Quantum Algorithms for a set of Group Theoretic Problems

Stephen A. Fenner[*]
University of South Carolina

Yong Zhang[*]
University of South Carolina

October 8, 2018

Abstract

We study two group theoretic problems, GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP, in the setting of black-box groups, where DOUBLE COSET MEMBERSHIP generalizes a set of problems, including GROUP MEMBERSHIP, GROUP FACTORIZATION, and COSET INTERSECTION. No polynomial-time classical algorithms are known for these problems. We show that for solvable groups, there exist 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 study the decision versions of STABILIZER and ORBIT COSET, which generalizes GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP, respectively. We show that they reduce to ORBIT SUPERPOSITION under certain conditions. Finally, we show that DOUBLE COSET MEMBERSHIP and DOUBLE COSET NONMEMBERSHIP have zero knowledge proof systems.

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. These results come in three sections. First, we concentrate on two particular group theoretic problems, GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP, showing that these problems reduce to other group problems with known efficient quantum algorithms for many instances, yielding
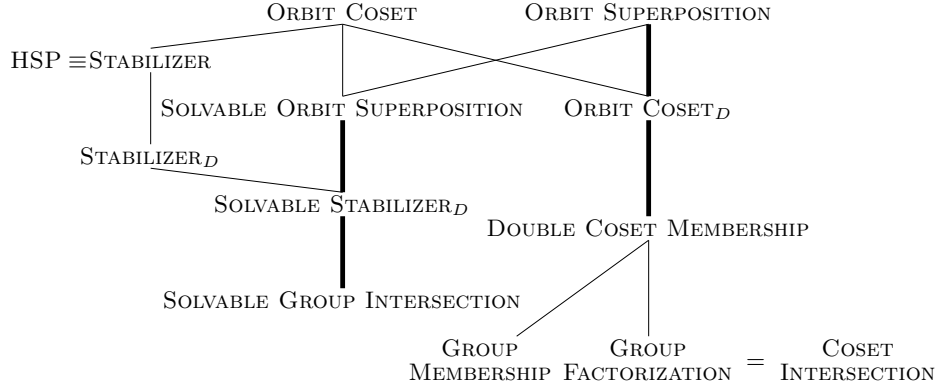
Figure 1: Known reducibilities between various group theoretic problems. Thick lines represent nontrivial reducibilities shown in the current work.

efficient quantum algorithms for GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP on the same types of groups. Second, we generalize and refine our results in the first section by introducing decision versions of the STABILIZER and ORBIT COSET problems (see [FIM+03]), and showing that these new problems lie in between GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP on the one hand, and the problem ORBIT SUPERPOSITION, defined in [FIM+03], on the other. Third, we relate our results on DOUBLE COSET MEMBERSHIP to recent work of Aharonov & Ta-Shma [ATS03] by showing that DOUBLE COSET MEMBERSHIP and its complement have perfect zero knowledge proofs. Our results and other known reducibility relationships between these and other various group theoretic problems are summarized in Figure 1. A common theme running through all three sections is the surprising usefulness of producing certain uniform quantum superpositions.

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 (HSP) for abelian groups, which can be solved using the Quantum Fourier Transform [Mos99, Joz00]. Other interesting problems, such as GRAPH ISOMORPHISM are special cases of general HIDDEN SUBGROUP, for which no efficient quantum algorithm is currently known. The idea that underlying algebraic structures may be essential for problems having exponential quantum speedup has prompted several researchers to study problems in computational group theory. Watrous [Wat01] first 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 [BB93], Ivanyos, Magniez, and Santha [IMS01] obtained efficient quantum algorithms for ORDER VERIFICATION as well as several other group theoretic problems. Recently, Friedl et al.[FIM+03] introduced the problems STABILIZER, ORBIT COSET, and ORBIT SUPERPOSITION, and showed that these problems can be solved efficiently on quantum computers if the underlying groups satisfy certain stronger solvability criteria.

Watrous asked in [Wat01] whether there are efficient quantum algorithms for problems

such as GROUP INTERSECTION and COSET INTERSECTION. We show that for solvable groups, there are efficient quantum algorithms for GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP (which generalizes COSET INTERSECTION as well as GROUP MEMBERSHIP and GROUP FACTORIZATION) under certain conditions. We obtain these results by showing that these two problems reduce to STABILIZER and ORBIT COSET, respectively.

One key component in our proof is the construction of approximately uniform quantum superpositions over elements of a given solvable group, which is a very useful byproduct of [Wat01]. In classical computational group theory, the ability to sample group elements uniformly at random is very useful in designing many classical group algorithms. We believe that its quantum analog—uniform quantum superpositions over group elements—will continue to be useful in designing quantum group algorithms. Our results also imply that for *abelian* groups, GROUP INTERSECTION and DOUBLE COSET MEMBERSHIP are in the complexity class **BQP**, which yields a new proof that they are low for the class **PP** [AV97, FR99].

We observe that in the reduction from GROUP INTERSECTION (respectively DOUBLE COSET MEMBERSHIP) to STABILIZER (respectively ORBIT COSET), we don't actually need the full power of STABILIZER or ORBIT COSET. This inspires us to study simplified versions of these two problems. Here we use STABILIZER$_D$ and ORBIT COSET$_D$ to denote the decision versions of these two problems, where we are only interested in a trivial/non-trivial answer. 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. In particular, we show that for solvable groups, STABILIZER$_D$ reduces to ORBIT SUPERPOSITION, and for any finite groups, ORBIT COSET$_D$ reduces to ORBIT SUPERPOSITION in bounded-error quantum polynomial time. This again reinforces our idea that certain uniform quantum superpositions are key components in quantum group algorithms.

A recent paper by Aharonov and Ta-Shma [ATS03] shares a similar point of view. They studied the problem CIRCUIT QUANTUM SAMPLING (CQS), which basically concerns generating quantum states corresponding to classical probability distributions. Furthermore, they showed interesting connections between CQS and many different areas such as Statistical Zero Knowledge (**SZK**) and adiabatic evolution. In particular, they showed that any language in **SZK** can be reduced to a family of instances of CQS. Inspired by this, we obtain connections between our group theoretic problems and the complexity class **SZK**. We show that DOUBLE COSET MEMBERSHIP has a zero knowledge proof system, therefore it is in **SZK**. This is an improvement of Babai's result [Bab92] that DOUBLE COSET MEMBERSHIP is in **AM** $\cap$ co**AM**. We also give an explicit zero knowledge proof system for the complement of DOUBLE COSET MEMBERSHIP, namely, DOUBLE COSET NONMEMBERSHIP. While Watrous [Wat00] showed that GROUP NONMEMBERSHIP is in the complexity class **QMA**, another implication of our results is that GROUP NONMEMBERSHIP has a zero knowledge interactive proof system.

2 Preliminaries

Background on general group theory and quantum computation can be found in the standard textbooks [Bur55, NC00].

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 [BS84] as a general framework for studying algorithmic problems for finite groups. It has been extensively studied (see [Wat01]). Here we will use descriptions similar to those in [AV97].

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 [BS84]. 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 [Wat01].

Definition 2.1 ([AV97]) *Let $\mathcal{B} = \{B_m\}_{m \geq 1}$ be a group family. Let e denote the identity element of each B_m. 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.*

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

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 $G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(n)} = \{e\}$ 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 [BCF+95].

　　The term *smoothly solvable* is first introduced in [FIM+03]. 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 whose exponent is bounded by a constant 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 [Wat01] obtained as a byproduct a method to construct approximately uniform quantum superpositions over elements of a given solvable group.

Theorem 2.2 ([Wat01]) *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　Stabilizer, Orbit Coset **and** Orbit Superposition

A recent paper by Friedl et al. [FIM+03] 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 2.2 can be considered as an instance of ORBIT SUPERPOSITION.

　　In the following we will state the problems and results that will be used in this paper. We refer interested readers to their paper [FIM+03] for detailed information.

Let G be a finite group. Let Γ be a set of mutually orthogonal quantum states. Let $\alpha : G \times \Gamma \to \Gamma$ 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 2.3 ([FIM$^+$03]) *Let G be a finite group and Γ be a set of mutually orthogonal quantum states. Fix the group action $\alpha : G \times \Gamma \to \Gamma$.*

- *Given generators for G and a quantum states $|\phi\rangle \in \Gamma$, the problem* STABILIZER *is to find a generating set for the subgroup $G_{|\phi\rangle}$.*

- *Given generators for G and two quantum states $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$, the problem* ORBIT COSET *is to either reject the input if $G(|\phi_0\rangle) \cap G(|\phi_1\rangle) = \emptyset$ or output a generating set for $G_{|\phi_1\rangle}$ of size $O(\log |G|)$ and a $u \in G$ such that $|u \cdot \phi_1\rangle = |\phi_0\rangle$.*

- *Given generators for G and a quantum state $|\phi\rangle \in \Gamma$, the problem* ORBIT SUPERPOSITION *is to construct the uniform superposition*

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

ORBIT COSET and STABILIZER can be solved in quantum polynomial time under certain stronger solvability criteria.

Theorem 2.4 ([FIM$^+$03]) *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 *can be solved in G for α^t in quantum time $poly(\log |G|) \log(1/\epsilon)$ with error ϵ.*

Theorem 2.5 ([FIM$^+$03]) *Let G be a finite solvable group having a smoothly solvable commutator subgroup and let α be a group action of G. When $t = (\log^{\Omega(1)} |G|) \log(1/\epsilon)$,* STABILIZER *can solved in G for α^t in quantum time $poly(\log |G|) \log(1/\epsilon)$ with error ϵ.*

Another interesting result in [FIM$^+$03] is that ORBIT SUPERPOSITION reduces to ORBIT COSET for solvable groups in quantum polynomial time. It is not clear if there is a reduction in the reverse direction.

2.4 Zero Knowledge Proof Systems

We use standard notions of interactive proof systems and zero knowledge interactive proof systems. Information about zero knowledge systems can be found in a variety of places, including Vadhan's Ph.D. thesis [Vad99], and Goldreich, Micali, & Wigderson [GMW91].

SZK is the class of languages that have statistical zero knowledge proofs. It is known that **BPP** $\subseteq$ **SZK** $\subseteq$ **AM** $\cap$ co**AM** and that **SZK** is closed under complement. **SZK** does not contain any **NP**-complete language unless the polynomial hierarchy collapses [Vad99].

2.5 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 Quantum algorithms

In this section we report progress on finding quantum algorithms for GROUP INTERSECTION, and DOUBLE COSET MEMBERSHIP.

Theorem 3.1 GROUP INTERSECTION *reduces to* STABILIZER *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 2.2 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 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 $|H\rangle$. $\square$

Corollary 3.2 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 3.1 and 2.5. $\square$

It is not clear if similar reduction to STABILIZER exists for DOUBLE COSET MEMBERSHIP. However, with the help of certain uniform superpositions, DOUBLE COSET MEMBERSHIP can be nicely put into the framework of ORBIT COSET.

Theorem 3.3 DOUBLE COSET MEMBERSHIP *over solvable groups reduces to* ORBIT COSET *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, first we check if g is an element of G or H. This can be done using the quantum algorithm for GROUP MEMBERSHIP in [Wat01]. For example, to check if g is an element of G, the algorithm will check if the group $\langle S_1, g \rangle$ is still solvable, and in the case that it is solvable compute the order of $\langle S_1, g \rangle$ and check if it is equal to the order of G. If g is an element of G or H, quit and output "yes."

In the case that g is not an element of G or H, we construct the input for ORBIT COSET 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 2.2. It is not hard to check that there exists an $u \in G$ such that $|u \cdot \phi_1\rangle = |\phi_0\rangle$ if and only if $g \in GhH$. $\qquad\square$

Corollary 3.4 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, the result follows from Theorem 2.4. 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. $\qquad\square$

4   The decision versions of STABILIZER and ORBIT COSET

An interesting observation is that to solve our group theoretic problems, we don't actually need the full power of STABILIZER and ORBIT COSET. For example, for the problem GROUP INTERSECTION, we care about whether the intersection of the two input groups is trivial or non-trivial. We don't ask for a generating set in the case of a non-trivial intersection. This inspires us to define and study the decision versions of STABILIZER and ORBIT COSET. denoted as STABILIZER$_D$ and ORBIT COSET$_D$, respectively.

Definition 4.1 *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 $|\phi\rangle \in \Gamma$, the problem STABILIZER$_D$ is to check if the subgroup $G_{|\phi\rangle}$ is the trivial subgroup $\{e\}$.*

- *Given generators for G and two quantum states $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$, the problem 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 $G(|\phi_0\rangle) = G(|\phi_1\rangle)$.*

It is clear that the reductions in Theorem 3.1 and Theorem 3.3 still work if we replace STABILIZER (respectively ORBIT COSET) with STABILIZER$_D$ (respectively ORBIT COSET$_D$). We remark that although ORBIT COSET generalizes STABILIZER, ORBIT COSET$_D$ does not seem to generalize STABILIZER$_D$. Next we show that the ability of constructing certain quantum superpositions will help us to attack these two problems. The problem ORBIT SUPERPOSITION provides a way to construct quantum superpositions. In fact, Watrous' result in Theorem 2.2 solves a special case of ORBIT SUPERPOSITION, where the group G acts on the quantum state of the identity element.

We will use the following result from [IMS01]:

Theorem 4.2 ([IMS01]) *Assume that G is a 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 $n + \nu(G/N)$, where n is the input size and the parameter $\nu(G)$ is defined in [BB93] and equals one for any solvable group G.*

Please note that we can apply Theorem 4.2 to factor groups since it uses the non-unique encoding black-box groups model.

Theorem 4.3 *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 of STABILIZER$_D$. We can find in classical polynomial time generators for each element in the derived series of G [BCF$^+$95], 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 2.2 we can compute 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 will 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 4.2 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 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 $G_i S_{i+1}/G_i$ 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

9

$x_1^{-1}g_1^{-1}g_2x_2 \in S_{i+1}$. 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. □

Corollary 4.4 *Over solvable groups,* GROUP INTERSECTION *reduces to* ORBIT SUPERPOSITION *in bounded-error quantum polynomial time.*

We can also 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 [Wat00] and Buhrman et al. [BCWdW01] used to differentiate two quantum states.

Theorem 4.5 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 OR-BIT 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. [BCWdW01].

□

Corollary 4.6 DOUBLE COSET MEMBERSHIP *reduces to* ORBIT SUPERPOSITION *in bounded-error quantum polynomial time.*

5 Statistical Zero Knowledge

A recent paper by Aharonov and Ta-Shma [ATS03] 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 4.3 and Theorem 4.5, We would like to ask if there are connections between **SZK** and our group theoretic problems. As a first step, we show that DOUBLE COSET MEMBERSHIP has a perfect zero knowledge proof system, and thus is in **SZK**. This is an improvement of Babai's result [Bab92] that DOUBLE COSET MEMBERSHIP

is in $\mathbf{AM} \cap \mathrm{co}\mathbf{AM}$. Our proof shares the same flavor with Goldreich, Micali and Wigderson's proof that GRAPH ISOMORPHISM is in $\mathbf{SZK}$ [GMW91]. The intuitive idea is to break the process into two parts, where the verification of each individual part does not reveal any information about the claim.

The following theorem due to Babai [Bab91] 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 $(2^k/|G|)(1 + \epsilon)$ ways as a subproduct of the h_i.

Theorem 5.1 ([Bab91]) *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 5.1 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 5.2 DOUBLE COSET MEMBERSHIP *has a perfect 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 provers select x and y, which are random elements from G and H. The prover sends $z = xgy$ 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 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 not hard to verify that this is a perfect zero knowledge proof system. We omit the formal proof due to lack of space.   □

Since **SZK** is closed under complement, the complement of DOUBLE COSET MEMBERSHIP, DOUBLE COSET NONMEMBERSHIP, is also in **SZK**. In fact, by adapting proofs in [GMW91], we can give explicitly a perfect zero knowledge proof system for DOUBLE COSET NONMEMBERSHIP.

Theorem 5.3 DOUBLE COSET NONMEMBERSHIP *has a perfect zero knowledge proof system.*

Proof.[sketch] A simple interactive proof system for DOUBLE COSET NONMEMBERSHIP is as follows. Given G, H and g, h as inputs, the prover wants to convince the verifier that g is not in the double coset GhH. The verifier will generate random elements $x \in G$ and $y \in H$, and then flip a random coin and send either xgy or xhy to the prover. The prover has to tell correctly which one the verifier sends. After several rounds, the verifier is convinced. This protocol is not zero knowledge since a cheating verifier can use the protocol to gain knowledge such as whether an element z is in the double coset GgH. The way to fix this flaw is to let the verifier first "prove" to the prover that he knows the answer of his own question.

For the sake of simplicity, let n denote the input size. Given groups G, H and elements g, h, the prover wants to convince the verifier that g is not in the double coset GhH. Before the protocol starts, the verifier will compute ϵ-uniform Erdős-Rényi generators $g_1, \ldots, g_m$ and $h_1, \ldots, h_n$ for G and H for a sufficiently small ϵ, and send them to the prover.

The following protocol will be executed m times, each time using independent random coin tosses.

(V1) The verifier computes random elements $x \in G$ and $y \in H$ using the Erdős-Rényi generators, and chooses at random $\alpha \in_R \{0, 1\}$. If $\alpha = 0$, he computes $z = xgy$. If $\alpha = 1$, he computes $z = xhy$. The element z will be called the *question*. In addition to z, the verifier constructs n^2 pairs of group elements such that each pair consists of one random element of GgH and one random element of GhH. The two elements in each pair are placed at random order. These pairs will be used by the prover to test whether the verifier is cheating. In specific, for each $1 \leq i \leq n^2$, the verifier constructs the i'th pair $(T_{i,0}, T_{i,1})$ as follows. He computes random elements $x_{i,0}, x_{i,1} \in G$ and $y_{i,0}, y_{i,1} \in H$, and chooses at random a bit $\gamma_i \in_R \{0, 1\}$. Then he computes $T_{i,\gamma_i} = x_{i,\gamma_i} g y_{i,\gamma_i}$ and $T_{i,1-\gamma_i} = x_{i,1-\gamma_i} g y_{i,1-\gamma_i}$. The verifier sends z and the sequence of pairs $(T_{1,0}, T_{1,1}), \ldots, (T_{n^2,0}, T_{n^2,1})$ to the prover.

(P1) The prover chooses at random a subset $I \subseteq \{1, \ldots, n^2\}$ (uniformly among all 2^{n^2} subsets) and sends I to the verifier.

(V2) If I is not a subset of $\{1, \ldots, n^2\}$, then the verifier halts and rejects. Otherwise, the verifier replies with $\{(\gamma_i, x_{i,0}, x_{i,1}, y_{i,0}, y_{i,1}) : i \in I\}$ and $\{(\alpha_i \in \{0,1\}, a_i \in G, b_i \in H) \text{ such that } z = a_i T_{i,\alpha_i} b_i : i \notin I\}$. Intuitively, for $i \in I$ the verifier shows that the i'th pair is properly constructed by giving explicitly $(\gamma_i, x_{i,0}, x_{i,1}, y_{i,0}, y_{i,1})$; for $i \notin I\}$ the verifier shows that z is also properly constructed by showing that z is in the same double coset with one of the elements in the i'th pair. (α_i, a_i, b_i) can be easily computed by the verifier, i.e., $\alpha_i = (\alpha + \gamma_i) \mod 2$, $a_i = x x_{i,\alpha_i}^{-1}$, and $b_i = y_{i,\alpha_i}^{-1} y$.

(P2) For every $i \in I$, the prover checks whether $x_{i,0}, x_{i,1}$ (respectively $y_{i,0}, y_{i,1}$)) are indeed elements of G (respectively H), and whether $T_{i,\gamma_i} = x_{i,\gamma_i} g y_{i,\gamma_i}$ and $T_{i,1-\gamma_i} = x_{i,1-\gamma_i} g y_{i,1-\gamma_i}$ hold. For every $i \notin I$, the prover checks whether a_i (respectively b_i) is indeed an element of G (respectively H), and whether $z = a_i T_{i,\alpha_i} b_i$ holds. If any of these conditions does not hold, the prover stops. Otherwise, the prover answers with $\beta \in \{0,1\}$.

(V3) The verifier checks whether $\alpha = \beta$. If the condition is violated, the verifier stops and rejects; otherwise, he continues.

After m rounds of successful iterations, the verifier accepts.

This is still an interactive proof system for DOUBLE COSET NONMEMBERSHIP. If g is not in the double coset GhH, then GgH and GhH are disjoint sets and the prover will always succeed in convincing the verifier. If, on the other hand, g is in the double coset GhH, then GgH and GhH are the same set and with probability at least a half the prover will fail to fool the verifier.

To prove that this protocol is zero knowledge, the simulator has to produce the same probability distribution without interacting with the prover. What the simulator does is to extract from the verifier the knowledge he has about his question. We omit the formal proof here. We note that the formal proof is similar in principle to the proof that GRAPH NONISOMORPHISM has a zero knowledge proof system [GMW91], based on which and the above protocol interested readers are able to construct the formal proof. □

Although GROUP INTERSECTION is also known to be in $\mathbf{AM} \cap \mathrm{co}\mathbf{AM}$ [Bab92], it is not clear whether GROUP INTERSECTION has a zero knowledge proof system. This seems to be consistent with the fact that we have not found a reduction from GROUP INTERSECTION to ORBIT SUPERPOSITION over arbitrary finite groups (Corollary 4.4).

References

[ATS03]   D. Aharonov and A. Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. In *Proceedings of the 35th ACM Symposium on the Theory of Computing*, pages 20–29, 2003.

[AV97]   V. Arvind and N. V. Vinodchandran. Solvable black-box group problems are low for PP. *Theoretical Computer Science*, 180:17–45, 1997.

[Bab91]   L. Babai. Local expansion of vertex-transitive graphs and random generation in finite graphs. In *Proceedings of the 23rd ACM Symposium on the Theory of Computing*, pages 164–174, 1991.

[Bab92]   L. Babai. Bounded round interactive proofs in finite groups. *SIAM Journal on Computing*, 5(1):88–111, February 1992.

[BB93]   R. Beals and L. Babai. Las Vegas algorithms for matrix groups. In *Proceedings of the 34th IEEE Symposium on Foundations of Computer Science*, pages 427–436, 1993.

[BCF$^+$95]   L. Babai, G. Cooperman, L. Finkelstein, E. Luks, and A. Seress. Fast Monte Carol algorithms for permutation groups. *Journal of Computer and System Sciences*, 50:296–307, 1995.

[BCWdW01]   H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, October 2001.

[BS84]   L. Babai and E. Szemerédi. On the complexity of matrix group problems I. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science*, pages 229–240, 1984.

[Bur55]   W. Burnside. *Theory of Groups of Finite Order*. Dover Publications, Inc, 1955.

[FIM$^+$03]   K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proceedings of the 35th ACM Symposium on the Theory of Computing*, pages 1–9, 2003.

[FR99]   L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999, cs.CC/9811023.

[GMW91]   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.

[IMS01]   G. Ivanyos, F. Magniez, and M. Santha. 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*, pages 263–270, 2001, quant-ph/0102014.

[Joz00]   R. Jozsa. Quantum factoring, discrete algorithm and the hidden subgroup problem, 2000, quant-ph/0012084. Manuscript.

[Mos99]   M. Mosca. *Quantum Computer Algorithms*. PhD thesis, University of Oxford, 1999.

[NC00]   M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Vad99]   S. Vadhan. *A study of statistical zero knowledge proofs*. PhD thesis, M.I.T., 1999.

[Wat00]   J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, 2000, cs.CC/0009002.

[Wat01]   J. Watrous. Quantum algorithms for solvable groups. In *Proceedings of the 33rd ACM Symposium on the Theory of Computing*, pages 60–67, 2001.