothly solvable commutator subgroup.*

**Proof.** Follows directly from Theorem 7 and the proof of Theorem 9. □

We observe that a similar reduction to Stabilizer$_D$ holds for Multiple Group Intersection.

**Proposition 11.** Multiple Group Intersection *reduces to* Stabilizer$_D$ *in bounded-error quantum polynomial time if all but one of the underlying groups are solvable.*

**Proof.** For simplicity, we illustrate the proof for the case $k = 3$. The argument can be generalized in a straightforward way for cases $k > 3$. Suppose we have three input groups $G$, $H$, and $K$, where $H$ and $K$ are solvable. We let $\Gamma$ be the set $\{|gH\rangle \otimes |gK\rangle | g \in G\}$ and the group action $\alpha : G \times \Gamma \to \Gamma$ be that for every $g \in G$ and every $|\phi\rangle \otimes |\psi\rangle \in \Gamma$, $\alpha(g, |\phi\rangle \otimes |\psi\rangle) = |g\phi\rangle \otimes |g\psi\rangle$. Then $G \cap H \cap K$ is the stabilizer subgroup of $G$ that stabilizes the quantum state $|H\rangle \otimes |K\rangle$. □

It is not clear if a similar reduction to STABILIZER$_D$ exists for DOUBLE COSET MEMBERSHIP. However, DOUBLE COSET MEMBERSHIP can be nicely put into the framework of TRANSLATING COSET$_D$.

**Theorem 12.** DOUBLE COSET MEMBERSHIP *over solvable groups reduces to* TRANSLATING COSET$_D$ *in bounded-error quantum polynomial time.*

**Proof.** Given input for DOUBLE COSET MEMBERSHIP $S_1$, $S_2$, $g$ and $h$, where $G = \langle S_1 \rangle$ and $H = \langle S_2 \rangle$ are solvable groups, we construct the input for TRANSLATING COSET$_D$ as follows. Let $\Gamma = \{|xH\rangle | x \in \langle S_1, S_2, g, h \rangle\}$. Define group action $\alpha : G \times \Gamma \to \Gamma$ to be $\alpha(x, |\phi\rangle) = |x\phi\rangle$ for any $x \in G$ and $|\phi\rangle \in \Gamma$. Let two input quantum states $|\phi_0\rangle$ and $|\phi_1\rangle$ be $|gH\rangle$ and $|hH\rangle$, which can be constructed using Theorem 2. It is easy to check that $G(|\phi_0\rangle) = G(|\phi_1\rangle)$ if and only if $g \in GhH$. □

**Corollary 13.** DOUBLE COSET MEMBERSHIP *over solvable groups can be solved within error* $\epsilon$ *by a quantum algorithm that runs in time polynomial in* $m + \log(1/\epsilon)$*, where* $m$ *is the size of the input, provided one of the underlying groups is smoothly solvable.*

**Proof.** Given input for DOUBLE COSET MEMBERSHIP $S_1$, $S_2$, $g$ and $h$, suppose that $G = \langle S_1 \rangle$ is smoothly solvable and $H = \langle S_2 \rangle$ is solvable. Let $S_1, |gH\rangle, |hH\rangle$ be the input for TRANSLATING COSET$_D$. The result follows from Theorem 8. If instead $H$ is the one which is smoothly solvable, then we modify the input by swapping $S_1$ and $S_2$ and using $g^{-1}, h^{-1}$ to replace $g, h$. Note that this modification will not change the final answer. □

## 5. Statistical Zero Knowledge

Aharonov and Ta-Shma [2] proposed a new way to generate certain quantum states using Adiabatic quantum methods. In particular, they introduced the problem CIRCUIT QUANTUM SAMPLING (CQS) and its connection to the complexity class Statistical Zero Knowledge (**SZK**). Informally speaking, CQS is to generate quantum states corresponding to classical probability distributions obtained from some classical circuits. Although CQS and ORBIT SUPERPOSITION are different problems, they bear a certain level of resemblance. Both problems are concerned about generation of non-trivial quantum states. In their paper they showed that any language in **SZK** can be reduced to a family of instances of CQS. Based on Theorem 5 and

Theorem 6, we would like to ask if there are connections between **SZK** and the two group-theoretic problems discussed in Sec. 4.

Our results are that Group Intersection and Double Coset Membership have honest-verifier zero knowledge proofs, and thus are in **SZK**. This is an improvement of Babai's result [5] that these two problems are in $\mathbf{AM} \cap \text{co}\mathbf{AM}$. One of our proofs shares the same flavor with Goldreich, Micali and Wigderson's proof that Graph Isomorphism is in **SZK** [20].

For standard notions of interactive proof systems and zero knowledge interactive proof systems, see Vadhan's Ph.D. thesis [34]. Here we only use honest-verifier zero knowledge proof systems. Let $\langle P, V\rangle$ be an interactive proof system for an language $L$. We say that $\langle P, V\rangle$ is *honest-verifier perfect zero knowledge* (**HVPZK**) if there exists a probabilistic polynomial-time algorithm $M$ (*simulator*) such that for every $x \in L$ the output probability distribution of $V$ (after interacting with $P$) and $M$, denoted as $\langle P, V\rangle(x)$ and $M(x)$, are identical. Similarly, we say $\langle P, V\rangle$ is *honest-verifier statistical zero knowledge* (**HVSZK**) if $\langle P, V\rangle(x)$ and $M(x)$ are statistically indistinguishable. It is clear that **HVPZK** $\subseteq$ **HVSZK**. Goldreich, Sahai, and Vadhan showed that **HVSZK** and **SZK** are actually the same class [21]. Some complexity results concerning **SZK** (**HVSZK**) include that **BPP** $\subseteq$ **SZK** $\subseteq$ $\mathbf{AM} \cap \text{co}\mathbf{AM}$, and **SZK** is closed under complement, and **SZK** does not contain any **NP**-complete language unless the polynomial hierarchy collapses (see Vadhan [34]).

The following theorem due to Babai [4] will be used in our proof. Let $G$ be a finite group. Let $g_1, \ldots, g_k \in G$ be a sequence of group elements. A *subproduct* of this sequence is an element of the form $g_1^{e_1} \ldots g_k^{e_k}$, where $e_i \in \{0, 1\}$. We call a sequence $h_1, \ldots, h_k \in G$ *a sequence of $\epsilon$-uniform Erdős-Rényi generators* if every element of $G$ is represented in $(2^k/|G|)(1 \pm \epsilon)$ ways as a subproduct of the $h_i$. Note that the order of the $h_i$ is fixed in the subproduct, i.e., every element can be written as $h_1^{e_1} \ldots h_k^{e_k}$ with $e_i \in \{0, 1\}$.

**Theorem 14.** [4] *Let $c, C > 0$ be given constants, and let $\epsilon = N^{-c}$ where $N$ is a given upper bound on the order of the group $G$. There is a Monte Carlo algorithm which, given any set of generators of $G$, constructs a sequence of $O(\log N)$ $\epsilon$-uniform Erdős-Rényi generators at a cost of $O((\log N)^5)$ group operations. The probability that the algorithm fails is $\leq N^{-C}$. If the algorithm succeeds, it permits the construction of $\epsilon$-uniform distributed random elements of $G$ at a cost of $O(\log N)$ group operations per random element.*

Basically what Theorem 14 says is that we can randomly sample elements from $G$ and verify the membership of the random sample efficiently. Given a group $G$ and a sequence of $O(\log N)$ $\epsilon$-uniform Erdős-Rényi generators $h_1, \ldots, h_k$ for $G$, we say that $e_1 \ldots e_k$ where $e_i \in \{0, 1\}$ is a *witness* of $g \in G$ if $g = h_1^{e_1} \ldots h_k^{e_k}$.

**Theorem 15.** Group Intersection *has an honest-verifier statistical zero knowledge proof system.*

**Proof.** Given groups $G$ and $H$, the prover wants to convince the verifier that the intersection of $G$ and $H$ is the trivial group $\{e\}$. Fix a sufficiently small $\epsilon > 0$. The protocol is as follows:

**(V0)** The verifier computes $\epsilon$-uniform Erdős-Rényi generators $g_1, \ldots, g_m$ and $h_1, \ldots, h_n$ for $G$ and $H$. The verifier sends the generators to the prover.
**(V1)** The verifier randomly selects $x \in G$ and $y \in H$ and computes $z = xy$. He then sends $z$ to the prover.
**(P1)** The prover sends two elements, denoted as $x'$ and $y'$, to the verifier.
**(V2)** The verifier verifies if $x$ is equal to $x'$, and $y$ is equal to $y'$. The verifier stops and rejects if any of the verifications fails. Otherwise, he repeats steps from (V1) to (V2).

If $G \cap H$ is trivial, $z$ will be uniquely factorized into $x \in G$ and $y \in H$. Therefore the prover can always answer correctly. On the other hand, if the $G \cap H$ is nontrivial, the factorization of $z$ is not unique, thus with probability at least one half the prover will fail to answer correctly. The verifier can complete a large number of iterations of the above steps to make the probability of a cheating prover succeeding arbitrarily low. For a honest verifier $V$, this protocol is statistical zero-knowledge. □

We observe that the above zero knowledge proof does not apply to Multiple Group Intersection. If there are more than two input groups, the factorization of $z$ will not be unique even if the intersection of input groups is trivial.

**Theorem 16.** Double Coset Membership *has a honest-prover statistical zero knowledge proof system.*

**Proof.** Given groups $G$, $H$ and elements $g$, $h$, the prover wants to convince the verifier that $g = xhy$ for some $x \in G$ and $y \in H$. Fix a sufficiently small $\epsilon > 0$. The protocol is as follows:

**(V0)** The verifier computes $\epsilon$-uniform Erdős-Rényi generators $g_1, \ldots, g_m$ and $h_1, \ldots, h_n$ for $G$ and $H$. The verifier sends the generators to the prover.
**(P1)** The prover selects random elements $x \in G$ and $y \in H$ and computes $z = xgy$. He then sends $z$ to the verifier .
**(V1)** The verifier chooses at random $\alpha \in_R \{0, 1\}$, and sends $\alpha$ to the prover.
**(P2)** If $\alpha = 0$, then the prover sends $x$ and $y$ to the verifier, together with witnesses that $x \in G$ and $y \in H$. If $\alpha = 1$, then the prover sends over two other elements, denoted as $x'$ and $y'$, together with witnesses that $x' \in G$ and $y' \in H$.
**(V2)** If $\alpha = 0$, then the verifier verifies that $x$ and $y$ are indeed elements of $G$ and $H$ and $z = xgy$. If $\alpha = 1$, then the verifier verifies that $x'$ and $y'$ are indeed elements of $G$ and $H$ and $z = x'hy'$. The verifier stops and rejects if any of the verifications fails. Otherwise, he repeats steps from (P1) to (V2).

It is easily seen that the above protocol is an interactive proof system for Double Coset Membership. Note that $z$ is in the double coset $GhH$ if and only if $g$ is in the double coset $GhH$. If $g \notin GhH$, then with probability at least a half the prover will fail to convince the verifier. The verifier can complete a large number of iterations of the above steps to make the probability of a cheating prover succeeding arbitrarily low.

If $g \in GhH$, let $g = ahb$ for some $a \in G$ and $b \in H$. Then it is clear that $x' = xa$ and $y' = by$ are also random elements of $G$ and $H$, thus revealing no information to the verifier. Therefore, to simulate the output of the prover, the simulator simply chooses random elements $x \in G$ and $y \in H$ and outputs $z$ to be $xgy$ if $\alpha = 0$ and $xhy$ if $\alpha = 1$ in the step P1. Given sufficiently small $\epsilon$, the two probability distributions are easily seen to be statistically indistinguishable. □

## 6. Future Research

A key component in our proofs is to construct uniform quantum superpositions over elements of a group, which is addressed by the problem Orbit Superposition. Watrous [36] showed how to construct such superpositions over elements of a solvable group. We would like to find new ways to construct such superpositions over a larger class of non-abelian groups. Aharonov and Ta-Shma [2] used adiabatic quantum computation to construct certain quantum superpositions such as the superposition over all perfect matchings in a given bipartite graph. An interesting question is whether adiabatic quantum computation can help to construct superpositions over group elements.

Besides the decision versions, we can also define the order versions of Stabilizer and Translating Coset, where we only care about the order of the stabilizer subgroups. In fact, the procedure described in the proof of Theorem 5 is also a reduction from the order version of Stabilizer to Orbit Superposition. An interesting question is to further characterize the relationship among the decision versions, the order versions, and the original versions of Stabilizer and Translating Coset.

## Acknowledgments

We would like to thank George McNulty, Frédéric Magniez, John Watrous, Variyam Vinodchandran, Derek Robinson for many useful discussions. We thank an anonymous reviewer for many valuable comments.

## References

[1] S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. In *Proceedings of the* 22*nd IEEE Conference on Computational Complexity*, pages 115–128. IEEE, 2007.

[2] D. Aharonov and A. Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. In *Proceedings of the* 35*th ACM Symposium on the Theory of Computing*, pages 20–29, 2003.

[3] V. Arvind and N. V. Vinodchandran. Solvable black-box group problems are low for PP. *Theoretical Computer Science*, 180:17–45, 1997.

[4] L. Babai. Local expansion of vertex-transitive graphs and random generation in finite graphs. In *Proceedings of the* 23*rd ACM Symposium on the Theory of Computing*, pages 164–174, 1991.

[5] L. Babai. Bounded round interactive proofs in finite groups. *SIAM Journal on Computing*, 5(1):88–111, February 1992.

[6] L. Babai, G. Cooperman, L. Finkelstein, E. Luks, and A. Seress. Fast Monte Carlo algorithms for permutation groups. *Journal of Computer and System Sciences*, 50:296–307, 1995.

[7] L. Babai and E. Szemerédi. On the complexity of matrix group problems I. In *Proceedings of the* 25*th IEEE Symposium on Foundations of Computer Science*, pages 229–240, 1984.

[8] R. Beals and L. Babai. Las Vegas algorithms for matrix groups. In *Proceedings of the* 34*th IEEE Symposium on Foundations of Computer Science*, pages 427–436, 1993.

[9] D. Boneh and R. Lipton. Quantum crptanalysis of hidden linear functions. In *Proceedings of the* 15*th CRYPTO Conference*, pages 427–437, 1995.

[10] G. Brassard and P. Høyer. An exact quantum polynomial-time algorithm for Simon's problem. In *Proceedings of the Israeli Symposium on the Theory of Computing and Systems*, pages 12–23, 1997.

[11] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, October 2001.

[12] W. Burnside. *Theory of Groups of Finite Order*. Dover Publications, Inc, 1955.

[13] A. Childs, L. Schulman, and U. Vazirani. Quantum algorithms for hidden nonlinear structures. In *Proceedings of the* 48*th IEEE Symposium on Foundations of Computer Science*, pages 395–404. IEEE, 2007.

[14] A. Childs and W. van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1):1–52, 2010.

[15] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society London A*, 400:97–117, 1985.

[16] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In *Proceedings of the* 16*th Symposium on Theoretical Aspects of Computer Science*, pages 478–487, 1999.

[17] M. Ettinger, P. Høyer, and E. Knill. Hidden subgroup states are almost orthogonal, 1999. Manuscript.

[18] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[19] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and translating coset in quantum computing. *SIAM Journal on Computing*, 43(1):1–24, 2014.

[20] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(1):691–729, July 1991.

[21] O. Goldreich, A. Sahai, and S. Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proceedings of the* 30*th ACM Symposium on the Theory of Computing*, pages 399–408, 1998.

[22] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In *Proceedings of the* 33*rd ACM Symposium on the Theory of Computing*, pages 68–74, 2001.

[23] S. Hallgren, A. Russell, and A. Ta-shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the* 32*nd ACM Symposium on the Theory of Computing*, pages 627–635, 2000.

[24] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. *International Journal of Foundations of Computer Science*, 14(5):723–739, 2003.

[25] R. Jozsa. Quantum factoring, discrete algorithm and the hidden subgroup problem. *Computing in Science & Engineering*, 3:34, 2001.

[26] K. Kedlaya. Quantum computation of zeta functions of curves. *Computational Complexity*, 15:1–19, 2006.

[27] A. Yu. Kitaev. Quantum measurements and the Abelian Stabilizer problem, 1995. quant-ph/9511026.

[28] F. Magniez and A. Nayak. Quantum complexity for testing group commutativity. *Algorithmica*, 48:221–232, 2007.

[29] M. Mosca. *Quantum Computer Algorithms*. PhD thesis, University of Oxford, 1999.

[30] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[31] M. Rötteler and T. Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups, 1998. Manuscript.

[32] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.

[33] D. R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

[34] S. Vadhan. *A study of statistical zero knowledge proofs*. PhD thesis, M.I.T., 1999.

[35] J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings of the* 41*st IEEE Symposium on Foundations of Computer Science*, 2000.

[36] J. Watrous. Quantum algorithms for solvable groups. In *Proceedings of the* 33*rd ACM Symposium on the Theory of Computing*, pages 60–67, 2001.