Quantum Algorithms for a Set of Group Theoretic Problems*

Stephen A. Fenner and Yong Zhang

University of South Carolina Columbia,
SC 29208, USA
{fenner, zhang29}@cse.sc.edu

Abstract. This work introduces two decision problems, STABILIZER$_D$ and ORBIT COSET$_D$, and gives quantum reductions from them to the problem ORBIT SUPERPOSITION (Friedl et al., 2003), 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. Finally, it is shown that GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP are in the complexity class **SZK**.

1 Introduction

This paper makes progress in finding connections between quantum computation and computational group theory. We give results about quantum algorithms and reductions for group theoretic problems, concentrating mostly on solvable groups.

Many problems that have quantum algorithms exponentially faster than the best known classical algorithms turn out to be special cases of the HIDDEN SUBGROUP problem for abelian groups, which can be solved using the Quantum Fourier Transform [1,2]. The non-abelian HIDDEN SUBGROUP problem remains a very interesting open problem since it has as its special case the GRAPH ISOMORPHISM problem. Recently Friedl et al. [3] made progress on the non-abelian case by introducing STABILIZER and ORBIT COSET, both of which generalize HIDDEN SUBGROUP, and showing 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 relationship among STABILIZER, ORBIT COSET, and

* This work was supported in part by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) contract number DAAD 190210048.

M. Coppo et al. (Eds.): ICTCS 2005, LNCS 3701, pp. 215–227, 2005.

Orbit Superposition. We introduce two problems Stabilizer_D and Orbit Coset_D, which are the decision versions of Stabilizer and Orbit Coset. We show that in bounded error quantum polynomial time Stabilizer_D reduces to Orbit Superposition over solvable groups and Orbit Coset_D reduces to Orbit Superposition over any finite groups.

These reductions to Orbit Superposition suggest that the difficulty in Stabilizer_D and Orbit 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 [4,5]. What makes orbit superpositions interesting in our case, however, is their unexpected utility for solving a variety of different problems that may at first seem unrelated, including not only Stabilizer_D and Orbit Coset_D but also Group Intersection and Double Coset Membership, described below.[1]

Our results on Stabilizer_D and Orbit 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 [6] first used quantum computers to help solve problems in computational group theory. He constructed efficient quantum algorithms for several problems on solvable groups, such as Order Verification and Group Membership. Based on an algorithm of Beals and Babai [7], Ivanyos, Magniez, and Santha [8] obtained efficient quantum algorithms for Order Verification as well as several other group theoretic problems. Watrous asked in [6] whether there are efficient quantum algorithms for problems such as Group Intersection and Coset Intersection. Here 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 Orbit 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 [9] 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**. Arvind and Vinodchandran first proved this result [10].

Finally, motivated by a similar result in Aharonov and Ta-Shma [5], 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 [11] that Group Intersection and Double Coset

[1] Watrous's order-finding algorithm for solvable groups [6] also works by explicitly constructing a certain orbit superposition.

MEMBERSHIP are in **AM** ∩ co**AM**. While Watrous [12] showed that GROUP NONMEMBERSHIP is in the complexity class **QMA**, another implication of our results is that GROUP NONMEMBERSHIP is in **SZK**.

Our results and other known reducibility relationships between these and other various group theoretic problems are summarized in Figure 1.

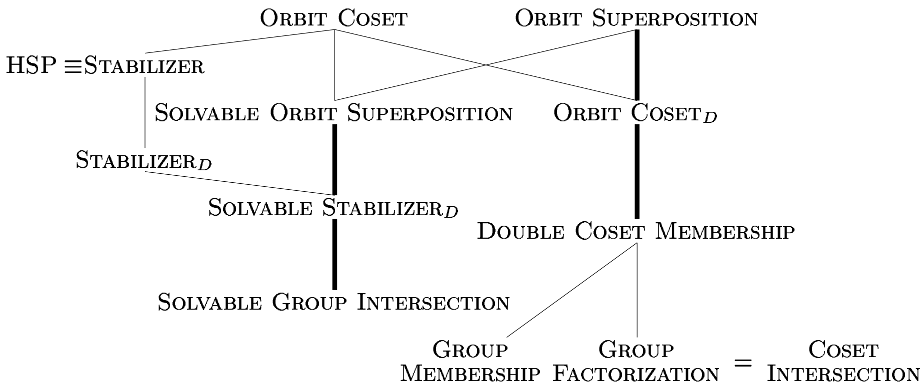

Fig. 1. Known reducibilities between various group theoretic problems. Thick lines represent nontrivial reducibilities shown in the current work.

2 Preliminaries

Background on general group theory and quantum computation can be found in the standard textbooks [13,14].

2.1 The Black-Box Group Model

All of the group theoretic problems discussed in this paper will be studied in the model of black-box groups. This model was first introduced by Babai and Szemerédi [15] as a general framework for studying algorithmic problems for finite groups. It has been extensively studied (see [6]). Here we will use descriptions similar to those in [10].

We 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 polynomials p and q 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). The order of B_m is computable in time bounded by $q(m)$, for each m. 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 [15]. 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, please see [6].

Definition 1 ([10]). *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 [16].

The term *smoothly solvable* is first introduced in [3]. 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 [6] obtained as a byproduct a method to construct approximately uniform quantum superpositions over elements of a given solvable group.

Theorem 1 ([6]). *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 ϵ 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 ρ that approximates the state $|G\rangle = |G|^{-1/2} \sum_{g \in G} |g\rangle$ with accuracy ϵ (in the trace norm metric).*

2.3 A Note on Quantum Reductions

In Sections 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 ORBIT COSET$_D$

Friedl et al. [3] introduced several problems which are closely related to HIDDEN SUBGROUP. In particular, they introduced STABILIZER, HIDDEN TRANSLATION, ORBIT 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. ORBIT COSET generalizes STABILIZER and HIDDEN TRANSLATION. ORBIT SUPERPOSITION is a relevant problem, which is also of independent interest. The superpositions Watrous constructed in Theorem 1 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 ORBIT COSET, denoted as STABILIZER$_D$ and ORBIT COSET$_D$. The original definitions of STABILIZER and ORBIT COSET concerns 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 Γ be a set of mutually orthogonal quantum states. Let $\alpha : G \times \Gamma \rightarrow \Gamma$ be a group action of G on Γ, i.e., for every $x \in G$ the function $\alpha_x : |\phi\rangle \to |\alpha(x, |\phi\rangle)\rangle$ is a permutation over Γ and the map h from G to the symmetric group over Γ 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 α 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 α^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 α^t because the input superpositions cannot be cloned in general.

Definition 2. *Let G be a finite group and Γ 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 $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$,* ORBIT 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*

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

Next we show that the difficulty of STABILIZER$_D$ and ORBIT 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 7 in Ivanyos, Magniez, and Santha [8]:

Theorem 2 ([8]). *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 the function f. Then the order of the factor group G/N can be computed by quantum algorithms in time polynomial in n, where n is the input size.*

Please note that we can apply Theorem 2 to factor groups since it uses the non-unique encoding black-box groups model.

Theorem 3. *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 [16], namely, $\{e\} = G_1 \triangleleft \cdots \triangleleft G_n = G$. For $1 \le i \le n$ let $S_i = (G_i)_{|\phi\rangle}$, the stabilizer of $|\phi\rangle$ in G_i. By Theorem 1 we can compute the orders of $G_1, \ldots, G_n$ and thus the order of G_{i+1}/G_i for any $1 \le i < n$. 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, $G_iS_{i+1}/G_i \cong S_{i+1}$. Consider the factor group G_{i+1}/G_i, we will define a function f such that f is constant on G_iS_{i+1}/G_i and distinct on left cosets of G_iS_{i+1}/G_i in G_{i+1}/G_i. Then by Theorem 2 we can compute the order of the factor group G_{i+1}/G_i over G_iS_{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 Γ be the set $\{|gG_i \cdot \phi\rangle | g \in G_{i+1}\}$. We define $f : G_{i+1}/G_i \to \Gamma$ be such that $f(gG_i) = |gG_i \cdot \phi\rangle$. What is left is to verify that f hides the subgroup G_iS_{i+1}/G_i in the group G_{i+1}/G_i. For any $g \in G_iS_{i+1}$, 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_iS_{i+1}, then $g_1 = g_2g$ for some $g \in G_iS_{i+1}$ and thus $|g_1G_i \cdot \phi\rangle = |g_2G_i \cdot \phi\rangle$. If g_1 and g_2 are not in the same left coset of G_iS_{i+1}, we will show that $|g_1G_i\phi\rangle$ and $|g_2G_i\phi\rangle$ are orthogonal quantum states. Suppose there exists $x_1, x_2 \in G_i$ such that $|g_1x_1 \cdot \phi\rangle = |g_2x_2 \cdot \phi\rangle$, then $x_1^{-1}g_1^{-1}g_2x_2 \in S_{i+1}$. But $x_1^{-1}g_1^{-1}g_2x_2 = x_1^{-1}x_2'g_1^{-1}g_2$ for some $x_2' \in G_i$. Thus $g_1^{-1}g_2 \in G_iS_{i+1}$. This contradicts the assumption that g_1 and g_2 are not in the same coset of G_iS_{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 ϵ. So the total running time is still polynomial in the input size.

We can also easily reduce Orbit Coset$_D$ to Orbit Superposition in quantum polynomial time. In this reduction, we don't require the underlying groups to be solvable. The proof uses similar techniques that Watrous [12] and Buhrman et al. [4] used to differentiate two quantum states.

Theorem 4. Orbit 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 Orbit Coset$_D$. Notice 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. [4].

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. [3].

Theorem 5 ([3]). *Let G be a finite solvable group having a smoothly solvable commutator subgroup. Let α be a group action of G.* STABILIZER$_D$ *can be solved in G for α^t in quantum time poly*$(\log|G|)\log(1/\epsilon)$ *with error ϵ when $t = (\log^{\Omega(1)}|G|)\log(1/\epsilon)$,*

Theorem 6 ([3]). *Let G be a smoothly solvable group and let α be a group action of G. When $t = (\log^{\Omega(1)}|G|)\log(1/\epsilon)$,* ORBIT COSET$_D$ *can be solved in G for α^t in quantum time poly*$(\log|G|)\log(1/\epsilon)$ *with error ϵ.*

First we show that with the help of certain uniform quantum superpositions over group elements, GROUP INTERSECTION can be reduced to STABILIZER$_D$.

Theorem 7. 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 1 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 Γ 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 1. GROUP INTERSECTION *over solvable groups can be solved within error ϵ 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 Theorems 7 and 5.

We observe that a similar reduction to STABILIZER$_D$ holds for MULTIPLE GROUP INTERSECTION.

Proposition 1. MULTIPLE GROUP INTERSECTION *reduces to* STABILIZER$_D$ *in bounded-error quantum polynomial time if all but one of the underlying groups are solvable.*

Proof. Without loss of generality, we illustrate the proof for the case $k = 3$. Suppose we have three input groups G, H, and K, where H and K are solvable. We let Γ 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 ORBIT COSET$_D$.

Theorem 8. Double Coset Membership *over solvable groups reduces to* Orbit 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 Orbit 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 1. It is not hard to check that $G(|\phi_0\rangle) = G(|\phi_1\rangle)$ if and only if $g \in GhH$.

Corollary 2. Double Coset Membership *over solvable groups can be solved within error* ϵ *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 Orbit Coset_D, the result follows from Theorem 6. 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

A recent paper by Aharonov and Ta-Shma [5] 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 3 and Theorem 4, we would like to ask if there are connections between **SZK** and the two group-theoretic problems discussed in section 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 [11] 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** [17].

For standard notions of interactive proof systems and zero knowledge interactive proof systems, see Vadhan's Ph.D. thesis [18]. 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 [19]. Some complexity results concerning **SZK** (**HVSZK**) include that **BPP** $\subseteq$ **SZK** $\subseteq$ **AM** $\cap$ co**AM**, and **SZK** is closed under complement, and **SZK** does not contain any **NP**-complete language unless the polynomial hierarchy collapses (see [18]).

The following theorem due to Babai [20] 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 ϵ-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.

Theorem 9 ([20]). *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 $O(\log N)$ ϵ-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 ϵ-uniform distributed random elements of G at a cost of $O(\log N)$ group operations per random element.*

Basically what Theorem 9 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 $O(\log N)$ ϵ-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 10. Group Intersection *has an honest-verifier perfect 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 $\{e\}$. The protocol is as follows.

- **(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 the verifier has completed m iterations of the above steps, then he accepts.

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. For a honest verifier V, clearly this protocol is perfect 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 11. Double Coset Membership *has a honest-prover statistical zero knowledge proof system.*

Proof (sketch). 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 ϵ-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 α 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).

If the verifier has completed m iterations of the above steps, then he accepts.

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. 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 ϵ, the two probability distribution 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 [6] 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 [5] 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 ORBIT COSET, where we only care about the order of the stabilizer subgroups. In fact, the procedure described in the proof of Theorem 3 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 ORBIT COSET.

Acknowledgments

We would like to thank George McNulty, Frédéric Magniez, John Watrous, Variyam Vinodchandran, Derek Robinson, Scott Aaronson, and Dorit Aharonov for many useful discussions.

References

1. Mosca, M.: Quantum Computer Algorithms. PhD thesis, University of Oxford (1999)
2. Jozsa, R.: Quantum factoring, discrete algorithm and the hidden subgroup problem (2000) Manuscript.
3. Friedl, K., Ivanyos, G., Magniez, F., Santha, M., Sen, P.: Hidden translation and orbit coset in quantum computing. In: Proceedings of the 35th ACM Symposium on the Theory of Computing. (2003) 1–9
4. Buhrman, H., Cleve, R., Watrous, J., de Wolf, R.: Quantum fingerprinting. Physical Review Letters **87** (2001) 167902
5. Aharonov, D., Ta-Shma, A.: Adiabatic quantum state generation and statistical zero knowledge. In: Proceedings of the 35th ACM Symposium on the Theory of Computing. (2003) 20–29
6. Watrous, J.: Quantum algorithms for solvable groups. In: Proceedings of the 33rd ACM Symposium on the Theory of Computing. (2001) 60–67
7. Beals, R., Babai, L.: Las Vegas algorithms for matrix groups. In: Proceedings of the 34th IEEE Symposium on Foundations of Computer Science. (1993) 427–436
8. Ivanyos, G., Magniez, F., Santha, M.: Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. In: Proceedings of 13th ACM Symposium on Parallelism in Algorithms and Architectures. (2001) 263–270
9. Fortnow, L., Rogers, J.: Complexity limitations on quantum computation. Journal of Computer and System Sciences **59** (1999) 240–252
10. Arvind, V., Vinodchandran, N.V.: Solvable black-box group problems are low for PP. Theoretical Computer Science **180** (1997) 17–45
11. Babai, L.: Bounded round interactive proofs in finite groups. SIAM Journal on Computing **5** (1992) 88–111
12. Watrous, J.: Succinct quantum proofs for properties of finite groups. In: Proceedings of the 41st IEEE Symposium on Foundations of Computer Science. (2000)
13. Burnside, W.: Theory of Groups of Finite Order. Dover Publications, Inc (1955)

14. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
15. Babai, L., Szemerédi, E.: On the complexity of matrix group problems I. In: Proceedings of the 25th IEEE Symposium on Foundations of Computer Science. (1984) 229–240
16. Babai, L., Cooperman, G., Finkelstein, L., Luks, E., Seress, A.: Fast Monte Carlo algorithms for permutation groups. Journal of Computer and System Sciences **50** (1995) 296–307
17. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. Journal of the ACM **38** (1991) 691–729
18. Vadhan, S.: A study of statistical zero knowledge proofs. PhD thesis, M.I.T. (1999)
19. Goldreich, O., Sahai, A., Vadhan, S.: Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In: Proceedings of the 30th ACM Symposium on the Theory of Computing. (1998) 399–408
20. Babai, L.: Local expansion of vertex-transitive graphs and random generation in finite graphs. In: Proceedings of the 23rd ACM Symposium on the Theory of Computing. (1991) 164–174