Quantum testers for hidden group properties*

Katalin Friedl
Dept. of Comp. Sci.
Budapest Univ. of Technology and Economics
H-1521 Budapest, Hungary
friedl@cs.bme.hu

Frédéric Magniez
LRI, Univ Paris-Sud, CNRS
F-91405 Orsay, France
magniez@lri.fr

Miklos Santha
LRI, Univ Paris-Sud, CNRS
F-91405 Orsay, France
and CQT, Nat. Univ. of Singapore
Singapore 117543
santha@lri.fr

Pranab Sen
School of Technology and Computer Science
Tata Institute of Fundamental Research
Mumbai, India
pgdsen@tcs.tifr.res.in

Abstract. We construct efficient or query efficient quantum property testers for two existential group properties which have exponential query complexity both for their decision problem in the quantum and for their testing problem in the classical model of computing. These are periodicity in groups and the common coset range property of two functions having identical ranges within each coset of some normal subgroup. Our periodicity tester is efficient in Abelian groups and generalizes, in several aspects, previous periodicity testers. This is achieved by introducing a technique refining the majority correction process widely used for proving robustness of algebraic properties. The periodicity tester in non-Abelian groups and the common coset range tester are query efficient.

Keywords: Quantum Computing, Property Testing

Address for correspondence: magniez@lri.fr

*A preliminary version of this work appeared in *Proceedings of the 28th International Symposium on Mathematical Foundations of Computer Science*, volume 2747 of *Lecture Notes in Computer Science*, pages 419–428. Springer, 2003. Research supported in part by the European Commission IST Integrated Project Qubit Applications (QAP) 015848, and the ANR Blanc AlgoQP grant of the French Research Ministry.

1. Introduction

In the paradigm of property testing one would like to decide whether an object has a global property by performing random local checks. The goal is to distinguish with sufficient confidence the objects which satisfy the property from those objects that are far from having the property. In this sense, property testing is a notion of approximation for the corresponding decision problem. Property testers, with a slightly different objective, were first considered for programs under the name of self-testers. Following the pioneering approach of Blum, Kannan, Luby and Rubinfeld [4, 5], self-testers were constructed for programs purportedly computing functions with some algebraic properties such as linear functions, polynomial functions, and functions satisfying some functional equations [5, 25, 26]. The notion in its full generality was defined by Goldreich, Goldwasser and Ron and successfully applied among others to graph properties [10, 12]. For surveys on property testing see [11, 23, 18, 8].

Quantum computing (for surveys see e.g. [24, 1, 22, 21]) is an extremely active research area, 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 complexity of an algorithm is measured by the number of queries (*i.e.* evaluations of the function f), and also by the overall running time counting one query as one computational step. We say that an algorithm is *query efficient* (resp. *efficient*) if its query complexity (resp. overall 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 the HIDDEN SUBGROUP PROBLEM (HSP), 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, the biggest success of quantum computing until now is that it can be solved by a quantum algorithm *efficiently* whenever G is Abelian. We will refer to this algorithm as the *standard algorithm* for the HSP. 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 [17]. Simon's xor-mask finding [29], Shor's factorization and discrete logarithm finding algorithms [28], and Kitaev's algorithm [17] for the Abelian stabilizer problem are all special cases of this general solution. Fourier sampling was also successfully used to solve the closely related HIDDEN TRANSLATION PROBLEM (HTP). Here we are given two injective functions f_0 and f_1 from an Abelian group G to some finite set such that, for some group element u, the equality $f_0(x+u) = f_1(x)$ holds for every x. The task is to find the *translation* u. Indeed, the HTP is an instance of the HSP in the semi-direct product $G \rtimes \mathbb{Z}_2$ where the hiding function is $f(x,b) = f_b(x)$. In that group f hides the subgroup $H = \{(0,0),(u,1)\}$. Ettinger and Høyer [7] have shown that the HTP can be solved in cyclic groups $G = \mathbb{Z}_n$ by a two-step procedure: an efficient quantum algorithm followed by an exponential classical stage without further queries. They achieved this by applying Fourier sampling in the Abelian direct product group $G \times \mathbb{Z}_2$. Friedl, Ivanyos, Magniez, Santha and Sen [9] have shown that HTP can be solved by an efficient quantum algorithm in some groups of fixed exponent, for instance when $G = \mathbb{Z}_p^n$ for any fixed prime number p. This gives a quantum polynomial time algorithm for the HSP in $G \rtimes \mathbb{Z}_2$ using the quantum reduction of HSP to HTP [7]. In strong opposition to these positive results, a natural generalization of the HSP has exponential quantum query complexity even in Abelian groups. In this generalization, the function f may not be distinct on different cosets. Indeed, the unordered database search problem can be reduced to the decision problem whether a function on a cyclic group has a non-trivial period or not.

Two different extensions of property testing were studied in the quantum context. The first approach consists in testing quantum devices by classical procedures. Mayers and Yao [19] have designed tests for deciding if a photon source is perfect. These tests guarantee that if a source passes them, it is adequate for the security of the Bennett-Brassard [2] quantum key distribution protocol. Dam, Magniez, Mosca and Santha [6] considered the design of testers for quantum gates. They showed the possibility of classically testing quantum processes and they provided the first family of classical tests allowing one to estimate the reliability of quantum gates. In a subsequent paper byMagniez, Mayers, Mosca and Ollivier [20], both results were generalized for testing quantum circuits in polynomial time.

The second approach considers testing deterministic functions by a quantum procedure. Quantum testing of deterministic function families was introduced by Buhrman, Fortnow, Newman, and Röhrig [3], and they have constructed efficient quantum testers for several properties. One of their nicest contributions is that they have considered the possibility that quantum testing of periodicity might be easier than the corresponding decision problem. Indeed, they succeeded in giving a polynomial time quantum tester for periodic functions over $\mathbb{Z}_2^n$. They have also proved that any classical tester requires exponential time for this task. Independently and earlier, while working on the extension of the HSP to periodic functions over $\mathbb{Z}$ which may be many-to-one in each period, Hales and Hallgren [15] have given the essential ingredients for constructing a polynomial time quantum tester for periodic functions over the cyclic group $\mathbb{Z}_n$. But contrarily to [3], their result is not stated in the testing context.

In this work, we construct efficient or query efficient quantum testers for two *hidden group properties*, that is, existential properties over groups whose decision problems have exponential quantum query complexity. We also introduce a new technique in the analysis of quantum testers.

Our main contribution is a generalization of the periodicity property studied in [15, 3]. For any finite group G and any normal subgroup K, a function f satisfies the property LARGER-PERIOD(K) if there exists a normal subgroup $H > K$ for which f is H-periodic (*i.e.* $f(xh) = f(x)$ for all $x \in G$ and $h \in H$). For this property, we give an efficient tester whenever G is Abelian (**Theorem 3.1**). This result generalizes the previous periodicity testers in three aspects. First, we work in any finite Abelian group G, while previously only $G = \mathbb{Z}_n$ [15] and $G = \mathbb{Z}_2^n$ [3] were considered. Second, the property we test is parametrized by some known normal subgroup K, while previously only the case $K = \{0\}$ was considered. Third, our query complexity is only linear in the inverse of the distance parameter, whereas the previous works have a quadratic dependence. Our result implies that the period finding algorithm of [15] has, in fact, query complexity linear in the inverse of the distance parameter, as opposed to only quadratic dependence proved in that paper. These improvements are possible due to our more transparent analysis. We refine the standard method of classical testing, which consists in showing that a function f that passes the test can be corrected into another function g that has the desired property, and which is close to f. The novelty of our approach is that here the correction is not done directly; it involves an intermediate correction via a probabilistic function.

The main technical ingredient of the periodicity test in Abelian groups is efficient *Fourier sampling*. This procedure remains a powerful tool also in non-Abelian groups [16, 13]. Unfortunately, currently no efficient implementation is known for it in general groups. Therefore, when dealing with non-Abelian groups, our aim is to construct query efficient testers. We construct query efficient testers, with query complexity linear in the inverse of the distance parameter, for two properties. First, we show that the tester used for LARGER-PERIOD(K) in Abelian groups yields a query efficient tester when G is any finite group and K any normal subgroup (**Theorem 3.2**). Second, we study in any finite group G the property COMMON-COSET-RANGE(k,t) (for short CCR(k,t)). Let f, g be two functions from G to a finite set S. By definition, (f,g) satisfies CCR(k,t) if f and g have identical ranges within each coset for a normal subgroup $H \trianglelefteq G$ of size at most k, and which is the normal closure of a subgroup generated by at most t elements. For an Abelian group G with exponent k, CCR$(k,1)$ can be thought of as a generalization of the hidden translation property. The heart of the tester for CCR(k,t) is again Fourier sampling applied in the direct product group $G \times \mathbb{Z}_2$. Our tester is query efficient in any group if k is polylogarithmic in the size of the group (**Theorem 5.1**).

Different lower bounds can be proven on the query complexity of CCR(k,t). One observes easily that unordered database search can be reduced to CCR$(2,1)$ in $\mathbb{Z}_2^n$, and therefore CCR$(2,1)$ is quantumly exponentially hard to decide. Moreover, we show that classical testers also require an exponential number of queries for this problem (**Theorem 6.1**). We show this by adapting the techniques of [3], who proved the analogous result for classical testers for periodicity.

Independently from our work, Lisa Hales has also obtained in her thesis [14] polynomial time quantum testers for periodic functions over any finite Abelian group, although her results, just as those of [15], are not stated explicitly in the testing context. Her proof technique is also closely related to that of [15], and the query complexity of her tester remains quadratic in the inverse of the distance parameter. She pointed out to us that our periodicity tester can be generalized to the integers. For the sake of completeness, with her permission, we include here in Section 4 this efficient periodicity tester over the integers $\mathbb{Z}$. We present a complete correctness proof for this tester (**Theorem 4.1**) by combining Hales's ideas with our earlier periodicity testing results about finite Abelian groups.

2. Preliminaries

2.1. Fourier sampling over Abelian groups

For a finite set D, let the *uniform superposition over* D be $|D\rangle = \frac{1}{\sqrt{|D|}} \sum_{x \in D} |x\rangle$, and for a function f from D to a finite set S, let the *uniform superposition of* f be $|f\rangle = \frac{1}{\sqrt{|D|}} \sum_{x \in D} |x\rangle |f(x)\rangle$. For two functions f, g from D to S, their *distance* is $\mathsf{dist}(f,g) = |\{x \in D : f(x) \neq g(x)\}|/|D|$. The following proposition describes the relation between the distance of two functions and the distance between their uniform superpositions. In this paper, $\|\cdot\|$ denotes the ℓ_2-norm and $\|\cdot\|_1$ denotes the ℓ_1-norm of a vector.

Proposition 2.1. For functions f, g defined on the same finite set, $\mathsf{dist}(f,g) = \frac{1}{2} \left\| |f\rangle - |g\rangle \right\|^2$.

Let G be a finite Abelian group and $H \leq G$ a subgroup. The coset of $x \in G$ with respect to H is denoted by $x + H$. We use the notation $<X>$ for the subgroup generated by a subset X of G. 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 $H^\perp = \{y \in G : \forall h \in H, \chi_y(h) = 1\}$, and we set $|H^\perp(x)\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y \in H^\perp} \chi_y(x) |y\rangle$. The *quantum Fourier transform* over G, QFT_G, is the unitary transformation defined as follows: For every $x \in G$, $\mathrm{QFT}_G |x\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(x) |y\rangle$. The main property about QFT_G that we use is that it maps the uniform superposition on the coset $x + H$ to the uniform superposition on $H^\perp$, with appropriate phases.

Proposition 2.2. Let G be a finite Abelian group, $x \in G$ and $H \leq G$. Then $|x + H\rangle \xrightarrow{\mathrm{QFT}_G} |H^\perp(x)\rangle$.

The following well known quantum Fourier sampling algorithm will be used as a building block in our quantum testers. In the algorithm, $f : G \to S$ is given by a quantum oracle.

Fourier sampling$^f(G)$
1. Create zero-state $|0\rangle_G|0\rangle_S$.
2. Create the superposition $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle_G$ in the first register.
3. Query function f.
4. Apply QFT_G on the first register.
5. Observe and then output the first register.

The above algorithm is actually the main ingredient for solving the HSP on Abelian groups with hiding function f.

2.2. Property testing

Let D and S be two finite sets and let $\mathcal{C}$ be a family of functions from D to S. Let $\mathcal{F} \subseteq \mathcal{C}$ be the subfamily of functions of interest, that is, the set of functions possessing the desired property. In the testing problem, one is interested in distinguishing functions $f : D \to S$, given by an oracle, which belong to $\mathcal{F}$, from functions which are far from every function in $\mathcal{F}$.

Definition 2.1. (δ-tester)
Let $\mathcal{F} \subseteq \mathcal{C}$ and $0 \leq \delta < 1$. A *quantum* (resp. *probabilistic*) *δ-tester* for $\mathcal{F}$ on $\mathcal{C}$ is a quantum (resp. probabilistic) oracle Turing machine T such that, for every $f \in \mathcal{C}$,
1. if $f \in \mathcal{F}$ then $\mathsf{Pr}[T^f \text{ accepts}] = 1$,
2. if $\mathsf{dist}(f, \mathcal{F}) > \delta$ then $\mathsf{Pr}[T^f \text{ rejects}] \geq 2/3$,

where the probabilities are taken over the observation results (resp. the coin tosses) of T.

By our definition, a tester always accepts functions having the property $\mathcal{F}$. We may also consider testers with *two-sided error*, where this condition is relaxed, and one requires only that the tester accept functions from $\mathcal{F}$ with probability at least 2/3. Of course, the choice of the success probability $2/3$ is arbitrary, and can be replaced by γ for any constant $1/2 < \gamma < 1$.

3. Periodicity in finite groups

In this section, we design quantum testers for testing periodicity of functions from a finite group G to a finite set S. For a normal subgroup $H \trianglelefteq G$, a function $f : G \to S$ is H*-periodic* if for all $x \in G$ and $h \in H$, $f(xh) = f(x)$. Notice that our definition describes formally right H-periodicity, but this coincides with left H-periodicity since H is normal. The set of H-periodic functions is denoted by $\mathrm{Per}(H)$. For a known normal subgroup H, testing if $f \in \mathrm{Per}(H)$ can be easily done classically by sampling random elements $x \in G$ and $h \in H$ and verifying that $f(xh) = f(x)$, as can be seen from the following proposition.

Proposition 3.1. Let G be a finite group, $H \trianglelefteq G$ and $f : G \to S$ a function. Let $\eta = \mathsf{Pr}_{x \in G, h \in H}[f(xh) \neq f(x)]$. Then, $\eta/2 \leq \mathsf{dist}(f, \mathrm{Per}(H)) \leq 2\eta$.

On the other hand, testing if a function has a non-trivial period is classically hard even in $\mathbb{Z}_2^n$ [3]. The main result of this section is that we can test query efficiently by a quantum algorithm an even more general property: Does a function have a strictly larger period than a known normal subgroup $K \trianglelefteq G$? Indeed, we test the family

$$\text{LARGER-PERIOD}(K) = \{f : G \to S \quad | \quad \exists H \trianglelefteq G,\ H > K \text{ and } f \text{ is } H\text{-periodic}\}.$$

Moreover when G is Abelian, our tester is efficient.

For the sake of clarity we first present the result for Abelian groups. This enables us to highlight the new technique that we use. The standard way to ensure that the functions the tester accepts with high probability are close to functions having the desired property, is based on a direct correction process. This process has to produce a corrected function which has the desired property and is close to the original function. This is the approach taken by [15, 3, 14]. The novelty of our approach is that the correction is not done directly; it involves an intermediate corrected probabilistic function. This two-step process makes a more refined and cleaner analysis possible. We prove that our tester works in any finite group, and moreover, the query complexity of our algorithm turns out to be linear in the inverse of the distance parameter, unlike the quadratic dependence of the other works.

3.1. Finite Abelian case

In this subsection, we give our algorithm for testing periodicity in finite Abelian groups. Theorem 3.1 below states that this algorithm is efficient. The algorithm assumes that G has an efficient exact quantum Fourier transform. When G only has an efficient approximate quantum Fourier transform, the algorithm has two-sided error. Efficient implementations of approximate quantum Fourier transforms exist in every finite Abelian group [17].

Test Larger period$^f(G, K, \delta)$

1. $N \leftarrow 4\log(|G|)/\delta$.
2. For $i = 1, \ldots, N$ do $y_i \leftarrow$ **Fourier sampling**$^f(G)$.
3. Accept iff $<y_i>_{1 \leq i \leq N} < K^{\perp}$.

Theorem 3.1. For a finite set S, finite Abelian group G, subgroup $K \leq G$, and $0 < \delta < 1$, **Test Larger period**(G, K, δ) is a δ-tester for LARGER-PERIOD(K) on the family of all functions from G to S, with $O(\log(|G|)/\delta)$ query complexity and $(\log(|G|)/\delta)^{O(1)}$ time complexity.

Let S be a finite set and G a finite Abelian group. We describe now the ingredients of our two-step correction process. First, we generalize the notion of uniform superposition of a function to uniform superposition of a probabilistic function. By definition, a *probabilistic function* is a mapping $\mu : x \mapsto \mu_x$ from the domain G to probability distributions on S. For every $x \in G$, define the unit ℓ_1-norm vector

$|\mu_x\rangle = \sum_{s\in S}\mu_x(s)|s\rangle$. Then the uniform superposition of μ is defined as $|\mu\rangle = \frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|\mu_x\rangle$. Notice that $|\mu\rangle$ has unit ℓ_2-norm when μ is a (deterministic) function, otherwise its ℓ_2-norm is smaller.

A function $f : G \to S$ and a subgroup $H \le G$ naturally define an H-periodic probabilistic function $\mu^{f,H}$, where $\mu_x^{f,H}(s) = \frac{|f^{-1}(s)\cap(x+H)|}{|H|}$. The value $\mu_x^{f,H}(s)$ is the proportion of elements in the coset $x+H$ where f takes the value s. Observe that when f is H-periodic $|\mu^{f,H}\rangle = |f\rangle$, and so $\left\||\mu^{f,H}\rangle\right\| = 1$, otherwise $\left\||\mu^{f,H}\rangle\right\| < 1$.

First, we give the connection between the probability that **Fourier sampling** outputs an element outside $H^\perp$, and the distance between $|f\rangle$ and $|\mu^{f,H}\rangle$.

Lemma 3.1. $\left\||f\rangle - |\mu^{f,H}\rangle\right\|^2 = \mathsf{Pr}[$**Fourier sampling**$^f(G)$ outputs $y \notin H^\perp]$.

Proof:
Since $y \notin H^\perp$ iff $y \in \{0\}^\perp - H^\perp$, the probability term is

$$\left\| \frac{1}{\sqrt{|G|}}\sum_{x\in G}|\{0\}^\perp(x)\rangle|f(x)\rangle - \frac{1}{\sqrt{|G||H|}}\sum_{x\in G}|H^\perp(x)\rangle|f(x)\rangle \right\|^2.$$

We apply the inverse quantum Fourier transform QFT_G^{-1}, which is ℓ_2-norm preserving, to the first register in the above expression. The probability becomes $\left\| |f\rangle - \frac{1}{\sqrt{|G||H|}}\sum_{x\in G}|x+H\rangle|f(x)\rangle \right\|^2$, using Proposition 2.2. Changing the variables, the second term inside the norm is

$$\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle\frac{1}{|H|}\sum_{h\in H}|f(x-h)\rangle = \frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle\frac{1}{|H|}\sum_{h\in H}|f(x+h)\rangle,$$

where the equality holds because H is a subgroup of G. We conclude by observing that, by definition of $\mu^{f,H}$, $\frac{1}{|H|}\sum_{h\in H}|f(x+h)\rangle = \sum_{s\in S}\mu_x^{f,H}(s)|s\rangle = |\mu_x^{f,H}\rangle$. □

Second, we give the connection between $\mathsf{dist}(f, \mathrm{Per}(H))$ and the distance between $|f\rangle$ and $|\mu^{f,H}\rangle$.

Lemma 3.2. $\mathsf{dist}(f, \mathrm{Per}(H)) \le 2\left\||f\rangle - |\mu^{f,H}\rangle\right\|^2$.

Proof:
It will be useful to rewrite $|f\rangle$ as a probabilistic function $\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle\sum_{s\in S}\delta_x^f(s)|s\rangle$, where $\delta_x^f(s) = 1$ if $f(x) = s$ and 0 otherwise. Let us define the H-periodic function $g : G \to S$ by $g(x) = \mathsf{Maj}_{h\in H}\, f(x+h)$, where ties are decided arbitrarily. In fact, g is the correction of f with respect to H-periodicity. Proposition 2.1 and the H-periodicity of g imply $\mathsf{dist}(f, \mathrm{Per}(H)) \le \frac{1}{2}\left\||f\rangle - |g\rangle\right\|^2$. We will show that $\left\||g\rangle - |\mu^{f,H}\rangle\right\| \le \left\||f\rangle - |\mu^{f,H}\rangle\right\|$. This will allow us to prove the desired statement using the triangle inequality. Observe that for any function $h : G \to S$, we have

$$\left\||h\rangle - |\mu^{f,H}\rangle\right\|^2 = \frac{1}{|G|}\sum_{x\in G}\sum_{s\in S}|\delta_x^h(s) - \mu_x^{f,H}(s)|^2. \quad (1)$$

Moreover for every $x \in G$, one can establish

$$\begin{aligned}\sum_{s\in S}|\delta^g_x(s) - \mu^{f,H}_x(s)|^2 &= |1-\mu^{f,H}_x(g(x))|^2 + \sum_{s\neq g(x)}(\mu^{f,H}_x(s))^2 \\ &= 1 + \sum_{s\in S}(\mu^{f,H}_x(s))^2 - 2\mu^{f,H}_x(g(x)) \\ &\leq 1 + \sum_{s\in S}(\mu^{f,H}_x(s))^2 - 2\mu^{f,H}_x(f(x)) \\ &= \sum_{s\in S}|\delta^f_x(s) - \mu^{f,H}_x(s)|^2,\end{aligned} \tag{2}$$

where the inequality follows from $\mu^{f,H}_x(f(x)) \leq \mu^{f,H}_x(g(x))$, which in turn follows immediately from the definition of g.

From (1) and (2) we get that $\big\||g\rangle - |\mu^{f,H}\rangle\big\| \leq \big\||f\rangle - |\mu^{f,H}\rangle\big\|$, which completes the proof. □

Lemmas 3.1 and 3.2 together can be interpreted as the robustness [25, 26] in the quantum context [6] of the property that **Fourier sampling**$^f(G)$ outputs only $y \in H^\perp$: if f does not satisfy exactly the property but with error probability less than δ, then f is 2δ-close to a function that satisfies exactly the property. Using this fact, we can now prove Theorem 3.1.

Proof:
If $f \in$ LARGER-PERIOD(K), that is f is H-periodic for some $H > K$, then the quantum state before the observation of **Fourier sampling**$^f(G)$ is

$$\begin{aligned}& (\mathrm{QFT}_G \otimes I)\left(\frac{1}{\sqrt{|G|}}\sum_{x\in G}|x\rangle|f(x)\rangle\right) \\ = \;& (\mathrm{QFT}_G \otimes I)\left(\frac{1}{\sqrt{|G||H|}}\sum_{x\in G}|x+H\rangle|f(x)\rangle\right) \\ = \;& \frac{1}{\sqrt{|G||H|}}\sum_{x\in G}|H^\perp(x)\rangle|f(x)\rangle.\end{aligned}$$

Above, I denotes the $|S| \times |S|$ identity matrix. Therefore, the procedure **Fourier sampling**$^f(G)$ only outputs elements in $H^\perp$. Since $H^\perp < K^\perp$, the test always accepts.

Let f be now δ-far from the family LARGER-PERIOD(K). Then for every $H > K$, $\mathsf{dist}(f, \mathrm{Per}(H)) > \delta$, and by Lemmas 3.1 and 3.2, Pr[**Fourier sampling**$^f(G)$ outputs $y \notin H^\perp$] $> \delta/2$. Using these inequalities, we can upper bound the acceptance probability of the test as follows.

$$\begin{aligned}& \mathsf{Pr}[<y_i>_{1\leq i\leq N} < K^\perp] \\ = \;& \mathsf{Pr}[\exists H > K, <y_i>_{1\leq i\leq N} \leq H^\perp] \\ = \;& \mathsf{Pr}[\exists x \in G - K, y_i \in <K,x>^\perp \text{ for } 1 \leq i \leq N] \\ \leq \;& |G| \cdot \left(\mathsf{Max}_{H>K}\left\{\mathsf{Pr}[\textbf{Fourier sampling}^f(G) \text{ outputs } y \in H^\perp]\right\}\right)^N \\ < \;& |G|(1-\delta/2)^N \leq 1/3.\end{aligned}$$

□

3.2. Finite general case

We now give our algorithm for testing periodicity in general finite groups. Our main tool continues to be the quantum Fourier transform (over a general finite group). Our notation and techniques are similar to those in [16, 13]. We start with a few definitions. For any $d \times d$ matrix M, define $|M\rangle = \sqrt{d}\sum_{1\leq i,j\leq d} M_{i,j}|M,i,j\rangle$. Let G be any finite group and let $\widehat{G}$ be a complete set of finite dimensional inequivalent irreducible unitary representations of G. Thus, for any $\rho \in \widehat{G}$ of dimension d_ρ and $x \in G$, $|\rho(x)\rangle = \sqrt{d_\rho}\sum_{1\leq i,j\leq d_\rho}(\rho(x))_{i,j}|\rho,i,j\rangle$. The *quantum Fourier transform* over G is the unitary transformation defined as follows: For every $x \in G$, $\mathrm{QFT}_G|x\rangle = \frac{1}{\sqrt{|G|}}\sum_{\rho\in\widehat{G}}|\rho(x)\rangle$. For any $H \trianglelefteq G$ set $H^\perp = \{\rho \in \widehat{G} : \forall h \in H, \rho(h) = I_{d_\rho}\}$, where I_{d_ρ} is the $d_\rho \times d_\rho$ identity matrix. Let $|H^\perp(x)\rangle = \sqrt{\frac{|H|}{|G|}}\sum_{\rho\in H^\perp}|\rho(x)\rangle$.

Proposition 3.2. Let G be a finite group, $x \in G$ and $H \trianglelefteq G$. Then $|xH\rangle \xrightarrow{\mathrm{QFT}_G} |H^\perp(x)\rangle$.

Proof:
We first prove that when H is normal, the matrix $L = \sum_{h\in H}\rho(h)$ is $|H| \cdot I_{d_\rho}$ if $\rho \in H^\perp$, and 0 otherwise. By definition of $H^\perp$, the condition $\rho \in H^\perp$ implies $\rho(h) = I_{d_\rho}$ for every $h \in H$, which gives the first part of the above. Now suppose that $\rho \notin H^\perp$. Observe that since H is normal, L commutes with $\rho(x)$ for every $x \in G$. Therefore according to Schur's lemma (see for instance [27, Chap. 2, Prop. 4]), $L = \lambda \cdot I_{d_\rho}$ for some $\lambda \in \mathbb{C}$. Since $\rho \notin H^\perp$, we can pick some $h \in H$ such that $\rho(h) \neq I_{d_\rho}$; then applying $\rho(h) \cdot L = L$ gives a contradiction if $\lambda \neq 0$. This proves the second part of the above.

We now complete the proof of the proposition as follows.

$$\begin{aligned}\mathrm{QFT}_G|xH\rangle &= \frac{1}{\sqrt{|H|}}\sum_{h\in H}\mathrm{QFT}_G|xh\rangle = \frac{1}{\sqrt{|H||G|}}\sum_{h\in H}\sum_{\rho\in\widehat{G}}|\rho(xh)\rangle \\ &= \frac{1}{\sqrt{|H||G|}}\sum_{\rho\in\widehat{G}}|\sum_{h\in H}\rho(xh)\rangle = \frac{1}{\sqrt{|H||G|}}\sum_{\rho\in\widehat{G}}|\rho(x)\cdot L\rangle \\ &= \sqrt{\frac{|H|}{|G|}}\sum_{\rho\in H^\perp}|\rho(x)\rangle = |H^\perp(x)\rangle,\end{aligned}$$

where the penultimate equality follows from the above property of the matrix L. □

Test Larger period$^f(G, K, \delta)$
1. $N \leftarrow 4\log(|G|)/\delta$.
2. For $i = 1, \ldots, N$ do $\rho_i \leftarrow$ **Fourier sampling**$^f(G)$.
3. Accept iff $\cap_{1\leq i\leq N}\ker\rho_i > K$.

In the above algorithm, **Fourier sampling**$^f(G)$ is as before, except that we only observe the representation ρ, and not the indices i, j. Thus, the output of **Fourier sampling**$^f(G)$ is an element of $\widehat{G}$. K is assumed to be a normal subgroup of G. For any $\rho \in \widehat{G}$, $\ker\rho$ denotes its kernel.

We now prove the robustness of the property that **Fourier sampling**$^f(G)$ outputs only $\rho \in H^\perp$, for any finite group G, normal subgroup H and H-periodic function f. This robustness corresponds to Lemmas 3.1 and 3.2 of the Abelian case.

Lemma 3.3. Let $f : G \to S$ and $H \trianglelefteq G$. Then

$$\mathsf{dist}(f, \mathrm{Per}(H)) \leq 2 \cdot \mathsf{Pr}[\textbf{Fourier sampling}^f(G) \text{ outputs } \rho \notin H^\perp].$$

Proof:
The proof has the structure of the Abelian case (see Lemmas 3.1 and 3.2). Define $|\mu^{f,H}\rangle$ in the same way. Observe that Lemma 3.2 is true in a general finite group. The proof of Lemma 3.1 for the general case follows the one for the Abelian case. The only difference is that we have to use Proposition 3.2 instead of Proposition 2.2. □

Our second theorem states that **Test Larger period** is a query efficient tester for LARGER-PERIOD(K) for any finite group G.

Theorem 3.2. For a finite set S, finite group G, normal subgroup $K \trianglelefteq G$, and $0 < \delta < 1$, **Test Larger period**(G, K, δ) is a δ-tester for LARGER-PERIOD(K) on the family of all functions from G to S, with $O(\log(|G|)/\delta)$ query complexity.

Proof:
The proof is similar to that of the Abelian case. Note that, while upper bounding the acceptance probability of the test when f is δ-far from LARGER-PERIOD(K), one has to consider only those normal subgroups H of the form $H =$ Normal-closure($<K, x>$), where x ranges over $G - K$. □

4. Periodicity on $\mathbb{Z}$

We address here the problem of periodicity testing when the group is finitely generated Abelian, but possibly infinite. For $\mathbb{Z}$, it is still possible to test if a function is periodic. The proof involves Fourier sampling methods of [15] and the following lemma which was communicated to us by Hales.

Lemma 4.1. Let G be a finite Abelian group, $f : G \to S$ a function and $\delta > 0$. Set $N = 4(\log|G|)^2/\delta$. For $i = 1, \ldots, N$, let $y_i =$ **Fourier sampling**$^f(G)$ and set $Y = <y_i>_{1 \leq i \leq N}$. Then $\mathsf{Pr}[f$ is δ-close to $\mathrm{Per}(Y^\perp)] \geq 2/3$.

Proof:
Let E be the complementary event $\mathsf{dist}(f, \mathrm{Per}(Y^\perp)) > \delta$. Then E is realized exactly when there is a subgroup $H \leq G$ such that $\mathsf{dist}(f, \mathrm{Per}(H)) > \delta$ and $H^\perp = Y$. Therefore

$$\begin{aligned} \mathsf{Pr}[E] &\leq \sum_{H \leq G} \mathsf{Pr}[\mathsf{dist}(f, \mathrm{Per}(H)) > \delta \text{ and } H^\perp = Y] \\ &\leq \sum_{H \leq G, \mathsf{dist}(f, \mathrm{Per}(H)) > \delta} (\mathsf{Pr}[y_1 \in H^\perp])^N. \end{aligned}$$

The number of subgroups of G is at most $|G|^{\log|G|}$, and since by Lemmas 3.1 and 3.2 the probability that y_1 is in $H^\perp$ is at most $1 - \delta/2$, the probability $\mathsf{Pr}[E]$ is upper bounded by $|G|^{\log|G|}(1-\delta/2)^N \leq 1/3$. □

For the sake of clarity, we now restrict ourselves to functions defined over the natural numbers $\mathbb{N}$. For any positive integer T, we identify the set $\{0,\ldots,T-1\}$ with $\mathbb{Z}_T$ in the usual way. We recast **Test Larger period**(G,K,δ) in the arithmetic formalism when $G=\mathbb{Z}_T$ and $K=<p_0>\leq G$, for some p_0 dividing T.

> **Test Dividing period**$^f(T,p_0,\delta)$
> 1. $N \leftarrow 4\log(T)/\delta$.
> 2. For $i=1,\ldots,N$ do $y_i \leftarrow$ **Fourier sampling**$^f(\mathbb{Z}_T)$ and compute the reduced fraction $\frac{a_i}{b_i}$ of $\frac{y_i}{T}$.
> 3. $p \leftarrow \mathrm{lcm}\{b_i : 1\leq i\leq N\}$.
> 4. Accept iff p divides $T$and is less than p_0.

Then Lemma 4.1 can be also rewritten as follows.

Corollary 4.1. Let $T\geq 1$ be an integer, $f:\mathbb{Z}_T\to S$ a function and $\delta>0$. Set $N=4(\log T)^2/\delta$. For $i=1,\ldots,N$ let $y_i=$ **Fourier sampling**$^f(\mathbb{Z}_T)$, $\frac{a_i}{b_i}$ be the reduced fraction of $\frac{y_i}{T}$, and set $p=\mathrm{lcm}\{b_i : 1\leq i\leq N\}$. Then $\Pr[f$ is δ-close to $\mathrm{Per}(<p>)]\geq 2/3$.

We want to test periodicity in the family of functions defined on $\mathbb{N}$. To make the problem finite, we fix an upper bound on the period. Then, a function $f:\{0,\ldots,T-1\}\to S$ is *q-periodic*, for $1\leq q<T$, if $f(x+aq)=f(x)$, for every $x,a\in\mathbb{N}$ such that $x+aq<T$. The problem we now want to test is if there exists a period less than some given number t. More precisely, we define for integers $2\leq t\leq T$,

$$\text{INT-PERIOD}(T,t) = \{f : \{0,\ldots,T-1\}\to S \mid \exists q : 1\leq q<t \text{ and } f \text{ is } q\text{-periodic}\}.$$

Here we do not require that q divides T since we do not have any finite group structure.

> **Test Integer period**$^f(T,t,\delta)$
> 1. $N \leftarrow \Omega((\log T)^2/\delta)$.
> 2. For $i=1,\ldots,N$ do $y_i \leftarrow$ **Fourier sampling**$^f(\mathbb{Z}_T)$, and use the continued fractions method to round $\frac{y_i}{T}$ to the nearest fraction $\frac{a_i}{b_i}$ with $b_i<t$.
> 3. $p \leftarrow \mathrm{lcm}\{b_i : 1\leq i\leq N\}$.
> 4. If $p\geq t$, reject.
> 5. $T_p \leftarrow \lfloor T/p\rfloor p$.
> 6. $M \leftarrow \Omega(1/\delta)$.
> 7. For $i=1,\ldots,M$ let $a_i,x_i \in_{\mathrm{R}} \mathbb{Z}_{T_p}$.
> 8. Accept iff $\frac{1}{M}|\{i : f(x_i+a_ip \mod T_p)\neq f(x_i)\}|<\frac{\delta}{3}$.

Theorem 4.1. For a finite set S, $0 < \delta < 1$, and integers $2 \leq t \leq T$ such that $T/(\log T)^4 = \Omega((t \log t/\delta)^2)$, **Test Integer period**(T, t, δ) is a δ-tester with two-sided error for INT-PERIOD(T, t) on the family of functions from $\{0, \ldots, T-1\}$ to S, with $O((\log T)^2/\delta)$ query complexity and $(\log T/\delta)^{O(1)}$ time complexity.

Proof:
First suppose that f is δ-far from INT-PERIOD(T, t). In Step 4 if $p \geq t$, we reject. If $p < t$, then f is $(15\delta/16)$-far from $\mathrm{Per}(<p>)$ in the group $\mathbb{Z}_{T_p}$. Indeed $\mathsf{dist}(f, \text{INT-PERIOD}(T, t)) \leq \mathsf{dist}(f|_{\{0,\ldots,T_p-1\}}, \mathrm{Per}(<p>)) + t/T$, where the latter term is upper bounded by $\delta/16$. Thus, from Proposition 3.1 and Chernoff bounds, Step 8 accepts with probability less than $1/3$.

Now suppose that $f \in$ INT-PERIOD(T, t), and let q be the period of f, then $1 \leq q < t$. Define $T_q = \lfloor T/q \rfloor q$. Let D (resp. D') denote the distribution on b_1 after Step 2 of **Test Dividing period**$^f(T_q, q, \delta)$ (resp. **Test Integer period**$^f(T, t, \delta)$). Then from [14, Chapter 5, Lemma 3], we get that $\|D - D'\|_1 \leq O(t \log t/\sqrt{T}) = O(1/N)$. Therefore the total variation distance between the corresponding distributions of $(b_1, \ldots, b_N)$, that is $\left\|D^{\otimes N} - D'^{\otimes N}\right\|_1$, is an arbitrarily small constant. Thus, with probability a constant arbitrarily close to 1, $p \mid q$ and, by Corollary 4.1, f is $(\delta/16)$-close to $\mathrm{Per}(<p>)$ in the group $\mathbb{Z}_{T_q}$. When these events indeed occur, by an argument similar to the one used in the above paragraph, f is also $(\delta/8)$-close to $\mathrm{Per}(<p>)$ in the group $\mathbb{Z}_{T_p}$. From Proposition 3.1 and Chernoff bounds, Step 8 accepts with probability arbitrarily close to 1. Thus, the overall acceptance probability of **Test Integer period**$^f(T, t, \delta)$ is at least $2/3$. □

5. Common Coset Range

In this section, G denotes a finite group and S a finite set. Let f_0, f_1 be functions from G to S. For a normal subgroup $H \trianglelefteq G$, we say that f_0 and f_1 are *H-similar* if on all cosets of H the ranges of f_0 and f_1 are the same, that is, the multiset equality $f_0(xH) = f_1(xH)$ holds for every $x \in G$. Consider the 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 denote by $\mathrm{Range}(H)$ the set of functions f such that f_0 and f_1 are H-similar. We say that H is *t-generated*, for some positive integer t, if it is the normal closure of a subgroup generated by at most t elements. The aim of this section is to establish that for any positive integers k and t, the family COMMON-COSET-RANGE(k, t) (for short CCR(k, t)), defined as

$$\text{CCR}(k, t) = \{f : G \times \mathbb{Z}_2 \to S \mid \exists H \trianglelefteq G, |H| \leq k, H \text{ is } t\text{-generated}, f_0 \text{ and } f_1 \text{ are } H\text{-similar}\},$$

can be tested by the following quantum test. Note that a subgroup of size k is always generated by at most $\log k$ elements, therefore we always assume that $t \leq \log k$. In the testing algorithm, we assume that we have a quantum oracle for the function $f : G \times \mathbb{Z}_2 \to S$.

Test Common coset range$^f(G, k, t, \delta)$

1. $N \leftarrow 2kt\log(|G|)/\delta$.
2. For $i = 1, \ldots, N$ do $(\rho_i, b_i) \leftarrow$ **Fourier sampling**$^f(G \times \mathbb{Z}_2)$.
3. Accept iff
   $\exists H \trianglelefteq G, |H| \leq k, H$ is t-generated and $\quad \forall i\ (b_i = 1 \implies \rho_i \notin H^\perp)$.

We first prove the robustness of the property that when **Fourier sampling**$^f(G \times \mathbb{Z}_2)$ outputs $(\rho, 1)$, where G is any finite group, $H \trianglelefteq G$ and $f \in \mathrm{Range}(H)$, then ρ is not in $H^\perp$.

Lemma 5.1. Let S be a finite set and G a finite group. Let $f : G \times \mathbb{Z}_2 \rightarrow S$ and $H \trianglelefteq G$. Then $\mathsf{dist}(f, \mathrm{Range}(H)) \leq |H| \cdot \mathsf{Pr}[$**Fourier sampling**$^f(G \times \mathbb{Z}_2)$ outputs $(\rho, 1)$ such that $\rho \in H^\perp]$.

Proof:
We use the notations of Section 3.1 for f_0 and f_1. We define $|f, H\rangle = \frac{1}{\sqrt{2}}(|\mu^{f_0,H}\rangle - |\mu^{f_1,H}\rangle)$, and the multiplicity functions $m_x^{f_b,H} = |H| \cdot \mu_x^{f_b,H}$.

First, we prove that $\mathsf{dist}(f, \mathrm{Range}(H)) \leq \| |f, H\rangle \|^2 \cdot |H|/2$. For this, we define a function $g_1 : G \rightarrow S$, the correction of f_1. The definition is done according to the cosets of H in G. For every $x \in G$ and $s \in S$, the function g_1 remains identical to f_1 in $\mathsf{Min}\{m_x^{f_0,H}(s), m_x^{f_1,H}(s)\}$ elements of xH, and the value of g_1 at those elements is s; at the remaining elements of xH, the values of g_1 are defined so as to make the multisets $f_0(xH)$ and $g_1(xH)$ equal. If we define $g_0 = f_0$ then clearly $g = (g_0, g_1) : G \times \mathbb{Z}_2 \rightarrow S$ is in $\mathrm{Range}(H)$ and $\mathsf{dist}(f, g) = \mathsf{dist}(f_1, g_1)/2$. Since in every coset xH, f_1 and g_1 have different values in $\sum_{s \in S} |m_x^{f_0,H}(s) - m_x^{f_1,H}(s)|/2$ elements, we have $\mathsf{dist}(f, g) = \frac{1}{4|G|} \sum_{x \in G/H} \sum_{s \in S} |m_x^{f_0,H}(s) - m_x^{f_1,H}(s)|$. The right hand side becomes $\| |f, H\rangle \|^2 \cdot |H|/2$ if we replace the terms $|m_x^{f_0,H}(s) - m_x^{f_1,H}(s)|$ by their respective squared values. This can only increase the right hand side since the values $m_x^{f_b,H}(s)$ are integers. Thus, $\mathsf{dist}(f, g) \leq \| |f, H\rangle \|^2 \cdot |H|/2$.

We now prove that $\| |f, H\rangle \|^2 = 2 \cdot \mathsf{Pr}[$**Fourier sampling**$^f(G \times \mathbb{Z}_2)$ outputs $(\rho, 1)$ such that $\rho \in H^\perp]$. The probability term is $\left\| \frac{1}{2\sqrt{|H||G|}} \sum_{x \in G} |H^\perp(x)\rangle |1\rangle (|f_0(x)\rangle - |f_1(x)\rangle) \right\|^2$. We apply the inverse quantum Fourier transform QFT_G^{-1}, which is ℓ_2-norm preserving, to the first register in the above expression. Using Proposition 3.2 and the fact that H is a subgroup of G, the probability becomes $\left\| \frac{1}{2|H|\sqrt{|G|}} \sum_{x \in G} \sum_{h \in H} |x\rangle |1\rangle (|f_0(xh)\rangle - |f_1(xh)\rangle) \right\|^2$. Now one can conclude the above statement and hence the lemma, since by definition of $\mu^{f_b,H}$, the equality $\frac{1}{|H|} \sum_{h \in H} |f_b(xh)\rangle = \sum_{s \in S} \mu_x^{f_b,H}(s) |s\rangle = |\mu_x^{f_b,H}\rangle$ holds. □

Our next theorem implies that $\mathrm{CCR}(k, t)$ is query efficiently testable when k is polynomial in $\log|G|$.

Theorem 5.1. For any finite set S, finite group G, integers $k \geq 1$, $1 \leq t \leq \log k$, and $0 < \delta < 1$, **Test Common coset range**(G, k, t, δ) is a δ-tester for $\mathrm{CCR}(k, t)$ on the family of all functions from $G \times \mathbb{Z}_2$ to S, with $O(kt\log(|G|)/\delta)$ query complexity.

Proof:
First consider the case $f \in \mathrm{CCR}(k,t)$, that is f is in $\mathrm{Range}(H)$ for some $H \trianglelefteq G$, $|H| \leq k$ and H is t-generated. From the proof of Lemma 5.1, we see that whenever **Fourier sampling**$^f(G \times \mathbb{Z}_2)$ outputs an element $(\rho, 1)$, then $\rho \notin H^\perp$. Thus the test always accepts.

Now, let $f : G \rightarrow S$ be δ-far from $\mathrm{CCR}(k,t)$ and let H be a t-generated normal subgroup of size at most k. Then, $\mathsf{dist}(f, \mathrm{Range}(H)) > \delta$ and by Lemma 5.1, Pr[**Fourier sampling**^{f} outputs $(\rho,1)$ such that $\rho \in H^\perp] > \delta/|H| \geq \delta/k$. Using these inequalities, we can upper bound the acceptance probability of the test, which is

$$\begin{aligned}
& \mathsf{Pr}[\exists H \trianglelefteq G, |H| \leq k, H \text{ is } t\text{-generated} \quad \forall i\ (b_i = 1 \implies \rho_i \notin H^\perp)] \\
= \ & \mathsf{Pr}\left[\begin{array}{r} \exists u_1, \dots u_t \in G,\ \text{Normal-closure}(<u_1, \dots u_t>) = H, |H| \leq k \\ \text{and} \quad \forall i\ (b_i = 1 \implies \rho_i \notin H^\perp) \end{array}\right] \\
\leq \ & |G|^t \left(\operatorname*{Max}_{\substack{H \trianglelefteq G, |H| \leq k, \\ H \text{ is } t\text{-generated}}} \left\{ \mathsf{Pr}\left[\begin{array}{r} \textbf{Fourier sampling}^f \text{ outputs } (\rho, b), \\ \text{and} \quad (b = 1 \implies \rho \notin H^\perp) \end{array}\right] \right\} \right)^N \\
< \ & |G|^t (1 - \delta/k)^N \leq 1/3.
\end{aligned}$$

□

6. A classical lower bound

Let G be any finite Abelian group with exponent k. In this section, we study the property $\mathrm{CCR}(k,1)$. We already know from Theorem 5.1 that this problem has a query efficient quantum tester if $k = (\log|G|)^{O(1)}$. We now prove an exponential lower bound on the classical testing query complexity of this problem, even for constant k. Recall that the *exponent* of a group G is the smallest integer m such that $x^m = 1$ for every element $x \in G$. We prove our lower bound by adapting the proof of Theorem 4.2 of Buhrman et al. [3]. We use Yao's minimax principle. We construct two probability distributions D'_1 and D'_2 on the set of pairs of functions (f_0, f_1), $f_0, f_1 : G \rightarrow S$, where S is a finite set of size $|S| = |G|^3$. Let D'_1 be the uniform distribution on pairs of injective functions (f_0, f_1) such that $f_1(x) = f_0(x+u)$ for some element $u \in G$ and all $x \in G$. Thus, f_0 and f_1 are $<u>$-similar, and $|<u>| \leq k$. Let D'_2 be the uniform distribution on pairs of injective functions (f_0, f_1) such that the ranges $f_0(G)$ and $f_1(G)$ are disjoint. Thus, D'_1 is supported on positive instances of $\mathrm{CCR}(k,1)$, and D'_2 is supported on negative instances of $\mathrm{CCR}(k,1)$ which are $1/2$-distant from positive instances.

As in [3], instead of working with D'_1, D'_2, we shall work with distributions D_1 and D_2 on pairs of functions (f_0, f_1), approximating distributions D'_1 and D'_2 respectively. D_1 is obtained by choosing $f_0 : G \rightarrow S$ and $u \in G$ independently and uniformly at random, and setting $f_1 : G \rightarrow S$ to be $f_1(x) = f_0(x+u)$ for all $x \in G$. Since the probability that f_0 is not injective is at most $\binom{|G|}{2}/|G|^3 = O(1/|G|)$, we get that $\|D_1 - D'_1\|_1 = O(1/|G|)$. D_2 is obtained by choosing $f_0 : G \rightarrow S$ and $f_1 : G \rightarrow S$ independently and uniformly at random. The probability that at least one of f_0, f_1 is not injective is $O(1/|G|)$. The probability that their ranges $f_0(G)$ and $f_1(G)$ are not disjoint is also $O(1/|G|)$. Thus, $\|D_2 - D'_2\|_1 = O(1/|G|)$.

By applying the proof technique of Theorem 4.2 of [3] for distributions D_1, D_2, we get the following theorem.

Theorem 6.1. Let G be a finite Abelian group and let k be the exponent of G. For testing $\mathrm{CCR}(k, 1)$ on G, any classical randomized bounded error query algorithm on G requires $\Omega(\sqrt{|G|})$ queries.

Acknowledgements

We would like to thank Lisa Hales for giving us the basic ideas about how to extend our finite Abelian case tester to $\mathbb{Z}$, and letting us include the result into this paper.

References

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

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[3] H. Buhrman, L. Fortnow, I. Newman, and H. Röhrig. Quantum property testing. In *Proc. ACM-SIAM Symposium on Discrete Algorithms*, pages 480–488, 2003.

[4] M. Blum and S. Kannan. Designing programs that check their work. *J. ACM*, 42(1):269–291, 1995.

[5] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. System Sci.*, 47(3):549–595, 1993.

[6] W. van Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM Journal of Computing*, Vol. 37, No. 2, pp. 611–629, 2007.

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

[8] E. Fischer. The art of uninformed decisions: A primer to property testing, the computational complexity. In *The Computational Complexity Column*, Bulletin of the EATCS, volume 75, pp. 97–126, 2001.

[9] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proc. 35th ACM STOC*, pages 1–9, 2003.

[10] O. Goldreich, S. Goldwasser, and D. Ron. Property testing and its connection to learning and approximation. *J. ACM*, 45(4):653–750, 1998.

[11] O. Goldreich. Combinatorial property testing – A survey. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 1998.

[12] O. Goldreich and D. Ron. Property testing in bounded degree graphs. In *Proc. 27th ACM STOC*, pages 406–415, 1997.

[13] 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.

[14] L. Hales. *The Quantum Fourier Transform and Extensions of the Abelian Hidden Subgroup Problem*. PhD thesis, University of California, Berkeley, 2002.

[15] L. Hales and S. Hallgren. An improved quantum Fourier transform algorithm and applications. In *Proc. 41st IEEE FOCS*, pages 515–525, 2000.

[16] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. *SIAM J. Comp.*, 32(4): 916-934, 2003.

[17] A. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. Technical report no. 9511026, Quantum Physics e-Print archive, 1995.

[18] M. Kiwi, F. Magniez, and M. Santha. Exact and approximate testing/correcting of algebraic functions: A survey. In *Proc. 1st SOTACS*, volume 2292, pages 30–83. LNCS, 2000.

[19] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proc. 39th IEEE FOCS*, pages 503–509, 1998.

[20] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier. Self-testing of quantum circuits. In *Proc. 33rd ICALP*, volume 4051 of *Lecture Notes in Computer Science*, pages 72–83. Verlag, 2006.

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

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

[23] D. Ron. Property testing (a tutorial). In *Handbook on Randomization*, Kluwer Press, 2001.

[24] E. G. Rieffel and W. Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, 2000.

[25] R. Rubinfeld and M. Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. Comp.*, 25(2):23–32, 1996.

[26] R. Rubinfeld. On the robustness of functional equations. *SIAM J. Comp.*, 28(6):1972–1997, 1999.

[27] J.-P. Serre. Linear representations of finite groups. In *Graduate Texts in Mathematics*, volume 42. Springer-Verlag, 1977.

[28] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Comp.*, 26(5):1484–1509, 1997.

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