# Hidden Translation and Orbit Coset in Quantum Computing[*]

Katalin Friedl
SZTAKI, Hungarian
Academy of Sciences
H-1111 Budapest, Hungary
friedl@sztaki.hu

Gábor Ivanyos
SZTAKI, Hungarian
Academy of Sciences
H-1111 Budapest, Hungary
ivanyos@sztaki.hu

Frédéric Magniez
CNRS–LRI, UMR 8623
Université Paris–Sud
91405 Orsay, France
magniez@lri.fr

Miklos Santha
CNRS–LRI, UMR 8623
Université Paris–Sud
91405 Orsay, France
santha@lri.fr

Pranab Sen
LRI, UMR 8623
Université Paris–Sud
91405 Orsay, France
pranab@lri.fr

## ABSTRACT

We give efficient quantum algorithms for the problems of HIDDEN TRANSLATION and HIDDEN SUBGROUP in a large class of non-abelian groups including solvable groups of constant exponent and of constant length derived series. Our algorithms are recursive. For the base case, we solve efficiently HIDDEN TRANSLATION in $\mathbb{Z}_p^n$, whenever $p$ is a fixed prime. For the induction step, we introduce the problem ORBIT COSET generalizing both HIDDEN TRANSLATION and HIDDEN SUBGROUP, and prove a powerful self-reducibility result: ORBIT COSET in a finite group $G$ is reducible to ORBIT COSET in $G/N$ and subgroups of $N$, for any solvable normal subgroup $N$ of $G$.

## 1. INTRODUCTION

Quantum computing is an extremely active research area (for introductions see e.g. [15, 1, 18, 16]), where a growing trend is to cast quantum algorithms in a group theoretical setting. In this setting, we are given a finite group $G$ and, besides the group operations, we also have at our disposal a function $f$ mapping $G$ into a finite set. The function $f$ can be queried via an oracle. The time complexity of an algorithm is measured by the overall running time counting one query as one computational step. We say that an algorithm is *efficient* if its time complexity is polynomial in the logarithm of the order of $G$. The most important unifying problem of group theory for the purpose of quantum algorithms has turned out to be HIDDEN SUBGROUP, which can be cast in the following broad terms: Let $H$ be a subgroup of $G$ such that $f$ is constant on each left coset of $H$ and distinct on different left cosets. We say that $f$ *hides* the subgroup $H$. The task is to determine the *hidden subgroup* $H$.

While no classical algorithm can solve this problem with polynomial query complexity even if $G$ is abelian, the biggest success of quantum computing until now is that it can be solved by a quantum algorithm efficiently for abelian $G$. We will refer to this quantum algorithm as the standard algorithm for HIDDEN SUBGROUP. The main tool for this solution is Fourier sampling based on the (approximate) quantum Fourier transform for abelian groups which can be efficiently implemented quantumly [14]. Simon's xor-mask finding [21], Shor's factorization and discrete logarithm finding algorithms [20], and Kitaev's algorithm [14] for the abelian stabilizer problem are all special cases of this general solution.

Finding an efficient algorithm for HIDDEN SUBGROUP for non-abelian groups $G$ is considered to be one of the most important challenges at present in quantum computing. Besides its intrinsic mathematical interest, the importance of this problem is enhanced by the fact that it contains as a special case the graph isomorphism problem. Unfortunately, non-abelian HIDDEN SUBGROUP seems to be much more difficult than the abelian case, and although considerable efforts were spent on it in the last few years, only a small number of successes can be reported. They can be divided into two categories. The standard abelian Fourier sampling based algorithm has been extended to some non-abelian groups in [19, 12, 11] using the quantum Fourier transform over these (non-abelian) groups. Unfortunately, efficient quantum Fourier transform implementations are known only for a few non-abelian groups [5, 17, 19, 12]. In a different approach, HIDDEN SUBGROUP was efficiently solved

[*]Research partially supported by the EU 5th framework programs QAIP IST-1999-11234, RESQ IST-2001-37559, and RAND-APX IST-1999-14036, by CNRS/STIC 01N80/0502 and 01N80/0607 grants, by ACI Cryptologie CR/02 02 0040 grant of the French Research Ministry, and by OTKA T030059, T030132, and NWO-OTKA N34040 grants. Part of the work of the last three authors was done while visiting MSRI, Berkeley.

*STOC'03,* June 9–11, 2003, San Diego, California, USA.
Copyright 2003 ACM 1-58113-674-9/03/0006 ...$5.00.

in the context of specific non-abelian black-box groups [6, 23] by [13] without using the Fourier transform on the group.

In face of the apparent hardness of HIDDEN SUBGROUP in non-abelian groups, a natural line of research is to address subproblems of HIDDEN SUBGROUP which, in some groups, capture the main difficulty of the original problem. In a pioneering paper, Ettinger and Høyer [9], in the case of dihedral groups, implicitly considered another paradigmatic group problem, HIDDEN TRANSLATION. Here we are given two injective functions $f_0$ and $f_1$ from a finite group $G$ to some finite set such that, for some group element $u$, the equality $f_1(xu) = f_0(x)$ holds for every $x$. The task is to find the *translation* $u$. In fact, whenever $G$ is abelian, HIDDEN TRANSLATION is an instance of HIDDEN SUBGROUP in the semi-direct product $G \rtimes \mathbb{Z}_2$, where the hiding function is $f(x, b) = f_b(x)$. The group action in $G \rtimes \mathbb{Z}_2$ is defined as $(x_1, b_1) \cdot (x_2, b_2) = (x_1 + (-1)^{b_1} x_2, b_1 \oplus b_2)$, where $+$ denotes the group operation in $G$ and $\oplus$ denotes the group operation in $Z_2$. In $G \rtimes \mathbb{Z}_2$, $f$ hides the subgroup $H = \{(0, 0), (u, 1)\}$. Actually, there is an efficient quantum reduction in the other direction also, and the two problems are quantum polynomial time equivalent [9]. A nice consequence of this equivalence is that instead of dealing with HIDDEN SUBGROUP in the non-abelian group $G \rtimes \mathbb{Z}_2$, we can address HIDDEN TRANSLATION in the abelian group $G$. Ettinger and Høyer [9] have shown that HIDDEN TRANSLATION can be solved by a two-step procedure when $G = \mathbb{Z}_N$ is cyclic: polynomial number of Fourier samplings over the abelian group $\mathbb{Z}_N \times \mathbb{Z}_2$ followed by an exponential classical stage without further queries.

Recently, Dam, Hallgren and Ip [8] have given efficient solutions for three cases of the hidden shift problem what they put in the framework of the more general hidden coset problem. This is also a generalization of HIDDEN TRANSLATION to not necessarily injective functions. While this paper shows how to solve HIDDEN TRANSLATION in some specific groups for any (injective) functions, the hidden coset problem in general is of exponential query complexity, even in $\mathbb{Z}_2^n$.

Our first result (**Theorem 1**) is an efficient quantum algorithm for HIDDEN TRANSLATION in the case of elementary abelian $p$-groups, that is groups $\mathbb{Z}_p^n$, for any fixed prime number $p$. The quantum part of our algorithm is the same as in Ettinger and Høyer's [9] procedure: it consists of performing Fourier sampling over the abelian group $\mathbb{Z}_p^n \times \mathbb{Z}_2$. But while their classical post processing requires exponential time, here we are able to recover classically the translation in polynomial time from the sampling. It turns out that Fourier sampling produces vectors $y$ non-orthogonal to the translation $u$, that is we obtain linear inequations for the unknown $u$. This is different from the situation in the standard algorithm for the abelian HIDDEN SUBGROUP, where only vectors orthogonal to the hidden subgroup are generated. We show that, after a polynomial number of samplings, the system of linear inequations has a unique solution with high probability, which we are able to determine in deterministic polynomial time. An immediate consequence of Theorem 1 is that HIDDEN SUBGROUP is efficiently solvable by a quantum algorithm in $\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$.

In Appendix A, we show how to extend the previous approach to solve HIDDEN TRANSLATION in the groups $\mathbb{Z}_{p^k}^n$ where $p^k$ is a fixed prime power, but we do not know how to extend it to an arbitrary abelian group, even of constant exponent. To solve HIDDEN TRANSLATION over other groups (which include abelian groups of constant exponent), we embark in a radically new direction whose basic idea is *self-reducibility*. Since HIDDEN TRANSLATION is not well-suited for this self-reducibility based approach, we define a new paradigmatic group problem ORBIT COSET which is a quantum generalization of both HIDDEN TRANSLATION and HIDDEN SUBGROUP. ORBIT COSET involves quantum group actions, that is groups acting on a finite set of mutually orthogonal quantum states. Given two such states $|\phi_0\rangle$ and $|\phi_1\rangle$, the problem consists of finding their *orbit coset*, that is the stabilizer subgroup of $|\phi_1\rangle$ and a group element that maps $|\phi_1\rangle$ to $|\phi_0\rangle$.

With a slight modification, our algorithm of Theorem 1 also works for ORBIT COSET in $\mathbb{Z}_p^n$ whenever many copies of the input states are given. Moreover, we show that ORBIT COSET has the following self-reducibility property in any finite group $G$: it is reducible to ORBIT COSET in $G/N$ and subgroups of $N$, for any solvable subgroup $N \lhd G$ (**Theorem 3**). This is the first time that such a general self-reducibility result has been obtained for a problem incorporating HIDDEN SUBGROUP. The proof of the result involves a new technique which is based upon constructing the uniform superposition of the orbit of a given quantum state (ORBIT SUPERPOSITION). The importance of generating some specific superpositions, for example uniform orbit superposition, is in the center of the recent paper of Aharonov and Ta-Shma [2]. We show how ORBIT SUPERPOSITION is related to ORBIT COSET (**Theorem 2**). The self-reducibility of ORBIT COSET combined with its solvability for $\mathbb{Z}_p^n$ enables us to design an efficient quantum algorithm for ORBIT COSET in groups that we call smoothly solvable groups (**Theorem 4**). These groups include solvable groups of constant exponent and constant length derived series; in particular, unitriangular matrix groups of constant dimension over finite fields of constant characteristic. For the special case of STABILIZER (i.e. ORBIT COSET when $|\phi_1\rangle = |\phi_0\rangle$), we obtain an efficient quantum algorithm for an even larger class of solvable groups viz. for solvable groups having a smoothly solvable commutator subgroup (**Theorem 5**). As an immediate consequence, we get efficient quantum algorithms for HIDDEN TRANSLATION and HIDDEN SUBGROUP for the same groups as ORBIT COSET and STABILIZER respectively.

# 2. PRELIMINARIES

## 2.1 Group theory and quantum computation backgrounds

We say that a quantum algorithm solves a problem with error $\varepsilon$ if for every input it produces an output whose trace distance (see e.g. [16] for the definition) from a correct one is at most $\varepsilon$. We say that a problem $\mathcal{P}$ is *reducible* to a finite set of problems $\{\mathcal{Q}_i : i \in I\}$ with *error expansion* $c > 0$, if whenever each problem $\mathcal{Q}_i$ has a quantum polynomial time algorithm with error $\varepsilon$, problem $\mathcal{P}$ has also one with error $c\varepsilon$. We say that a computational problem can be solved in quantum polynomial time if there exists a quantum polynomial time algorithm that outputs the required solution with exponentially small error.

Our results concern groups represented in the general framework of black-box groups [6, 23] with unique encoding. In this model, the elements of a finite group $G$ are uniquely encoded by binary strings of length $O(\log|G|)$ and the group operations are performed by an oracle (the black-box). The groups are assumed to be input by generators. In the case of an abelian group $G$, this implies also that we have at our disposal an efficiently computable isomorphism $\theta : \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}} \to G$, where $p_i^{k_i}$ are prime powers [7]. We use the notation $<X>$ for the subgroup generated by a subset $X$ of $G$. We denote by induction $G^{(k+1)}$ the commutator $(G^{(k)})'$ of $G^{(k)}$, where $H' = <\{h^{-1}k^{-1}hk : h, k \in H\}>$ for any subgroup $H$. Whenever $G$ is solvable, the decomposition of $G$ into its *derived series* $G = G^{(0)} \rhd G^{(1)} \rhd \ldots \rhd G^{(m)} = \{1_G\}$ can be computed by a classical randomized procedure [3]. Using quantum procedures of [23][13, Theorem 10], we can compute the cyclic decomposition of each abelian factor group, and thereby expand the derived series to a *composition series*, where factor groups are cyclic of prime order. We introduce a shorthand notation for the specific solvable groups for which most of our results will apply. We say that an abelian group $G$ is *smoothly abelian* if it can be expressed as the direct product of a subgroup of constant exponent and a subgroup of size $\log^{O(1)}(|G|)$. A solvable group $G$ is *smoothly solvable* if its derived series is of constant length and has smoothly abelian factor groups. For a smoothly solvable group $G$, by combining the procedures of [7, 23, 13], we can compute in quantum polynomial time a *smooth series* $G = G_0 \rhd G_1 \rhd \ldots \rhd G_m = \{1_G\}$, where $m$ is constant, each factor group $G_i/G_{i+1}$ is either elementary abelian of constant exponent or abelian of size $\log^{O(1)}(|G|)$.

When $G$ is abelian, we identify with $G$ the set $\widehat{G}$ of characters of $G$ via some fixed isomorphism $y \mapsto \chi_y$. The *orthogonal of* $H \leq G$ is defined as $H^\perp = \{y \in G : \forall h \in H, \chi_y(h) = 1\}$. The *quantum Fourier transform* over $G$ is the unitary transformation defined for every $x \in G$ by $\mathrm{QFT}_G|x\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(x)|y\rangle$. For the sake of convenience, we will use the exact abelian quantum Fourier transform in our algorithm. The actual implementation [14] introduces only exponentially small errors.

The following well known quantum Fourier sampling algorithm will be used as a building block, where $G$ is a finite abelian group, $S$ is a finite set and $f : G \to S$ is given by a quantum oracle. This algorithm is actually the main ingredient for solving Hidden Subgroup in abelian groups when the function $f$ hides a subgroup $H \leq G$. In that case, **Fourier sampling**$^f(G)$ generates the uniform distribution over $H^\perp$. In the algorithm, $|0\rangle_S$ stands for an arbitrary but fixed element of $S$.

```
Fourier sampling^f(G)
  1. Create zero-state $|0\rangle_G|0\rangle_S$.
  2. Create uniform superposition on first register.
  3. Query function $f$.
  4. Compute $\mathrm{QFT}_G$ on first register.
  5. Observe and then output the first register.
```

A function $f : G \to \mathbb{C}^S$ is a *quantum function* if, for every $x \in G$, the vector $|f(x)\rangle$ has unit norm, and, for every $x, y \in G$, the vectors $|f(x)\rangle$ and $|f(y)\rangle$ are either the same or orthogonal. We say that the quantum function $f$ is *given* by a quantum oracle if we have at our disposal a unitary transformation $U_f$ satisfying $U_f|x\rangle_G|0\rangle_S = |x\rangle_G|f(x)\rangle_S$, for every $x \in G$.

## 2.2 The problems

Here we define the problems we are dealing with.

Let $G$ be a finite group and let $f_0, f_1$ be two injective functions from $G$ to some finite set $S$. The couple of functions $(f_0, f_1)$ can equivalently be considered as a single function $f : G \times \mathbb{Z}_2 \to S$, where by definition $f(x, b) = f_b(x)$. We will use $f$ for $(f_0, f_1)$ when it is convenient in the coming discussion. We call an element $u \in G$ the *translation* of $f$ if for every $x \in G$, we have $f_1(xu) = f_0(x)$.

> Hidden Translation
> *Input:* A finite group $G$ and two injective functions $f_0, f_1$ from $G$ to some finite set $S$ such that $f = (f_0, f_1)$ has a translation $u \in G$.
> *Output:* $u$.

For a finite group $G$ and a finite set $\Gamma$ of mutually orthogonal quantum states, we consider group actions of $G$ on $\Gamma$. By definition, $\alpha : G \times \Gamma \to \Gamma$ is a *group action* if for every $x \in G$ the quantum function $\alpha_x : |\phi\rangle \mapsto |\alpha(x, |\phi\rangle)\rangle$ is a permutation over $\Gamma$, such that the map $x \mapsto \alpha_x$ is a homomorphism from $G$ to the permutation group on $\Gamma$. We extend $\alpha$ linearly to superpositions over $\Gamma$. When the group action $\alpha$ is fixed, we use the notation $|x \cdot \phi\rangle$ for the state $|\alpha(x, |\phi\rangle)\rangle$. Having a group action $\alpha$ at our disposal means having a quantum oracle realizing the unitary transformation $|x\rangle|\phi\rangle \mapsto |x\rangle|x \cdot \phi\rangle$. For any positive integer $t$, we denote by $\alpha^t$ the group action of $G$ on $\Gamma^t = \{|\phi\rangle^{\otimes t} : |\phi\rangle \in \Gamma\}$ defined by $\alpha^t(x, |\phi\rangle^{\otimes t}) = |x \cdot \phi\rangle^{\otimes t}$. The group action $\alpha^t$ is equivalent to $\alpha$ from the algebraic point of view. Observe that one can construct a quantum oracle for $\alpha^t$ using $t$ queries to a quantum oracle for $\alpha$. We need the notion of $\alpha^t$ for the following reason. Below, we define problems where the input superpositions cannot, in general, be cloned. But in many cases, we can start off the algorithm with several independent copies of the input superpositions. We want to exploit this in order to get a reasonably accurate solution to the problem. The notion of $\alpha^t$ allows us to capture such situations.

The *stabilizer* of a state $|\phi\rangle \in \Gamma$ is the subgroup $G_{|\phi\rangle} = \{x \in G : |x \cdot \phi\rangle = |\phi\rangle\}$. Given $|\phi\rangle \in \Gamma$, the problem Stabilizer consists of finding $O(\log|G|)$ generators for the subgroup $G_{|\phi\rangle}$.

Proposition 1. *Let $G$ be a finite abelian group and let $\alpha$ be a group action of $G$. When $t = \Omega(\log(|G|)\log(1/\varepsilon))$, then* Stabilizer *in $G$ for the group action $\alpha^t$ can be solved in quantum time $\mathrm{poly}(\log|G|)\log(1/\varepsilon)$ with error $\varepsilon$.*

Proof. Let $|\phi\rangle^{\otimes t}$ be the input of Stabilizer. Let $f$ be the quantum function on $G$ defined by $|f(x)\rangle = |x \cdot \phi\rangle$, for every $x \in G$. Observe that $f$ is an instance of the natural extension of Hidden Subgroup to quantum functions and it hides the stabilizer $G_{|\phi\rangle}$.

The algorithm for Stabilizer is simply the standard algorithm for the abelian Hidden Subgroup with error $\varepsilon$. In this algorithm, every query is of the form $|x\rangle_G|0\rangle_S$. We simulate the $i^{\text{th}}$ query $|x\rangle_G|0\rangle_S$ using the $i^{\text{th}}$ copy of $|\phi\rangle$. The second register of the query is swapped with $|\phi\rangle$, and then we let act $x$ on it. We remark that the standard algorithm for abelian Hidden Subgroup outputs $O(\log|G|)$ generators for the hidden subgroup. □

Note that in general, the input superposition $|\phi\rangle^{\otimes t}$ gets destroyed by the above algorithm.

The *orbit* of a state $|\phi\rangle \in \Gamma$ is the subset $G(|\phi\rangle) = \{|x \cdot \phi\rangle : x \in G\}$. The *orbit coset* of two states $|\phi_0\rangle$ and $|\phi_1\rangle$ of $\Gamma$ is the set $\{u \in G : |u \cdot \phi_1\rangle = |\phi_0\rangle\}$. The orbit coset of $|\phi_0\rangle$ and $|\phi_1\rangle$ is either empty or a left coset $uG_{|\phi_1\rangle}$ (or equivalently a right coset $G_{|\phi_0\rangle}u$), for some $u \in G$. If the latter case occurs, $|\phi_0\rangle$ and $|\phi_1\rangle$ have conjugated stabilizers: $G_{|\phi_0\rangle} = uG_{|\phi_1\rangle}u^{-1}$. Orbit Coset is a generalization of Stabilizer:

> Orbit Coset
> *Input:* A finite group $G$ acting on a finite set $\Gamma$ of mutually orthogonal quantum states, and two quantum states $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$.
> *Output:* $\begin{cases} \texttt{reject}, \text{if } G(|\phi_0\rangle) \cap G(|\phi_1\rangle) = \emptyset; \\ u \in G \text{ such that } |u \cdot \phi_1\rangle = |\phi_0\rangle, \\ \text{and } O(\log|G|) \text{ generators} \\ \text{for } G_{|\phi_1\rangle}, \text{ otherwise.} \end{cases}$

For a function $f$ on $G$, the *superposition* of $f$ on $G$ is $|f\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$, and for $x \in G$, the *$x$-translate* of $f$ is the function $x \cdot f : g \mapsto f(gx)$. Let $\Gamma(f) = \{|x \cdot f\rangle : x \in G\}$. Then a group element $x$ acts naturally on $|f'\rangle \in \Gamma(f)$ by mapping it to the superposition $|x \cdot f'\rangle$ of its $x$-translate. We call this group action the *translation action.* The mapping $|x\rangle|f'\rangle \mapsto |x\rangle|x \cdot f'\rangle$ is realized by right multiplying the first register of $|f'\rangle$ by $x^{-1}$.

Proposition 2. *Suppose $G$ is a finite group and let $t = \mathrm{poly}(\log|G|)$. Then* Hidden Translation *(resp.* Hidden Subgroup*) is reducible to* Orbit Coset *(resp.* Stabilizer*) for the group action $\tau^t$, where $\tau$ denotes the translation action. The error expansion is* 1.

Proof. Let $f$ be an instance of Hidden Subgroup. Then the stabilizer of $|f\rangle^{\otimes t}$ is the group hidden by $f$. Let $(f_0, f_1)$ be an instance of Hidden Translation. Then the orbit coset of $|f_0\rangle^{\otimes t}$ and $|f_1\rangle^{\otimes t}$ is the translation of $(f_0, f_1)$. □

Given $|\phi\rangle \in \Gamma$, the problem Orbit Superposition consists of realizing the uniform superposition $|G \cdot \phi\rangle = \frac{1}{\sqrt{|G(|\phi\rangle)|}} \sum_{|\phi'\rangle \in G(|\phi\rangle)} |\phi'\rangle$. Note that this superposition can be also written as $\frac{1}{\sqrt{|G/G_{|\phi\rangle}|}} \sum_{x \in G/G_{|\phi\rangle}} |x \cdot \phi\rangle$.

## 3. HIDDEN TRANSLATION OVER $\mathbb{Z}_p^n$

In this section, we show that Hidden Translation can be solved in polynomial time by a quantum algorithm in the special case when $G = \mathbb{Z}_p^n$ for any fixed prime number $p > 2$. In this section we use the additive notation for the group operation and $x \cdot y$ stands for the standard inner product for $x, y \in \mathbb{Z}_p^n$. Since $\mathbb{Z}_2^n \rtimes Z_2$ is isomorphic to the abelian group $\mathbb{Z}_2^n \times Z_2$, one already has a quantum polynomial time algorithm for Hidden Translation over $\mathbb{Z}_2^n$ by reducing it to Hidden Subgroup over $\mathbb{Z}_2^{n+1}$ [9].

The quantum part of our algorithm consists of performing **Fourier sampling** over the abelian group $\mathbb{Z}_p^n \times \mathbb{Z}_2$. It turns out that from the samples we will only use elements of the form $(y, 1)$. The important property of these elements $y$ is that they are *not* orthogonal to the hidden translation. Some properties of the distribution of the samples are stated for general abelian groups in the following lemma.

Lemma 1. *Let $f = (f_0, f_1)$, $f : G \times \mathbb{Z}_2 \to S$ be an instance of* Hidden Translation *in a finite abelian group $G$ having a translation $u \neq 0$. Then* ***Fourier sampling***$^f(G \times \mathbb{Z}_2)$ *outputs an element in $G \times \{1\}$ with probability $1/2$. Moreover, the probability of sampling the element $(y, 1)$ depends only on $\chi_y(u)$, and is $0$ if $y \in u^\perp$.*

Proof. The state vector of **Fourier sampling**$^f(G \times \mathbb{Z}_2)$ before the final observation is

$$\frac{1}{2|G|} \sum_{x \in G} \sum_{y \in G} \sum_{c=0,1} \chi_y(x)\big(1 + (-1)^c \chi_y(u)\big)|y\rangle|c\rangle|f_0(x)\rangle.$$

The lemma now follows trivially. □

When $G = \mathbb{Z}_p^n$, the value $\chi_y(u)$ depends only on the inner product $y \cdot u$ over $\mathbb{Z}_p$, and $y \in u^\perp$ exactly when $y \cdot u = 0$. Therefore every $(y, 1)$ generated satisfies $y \cdot u \neq 0$. Thus the output distribution is different from the usual one obtained for the abelian Hidden Subgroup where only vectors orthogonal to the hidden subgroup are generated. We overcome the main obstacle, which is that we do not know the actual value of the inner product $y \cdot u$, by raising these inequations to the power $p-1$. They become a system of polynomial equations since $a^{p-1} = 1$ for every non-zero $a \in \mathbb{Z}_p$. In general, solving systems of polynomial equations over any finite field is NP-complete. But using the other special feature of our distribution, which is that the probability of sampling $(y, 1)$ depends only on the inner product $y \cdot u$, we are able to show that after a polynomial number of samplings, our system of equations has a unique solution with constant probability, and the solution can be determined in deterministic polynomial time.

To solve our system of polynomial equations, we linearize it in the $(p-1)^{\text{st}}$ symmetric power of $\mathbb{Z}_p^n$. We think of $\mathbb{Z}_p^n$ as an $n$-dimensional vector space over $\mathbb{Z}_p$. For a fixed prime number $p$ and an integer $k \geq 0$, let $\mathbb{Z}_p^{(k)}[x_1, \ldots, x_n]$ be the $k^{\text{th}}$ symmetric power of $\mathbb{Z}_p^n$ which will be thought of as the vector space, over the finite field $\mathbb{Z}_p$, of homogeneous polynomials of degree $k$ in variables $x_1, \ldots, x_n$. The monomials of degree $p-1$ form a basis of $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$, whose dimension is therefore $\binom{n+p-2}{p-1}$, which is polynomial in $n$. $\mathbb{Z}_p^{(1)}[x_1, \ldots, x_n]$ is isomorphic to $\mathbb{Z}_p^n$ as a vector space. For two vectors $Y_1, Y_2 \in \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$, we denote their standard inner product over the monomial basis by $Y_1 \cdot Y_2$.

For every $y = (a_1, \ldots, a_n) \in \mathbb{Z}_p^n$, we define $y^{(k)} \in \mathbb{Z}_p^{(k)}[x_1, \ldots, x_n]$ as the polynomial $(\sum_{j=1}^n a_j x_j)^k$. Now observe that if $u = (u_1, \ldots, u_n)$ is the hidden translation vector , then the vector $u^* \in \mathbb{Z}_p^{(k)}[x_1, \ldots, x_n]$ which for every monomial $x_1^{e_1} \cdots x_n^{e_n}$ has coordinate $u_1^{e_1} \cdots u_n^{e_n}$ satisfies $y^{(p-1)} \cdot u^* = (y \cdot u)^{p-1}$. Therefore each linear inequation $y \cdot u \neq 0$ over $\mathbb{Z}_p^n$ will be transformed into the linear equation $y^{(p-1)} \cdot U = 1$ over $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$, where $U$ is a $\dim \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$-sized vector of unknowns.

We will see below that the vectors $y^{(p-1)}$ span the space $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ when $y$ ranges over $\mathbb{Z}_p^n$. Moreover, in what is the main part of our proof, we show in Lemma 3 that whenever the span of $y^{(p-1)}$ for the samples $y$ is not $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$, our sampling process furnishes with constant probability a vector $z \in \mathbb{Z}_p^n$ such that $z^{(p-1)}$ is linearly independent from the $y^{(p-1)}$ for the previously sampled $y$. This immediately implies that if our sample size is of the order of the dimension of $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$, the span of $y^{(p-1)}$ for the samples $y$ is $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ with high probability. In that case, the linear equations $y^{(p-1)} \cdot U = 1$ have exactly one solution which is $u^*$. From this unique solution one can easily recover a vector $v$ such that $v = au$ for some $0 < a < p$ (note that $v^* = u^*$). Now $u$ can be found by checking the $p-1$ possibilities.

The following combinatorial lemma is at the basis of the correctness of our procedure.

Lemma 2 (Line Lemma). *Let $y, z \in \mathbb{Z}_p^n$ and $1 \le l \le p-1$. Define $L_{z,y}^l = \{(z+ay)^{(l)} : 0 \le a \le l\}$. Then $y^{(l)} \in \mathrm{Span}(L_{z,y})$.*

Proof. Let $M_{z,y}^l = \{z^{(k)}y^{(l-k)} : 0 \le k \le l\}$. Clearly, $\mathrm{Span}(L_{z,y}^l) \subseteq \mathrm{Span}(M_{z,y}^l)$. We claim that the inverse inclusion is also true since the determinant of $L_{z,y}^l$ in $M_{z,y}^l$ is non-zero. Indeed, it is $\left(\prod_{k=0}^{l}\binom{l}{k}\right) V(0,1,2,\ldots,l)$, where $V$ denotes the Vandermonde determinant. The lemma now follows because $M_{z,y}^l$ contains $y^{(l)}$. □

Proposition 3. *For $1 \le k \le p-1$, $\mathbb{Z}_p^{(k)}[x_1,\ldots,x_n]$ is spanned by $y^{(k)}$ as $y$ ranges over $\mathbb{Z}_p^n$.*

We are now ready to prove our main lemma.

Lemma 3. *Let $u \in \mathbb{Z}_p^n$, $u \neq 0$ and $W$ be a subspace of $\mathbb{Z}_p^{(p-1)}[x_1,\ldots,x_n]$. We set $R = \{y \in \mathbb{Z}_p^n : y^{(p-1)} \in W\}$. For $k = 0,\ldots,p-1$, let $V_k = \{y \in \mathbb{Z}_p^n : y \cdot u = k\}$ and $R_k = R \cap V_k$. If $W \neq \mathbb{Z}_p^{(p-1)}[x_1,\ldots,x_n]$, then $|R_k|/|V_k| \le (p-1)/p$ for $k = 1,\ldots,p-1$.*

Proof. Observe that $R_k = \{ky : y \in R_1\}$ for $0 < k < p$. Therefore the sets $R_k$, $0 < k < p$ have the same size. Observe also that the sets $V_k$, $0 \le k < p$ have the same size, and they partition $\mathbb{Z}_p^n$. Hence the values $|R_k|/|V_k|$ are the same for $0 < k < p$.

Since $W \neq \mathbb{Z}_p^{(p-1)}[x_1,\ldots,x_n]$, Proposition 3 implies that $R \neq \mathbb{Z}_p^n$. We consider two cases. In the first case, $V_0 \subseteq R$. This implies that $R_1$ is a proper subset of $V_1$. Choose any $y \in V_1 \setminus R_1$. Then by Lemma 2, in every coset of $<y>$ there is an element outside of $R$. A coset of $<y>$ contains exactly one element from each $V_k$, $k = 0,\ldots,p-1$. Hence $\cup_{k\neq 0} V_k$ is partitioned into equal parts, each part of size $p-1$, by intersecting with the cosets of $<y>$. In each part, there is an element outside of $R$. Therefore $|\cup_{k\neq 0} R_k|/|\cup_{k\neq 0} V_k| \le (p-2)/(p-1)$. Hence, $|R_k|/|V_k| \le (p-2)/(p-1) < (p-1)/p$ for $k = 1, ldots, p-1$, and the statement follows.

In the second case, $V_0 \not\subseteq R$. Therefore, there is an element $y \in V_0 \setminus R_0$. Then every $V_k$, $k = 0,\ldots,p-1$, is a union of cosets of $<y>$. Lemma 2 implies that every coset of $<y>$ contains an element outside of $R$. This proves that $|R_k|/|V_k| \le (p-1)/p$ for $k = 0,\ldots,p-1$. This completes the proof of the lemma. □

We now specify the algorithm **Translation finding** and prove that, with high probability, it finds the hidden translation in quantum polynomial time.

```
Translation finding^f(Z_p^n)
 0. If $f_0(0) = f_1(0)$ then output 0.
 1. $N \leftarrow 13p\binom{n+p-2}{p-1}$.
 2. For $i = 1,\ldots,N$ do
        $(z_i, b_i) \leftarrow$ Fourier sampling$^f(\mathbb{Z}_p^n \times \mathbb{Z}_2)$.
 3. $\{y_1,\ldots,y_M\} \leftarrow \{z_i : b_i = 1\}$.
 4. For $i = 1,\ldots,M$ do $Y_i \leftarrow y_i^{(p-1)}$.
 5. Solve the system of linear equations
        $Y_1 \cdot U = 1, \ldots, Y_M \cdot U = 1$.
 6. If there are no solutions or more than one solution
    then abort.
 7. Let $1 \le j \le n$ be such that the coefficient of $x_j^{p-1}$
    is 1 in $U$.
 8. Let $v = (v_1,\ldots,v_n) \in \mathbb{Z}_p^n$ be such that $v_j = 1$ and
    $v_k$ is the coordinate of $x_k x_j^{p-2}$ in $U$ for $k \neq j$.
 9. Find $0 < a < p$ such that $f_0(0) = f_1(av)$.
10. Output $av$.
```

Theorem 1. *For every prime number $p$, every integer $n \ge 1$, and every function $f : \mathbb{Z}_p^n \times Z_2 \to S$ having a translation given via a quantum oracle, algorithm **Translation Finding**$^f(\mathbb{Z}_p^n)$ aborts with probability less than $1/2$, and when it does not abort it outputs the translation of $f$. The query complexity of the algorithm is $O(p(n+p)^{p-1})$, and its time complexity is $(n+p)^{O(p)}$.*

Proof. Because of Step 0 of the algorithm, we can suppose w.l.o.g. that the translation $u$ of $f$ is non-zero.

If the algorithm does not abort, then $U = u^*$ is the unique solution of the system in Step 5. When the coefficient of $x_j^{p-1}$ is 1 in $U$, then $u_j \neq 0$. Also, $u_k = u_j v_k$ for every $k$. Thus, $u = u_j v$ and $u$ is found in Step 9 for $a = u_j$.

From Lemma 1, we see that the probability that the algorithm **Fourier sampling**$^f(\mathbb{Z}_p^n \times \mathbb{Z}_2)$ outputs $(y,1)$ for some $y$ is $1/2$. Therefore the expected value of $M$ is $N/2$, and $M > N/3$ with probability $1 - e^{-N/18} < 1/4$ because of Chernoff bound. If the system $Y_1,\ldots,Y_M$ has full rank, then it has a unique solution. By Lemmas 1 and 3, the expected number of linear equations that guarantee that the system has full rank is at most $p\binom{n+p-2}{p-1}$. Since $N/3 > 4p\binom{n+p-2}{p-1}$, by Markov's inequality, the solution $U$ is unique with probability at least $3/4$. Thus, the total probability of aborting is less than $1/2$. □

Corollary 1. *Let $p$ be a fixed prime. Then the problem of* Hidden Translation *over $\mathbb{Z}_p^n$ can be solved in quantum polynomial time.*

Proof. We perform two modifications in the algorithm **Translation finding**. First, to get error $\varepsilon$, the integer $N$ is multiplied by $O(\log(1/\varepsilon))$. Moreover, we assumed in the algorithm that there is an oracle for $f = (f_0, f_1)$, that is the functions $f_0$ and $f_1$ can be quantumly selected. This is not possible in general when $f_0$ and $f_1$ are given by two distinct oracles. Therefore we replace the oracle access $|x\rangle|b\rangle|0\rangle_S \mapsto |x\rangle|b\rangle|f_b(x)\rangle_S$ by

$$|x\rangle|b\rangle|0\rangle_S|0\rangle_S \mapsto |x\rangle|b\rangle|f_b(x)\rangle_S|f_{1-b}(-x)\rangle_S.$$

With this type of oracle access the algorithm **Translation finding** performs just as well.

Let us now show how to simulate this new oracle access. From $|x\rangle|b\rangle|0\rangle_S|0\rangle_S$ we compute $|(-1)^b x\rangle|b\rangle|0\rangle_S|0\rangle_S$, and then we call $f_0$ and get $|(-1)^b x\rangle|b\rangle|f_0((-1)^b x)\rangle_S|0\rangle_S$. We multiply the first register by $(-1)$ and call $f_1$ which gives $|{\scriptstyle(-1)}^{b+1}x\rangle|b\rangle|f_0({\scriptstyle(-1)}^{b}x)\rangle_S|f_1({\scriptstyle(-1)}^{b+1}x)\rangle_S$. Finally, we multiply the first register by ${\scriptstyle(-1)}^{b+1}$, and swap the last two registers when $b=1$. □

As there is a quantum reduction from Hidden Subgroup over $\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$ to Hidden Translation over $\mathbb{Z}_p^n$ [9], we obtain the following corollary.

Corollary 2. *Let $p$ be a fixed prime. Then the problem of* Hidden Subgroup *over $\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$ can be solved in quantum polynomial time.*

The algorithm **Translation finding** can also be extended to solve Orbit Coset in $\mathbb{Z}_p^n$.

Corollary 3. *Let $p$ be a fixed prime. Let $\alpha$ be a group action of $\mathbb{Z}_p^n$. When $t=\Omega(p(n+p)^{p-1}\log(1/\varepsilon))$,* Orbit Coset *in $\mathbb{Z}_p^n$ for $\alpha^t$ can be solved in quantum time $(n+p)^{O(p)}\log(1/\varepsilon)$ with error $\varepsilon$.*

Proof. Let the input of the Orbit Coset problem be $(|\phi_0\rangle^{\otimes t}, |\phi_1\rangle^{\otimes t})$. We can suppose w.l.o.g. that the stabilizers of $|\phi_0\rangle$ and $|\phi_1\rangle$ are trivial. Indeed the stabilizers can be computed by Proposition 1. If they are different then the algorithm obviously has to reject, otherwise we can work in the factor group $\mathbb{Z}_p^n/G_{|\phi_0\rangle} = \mathbb{Z}_p^{n'}$, for some $n' \le n$.

For $b=0,1$, let $f_b$ be the injective quantum function on $G$ defined by $|f_b(x)\rangle = |x\cdot\phi_b\rangle$, for every $x\in G$. If the orbit coset of $(|\phi_0\rangle,|\phi_1\rangle)$ is empty, then $f_0$ and $f_1$ have distinct ranges. Otherwise the orbit coset of $(|\phi_0\rangle,|\phi_1\rangle)$ is a singleton $\{u\}$, and $(f_0,f_1)$ have the translation $u$.

The algorithm for Orbit Coset on input $(|\phi_0\rangle^{\otimes t}, |\phi_1\rangle^{\otimes t})$ is the algorithm **Translation finding** on input $(f_0,f_1)$ with a few modifications described below. The oracle access to $(f_0,f_1)$ is modified in the same way as Corollary 1. We simulate the $i^{\text{th}}$ query $|x\rangle|b\rangle|0\rangle_S|0\rangle_S$ using the $i^{\text{th}}$ copy of $|\phi_0\rangle|\phi_1\rangle$. The two registers $|0\rangle_S|0\rangle_S$ are swapped with $|\phi_b\rangle|\phi_{1-b}\rangle$, and then we let act $x$ on $|\phi_b\rangle$ and $(-x)$ on $|\phi_{1-b}\rangle$.

The equality tests in steps 0 and 9 are replaced by the swap test [4, 10] iterated $O(\log(1/\varepsilon))$ times. Finally, $N$ is multiplied by $O(\log(1/\varepsilon))$, and the algorithm rejects whenever the algorithm **Translation finding** aborts or there is no solution in step 9. □

## 4. ORBIT SUPERPOSITION

In this section, we show that Orbit Superposition is reducible to Orbit Coset for solvable groups $G$. The proof will be by induction along a composition series of $G$. The induction step is based on the technique of Watrous [23] to create a uniform superposition of elements of $G$. One way of stating Watrous's result is that it solves Orbit Superposition for the case of the special action when $G$ acts on itself by left multiplication. More precisely, the induction step uses the following lemma.

Lemma 4. *Let $K$ be a finite group and $\alpha$ be a group action of $K$ on $\Gamma$. Let $L \lhd K$ such that $K/L$ is cyclic of prime order $r$, and $|\phi\rangle\in\Gamma$. Let $t$ be a positive integer. Given an element $z\in K-L$, the number $r$ and $|\phi\rangle|L\cdot\phi\rangle^{\otimes t}$, realizing $|\phi\rangle|K\cdot\phi\rangle^{\otimes(t-1)}$ is reducible to* Orbit Coset *in $K$ for $\alpha$ with error expansion $O(t)$.*

Proof. The analysis of the algorithm will distinguish between two cases: case one is when $K_{|\phi\rangle}\not\subseteq L$, and case two is when $K_{|\phi\rangle}\subseteq L$. In the first case, for every $x\in G$, $|x\cdot(L\cdot\phi)\rangle = |K\cdot\phi\rangle$, and in particular, $|L\cdot\phi\rangle = |K\cdot\phi\rangle$. In the second case, $|K\cdot\phi\rangle = \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}|z^i\cdot(L\cdot\phi)\rangle$.

We first compute the state $\left(\frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}|i\rangle|z^i\cdot(L\cdot\phi)\rangle\right)^{\otimes t}$ from $|L\cdot\phi\rangle^{\otimes t}$. We then disentangle the first registers from the second using Watrous's method. We apply the quantum Fourier transform over $\mathbb{Z}_r$ to the first registers. In the first case we obtain the state $(|0\rangle|K\cdot\phi\rangle)^{\otimes t}$, and in the second case we obtain the state $(\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}|j\rangle|\psi_j\rangle)^{\otimes t}$, where $|\psi_j\rangle = \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\omega_r^{ij}|z^i\cdot(L\cdot\phi)\rangle$, and $\omega_r$ is a fixed primitive $r^{\text{th}}$-root of unity.

We now describe the rest of the algorithm by specifying how it behaves on the terms in the expansion of the above tensor power. Let $|j_0\rangle|\psi_{j_0}\rangle|j_1\rangle|\psi_{j_1}\rangle\ldots|j_{t-1}\rangle|\psi_{j_{t-1}}\rangle$ be such a term. If all the values $j$ are 0 then the algorithm does nothing. Observe that if this happens, we already have $t$ copies of the desired superposition $|K\cdot\phi\rangle$, independently of which case we are in. Otherwise, let $j'$ be the first nonzero $j$. Note that this can only happen in case two. We swap $|j_0\rangle|\psi_{j_0}\rangle$ and $|j'\rangle|\psi_{j'}\rangle$, and record the value $j'$ in an ancilla register. For convenience of notation, we continue to refer to the first two registers as $|j_0\rangle|\psi_{j_0}\rangle$. Thus, we have ensured that $j_0\neq 0$. Using $|\psi_{j_0}\rangle$ our purpose will be to cancel the phases of all the other states $|\psi_{j_i}\rangle$, $i\neq 0$ for which $j_i\neq 0$. Observe that $|l\cdot\psi_{j_0}\rangle = |\psi_{j_0}\rangle$ for every $l\in L$ (and hence for every $k\in K_{|\phi\rangle}$), and $|z\cdot\psi_{j_0}\rangle = \omega_r^{-j_0}|\psi_{j_0}\rangle$. Therefore if we set $f=j(j_0)^{-1} \mod r$ for some $j\neq 0$, then, for every $i\in\{0,\ldots,r-1\}$, $l\in L$, and $k\in K_{|\phi\rangle}$, $|(z^ilk)^f\cdot\psi_{j_0}\rangle = \omega_r^{-ij}|\psi_{j_0}\rangle$.

We now complete the reduction by computing the state $|\phi\rangle|\psi_{j_0}\rangle|K\cdot\phi\rangle$ from $|\phi\rangle|\psi_{j_0}\rangle|\psi_j\rangle$, when $j\neq 0$. Note that if $j=0$, $|\psi_j\rangle$ is already equal to $|K\cdot\phi\rangle$. For every state $|z^il\cdot\phi\rangle$ appearing the expansion of $|\psi_j\rangle$, we find the coset $z^ilK_{|\phi\rangle}$ using Orbit Coset in $K$ for $|z^il\cdot\phi\rangle$ and $|\phi\rangle$. Let $z^ilk$ be some representative of the coset where $k\in K_{|\phi\rangle}$. We let $(z^ilk)^f$ act on $|\psi_{j_0}\rangle$ and reverse the previous Orbit Coset procedure. This realizes the transformation $|\phi\rangle|\psi_{j_0}\rangle|z^il\cdot\phi\rangle \mapsto \omega_r^{-ij}|\phi\rangle|\psi_{j_0}\rangle|z^il\cdot\phi\rangle$. The effect on $|\phi\rangle|\psi_{j_0}\rangle|\psi_j\rangle$ is $|\phi\rangle|\psi_{j_0}\rangle|K\cdot\phi\rangle$. Since the first pair of registers remains unchanged, the process can be repeated for the other states, and therefore we get $|\phi\rangle|j_0\rangle|\psi_{j_0}\rangle|j_1\rangle|K\cdot\phi\rangle\ldots|j_{t-1}\rangle|K\cdot\phi\rangle$, together with some garbage in the ancilla register. The output of the algorithm is thus $|\phi\rangle|K\cdot\phi\rangle^{\otimes(t-1)}|\theta\rangle$, where $|\theta\rangle$ is a state vector on the rest of the qubits.

The above analysis assumed that the procedure for the Orbit Coset problem in $K$ is error-free. If not, one can see easily that the error expansion is $O(t)$. □

Theorem 2. *Let $G$ be a finite solvable group and let $\alpha$ be a group action on $\Gamma$. Let $|\phi\rangle\in\Gamma$. Given $|\phi\rangle^{\otimes(s+\lfloor\log|G|\rfloor+1)}$, realizing $|\phi\rangle|G\cdot\phi\rangle^{\otimes s}$ is reducible to* Orbit Coset *in subgroups of $G$ for $\alpha$ with error expansion $O(s\log|G|+\log^2|G|)$.*

Proof. Let us recall that the group $G$ can be given with elements $z_i$ and primes $r_i$, for $i=0,\ldots,m-1$, such that $G$ has a composition series $G=G_0 \rhd G_1 \rhd \ldots \rhd G_m = \{1_G\}$, where $G_i/G_{i+1}$ is cyclic of order $r_i$ and is generated by $z_iG_{i+1}$. Note that $m\le\lfloor\log|G|\rfloor$. By induction, for $i=m$ down to $i=0$, we will produce the state $|\phi\rangle|G_i\cdot\phi\rangle^{\otimes(s+i)}$.

For $i=m$, by the induction hypothesis we have at least $s+m+1$ independent copies of states $|\phi\rangle = |G_m\cdot\phi\rangle$ since

$m \leq \log|G|$. Assume now that we have $|\phi\rangle|G_i \cdot \phi\rangle^{\otimes(s+i)}$. By applying Lemma 4 with $K = G_{i-1}$, $L = G_i$, $z = z_{i-1}$ and $r = r_{i-1}$, we get the state $|\phi\rangle|G_{i-1} \cdot \phi\rangle^{\otimes(s+i-1)}$ using Orbit Coset in $G_{i-1}$. When $i = 0$, we obtain $|\phi\rangle|G \cdot \phi\rangle^{\otimes s}$. The error expansion is $O(m(s + m)) = O(s \log|G| + \log^2|G|)$. □

## 5. ORBIT COSET SELF-REDUCIBILITY

This section is based on the following theorem stating the reducibility of Orbit Coset in $G$ to Orbit Coset in proper normal subgroups of $G$ under some conditions. Given a group action $\alpha$ of $G$ on a finite set $\Gamma$ of mutually orthogonal quantum states, we define for every proper normal subgroup $N \lhd G$ the group action $\alpha_N$ of $G/N$ on $\{|N \cdot \phi\rangle : |\phi\rangle \in \Gamma\}$ by $\alpha_N(xN, |N \cdot \phi\rangle) = |x \cdot (N \cdot \phi)\rangle$, for every $x \in G$ and $|\phi\rangle \in \Gamma$. Note that this action is independent of the coset representative chosen.

Theorem 3. *Let $G$ be a finite group and let $N \lhd G, N \neq G$ be solvable such that $G$, $N$ and $G/N$ are black-box groups with unique encoding. Let $\alpha$ be a group action of $G$ and let $s \geq 1$ be an integer. When $t = \Omega(s + \log|G|)$,* Orbit Coset *(resp.* Stabilizer*) in $G$ for $\alpha^t$ is reducible to* Orbit Coset *in subgroups of $N$ for $\alpha$ and* Orbit Coset *(resp.* Stabilizer*) in $G/N$ for $(\alpha_N)^s$ with error expansion $O(s \log|G| + \log^2|G|)$.*

Proof. We first prove the statement for the Stabilizer reduction. The proof for the Orbit Coset reduction uses the result for Stabilizer. This is indeed legitimate since Stabilizer is the special case of Orbit Coset when the two inputs are identical.

Let $|\phi\rangle^{\otimes t}$ be an instance of Stabilizer. Its stabilizer $H$ is the same as the stabilizer of $|\phi\rangle$. First we compute $O(\log|N|)$ generators for the intersection $H_0 = H \cap N$ using Stabilizer in $N$ for $\alpha$ in quantum polynomial time. Then we use Orbit Coset in subgroups of $N$ and Stabilizer in $G/N$ to construct a subgroup $H_1 \leq G$ which in fact will turn out to be $H$. The properties which will ensure that equality are $H_0 \leq H_1 \leq H$ and $H_1N/N = HN/N$. Indeed, the first property clearly implies that $H_1 \cap N = H \cap N$, which together with the second one gives that $H_1 = H$ by standard group-theoretic arguments.

To construct $H_1$ we add to $H_0$ generators in $H$ of $HN/N$. The construction proceeds in two steps. First, we find a set $V \subseteq G$, $|V| = O(\log|G/N|)$ which, when its elements are considered as coset representatives, is a generator set for $HN/N$. Then, for every coset $zN$ where $z \in V$, we find a coset representative of $zN$ in $H$. This step is achieved via a reduction to Orbit Coset in $N$. The collection of those representatives and $H_0$ together generate the desired subgroup $H_1$.

The stabilizer of $|N \cdot \phi\rangle$ for $\alpha_N$ in $G/N$ is $HN/N$. Therefore finding $V$ is reducible to Stabilizer in $G/N$ for $(\alpha_N)^s$ on input $|N \cdot \phi\rangle^{\otimes s}$. By Theorem 2, creating this input is also reducible to Orbit Coset in subgroups of $N$ for $\alpha$ on input $|\phi\rangle^{\otimes s + \lfloor \log|G| \rfloor + 1}$ with error expansion $O(s \log|G| + \log^2|G|)$. Note that the size of $V$ is $O(\log|G/N|)$.

We describe now how to find, using Orbit Coset in $N$, for each $z \in V$, an element $n \in N$ such that $zn \in H$. Fix $z \in V$. We can construct $|\phi'\rangle = |z^{-1} \cdot \phi\rangle$ using a copy of $|\phi\rangle$. In the subgroup $N$, the states $|\phi'\rangle$ and $|\phi\rangle$ have the orbit coset $nH_0$. Thus the coset $nH_0$ can be found using Orbit Coset in $N$ for $\alpha$. The error expansion due to this process is $O(|V|) = O(\log|G|)$. This completes the proof of the theorem for Stabilizer.

We now turn to the proof of the Orbit Coset reduction. Let $(|\phi_0\rangle^{\otimes t}, |\phi_1\rangle^{\otimes t})$ be the input of Orbit Coset. Their orbit coset is identical to the orbit coset of $(|\phi_0\rangle, |\phi_1\rangle)$, and it is either empty or $uG_{|\phi_1\rangle}$, for some $u \in G$. We compute $H = G_{|\phi_1\rangle}$ using the above construction. When the orbit coset of the input is empty, the states $|N \cdot \phi_0\rangle^{\otimes s}$ and $|N \cdot \phi_1\rangle^{\otimes s}$ have also empty orbit coset. Otherwise they have the orbit coset $u(HN/N)$.

By Theorem 2, the constructions of states $|N \cdot \phi_0\rangle^{\otimes s}$ and $|N \cdot \phi_1\rangle^{\otimes s}$ are reducible to Orbit Coset in subgroups of $N$ for $\alpha$ on input $(|\phi_0\rangle^{\otimes s + \lfloor \log|G| \rfloor + 1}, |\phi_1\rangle^{\otimes s + \lfloor \log|G| \rfloor + 1})$ with error expansion $O(s \log|G| + \log^2|G|)$. Then using Orbit Coset in $G/N$ for $(\alpha_N)^s$ in input $|N \cdot \phi_0\rangle^{\otimes s}$ and $|N \cdot \phi_1\rangle^{\otimes s}$, we reject if the inputs have empty orbit coset, or we find the coset $u(HN/N)$, that is an element $v \in uHN$.

Using Orbit Coset in $N$, we now describe how to find an element $n \in N$ such that $vn \in uH$. We construct the state $|\phi_0'\rangle = |v^{-1} \cdot \phi_0\rangle$ using one copy of $|\phi_0\rangle$. Let us denote $H_0 = H \cap N$. In the subgroup $N$, the states $|\phi_0'\rangle$ and $|\phi_1\rangle$ have the orbit coset $nH_0$, which can be found using Orbit Coset in $N$ for $\alpha$. This completes the proof of the theorem for Orbit Coset. □

Theorem 4. *Let $G$ be a smoothly solvable group and let $\alpha$ be a group action of $G$. When $t = (\log^{\Omega(1)}|G|) \log(1/\varepsilon)$,* Orbit Coset *can be solved in $G$ for $\alpha^t$ in quantum time $\mathrm{poly}(\log|G|) \log(1/\varepsilon)$ with error $\varepsilon$.*

Proof. As $G$ is smoothly solvable, it has a smooth series $G = G_0 \rhd G_1 \rhd \ldots G_{m-1} \rhd G_m = \{1_G\}$, where $m$ is constant, $G_i/G_{i+1}$ is either elementary abelian of constant exponent or of size polylogarithmic in the order of $G$. Observe that we have a cyclic prime power decomposition of each factor group $G_i/G_{i+1}$, and for this representation, we have a black-box oracle for the group action of $G_i/G_{i+1}$ on $\{|G_{i+1} \cdot \phi\rangle : |\phi\rangle \in \Gamma\}$.

The proof is by induction on $m$. The case $m = 0$ is trivial. For the induction, we can efficiently solve Orbit Coset in the factor group $G_0/G_1$: if it is of polylogarithmic size we just do an exhaustive search, otherwise we apply Corollary 3. Therefore Theorem 3 reduces Orbit Coset in $G$ to Orbit Coset in subgroups of $G_1$. Any subgroup $K$ of $G_1$ has a smooth series of length at most $m-1$, since the intersection of a smooth series for $G_1$ with $K$ gives a smooth series for $K$. The running time of the overall procedure is $(\log|G|)^{O(m)} \log(1/\varepsilon)$. □

Theorem 5. *Let $G$ be a finite solvable group having a smoothly solvable commutator subgroup and let $\alpha$ be a group action of $G$. When $t = (\log^{\Omega(1)}|G|) \log(1/\varepsilon)$,* Stabilizer *can be solved in $G$ for $\alpha^t$ in quantum time $\mathrm{poly}(\log(|G|) \log(1/\varepsilon)$ with error $\varepsilon$.*

Proof. By Theorem 3, Stabilizer in $G$ is reducible to Stabilizer in $G/G'$ and Orbit Coset in subgroups of $G'$. The factor group $G/G'$ is abelian and subgroups of $G'$ are smoothly solvable. Therefore, from Proposition 1 and Theorem 4 the statement follows. □

Corollary 4. *The* Hidden Translation *problem can be solved over smoothly solvable groups in quantum polynomial time. The* Hidden Subgroup *problem can be solved over solvable groups having a smoothly solvable commutator subgroup in quantum polynomial time.*

## Acknowledgements

We wish to thank Mark Ettinger and Peter Høyer for sharing their knowledge and ideas about HIDDEN TRANSLATION with us, and Martin Rötteler for several useful discussions on HIDDEN SUBGROUP.

## 6. REFERENCES

[1] D. Aharonov. Quantum computation – A review. In *Annual Review of Computational Physics*, volume VI. World Scientific, 1998.

[2] D. Aharonov and A. Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. These proceedings.

[3] L. Babai, G. Cooperman, L. Finkelstein, E. Luks, and A. Seress. Fast Monte Carlo algorithms for permutation groups. *J. Comput. System Sci.*, 50:296–307, 1995.

[4] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16), 2001. Article 167902.

[5] R. Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proc. 29th ACM STOC*, pages 48–53, 1997.

[6] L. Babai and E. Szemerédi. On the complexity of matrix group problems I. In *Proc. 25th FOCS*, pages 229–240, 1984.

[7] K. Cheung and M. Mosca. Decomposing finite abelian groups. *J. Quantum Inf. Comp.*, 1(3), 2001.

[8] W. van Dam, S. Hallgren, and L. Ip. Quantum algorithms for some hidden shift problems. In *Proc. 14th ACM-SIAM SODA*, 2003.

[9] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. *Adv. in Appl. Math.*, 25(3):239–251, 2000.

[10] D. Gottesman and I. Chuang. Quantum digital signatures. Technical report, Quantum Physics e-Print archive, 2001. `http://xxx.lanl.gov/abs/quant-ph/0105032`.

[11] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the nonabelian Hidden Subgroup Problem. In *Proc. 33rd ACM STOC*, pages 68–74, 2001.

[12] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proc. 32nd ACM STOC*, pages 627–635, 2000.

[13] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem. In *Proc. 13th ACM SPAA*, pages 263–270, 2001.

[14] A. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. Technical report, Quantum Physics e-Print archive, 1995. `http://xxx.lanl.gov/abs/quant-ph/9511026`.

[15] A. Kitaev. *Classical and Quantum Computation.* Graduate Studies in Mathematics, vol. 47, American Mathematical Society, 2002.

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

[17] M. Püschel, M. Rötteler, and T. Beth. Fast quantum Fourier transforms for a class of non-Abelian groups. In *Proc. 13th AAECC*, volume 1719, pages 148–159. LNCS, 1999.

[18] J. Preskill. Quantum information and computation. `http://www.theory.caltech.edu/people/preskill/ph229`, 1998.

[19] M. Rötteler and T. Beth. Polynomial-time solution to the Hidden Subgroup Problem for a class of non-abelian groups. Technical report, Quantum Physics e-Print archive, 1998. `http://xxx.lanl.gov/abs/quant-ph/9812070`.

[20] P. Shor. Algorithms for quantum computation: Discrete logarithm and factoring. *SIAM J. Comp.*, 26(5):1484–1509, 1997.

[21] D. Simon. On the power of quantum computation. *SIAM J. Comp.*, 26(5):1474–1483, 1997.

[22] M. Sudan. Notes on algebra. Lecture 2.5 of the course *Algorithmic Introduction to Coding Theory.* Course notes at `http://theory.lcs.mit.edu/~madhu/FT01`.

[23] J. Watrous. Quantum algorithms for solvable groups. In *Proc. 33rd ACM STOC*, pages 60–67, 2001.

# APPENDIX

## A. HIDDEN TRANSLATION OVER $\mathbb{Z}_{p^k}^n$

In this section, we describe a quantum algorithm to directly solve HIDDEN TRANSLATION for groups of the form $\mathbb{Z}_{p^k}^n$, for every fixed prime power $p^k$. This algorithm does not use ORBIT COSET. Rather, it can be viewed as a generalization of the algorithm of Section 3.

We identify elements of $\mathbb{Z}_p^k$ with elements of $\mathbb{Z}_{p^k}$ by the bijection $(a_0, \ldots, a_{k-1}) \mapsto \sum_{j=0}^{k-1} a_j p^j$. We denote by $\overline{a} \in \mathbb{Z}_p^k$ the element that is mapped to $a \in \mathbb{Z}_{p^k}$ by the above bijection. This notation can be extended to $y \in \mathbb{Z}_{p^k}^n$ in the following way. Let $m = kn$ in the rest of this section. Let $y = (y_1, \ldots, y_n) \in \mathbb{Z}_{p^k}^n$. Then $\overline{y}$ denotes the vector $(\overline{y_1}, \ldots, \overline{y_n}) \in \mathbb{Z}_p^m$, and $y_{i,j}$ denotes the $j^{\text{th}}$ coordinate of $\overline{y_i} \in \mathbb{Z}_p^k$.

LEMMA 5. *There is a polynomial $C(x, y) \in \mathbb{Z}_p[x, y]$ of degree at most $2p-2$ such that for every $a, b \in \mathbb{Z}_p$, $C(a, b) = 0$ if $a + b < p$ and $C(a, b) = 1$ otherwise.*

PROOF. Let $L_i(z) = \prod_{0 \leq j < p : j \neq i}(z - j)/(i - j)$, $L_i(z) \in \mathbb{Z}_p[z]$ denote the Lagrange polynomial. We have that $L_i(i) = 1$ and $L_i(j) = 0$ for $j \neq i$. Define $C(x, y) = \sum_{0 \leq i,j < p : i+j \geq p} L_i(x)L_j(y)$. □

For $0 \leq a, b < p$, $C(a, b)$ represents the *carry* term of $a + b$ when integer addition is done in base $p$.

LEMMA 6. *For every integer $T \geq 1$, there exist polynomials $Q_i \in \mathbb{Z}_p[y_{1,0}, \ldots, y_{1,k-1}, \ldots, y_{T,0}, \ldots, y_{T,k-1}]$, for $i = 0, \ldots, k-1$, of total degree at most $(2p-2)^l$,such that*

$$\overline{\sum_{t=1}^{T} a_d \mod p^k} = (Q_0(\overline{a_1}, \ldots, \overline{a_T}), \ldots, Q_{k-1}(\overline{a_1}, \ldots, \overline{a_T}))$$

*for every $a_1, \ldots, a_T \in \mathbb{Z}_{p^k}$.*

In other words, the polynomials $Q_l$ express the digits of the sum $\left(\sum_{d=1}^{T} a_d \mod p^k\right)$ in base $p$.

PROOF. The proof is accomplished by induction on $k$. For $k = 1$ the statement is obvious: $Q_0 = \sum_{t=1}^{T} y_{t,0}$. Now let

$k > 1$. For $t = 2, \dots, T$ set $Q_0 = \sum_{t=1}^{T} y_{t,0}$ and $C_t = C\left( (\sum_{j=1}^{t-1} y_{j,0}), y_{t,0} \right)$. Then for every $a_1, \dots, a_T \in \mathbb{Z}_{p^k}$, the sum $s = \sum_{t=1}^{T} a_t \mod p^k$ satisfies

$$\begin{aligned} s_0 &= Q_0(a_{1,0}, \dots, a_{n,0}) \mod p, \\ (s_1, \dots, s_{k-1}) &= \overline{\left( \sum_{t=1}^{T} \lfloor a_t/p \rfloor + \sum_{t=2}^{T} c_t \right)} \mod p^{k-1}, \end{aligned}$$

where $c_t = C_t(a_{1,0}, \dots, a_{t,0})$. In other words, the $0^{\text{th}}$ coordinate of the sum $s$ is a linear polynomial in $a_{t,0}$, and, for $1 \leq j \leq k-1$, the $j^{\text{th}}$ coordinate is the $(j-1)^{\text{th}}$ coordinate in the RHS term of the second equation. Observe that each coordinate is a polynomial of degree at most $2p-2$ in the $a_{t,j}$. Therefore we can conclude using the inductive hypothesis. □

Corollary 5. *For every $u \in \mathbb{Z}_{p^k}^n$, there exist polynomials $Q_i \in \mathbb{Z}_p[x_1, \dots, x_m]$ of total degree at most $(2p-2)^i$, for $i = 0, \dots, k-1$, such that $\overline{y \cdot u} = (Q_0(\overline{y}), \dots, Q_{k-1}(\overline{y}))$ for every $y \in \mathbb{Z}_{p^k}^n$.*

Proof. Follows from Lemma 6 by repeating $u_i$ times the coordinate $y_i$, and taking the sum of all the terms obtained this way modulo $p^k$. □

For every positive integer $D$, let $\mathbb{Z}_p^D[x_1, \dots, x_m]$ be the linear subspace of polynomials of $\mathbb{Z}_p[x_1, \dots, x_m]$ whose total degree is at most $D$ and partial degrees are at most $p-1$ in each variable. For every $\overline{y} \in \mathbb{Z}_p^m$, we denote by $l_{\overline{y}}$ the linear form over polynomials that satisfies $l_{\overline{y}}(Q) = Q(\overline{y})$, for every polynomial $Q \in \mathbb{Z}_p^D[x_1, \dots, x_m]$. Using the standard inner product of polynomials over the monomial basis, we identify the dual of $\mathbb{Z}_p^D[x_1, \dots, x_m]$ with itself. In particular, the linear form $l_{\overline{y}}$ is identified with the polynomial $L_{\overline{y}}$ whose coefficient in each monomial $M \in \mathbb{Z}_p^D[x_1, \dots, x_m]$ is $M(\overline{y})$. Then, the polynomial $L_{\overline{y}}$ satisfies $L_{\overline{y}} \cdot Q = Q(\overline{y})$, for every polynomial $Q \in \mathbb{Z}_p^D[x_1, \dots, x_m]$. Together with Fermat's little theorem, the previous corollary implies a polynomial characterization over $\mathbb{Z}_p$ of vectors in $\mathbb{Z}_{p^k}^n$ that are not orthogonal to a fixed vector $u \in \mathbb{Z}_{p^k}^n$.

Lemma 7. *Let $D = \frac{(p-1)((2p-2)^k - 1)}{2p-3}$. For every $u \in \mathbb{Z}_{p^k}^n$, there exists a polynomial $Q_u \in \mathbb{Z}_p^D[x_1, \dots, x_m]$ such that for every $y \in \mathbb{Z}_{p^k}^n$, $y \cdot u \neq 0 \mod p^k$ if and only if $L_{\overline{y}} \cdot Q_u = 0 \mod p$.*

Proof. Let $Q = \prod_{j=0}^{k-1} (Q_j^{p-1} - 1)$, where the polynomials $Q_j$ come from Corollary 5. This polynomial has the required total degree. To ensure that partial degrees are less than $p-1$, we substitute $x_i^p$ terms by $x_i$ until every partial degree is at most $p-1$. Let $Q_u$ be the final polynomial. Then $Q_u$ and $Q$ encode the same function over $\mathbb{Z}_p^m$. Therefore, since $L_{\overline{y}} \cdot Q_u = Q_u(\overline{y}) \mod p$, the polynomial $Q_u$ satisfies the required conditions. □

Proposition 4. *Let $D$ be a positive integer. Then $\mathbb{Z}_p^D[x_1, \dots, x_m]$ is generated by $\{\overline{y}^D : \overline{y} \in \mathbb{Z}_p^m\}$*

The following proposition is an extension of the well-known Schwarz-Zippel lemma on the maximum number of roots of a multivariate polynomial over a finite field, and can be proved similarly. A discussion can be found in e.g. [22].

Proposition 5. *Suppose $\mathbb{F}$ is a finite field of size $q$. Suppose polynomial $f \in \mathbb{F}[x_1, \dots, x_m]$ has partial degree at most $l$ in each $x_i$ and total degree at most $d$. Let $d = lk + r$, where $0 \leq r < l$. Then $f$ is non-zero on at least $\left(1 - \frac{l}{q}\right)^k \left(1 - \frac{r}{q}\right)$ fraction of the inputs from $\mathbb{F}^m$.*

Lemma 8. *Let $D$ be a positive integer. Let $W$ be a proper subspace of $\mathbb{Z}_p^D[x_1, \dots, x_m]$. If $\overline{y}$ is uniformly generated in $\mathbb{Z}_p^m$, then $L_{\overline{y}} \notin W$ with probability greater than $1/p^{\lceil D/(p-1) \rceil}$.*

Proof. Let $N = \dim(W)$. Let $Q_1, \dots, Q_N \in W$ be linearly independent polynomials. There exist $R_1, \dots, R_N \in \mathbb{Z}_p^D[x_1, \dots, x_m]$ such that the matrix $(Q_i \cdot R_j)_{1 \leq i,j \leq N}$ is the identity matrix. Let $\overline{y} \in \mathbb{Z}_p^m$ and $Q_{N+1} = L_{\overline{y}}$. Let $R_{N+1} \in \mathbb{Z}_p^D[x_1, \dots, x_m]$ be linearly independent from $R_1, \dots, R_N$. $R_{N+1}$ is a non-zero polynomial. The determinant of the matrix $(Q_i \cdot R_j)_{1 \leq i,j \leq N+1}$ is $Q_{N+1} \cdot R_{N+1} = R_{N+1}(\overline{y})$. $R_{N+1}(\overline{y}) \neq 0$ implies that the polynomials $Q_1, \dots, Q_{N+1}$ are linearly independent, that is, $L_{\overline{y}} \notin W$. By Proposition 4, there exists $\overline{y} \in \mathbb{Z}_p^m$ such that $L_{\overline{y}} \notin W$. Therefore by Proposition 5, $R_{N+1}(\overline{y}) \neq 0$ with probability at least $1/p^{\lceil D/(p-1) \rceil}$, when $\overline{y}$ is uniformly distributed in $\mathbb{Z}_p^m$. This completes the proof. □

We now state the following proposition which says that for every fixed integer $d \geq 2$, the (search version of) Hidden Translation in $\mathbb{Z}_d^n$ reduces to the decision version of Hidden Translation in $\mathbb{Z}_d^n$. The decision version of Hidden Translation is defined as follows: Given two injective functions $f_0$ and $f_1$ on an abelian group $G$ that have either a translation or distinct ranges, one has to distinguish between these two cases.

Proposition 6. *For every fixed integer $d \geq 2$, the search version of* Hidden Translation *in $\mathbb{Z}_d^n$ reduces in classical polynomial time to the decision version of* Hidden Translation *in $\mathbb{Z}_d^{n-1}$ using $d \times n$ calls.*

Theorem 6. *For every fixed prime power $p^k$ and positive integer $n$, the* Hidden Translation *over $\mathbb{Z}_{p^k}^n$ can be solved in quantum polynomial time.*

Proof. Suppose $f = (f_0, f_1)$ is the input to Hidden Translation. We can assume w.l.o.g. that $f_0 \neq f_1$, *i.e.* that they do not have the zero vector as their translation. By Proposition 6, it is enough to solve the decision version of Hidden Translation over $\mathbb{Z}_{p^k}^n$. Let $N = \Omega(p^{\lceil D/(p-1) \rceil} \times \dim(\mathbb{Z}_p^D[x_1, \dots, x_m]))$, where $D = \frac{(p-1)((2p-2)^k - 1)}{2p-3}$. Since $p$ and $k$ are constant, $N$ is a polynomial in $n$. The algorithm to solve the decision version of Hidden Translation over $\mathbb{Z}_{p^k}^n$ consists of calling $N$ times the quantum subroutine **Fourier sampling**$^f(\mathbb{Z}_{p^k}^n \times \mathbb{Z}_2)$ The sampled vectors are of the form $(z_i, b_i)$. Let $y_1, \dots, y_M$ be the $z_i$ of the vectors for which $b_i = 1$. The algorithm accepts if and only if $\{L_{\overline{y}_1}, \dots, L_{\overline{y}_M}\}$ does not span $\mathbb{Z}_p^D[x_1, \dots, x_m]$.

If $f_0$ and $f_1$ have the translation $u \in \mathbb{Z}_{p^k}^n$, then the polynomial $Q_u$ from Lemma 7 is orthogonal to the polynomials $L_{\overline{y}_1}, \dots, L_{\overline{y}_M}$. Therefore $\{L_{\overline{y}_1}, \dots, L_{\overline{y}_M}\}$ is never full rank in $\mathbb{Z}_p^D[x_1, \dots, x_m]$. On the other hand, if $f_0$ and $f_1$ have distinct ranges, the expected value of $M$ is $N/2$, and the vectors $y_i$ are uniformly generated in $\mathbb{Z}_{p^k}^n$. Therefore the vectors $\overline{y}_i$ are also uniformly generated in $\mathbb{Z}_p^m$, and by Lemma 8, we obtain that $\{L_{\overline{y}_1}, \dots, L_{\overline{y}_M}\}$ is full rank in $\mathbb{Z}_p^D[x_1, \dots, x_m]$ with probability greater than $2/3$. □