Quantum Testers for Hidden Group Properties*

Katalin Friedl[1], Frédéric Magniez[2], Miklos Santha[2], and Pranab Sen[2]

[1] CAI, Hungarian Academy of Sciences, H-1111 Budapest, Hungary,
[2] CNRS–LRI, UMR 8623 Université Paris-Sud, 91405 Orsay, France,

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.

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 [3], 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 [3, 14]. The notion in its full generality was defined by Goldreich, Goldwasser and Ron and successfully applied among others to graph properties [8]. For surveys on property testing see [6].

Quantum computing (for surveys see e.g. [13]) 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

* Research partially supported by the EU 5th framework programs RESQ IST-2001-37559 and RAND-APX IST-1999-14036, and 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 T42559, T42706, and NWO-OTKA N34040 grants.

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 [15, 11]. 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 [11]. 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 recently in the quantum context. The first approach consists in testing quantum devices by classical procedures. Mayers and Yao [12] 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 [1] quantum key distribution protocol. Dam, Magniez, Mosca and Santha [4] 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.

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 [2], 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 [10] 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 [2], 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 [10, 2]. 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 1**). This result generalizes the previous periodicity testers in three aspects. First, we work in any finite Abelian group G, while previously only $G = \mathbb{Z}_n$ [10] and $G = \mathbb{Z}_2^n$ [2] 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 [10] has, in fact, query complexity linear in the inverse of the distance parameter, as opposed to only quadratic dependence proved in that paper.

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. 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 2**). Second, we study in any finite group G the property COMMON-COSET-RANGE(k, t) (for short CCR(k, t)), can be thought of as a generalization of the hidden translation property [5, 7]. 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 4**).

After finishing this paper, we learnt from Lisa Hales that in her thesis [9], she has also obtained polynomial time quantum testers for periodic functions over any finite Abelian group, although her results, just as those of [10], are not stated explicitly in the testing context. Her proof technique is also closely related to that of [10], and the query complexity of her tester remains quadratic in the inverse of the distance parameter. After hearing a talk about our results, she has 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 3**) 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

$\mathsf{dist}(f,g) = |\{x \in D : f(x) \neq g(x)\}|/|D|$. In this paper, $\|\cdot\|$ denotes the ℓ_2-norm and $\|\cdot\|_1$ denotes the ℓ_1-norm of a vector.

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

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 $x \in G$, $\mathrm{QFT}_G|x\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(x)|y\rangle$.

Proposition 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 $\mathrm{QFT}_G$ on the first register.
 5. Observe and then output the first register.
```

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 sub-family 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 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 $2/3$.

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. *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 $\mathbb{Z}_2^n$ [2]. The main result of this section is that we can test query efficiently (and efficiently in the Abelian case) 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

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

3.1 Finite Abelian Case

In this subsection, we give our algorithm for testing periodicity in finite Abelian groups. Theorem 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 [11].

```
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 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 $H \leq G$ 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. When f is H-periodic $|\mu^{f,H}\rangle = |f\rangle$, and so $\left\| |\mu^{f,H}\rangle \right\| = 1$, otherwise $\left\| |\mu^{f,H}\rangle \right\| < 1$.

The next two lemmas, which imply Theorem 1, give the connection between the distance $\left\| |f\rangle - |\mu^{f,H}\rangle \right\|^2$ and respectively the probability that **Fourier sampling** outputs an element outside $H^\perp$, and $\mathsf{dist}(f, \mathrm{Per}(H))$.

Lemma 1. $\left\| |f\rangle - |\mu^{f,H}\rangle \right\|^2 = \mathsf{Pr}[\textbf{Fourier sampling}^f(G)$ *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. 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 $\frac{1}{|H|} \sum_{h \in H} |f(x+h)\rangle = \sum_{s \in S} \mu_x^{f,H}(s)|s\rangle = |\mu_x^{f,H}\rangle$. □

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

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 1 and the H-periodicity of g imply $\mathsf{dist}(f, \mathrm{Per}(H)) \leq \frac{1}{2} \left\| |f\rangle - |g\rangle \right\|^2$. We will show that $\left\| |g\rangle - |\mu^{f,H}\rangle \right\| \leq \left\| |f\rangle - |\mu^{f,H}\rangle \right\|$. This will allow us to prove the desired statement using the triangle inequality. Observe that for any function $h : G \to S$, we have

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

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

$$\begin{aligned} \sum_{s \in S} |\delta_x^g(s) - \mu_x^{f,H}(s)|^2 &= 1 + \sum_{s \in S} (\mu_x^{f,H}(s))^2 - 2\mu_x^{f,H}(g(x)) \\ \leq 1 + \sum_{s \in S} (\mu_x^{f,H}(s))^2 - 2\mu_x^{f,H}(f(x)) &= \sum_{s \in S} |\delta_x^f(s) - \mu_x^{f,H}(s)|^2, \end{aligned} \tag{2}$$

where the inequality follows from $\mu_x^{f,H}(f(x)) \leq \mu_x^{f,H}(g(x))$, 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. $\square$

Lemmas 1 and 2 together can be interpreted as the robustness [14] in the quantum context [4] 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.

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). 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 4. *If $x \in G$ and $H \trianglelefteq G$, then $|xH\rangle \xrightarrow{\mathrm{QFT}_G} |H^\perp(x)\rangle$.*

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

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 1 and 2 of the Abelian case.

Lemma 3. *Let $f : G \to S$ and $H \trianglelefteq G$. Then*

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

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

Theorem 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.*

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 [10] and the following lemma which was communicated to us by Hales.

Lemma 4. *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 $\mathsf{Pr}(E)$ is upper bounded by

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

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

For the sake of clarity, we now restrict ourselves to functions defined over the natural numbers $\mathbb{N}$. For any integer $T \geq 1$, 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 and is less than $p_0$.
```

Then Lemma 4 can be also rewritten as follows.

Corollary 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* $\mathsf{Pr}[f$ *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 $2 \leq t \leq T$,

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

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

```
**Test Integer period**$^f(T, t, \delta)$
$N \leftarrow \Omega((\log T)^2/\delta)$.
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 $b_i < t$.
$p \leftarrow \mathrm{lcm}\{b_i : 1 \leq i \leq N\}$.
If $p \geq t$, reject.
$T_p \leftarrow \lfloor T/p \rfloor p$.
$M \leftarrow \Omega(1/\delta)$.
For $i = 1, \ldots, M$ let $a_i, x_i \in_{\mathrm{R}} \mathbb{Z}_{T_p}$.
Accept iff $\frac{1}{M}|\{i : f(x_i + a_i p \mod T_p) \neq f(x_i)\}| < \frac{\delta}{2}$.
```

Theorem 3. *For* $0 < \delta < 1$*, 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.*

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 Range(H) the set of functions f such that f_0 and f_1 are H-similar. We say that H is (k, t)-*generated*, for some positive integers k, t, if $|H| \leq k$ and 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 the set

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

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

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 $f \in$ Range(H), then ρ is not in $H^\perp$.

Lemma 5. *Let S be a finite set and G a finite group. Let $f : G \times \mathbb{Z}_2 \to S$ 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* $\rho \in H^{\perp}]$.

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

Theorem 4. *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.*

The proof technique of Theorem 4.2 of [2] yields:

Theorem 5. *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.*

References

1. 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.
2. H. Buhrman, L. Fortnow, I. Newman, and H. Röhrig. Quantum property testing. In *Proc. ACM-SIAM Symposium on Discrete Algorithms*, 2003.
3. M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. System Sci.*, 47(3):549–595, 1993.
4. W. van Dam, F. Magniez, M. Mosca, and M. Santha. Self-testing of universal and fault-tolerant sets of quantum gates. *Proc. 32nd ACM STOC*, pp. 688–696, 2000.
5. M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. *Adv. in Appl. Math.*, 25(3):239–251, 2000.
6. E. Fischer. The art of uninformed decisions: A primer to property testing, the computational complexity. In *The Computational Complexity Column*, volume 75, pages 97–126. The Bulletin of the EATCS, 2001.
7. K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and orbit coset in quantum computing. In *Proc. 35th ACM STOC*, 2003.
8. O. Goldreich, S. Goldwasser, and D. Ron. Property testing and its connection to learning and approximation. *J. ACM*, 45(4):653–750, 1998.
9. L. Hales. *The Quantum Fourier Transform and Extensions of the Abelian Hidden Subgroup Problem.* PhD thesis, University of California, Berkeley, 2002.
10. L. Hales and S. Hallgren. An improved quantum Fourier transform algorithm and applications. In *Proc. 41st IEEE FOCS*, pages 515–525, 2000.
11. A. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. Technical report no. 9511026, Quantum Physics e-Print archive, 1995.
12. D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proc. 39th IEEE FOCS*, pages 503–509, 1998.
13. M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.
14. R. Rubinfeld and M. Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. Comp.*, 25(2):23–32, 1996.
15. P. Shor. Algorithms for quantum computation: Discrete logarithm and factoring. *SIAM J. Comp.*, 26(5):1484–1509, 1997.