Efficient Testing of Groups *

Katalin Friedl
Budapest University of Technology and Economics
H-1521 Budapest, Hungary
friedl@cs.bme.hu

Gábor Ivanyos
Computer and Automation Res. Inst. of Hung. Acad. Sci.
H-1518 Budapest, Hungary
Gabor.Ivanyos@sztaki.hu

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

ABSTRACT

We construct an efficient probabilistic algorithm that, given a finite set with a binary operation, tests if it is an abelian group. The distance used is an analogue of the edit distance for strings. The query complexity of the tester is polylogarithmic in the size of the set. Previous testers used Hamming type distances and had superlinear query complexity. A building block for our construction is a constant query complexity homomorphism tester for functions mapping an given finite group into an arbitrary set equipped with a binary operation.

Categories and Subject Descriptors

F.2 [**Analysis of algorithms and problem complexity**]: Miscellaneous

General Terms

Algorithms, Theory

Keywords

Group multiplication testing, edit distance, probabilistic computation, quantum computation

1. INTRODUCTION

Property testing is an active research area which mainly deals with algorithms that can distinguish functions having some specific property from functions which are far away in a certain distance from having that property. Let $\mathcal{C}$ be a family of functions and let $\mathcal{F} \subseteq \mathcal{C}$ be the subset of functions possessing the property. Property testers are randomized procedures which receive as input an oracle for some function $f \in \mathcal{C}$, and after querying it at some number of points accept if $f \in \mathcal{F}$ and reject with high probability if f is far from $\mathcal{F}$. They are relaxations of the standard decision algorithms in the sense that they can give an arbitrary answer on functions which do not have the given property but are close to some function possessing it.

A property tester usually repeats some basic trials and its answer depends on the number of successful trials. Its complexity is measured by the number of queries, which in turn is a function of the number of domain samples in the basic trials and the number of repetitions of the trials. This latter quantity depends on the relations between the rejection probability of the basic trials and the distance from $\mathcal{F}$ of the function they reject. The main advantage of not requiring a correct answer on all the inputs is that for a large variety of problems we can have property testers which run in sublinear time, and thus do not even read the whole input data. Indeed, sublinear property testers have been constructed in recent years for example for problems in algebra, graph theory, geometry, string and set operations, optimization and probability theory and quantum computing. For surveys on property testing see for example [11, 17, 13].

Historically the first property testers were constructed for algebraic problems under the name of self-testers [8, 14]. Many of these testers dealt with group theoretical problems, and they were using a Hamming type distance. Two problems which are of particular interest for our paper can be casted in the following general terms:

- Given a function from a group to another group, is it a homomorphism?
- Given a binary operation on a finite set, is it the multiplication operation for a group?

The first homomorphism tester for abelian groups was constructed by Blum, Luby and Rubinfeld [8]. To test if a function $f : G \to H$ is a homomorphism, where G and H are abelian groups, the following simple basic trial is repeated a constant number of times: pick two random elements $x, y \in G$ and verify that $f(x + y) = f(x) + f(y)$. Improved analyses relating the distance to the rejection probability have been given for this test in [3, 4, 2]. The BLR tester was extended to the case of non-abelian groups by Ben-Or, Coppersmith, Luby and Rubinfeld [5]. Several works have dealt with reducing the $2 \log |G|$ randomness per basic trial of the BLS tester in abelian groups [18, 12, 7]. Recently,

*Research partially supported by the EU 5th framework programs RESQ IST-2001-37559 and Centre of Excellence ICAI-CT-2000-70025, by OTKA T42706, T42481, T42559 grants, and by ACI CR 2002-40 and ACI SI 2003-24 grants of the French Research Ministry. The research of the third author was in part done while visiting the Computer and Automation Research Institute of the Hungarian Academy of Sciences.

STOC'05, May 22-24, 2005, Baltimore, Maryland, USA.

Shpilka and Wigderson [20] have constructed a homomorphism tester which works also in non-abelian groups and uses only $(1 + o(1)) \log |G|$ random bits per trial.

The obvious algorithm to decide if a binary operation on a finite set Γ is associative takes time $O(|\Gamma|^3)$. Rajagopalan and Schulman [15] gave an $O(|\Gamma|^2)$ randomized algorithm for this task, and they have also proven an $\Omega(|\Gamma|^2)$ lower bound. In the work which is the most closely related to ours, Ergün, Kannan, Kumar, Rubinfeld and Viswanathan [10] constructed a property tester for group multiplication which runs in time $O(|\Gamma|^{3/2}(\log |\Gamma|)^{O(1)})$. When the binary operation over Γ is guaranteed to be cancellative, the complexity of this tester is $O(|\Gamma|(\log |\Gamma|)^{O(1)})$. They measure the distance of binary operations over the same finite set by the fraction of pairs of elements where the operations differ, and in their case the distance is undefined if the two operations act on different sets. The reason of the relatively high query complexity of their tester is that even in the cancellative case same basic tests are performed for every element of Γ.

2. OUR RESULTS

Let m be a positive integer and let $r_1, r_2, \ldots, r_m$ be non-negative integers. A *finite algebraic structure S of type* $(r_1, r_2, \ldots . . r_m)$ is an m-tuple of operations on some finite set Γ such that the arity of the ith operation is r_i for $1 \le i \le m$. We call Γ the *groundset* of S.

We now define testers for families of finite algebraic structures. Contrary to [10] our testers don't have to know the groundset of the structure to be tested, only an upper bound of its size. As usual, we also suppose that random elements can be generated from the groundset.

Definition 1. (Property tester for finite algebraic structures). *Let $\mathcal{S}$ be a family of finite algebraic structures of some given type. Let Dist be a distance function from $\mathcal{S} \times \mathcal{S}$ to the real interval $[0, 1]$. Let $\mathcal{F} \subseteq \mathcal{S}$, and let $0 < \epsilon < 1$. An ϵ–*property tester *for $\mathcal{F}$ on $\mathcal{S}$ with distance* Dist *is a probabilistic oracle Turing machine T such that for every $S \in \mathcal{S}$, for every upper bound M on the size of the groundset of S, and for every confidence parameter $0 < c < 1$:*

- *if $\mathsf{Dist}(S, \mathcal{F}) = 0$, then $\mathbf{Pr}\left[T^S(M, c)\ \texttt{accepts}\right] = 1$,*
- *if $\mathsf{Dist}(S, \mathcal{F}) > \epsilon$, then $\mathbf{Pr}\left[T^S(M, c)\ \texttt{rejects}\right] \ge 1 - c$,*

where the probabilities are taken over the coin tosses of T.

We are interested in finite algebraic structures which generalize groups. A *finite group-like structure* $S = (b, u, 1)$ is a finite algebraic structure of type $(2, 1, 0)$. Finite groups are obviously finite group-like structures where b is the group multiplication, u is the inverse operation and 1 is the identity element. When it does not create misunderstanding, groups will be denoted by their groundset.

We now define the distance we use for group-like structures. It will be defined as an analogue of the edit distance for strings with respect to the binary operations of the structures. This will make it possible to correct group-like structures by changing the size of their groundsets. We define the edit distance on the tables of the binary operations so that it does not depend on the particular order of the elements.

A *table* of size k is a $k \times k$ matrix t whose element in row i and column j is denoted by t_{ij} for $1 \le i, j \le k$. We define three operations which transform a table t into a new table. An *exchange* operation at place (i, j) modifies the value t_{ij} and leaves unchanged the others. The cost of an exchange is 1. An *insert* operation at index i, where $1 \le i \le k + 1$, transforms the table t into a table t' of size $k+1$ by inserting $2k + 1$ elements to make a new row and a new column of index i, and by shifting down by one the rows of t of index at least i and by shifting to the right by one the columns of t of index at least i. The cost of an insert is $2k + 1$. A *delete* operation at index i, where $1 \le i \le k$, transforms the table t into a table t' of size $k-1$ by deleting the ith row and the ith column and by shifting up by one the rows of index at least $i+1$ and by shifting to the left by one the columns of index at least $i+1$. The cost of a delete is $2k-1$. For two tables t and t' respectively of size k and k', the *(relative) edit distance* $\mathsf{Edit}(t, t')$ is the minimal cost of exchange, insert and delete operations, divided by $(\mathrm{Max}(k, k'))^2$, which transform t to t'.

Let $p : \Gamma \times \Gamma \to \Gamma$ be a binary operation where Γ is some finite set of cardinality k. A table t of size k *represents* p if there exists a bijection $\pi : \{1, 2, \ldots, k\} \to \Gamma$ such that $t_{ij} = p(\pi(i), \pi(j))$ for $1 \le i, j \le k$. For two group-like structures $S = (b, u, 1)$ and $S' = (b', u', 1')$ the *(relative) edit distance* of S and S', denoted by $\mathsf{Edit}(S, S')$, is defined as the minimum of $\mathsf{Edit}(t, t')$ where t represents b and t' represents b'.

Notice that when the size of the groundsets are the same then the edit distance is the minimal Hamming distance of tables representing the binary operations. If we adjoin to or remove from a group a few random elements then an algorithm running in time $(\log |\Gamma|)^{O(1)}$ has negligible chance to hit any of these elements. Therefore for fast testers the edit distance appears to be more appropriate than the Hamming distance.

We defined here the distance of group-like structures as the relative edit distance of the binary operations. Actually, for finite groups the multiplication uniquely determines the other two operations. From this point of view it would have been desirable to consider structures of type (2) and to give efficient group testers based on merely the multiplication. Although the method presented in this paper needs also inverses, it might be possible to give a polylogarithmic group tester using only the multiplication. Of course, it would be also natural to give a notion of distance which takes into account all the three operations.

Our main result is the construction of a tester for the family of abelian groups on the family of group-like structures. The complexity dependency of our tester on the size of the group-like structure is exponentially smaller than in the tester of [10]: the number of calls it makes to the oracle is only polylogarithmic in the upper bound on the size of the group-like structure given explicitly to the tester. The distance measure we use is the edit distance.

Theorem 1. *Let $\mathcal{S}$ be the family of finite group-like structures and let $\mathcal{F} \subseteq \mathcal{S}$ be the family of finite abelian groups. For every $\epsilon > 0$, there exists an ϵ-tester T for $\mathcal{F}$ on $\mathcal{S}$ with distance* Edit *which for every $S \in \mathcal{S}$ with groundset Γ, for every upper bound M on the size of Γ, and for every confidence parameter c, uses $O((\log M \log \log M)^6 \epsilon^{-6} \log c^{-1})$ calls to the oracle. The total complexity of the tester is $(\epsilon^{-1} \log M)^{O(1)} \log c^{-1}$.*

In [10] associativity is tested in a clever, although rather direct way. Our approach is completely different. It originates in our idea of a quantum property tester for the same problem.

In a quantum property tester the probabilistic oracle Turing machine is replaced by a quantum oracle Turing machine where the oracle is supposed to implement a unitary transformation (see [6] for details). We briefly outline the main ingredients of our quantum tester. Let S be a finite structure of type (2) with groundset Γ and a commutative binary operation $a \cdot b$. Notice that Shor's quantum algorithm [19] can be used to calculate the "order" of the elements, that is the smallest period of the exponentiation function. Therefore we can obtain the identity element and also the inverses.

First we pick sufficiently many random elements $\alpha_1, \dots, \alpha_t$ from Γ so that if Γ is indeed a group then these elements generate Γ with high probability. We use the quantum algorithm of Cheung and Mosca [9] to find a basis $\gamma_1, \dots, \gamma_s$ for the "subgroup" generated by $\alpha_1, \dots, \alpha_t$, together with the orders $m_1, \dots, m_s$ of the basis elements. If the algorithm fails we reject Γ. Otherwise let G denote the group $\mathbb{Z}_{m_1} \times \dots \times Z_{m_s}$.

We have to assure that Γ is nearly isomorphic to G. For an element $\gamma \in \Gamma$, define its nonnegative powers via fast exponentiation. Since we don't suppose that the binary operation is associative, we fix an arbitrary way to parenthesize the terms. Let $g : G \to \Gamma$ be the mapping given as $g(u_1, \dots, u_s) = \gamma_1^{u_1} \cdot \gamma_2^{u_2} \cdots \gamma_s^{u_s}$, where again the multiplication is done according to some fixed way of parenthesizing. Using the quantum algorithm of Mosca and Ekert [16] for the Abelian hidden subgroup problem we can test basically if g is almost a bijection between G and Γ. If $g(uv) = g(u) \cdot g(v)$ also holds with sufficiently high probability for random $u, v \in G$, then it is not difficult to show that g is close to an isomorphism between G and some group that approximates Γ.

To eliminate the quantum parts from the algorithm, we needed some classical way to obtain (some multiple of) the orders of the elements and also to be able to test homomorphisms and ensure their surjectivity.

For the classical probabilistic tester let S be a finite group-like structure with groundset Γ, binary operation $a \cdot b$, unary operation a' and constant element 1. Again, we choose sufficiently many random elements $\gamma_1, \dots, \gamma_s$ from Γ. If we assume that some multiple of the orders of these elements are given, that is positive integers $m_1, \dots, m_s$ such that $\gamma_i^{m_i} = 1$, then as in the quantum case we can consider the group $G = \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s}$ and the same map $g : G \to \Gamma$, where $g(u_1, \dots, u_s) = \gamma_1^{u_1} \cdot \gamma_2^{u_2} \cdots \gamma_s^{u_s}$. Here again products are defined according to some fixed way of parenthesizing and powers by fast exponentiation. If Γ is an Abelian group then g is a homomorphism from $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_s}$ to Γ.

In Section 3 we consider maps from a not necessarily abelian group G to finite structures of type (2). In **Theorem 2** we establish that if $f : G \to \Gamma$ satisfies $f(uv) = f(u) \cdot f(v)$ with sufficiently high probability then it is close to a homomorphism from G to some group $\tilde{\Gamma}$.

We also would like to guarantee that the symmetrical difference of $\tilde{\Gamma}$ and Γ is sufficiently small. We achieve this as follows. Let G_i be the group $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_i} \times \{0\} \times \dots \times \{0\}$ and assume that the restriction of g to G_i passes the homomorphism test with high probability. Then by Theorem 2, for $i = 1, \dots, s$ there exist groups $\tilde{\Gamma}_i$ such that the restriction of g to G_i is close to a homomorphism onto the group $\tilde{\Gamma}_i$. In Lemma 8 we will give further probabilistic conditions which guarantee that the size of $\tilde{\Gamma}_i$ grows exponentially with i with reasonably high probability until $\tilde{\Gamma}_i$ is close to Γ. The number of these conditions is polylogarithmic in the size of Γ which gives the bound on the query complexity of our tester.

We can get rid of the assumption on the knowledge of m_i as follows. We extend exponentiation to negative powers as well by setting $\gamma^{-e} = (\gamma^e)'$. In Section 4, in **Theorem 3** we take a sufficiently large integer N and establish probabilistic conditions on the maps $g_i : \{-N, \dots, N\} \to \Gamma$, defined by $g_i(e) = \gamma_i^e$, under which there exist $m_i < N$ such that g_is are almost periodic with period m_i. In **Theorem 5** we prove that uniform sampling modulo m_i can be sufficiently well approximated by sampling in $\{-N, \dots, N\}$ so that the above mentioned conditions for g can be tested.

In Section 5, the results Theorem 3, Theorem 5 and Theorem 2 are put together in our main technical contribution which is **Theorem 4**. It proves the our tests are robust in the edit distance, that is if a group-like structure passes them with high probability then it is close to an abelian group. Proving robustness is the standard way to establish the existence of testers, and Theorem 1 will follow immediately.

3. APPROXIMATE GROUP HOMOMORPHISMS

For the purpose of this section we will fix $\eta < 1/120$. Let Γ be a set equipped with a binary operation denoted by $a \cdot b$. Let G be a finite, not necessarily abelian group and let $f : G \longrightarrow \Gamma$ be a map from G to Γ such that

$$\mathop{\mathbf{Pr}}_{x,y \in G}[f(xy) = f(x) \cdot f(y)] \geq 1 - \eta. \tag{1}$$

If Γ is a group then a new function $\tilde{f}$ can be defined as

$$\tilde{f}(x) = \mathop{\mathrm{Maj}}_{y \in G} f(xy) \cdot f(y^{-1}),$$

and it can be shown that $\tilde{f}$ is a homomorphism close to f (see, for example, [13] for the Abelian case). Unfortunately this approach does not work directly if Γ is not associative. However, we can construct a congruence relation on G using similar majority arguments. Recall that a congruence on G is an equivalence relation respecting the group operations or, equivalently, an equivalence relation where the classes are the cosets of a normal subgroup K. We shall identify a big part of the factor group G/K with a subset of Γ in a way so that f will be close to the natural homomorphism $G \to G/K$.

We define the binary relation $E \subseteq G \times G$ by

$$E(x, y) \Leftrightarrow \mathop{\mathbf{Pr}}_{u \in G}[f(xu) = f(yu)] \geq 1/2.$$

First we prove that the majority is actually overwhelming.

Lemma 1. *Let $x, y \in G$. Then $\mathbf{Pr}_{u \in G}[f(xu) = f(yu)] \geq 1 - 4\eta$ or $\mathbf{Pr}_{u \in G}[f(xu) \neq f(yu)] \geq 1 - 4\eta$.*

Proof. Condition (1) implies that

$$\mathop{\mathbf{Pr}}_{u,w \in G}[f(xuw) = f(xu) \cdot f(w)] \geq 1 - \eta,$$
$$\mathop{\mathbf{Pr}}_{u,w \in G}[f(yuw) = f(yu) \cdot f(w)] \geq 1 - \eta.$$

Therefore

$$\Pr_{u,w\in G}[f(xu)=f(yu) \implies f(xuw)=f(yuw)] \geq 1-2\eta.$$

Rewriting uw as v we obtain

$$\Pr_{u,v\in G}[f(xu)=f(yu) \implies f(xv)=f(yv)] \geq 1-2\eta,$$

whence, by symmetry,

$$\Pr_{u,v\in G}[f(xu)=f(yu) \iff f(xv)=f(yv)] \geq 1-4\eta.$$

Rewriting the left hand side gives

$$\Pr_{u\in G}[f(xu)=f(yu)]^2 + \Pr_{u\in G}[f(xu)\neq f(yu)]^2 \geq 1-4\eta.$$

From this the statement follows because one of the inequalities

$$\Pr_{u\in G}[f(xu)=f(yu)] \geq 1-4\eta,$$
$$\Pr_{u\in G}[f(xu)\neq f(yu)]\} \geq 1-4\eta$$

must hold. $\square$

Lemma 2. *E is an equivalence relation on G.*

Proof. The facts that E is reflexive and symmetric are immediate consequences of the definition. For transitivity assume that $E(x,y)$ and $E(y,z)$. Then Lemma 1 implies that $\mathbf{Pr}_{u\in G}[f(xu)=f(zu)] \geq 1-8\eta \geq 1/2$. Therefore E is transitive, so it is an equivalence relation. $\square$

We say that an element $x\in G$ is *well-behaving* if

$$\mathbf{Pr}_{u\in G}[f(xu)=f(x)\cdot f(u)] \geq 4/5, \quad (2)$$
$$\text{and} \quad \mathbf{Pr}_{u\in G}\left[(f(x)\cdot f(u))\cdot f(u^{-1})=f(x)\right] \geq 4/5. \quad (3)$$

Next we show that on well-behaving elements the equivalence classes correspond to different values of f and also, that most of the elements are well-behaving.

Lemma 3. *Let $x_1,x_2\in G$ well-behaving elements. Then $E(x_1,x_2)$ iff $f(x_1)=f(x_2)$.*

Proof. If $f(x_1)=f(x_2)$ then by (2) we have

$$\Pr_{u\in G}[f(x_1u)=f(x_2u)] \geq$$
$$\Pr_{u\in G}[f(x_1u)=f(x_1)\cdot f(u) \text{ and } f(x_2u)=f(x_2)\cdot f(u)].$$

The latter probability is at least $3/5$ and so $E(x_1,x_2)$ holds. On the other hand, when $E(x_1,x_2)$ then, by Lemma 1, $\mathbf{Pr}_{u\in G}[f(x_1u)=f(x_2u)] \geq 1-4\eta$. By assumptions (3) and (2), $\mathbf{Pr}_{u\in G}\left[f(x_i)=f(x_iu)\cdot f(u^{-1})\right] \geq 3/5$. Therefore $\mathbf{Pr}_{u\in G}[f(x_1)=f(x_2)] \geq 1-4\eta-4/5>0$. $\square$

Lemma 4. $\mathbf{Pr}_{x\in G}[$*x is not well-behaving* $] \leq 15\eta$.

Proof. From (1) follows that the probability that (2) does not hold for an x is at most 5η. Notice that the inequality $\mathbf{Pr}_{x,u\in G}\left[(f(x)\cdot f(u))\cdot f(u^{-1})=f(x)\right] > 1-2\eta$, therefore the probability that an x violates (3) is at most 10η. $\square$

Lemma 5. *There is a subgroup K of G such that $E(x,y)$ if and only if $Kx=Ky$.*

Proof. Let K be the equivalence class of the identity element. Then from the definition of E we obtain that

$$E(x,y) \Leftrightarrow \Pr_{u\in G}[f(xu)=f(yu)] \geq 1/2 \Leftrightarrow$$
$$\Pr_{u\in G}\left[f(xy^{-1}yu)=f(yu)\right] \geq 1/2 \Leftrightarrow$$
$$\Pr_{w\in G}\left[f(xy^{-1}w)=f(w)\right] \geq 1/2 \Leftrightarrow$$
$$E(xy^{-1},1) \Leftrightarrow xy^{-1}\in K.$$

If $x,y\in K$, then by definition, $E(1,x)$ and $E(1,y)$ hold. By transitivity $E(x,y)$ follows, therefore $xy^{-1}\in K$. $\square$

Lemma 6. *Let K denote the subgroup of G provided by Lemma 5. Then K is a normal subgroup of G.*

Proof. Define the relation E' by

$$E'(x,y) \Leftrightarrow \Pr_{u\in G}[f(ux)=f(uy)] \geq 1/2.$$

For E' all the preceding claims are true if we reverse the order of multiplication. In particular, there exists a subgroup H of G such that $E'(x,y)$ if and only if $xH=yH$. We say that an element $x\in G$ is *well-behaving on both sides* if x is well-behaving with respect to both orders of multiplication,

$$\Pr_{u\in G}[f(xu)=f(x)\cdot f(u)] \geq 4/5,$$
$$\Pr_{u\in G}[f(ux)=f(u)\cdot f(x)] \geq 4/5,$$
$$\Pr_{u\in G}\left[(f(x)\cdot f(u))\cdot f(u^{-1})=f(x)\right] \geq 4/5,$$
$$\text{and} \ \Pr_{u\in G}\left[f(u^{-1}\cdot (f(u)\cdot f(x))=f(x)\right] \geq 4/5.$$

Application of Lemma 4 to both orders of multiplication gives

$$\Pr_{x\in G}[x \text{ well-behaving on both sides }] \geq 1-30\eta.$$

Let $y\in G$ be an element such that

$$\Pr_{x\in Ky}[x \text{ well-behaving on both sides }] > 1/2$$

holds. Notice that more than half of the y's are like this because $\eta<120$.

Let $x\in Ky$ a well-behaving element on both sides. If $x'\in Ky$ is also a well-behaving element on both sides then, by Lemma 3, $f(x)=f(x')$, and again by Lemma 3 applied to the reverse order of multiplication, $xH=x'H$, so $x'\in xH$. Therefore, $|Ky\cap xH|>|K|/2$.

Consider the set $x^{-1}Ky=y^{-1}(yx^{-1}K)y$. Notice that $yx^{-1}\in K$ because of the choice $x\in Ky$. This ensures that $x^{-1}Ky=y^{-1}Ky$ is a group. The facts that $y^{-1}Ky\cap H$ is a subgroup of $y^{-1}Ky$ and $|y^{-1}Ky\cap H|=|x^{-1}Ky\cap H|=|x(x^{-1}Ky\cap H)|=|Ky\cap xH|>|K|/2$ imply that $y^{-1}Ky\leq H$ from which $|K|\leq|H|$ also follows. Similarly, we can obtain that $|H|\leq|K|$, so $|K|=|H|$ and $y^{-1}Ky=H$ must hold for every y such that

$$\Pr_{x\in Ky}[x \text{ well-behaving from both sides }] > 1/2.$$

Therefore $y^{-1}Ky=H$ holds for more than half of the elements $y\in G$. When $y^{-1}Ky=H$ and $z^{-1}Kz=H$ then yz^{-1} normalizes K, i.e., $(yz^{-1})^{-1}Kyz^{-1}=K$. It follows that the size of the normalizer group of K, $|N_G(K)|>|G|/2$, so $N_G(K)=G$ and the subgroup K is a normal subgroup in G. $\square$

We say that an element $x \in G$ is *good* if it is well-behaving and $f(x) = \mathrm{Maj}_{y:E(x,y)}(f(y))$, and *bad* otherwise. A coset Kx is *good* if it contains a good element.

LEMMA 7. $\mathbf{Pr}_{x\in G}[x \quad bad \quad] \leq 30\eta$

PROOF. We show that $\mathbf{Pr}_{x\in G}[x \text{ bad and well-behaving }] \leq \mathbf{Pr}_{x\in G}[x \text{ non well-behaving }]$. In fact we can prove the stronger statement, that this inequality holds when the probability is considered in an equivalence class. We know that the function f is constant on the well-behaving elements of an equivalence class (by Lemma 3). Since the bad well-behaving elements do not form a majority in the class, the number of non well-behaving elements must be greater. $\square$

THEOREM 2. *Let $\eta < 1/120$ and assume that the inequality $\mathbf{Pr}_{x,y\in G}[f(xy) = f(x)\cdot f(y)] > 1-\eta$ holds. Then there exists a group $\tilde{\Gamma}$ with multiplication $*$ and a homomorphism $\tilde{f} : G \to \tilde{\Gamma}$ such that*

(i) $|\tilde{\Gamma} \setminus \Gamma| \leq 30\eta|\tilde{\Gamma}|$,

(ii) $\mathbf{Pr}_{\gamma_1,\gamma_2\in\tilde{\Gamma}}[\gamma_1 * \gamma_2 \neq \gamma_1\cdot\gamma_2] \leq 91\eta$,

(iii) $\mathbf{Pr}_{x\in G}\left[\tilde{f}(x) \neq f(x)\right] \leq 30\eta.$

PROOF. Let $\tilde{\Gamma} = G/K$ and let $\tilde{f} : G \to \tilde{\Gamma}$ be the natural homomorphism. Consider a good coset $Kx \in G/K$. We identify Kx with $f(y)$ where y is a good element of Kx. This identification is legitimate since the function f is constant on the good elements of Kx, and it ensures that when x is a good element of G then $\tilde{f}(x) = f(x)$. Now we prove the three claims.

(i) For every $x \in G$ observe that $\tilde{f}(x) \notin \Gamma \Leftrightarrow Kx$ is bad. If Kx is bad, then each of its elements is bad, so Lemma 7 implies the statement.

(ii) Let $\gamma_1, \gamma_2 \in \tilde{\Gamma}$. Then there exist $x, y \in G$, such that $\tilde{f}(x) = \gamma_1$ and $\tilde{f}(y) = \gamma_2$. Also $\gamma_1*\gamma_2 = \tilde{f}(x)*\tilde{f}(y) = \tilde{f}(xy)$.

When $\gamma_1 \notin \Gamma$ or $\gamma_2 \notin \Gamma$ then $\gamma_1\cdot\gamma_2$ is not defined. This happens with probability at most 60η. The probability that xy is bad is at most 30η. If xy is good then $\tilde{f}(xy) = f(xy)$. The probability in this case that $f(xy) \neq f(x)\cdot f(y)$ is at most η.

(iii) If $\tilde{f}(x) \neq f(x)$ then x is bad and the statement follows from Lemma 7. $\square$

This result has an interesting corollary about the testability of group homomorphisms on the extended family of functions whose domain is some given group G, and whose range is some algebraic structure with a binary operation. Let $\mathcal{C}$ denote the family of these functions. The distance measure we use is a Hamming type distance. More precisely, let S_1 and S_2 be finite algebraic structures of type (2) with respective groundsets Γ_1 and Γ_2. For $i = 1, 2$ let $f_i : G \to \Gamma_i$. The distance Ham is defined by $\mathsf{Ham}(f_1, f_2) = \mathbf{Pr}_{x\in G}[f_1(x) \neq f_2(x)]$. Observe that the usual distance measure Ham' in the literature for homomorphism tests is different from Ham in the sense that $\mathsf{Ham}'(f_1, f_2)$ is only defined when $\Gamma_1 = \Gamma_2$ is a group. Let $\mathcal{H}$ be the family of homomorphisms from G to any group. Statement (iii) of Theorem 2 in fact says that the standard homomorphism test is $(\eta, 30\eta)$ robust for Ham, that is if the rejection probability of the test for f is at most η then f is at most 30η away from $\mathcal{H}$. From this robustness result the existence of a tester for $\mathcal{H}$ on $\mathcal{C}$ whose query complexity is independent of the size of G follows immediately.

We end this section with a lemma which will be used in Theorem 4. We establish further probabilistic conditions under which, if we apply Theorem 2 to groups $H < G$ in the context described in the outline given in Section 2, i.e. H is constructed from random elements of Γ and G is built by adding further random elements, yielding respectively groups $\tilde{\Pi}$ and $\tilde{\Gamma}$, then $\tilde{\Gamma}$ will be at least twice as large as $\tilde{\Pi}$ with reasonable probability unless $\tilde{\Pi}$ is close to Γ.

LEMMA 8. *Let $\eta < 1/120$, let $f : G \to \Gamma$ be a function, let H be a subgroup of G and let z be an arbitrary element of G. Assume that*

$$\mathbf{Pr}_{u,v\in H}[f(uv) = f(u)\cdot f(v)] \geq 1-\eta. \tag{4}$$

Let $\tilde{\Pi}$ be the group provided by Theorem 2 for H. Then there exists a subset $B = B(H)$ of Γ such that $|B| \leq |\tilde{\Pi}|$, and the following property holds: Assume also that f satisfies (1) and

$$\mathbf{Pr}_{u\in H,v\in G}[f(uv) = f(u)\cdot f(v)] \geq 1-\eta, \tag{5}$$

$$\mathbf{Pr}_{u\in H,v\in G}\left[f(uv)\cdot f(v^{-1}) = f(u)\right] \geq 1-\eta, \tag{6}$$

$$\mathbf{Pr}_{u\in H,v\in G}\left[f(zuv)\cdot f(v^{-1}) = f(xu)\right] \geq 1-\eta, \tag{7}$$

$$\mathbf{Pr}_{u\in H}\left[f(zu)\cdot f(u^{-1}) = f(x)\right] \geq 1-\eta. \tag{8}$$

Then either $|\tilde{\Gamma}| = |\tilde{\Pi}|$, or $|\tilde{\Gamma}| \geq 2|\tilde{\Pi}|$, where $\tilde{\Gamma}$ is the group provided by Theorem 2 for G. Moreover, if $|\tilde{\Gamma}| = |\tilde{\Pi}|$ then $f(z) \in B$.

PROOF. We define the relation E_H on H by

$$E_H(x, y) \iff \mathbf{Pr}_{u\in H}[f(xu) = f(yu)] \geq 1/2.$$

For every $x \in H$, let $\beta(x) = \mathrm{Maj}_{u\in H}\left(f(xu)\cdot f(u^{-1})\right)$. We say that x is a *majority element in H* if

$$\mathbf{Pr}_{u\in H}\left[\beta(x) = f(xu)\cdot f(u^{-1})\right] > 1/2 + 4\eta.$$

Notice that a well-behaving element x is always a majority element in H. We define the set

$$B = \{\beta(x) \ : \ x \ \text{ is a majority element in } \ H\}.$$

CLAIM 1. $|B| \leq |\tilde{\Pi}|$.

PROOF. It is sufficient to prove that the size of B is at most the number of equivalence classes of E_H. Let majority elements x, y belong to the same equivalence class of E_H. Then $\beta(x) = \beta(y)$ because

$$\mathbf{Pr}_{u\in H}\left[f(xu)\cdot f(u^{-1}) = f(yu)\cdot f(u^{-1})\right] > 1-4\eta.$$

$\square$

CLAIM 2. *For $y_1, y_2 \in H$, $E_H(y_1, y_2) \iff E_G(y_1, y_2)$.*

PROOF. Assume that $E_H(y_1, y_2)$. According to Lemma 1, $\mathbf{Pr}_{u\in H}[f(y_1u) = f(y_2u)] \geq 1-4\eta$. From (5) we infer that $\mathbf{Pr}_{u\in H,v\in G}[f(y_iuv) = f(y_iu)\cdot f(v)] \geq 1-\eta$ because $H = y_iH$. So

$$\mathbf{Pr}_{w\in G}[f(y_1w) = f(y_2w)] = \mathbf{Pr}_{u\in H,v\in G}[f(y_1uv) = f(y_2uv)]$$
$$\geq 1-6\eta > 1/2, \tag{9}$$

which means that $E_G(x, y)$.

To see the reverse implication, assume that $E_G(y_1, y_2)$. Then by Lemma 1

$$\mathop{\mathbf{Pr}}_{u\in H, v\in G}[f(y_1uv) = f(y_2uv)] = \mathop{\mathbf{Pr}}_{w\in G}[f(y_1w) = f(y_2(w)] \geq 1 - 4\eta. \quad (10)$$

By (6), $\mathbf{Pr}_{u\in G, v\in H}\left[f(y_iu) = f(y_iuv)\cdot f(v^{-1})\right] \geq 1-\eta$ holds, therefore $\mathbf{Pr}_{u\in H}[f(y_1u) = f(y_2u)] \geq 1 - 6\eta > 1/2$, and so $E_H(y_1, y_2)$. $\square$

Since the elements of $\tilde{\Pi}$ and $\tilde{\Gamma}$ are respectively the equivalence classes of E_H and E_G, it follows that $\tilde{\Gamma}$ has a subgroup isomorphic to $\tilde{\Pi}$, and therefore either $|\tilde{\Gamma}| = |\tilde{\Pi}|$ or $|\tilde{\Gamma}| \geq 2|\tilde{\Pi}|$.

Claim 3. *Let $y \in H$ such that $E_G(z, y)$. Then $f(z) = \beta(y)$ and y is a majority element in H.*

Proof. First observe that if u is a random element of H and v is a random element in G then uv is a random element in G. By Lemma 1,

$$\mathop{\mathbf{Pr}}_{u\in H, v\in G}[f(zuv) = f(yuv)] \geq 1 - 4\eta.$$

Therefore

$$\mathop{\mathbf{Pr}}_{u\in H, v\in G}\left[f(zuv)\cdot f(v^{-1}) = f(yuv)\cdot f(v^{-1})\right] \geq 1 - 4\eta.$$

From (7) and (6) follows that $\mathbf{Pr}_{u\in H}[f(zu) = f(yu)] \geq 1 - 6\eta$ and (8) implies that $\mathbf{Pr}_{u\in H}\left[f(z) = f(yu)\cdot f(u^{-1})\right] \geq 1 - 7\eta$. Because $1/2 + 4\eta < 1 - 7\eta$, it follows that y is a majority element in H and $f(z) = \beta(y)$. $\square$

To finish the proof of Lemma 8 let us suppose that $f(z) \notin B$. Then by Claim 3, $E_G(z, y)$ does not hold for any $y \in H$. Therefore E_G has more equivalence classes than E_H and thus $|\tilde{\Gamma}| > |\tilde{\Pi}|$. $\square$

4. NEAR PERIODICITY

Let Γ be a set equipped with a binary operation denoted by $a\cdot b$. We define $D_N = \{i \in \mathbb{Z} \ :\ |i| \leq N\}$ for any integer $N > 0$. For every positive integer m we identify $\mathbb{Z}_m$ with $\{0, 1, \ldots, m-1\} \subset \mathbb{Z}$.

Theorem 3. *Let d and N be positive integers such that $N/4d \geq |\Gamma| + 1$, and let $\eta < 1/1280d$. Suppose that $f : D_{16N} \longrightarrow \Gamma$ satisfies*

$$\mathbf{Pr}_{u,v\in D_{8N}}[f(u+v) = f(u)\cdot f(v)] \geq 1-\eta, \quad (11)$$
$$\mathbf{Pr}_{u,v\in D_{8N}}[f(u+v)\cdot f(-v) = f(u)] \geq 1-\eta. \quad (12)$$

Then there exists an integer $N/2d < m \leq N/d$, such that for every integer t with $|t| < \lfloor 2N/m \rfloor$,

$$\mathbf{Pr}_{u\in\mathbb{Z}_m}[f(u+tm) \neq f(u)] \leq 640d\eta. \quad (13)$$

The proof of the theorem is similar to that of Theorem 2. It is given in the appendix.

5. THE TESTER

5.1 Robustness

Let S be a group-like structure whose groundset is Γ. The binary operation of S is denoted by $a\cdot b$, the unary operation by a', and the constant element by 1.

For any $\gamma \in \Gamma$ and integer $e \geq 0$ we define the nonnegative powers of γ as follows: $\gamma^0 = 1, \gamma^1 = \gamma, \gamma^{2^i} = \gamma^{2^{i-1}}\cdot\gamma^{2^{i-1}}$ for $i > 0$, and for $e = \sum_{i=0}^{j} b_i 2^i$ where $b_i \in \{0, 1\}$, $\gamma^e = (\ldots(\gamma^{b_0 2^0}\cdot\gamma^{b_1 2^1})\ldots)\cdot\gamma^{b_j 2^j}$. The negative powers of γ are defined by $\gamma^{-i} = (\gamma^i)'$ for $i \geq 1$.

Let k and ℓ be integers which will be fixed later. For $i = 1, \ldots, k$ let $D^{(i)} = \prod_{t=1}^{i\ell} D_{4N} \times \prod_{t=i\ell+1}^{k\ell}\{0\}$ and let $D^{(k)}$ be denoted by D. For $i = 1, \ldots, k$ and $j = 1, \ldots, \ell$ let $x_{ij} = (0, \ldots, 0, 1, 0\ldots, 0) \in D$ where the 1 is in the $(i-1)\ell + j$th coordinate.

Set $\bar{\Gamma} = \Gamma^{k\ell}$. Let $\bar{\gamma} = (\gamma_{11}, \ldots, \gamma_{1\ell}, \ldots, \gamma_{k1}, \ldots, \gamma_{k\ell})$. For every such $\bar{\gamma} \in \bar{\Gamma}$ we define the functions $g_{ij} : \bar{\Gamma}\times D_{16N} \to \Gamma$ by $g_{ij}(\bar{\gamma}, e) = \gamma_{ij}^e$ and $g : \bar{\Gamma}\times D \to \Gamma$ by $g(\bar{\gamma}, e_{11}, \ldots, e_{k\ell}) = (\ldots(g_{11}(\bar{\gamma}, e_{11})\cdot g_{12}(\bar{\gamma}, e_{12}))\ldots)\cdot g_{k\ell}(\bar{\gamma}, e_{k\ell})$.

Theorem 4. *Let S be as above and let Γ be of size at most M. Let $0 < \epsilon < 1$. Set $k = \lceil\log_2 M\rceil$, $\ell = \lceil 9(\ln(2k))/\epsilon\rceil = \theta(\log\log M\cdot\frac{1}{\epsilon})$, $N = 4k\ell(M+1)$ and $\eta = \epsilon/(1200000k^2\ell^2) = \theta((\log M\log\log M)^{-2}\epsilon^3)$. If the inequalities*

$$\mathop{\mathbf{Pr}}_{u,v\in D_N^{k\ell}}[g(\bar{\gamma}, u+v) = g(\bar{\gamma}, u)\cdot g(\bar{\gamma}, v)] \geq 1-\eta, \quad (14)$$

for $i = 1, \ldots, k$ and $j = 1, \ldots, \ell$

$$\mathop{\mathbf{Pr}}_{u,v\in D_{8N}}[g_{ij}(\bar{\gamma}, u+v) = g_{ij}(\bar{\gamma}, u)\cdot g_{ij}(\bar{\gamma}, v)] \geq 1-\eta, \quad (15)$$

$$\mathop{\mathbf{Pr}}_{u,v\in D_{8N}}[g_{ij}(\bar{\gamma}, u+v)\cdot g_{ij}(\bar{\gamma}, -v) = g_{ij}(\bar{\gamma}, u)] \geq 1-\eta, \quad (16)$$

for $i = 2, \ldots, k$

$$\mathop{\mathbf{Pr}}_{u,v\in D^{(i-1)}}[g(\bar{\gamma}, u+v) = g(\bar{\gamma}, u)\cdot g(\bar{\gamma}, v)] \geq 1-\eta, \quad (17)$$

$$\mathop{\mathbf{Pr}}_{u\in D^{(i-1)}, v\in D^{(i)}}[g(\bar{\gamma}, u+v) = g(\bar{\gamma}, u)\cdot g(\bar{\gamma}, v)] \geq 1-\eta, \quad (18)$$

$$\mathop{\mathbf{Pr}}_{u\in D^{(i-1)}, v\in D^{(i)}}[g(\bar{\gamma}, u+v)\cdot g(\bar{\gamma}, -v) = g(\bar{\gamma}, u)] \geq 1-\eta, \quad (19)$$

for $i = 2, \ldots, k$ and $j = 1, \ldots, \ell$

$$\mathop{\mathbf{Pr}}_{u\in D^{(i-1)}, v\in D^{(i)}}[g(\bar{\gamma}, x_{ij}+u+v)\cdot g(\bar{\gamma}, -v) = g(\bar{\gamma}, x_{ij}+u)] \geq 1-\eta, \quad (20)$$

$$\mathop{\mathbf{Pr}}_{u\in D^{(i-1)}}[g(\bar{\gamma}, x_{ij}+u)\cdot g(\bar{\gamma}, -u) = g(\bar{\gamma}, x_{ij}))] \geq 1-\eta', \quad (21)$$

are simultaneously satisfied by a random $\bar{\gamma} \in \bar{\Gamma}$ with probability at least 1/2 then for every such $\bar{\gamma}$ there exists an abelian group $A(\bar{\gamma})$ with operation $\circ$ which satisfies the following properties:

(i) $|A(\bar{\gamma})\setminus\Gamma| \leq \epsilon|A(\bar{\gamma})|/9$,

(ii) $\mathbf{Pr}_{a,b\in\Gamma\cap A(\bar{\gamma})}[a\cdot b \neq a\circ b] \leq \epsilon/3$.

Moreover, there exists $\bar{\gamma} \in \bar{\Gamma}$ such that

(iii) $|\Gamma\setminus A(\bar{\gamma})| \leq 2\epsilon|\Gamma|/9$,

(iv) $\mathsf{Edit}(S, A(\bar{\gamma})) \leq \epsilon$.

5.2 Creating the group

In this subsection we prove Theorem 4. Fix now a $\bar{\gamma}$ which satisfies (14)–(21). For every $1 \le i \le k$, $1 \le j \le \ell$ we apply Theorem 3 to $f(z) = g_{ij}(\bar{\gamma}, z)$ with $d = k\ell$. This ensures that there exist $N/2k\ell < m_{ij} \le N/k\ell$ such that for every integer t such that $|t| < \lfloor 2N/m_{ij} \rfloor$,

$$\mathbf{Pr}_{u \in \mathbb{Z}_{m_{ij}}}\left[g_{ij}(\bar{\gamma}, u + tm_{ij}) \neq g_{ij}(\bar{\gamma}, u)\right] \le 640k\ell\eta. \quad (22)$$

We fix such m_{ij}s and set $\bar{m} = (m_{11}, \dots m_{k\ell})$ and $G(\bar{\gamma}) = G = \mathbb{Z}_{m_{11}} \times \dots \times \mathbb{Z}_{m_{k\ell}}$. For $i = 1, \dots, k$, we define $G^{(i)} = \prod_{t=1}^{i} \prod_{j=1}^{\ell} Z_{m_{tj}} \times \prod_{t=i\ell+1}^{k\ell} \{0\}$ subgroups of G. To shorten notation, we denote the map $g(\bar{\gamma}, \cdot)$ by $h(\cdot)$. We also identify G with $\{0, \dots, m_{11} - 1\} \times \dots \times \{0, \dots, m_{k\ell} - 1\} \subset D$. The operation $+$ will be used for usual addition of vectors of $\mathbb{Z}^{k\ell}$ and the addition in G will be denoted by $\oplus$.

First observe that by the union bound Theorem 3 implies that for every $\bar{t} = (t_{11}, \dots, t_{k\ell})$, where $|t_{ij}| < \lfloor 2N/m_{ij} \rfloor$ for $1 \le i \le k$, $1 \le j \le \ell$,

$$\mathbf{Pr}_{u \in G}\left[h(u) \neq h(u + \bar{t}\bar{m})\right] \le \lambda, \quad (23)$$

where $\lambda = 640k^2\ell^2\eta$. For every $\bar{t}$, where $|t_{ij}| < \lfloor 2N/m_{ij} \rfloor - 1$, we have

$$\mathop{\mathbf{Pr}}_{u \in G}\left[\exists \bar{r} \in \{0,1\}^{k\ell} \text{ such that } h(u + (\bar{t} + \bar{r}) \cdot \bar{m}) \neq h(u)\right] \le 2\lambda, \quad (24)$$

since (22) implies

$$\mathop{\mathbf{Pr}}_{u_{ij} \in \mathbb{Z}_{m_{ij}}}\left[g_{ij}(\bar{\gamma}, u_{ij} + t_{ij}m_{ij}) \neq g_{ij}(\bar{\gamma}, u_{ij}) \text{ or } g_{ij}(\bar{\gamma}, u_{ij} + (t_{ij}+1)m_{ij}) \neq g_{ij}(\bar{\gamma}, u_{ij})\right] \le 2 \cdot 640k\ell\eta,$$

and then one concludes from the union bound.

Let us now turn to the result which shows how to replace in the tests sampling in the groups $G^{(i)}$ by sampling in $\{-N, \dots, N\}$.

Theorem 5. *Let $\bar{\gamma}$ satisfy conditions (14)–(21) and set $\eta'' = 4000k^2\ell^2\eta$. Then*

$$\mathbf{Pr}_{u,v \in G}\left[h(u \oplus v) = h(u) \cdot h(v)\right] \ge 1 - \eta'', \quad (25)$$

for $i = 2, \dots, k$

$$\mathop{\mathbf{Pr}}_{u,v \in G^{(i-1)}}\left[h(u \oplus v) = h(u) \cdot h(v)\right] \ge 1 - \eta'' \quad (26)$$

$$\mathop{\mathbf{Pr}}_{u \in G^{(i-1)}, v \in G^{(i)}}\left[h(u \oplus v) = h(u) \cdot h(v)\right] \ge 1 - \eta'', \quad (27)$$

$$\mathop{\mathbf{Pr}}_{u \in G^{(i-1)}, v \in G^{(i)}}\left[h(u \oplus v) \cdot h(-v) = h(u)\right] \ge 1 - \eta'', \quad (28)$$

for $i = 2, \dots, k$ and for $j = 1, \dots, \ell$

$$\mathop{\mathbf{Pr}}_{u \in G^{(i-1)}, v \in G^{(i)}}\left[h(x_{ij} \oplus u \oplus v) \cdot h(-v) = h(x_{ij} \oplus u)\right] \ge 1 - \eta'', \quad (29)$$

$$\mathop{\mathbf{Pr}}_{u \in G^{(i-1)}}\left[h(x_{ij} \oplus u) \cdot h(-u) = h(x_{ij}))\right] \ge 1 - \eta''. \quad (30)$$

Proof. We prove here inequality (25), the other proofs are analogous.

Suppose that $\mathbf{Pr}_{u,v \in G}\left[h(u \oplus v) \neq h(u) \cdot h(v)\right] > \eta''$. The number of the translation pairs $(\bar{s} \cdot \bar{m}, \bar{t} \cdot \bar{m})$, such that $|s_{ij}|, |t_{ij}| < \lfloor N/m_{ij} \rfloor$ is equal to $\prod_{i,j}(2\lfloor N/m_{ij} \rfloor - 1)^2 > \prod_{i,j}(2N/m_{ij} - 3)^2$. Observe that for such a pair $s_{ij} + t_{ij} < \lfloor 2N/m_{ij} \rfloor - 1$ and for every $u, v \in G$ there exists a vector $\bar{r} \in \{0,1\}^{k\ell}$ such that

$$u + \bar{s} \cdot \bar{m} + v + \bar{t} \cdot \bar{m} = (u \oplus v) + (\bar{s} + \bar{t} + \bar{r})\bar{m}.$$

Therefore, whenever $h(u \oplus v) \neq h(u) \cdot h(v)$, but the equalities $h(u + \bar{s} \cdot \bar{m}) = h(u)$, $h(v + \bar{t} \cdot \bar{m}) = h(v)$ and $h(u \oplus v) = h((u \oplus v) + (\bar{s} + \bar{t} + \bar{r})\bar{m})$ hold for every $\bar{r} \in \{0,1\}$ then we also have $h(u + \bar{s} \cdot \bar{m} + v + \bar{t} \cdot \bar{m}) \neq h(u + \bar{s} \cdot \bar{m}) \cdot h(v + \bar{t} \cdot \bar{m})$. By (23) and (24), for every translation pair $(\bar{s} \cdot \bar{m}, \bar{t} \cdot \bar{m})$, there exist at least $(\eta'' - 4\lambda)|G|^2$ pairs $(u, v) \in G^2$ such that $h(u + \bar{s} \cdot \bar{m} + v + \bar{t} \cdot \bar{m}) \neq h(u + \bar{s} \cdot \bar{m}) \cdot h(v + \bar{t} \cdot \bar{m})$. Also, $u + \bar{s} \cdot \bar{m}, v + \bar{t} \cdot \bar{m} \in D_N^{k\ell}$. Therefore

$$\mathop{\mathbf{Pr}}_{x,y \in D_N^{k\ell}}\left[h(x + y) \neq h(x) \cdot h(y)\right] > \frac{\prod_{i,j}(2N/m_{ij} - 3)^2(\eta'' - 4\lambda)|G|^2}{(2N+1)^{2k\ell}} > (\eta'' - 4\lambda)/e^4 > \eta.$$

This contradicts to (14). $\square$

Proof of Theorem 4. Let $\bar{\gamma}$ satisfy (14)–(21). By Theorem 5, $G = G(\bar{\gamma})$ satisfies (25). We apply Theorem 2 with $f = h$ and $\eta = \eta''$ and define $A(\bar{\gamma})$ as the group $\tilde{\Gamma}$ provided by the result. Then (i) and (ii) of Theorem 2 imply respectively (i) and (ii) since $\eta'' = 4000k^2\ell^2\eta = \epsilon/300$.

We now turn to the proof of (iii). In fact we will prove that $|A(\bar{\gamma})| \ge (1 - \epsilon/9))|\Gamma|$ which together with (i) implies (iii). For an integer $1 \le t \le k$ let $\mathcal{E}_t$ stand for the event that $\bar{\gamma}$ satisfies (15)–(21) for $1 \le i \le t$ and (17) also holds for $i = t+1$. Observe that the groups $G^{(1)}, \dots, G^{(t)}$ depend only on $\gamma_{11}, \dots, \gamma_{t\ell}$ and the same holds for the restriction of h to $D^{(t)}$. Actually, these groups can already be defined when $\mathcal{E}_t$ holds and the proof of Theorem 5 works in this situation as well. Since $G^{(t)}$ satisfies (25) we can apply Theorem 2 with $G^{(t)}$ in place of G and η'' in place of η. Let $A_t(\bar{\gamma})$ be the group provided by Theorem 2. Also, if $\mathcal{E}_k$ holds then Theorem 5 implies that inequalities (4)–(8) hold for $H = G^{(t)}, G = G^{(t+1)}$, $\eta = \eta''$. Therefore Lemma 8 implies that either $|A_t(\bar{\gamma})| = |A_{t+1}(\bar{\gamma})|$ or $|A_{t+1}(\bar{\gamma})| \ge 2 \cdot |A_t(\bar{\gamma})|$, and, if the equality holds, then $\gamma_{t+1,1}, \dots, \gamma_{t+1,\ell}$ are in B, a set of size at most $|A_t(\bar{\gamma})|$.

By definition, for $1 \le t \le k$, let $\mathcal{E}'_t$ stand for the event that both $\mathcal{E}_t$ and $|A_t(\bar{\gamma})| < (1 - \epsilon)|\Gamma|$ hold. Obviously $\mathcal{E}'_t$ implies $\mathcal{E}'_{t-1}$ for every $t > 1$. Let us now make the indirect assumption that $\mathcal{E}'_k = \mathcal{E}_k$. This implies that if $\mathcal{E}_k$ holds for a $\bar{\gamma}$ then $|A_k(\bar{\gamma})| < (1 - \epsilon/9)|\Gamma|$ also holds. Notice that for every $t < k$ we have $\mathbf{Pr}_{\bar{\gamma}}\left[|A_{t+1}(\bar{\gamma})| = |A_t(\bar{\gamma})| \mid \mathcal{E}_k\right] \le \mathbf{Pr}_{\bar{\gamma}}\left[|A_{t+1}(\bar{\gamma})| = |A_t(\bar{\gamma})| \mid \mathcal{E}'_t\right] / \mathbf{Pr}_{\bar{\gamma}}\left[\mathcal{E}_k\right]$, because $\mathcal{E}'_k = \mathcal{E}_k$ implies $\mathcal{E}'_t$. We know that $|A_{t+1}(\bar{\gamma})| = |A_t(\bar{\gamma})|$ only can happen when $\gamma_{t+1,1}, \dots, \gamma_{t+1,\ell}$ comes form a subset of size at most $|A_t(\bar{\gamma})| \le (1 - \epsilon/9)|\Gamma|$. Using the assumption that $\mathbf{Pr}_{\bar{\gamma}}\left[\mathcal{E}_k\right] \ge 1/2$ the right hand side can be estimated as

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}}\left[|A_{t+1}(\bar{\gamma})| = |A_t(\bar{\gamma})| \mid \mathcal{E}'_t\right] / \mathop{\mathbf{Pr}}_{\bar{\gamma}}\left[\mathcal{E}_k\right] < 2(1 - \epsilon/9)^{\ell}$$

Clearly, if $|A_k(\bar{\gamma})| < |\Gamma|$ then for some $t < k$ the equality $|A_{t+1}(\bar{\gamma})| = |A_t(\bar{\gamma})|$ must hold. Therefore,

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}}\left[|A_k(\bar{\gamma})| < |\Gamma| \mid \mathcal{E}_k\right] < 2k(1 - \epsilon/9)^{\ell}.$$

By the indirect assumption, the left hand side is 1 and because of the choice of k and ℓ the right hand side is less than 1, which gives a contradiction.

Finally we prove (iv) by evaluating the relative cost of transforming $A(\bar{\gamma})$ to S. The cost of deletions by (i) is at most $2\epsilon/9$. The cost of exchange operations by (ii) is at most $\epsilon/3$. The cost of insertions by (iii) is at most $4\epsilon/9$, which finishes the proof. $\square$

5.3 Proof of Theorem 1

PROOF. We will set parameters k, l and N as in Theorem 4, and use the notations before that theorem. The goal of the tester T will be to statistically verify if the following inequalities hold simultaneously with $\eta' = \eta/16kl$:

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u,v\in D_N^{k\ell}} [g(\bar{\gamma}, u+v) = g(\bar{\gamma}, u) \cdot g(\bar{\gamma}, v)] \geq 1 - \eta', \quad (31)$$

for $i = 1, \ldots, k$ and $j = 1, \ldots, \ell$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u,v\in D_{8N}} [g_{ij}(\bar{\gamma}, u+v) = g_{ij}(\bar{\gamma}, u) \cdot g_{ij}(\bar{\gamma}, v)] \geq 1 - \eta', \quad (32)$$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u,v\in D_{8N}} [g_{ij}(\bar{\gamma}, u+v) \cdot g_{ij}(\bar{\gamma}, -v) = g_{ij}(\bar{\gamma}, u)] \geq 1 - \eta', \quad (33)$$

for $i = 2, \ldots, k$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u,v\in D^{(i-1)}} [g(\bar{\gamma}, u+v) = g(\bar{\gamma}, u) \cdot g(\bar{\gamma}, v)] \geq 1 - \eta', \quad (34)$$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u\in D^{(i-1)}, v\in D^{(i)}} [g(\bar{\gamma}, u+v) = g(\bar{\gamma}, u) \cdot g(\bar{\gamma}, v)] \geq 1 - \eta', \quad (35)$$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u\in D^{(i-1)}, v\in D^{(i)}} [g(\bar{\gamma}, u+v) \cdot g(\bar{\gamma}, -v) = g(\bar{\gamma}, u)] \geq 1 - \eta', \quad (36)$$

for $i = 2, \ldots, k$ and $j = 1, \ldots, \ell$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u\in D^{(i-1)}, v\in D^{(i)}} [g(\bar{\gamma}, x_{ij} + u + v) \cdot g(\bar{\gamma}, -v) = g(\bar{\gamma}, x_{ij} + u)] \geq 1 - \eta', \quad (37)$$

$$\mathop{\mathbf{Pr}}_{\bar{\gamma}\in\bar{\Gamma},\ u\in D^{(i-1)}} [g(\bar{\gamma}, x_{ij} + u) \cdot g(\bar{\gamma}, -u) = g(\bar{\gamma}, x_{ij}))] \geq 1 - \eta'. \quad (38)$$

For all inequalities the tester will approximate the probabilities of the events on the left hand side by $O((1/\eta')\log(1/c))$ independent trials. It accepts if the frequency of the failure of every event is less than $\eta'/2$. The evaluation of g at any point requires $O(k\ell \log N)$ calls to the oracle. Therefore the total number of oracle calls is $O(k^2\ell^2 \log N (1/\eta')\log(1/c))$ that, by our choice of the parameters $k = O(\log M)$, $\ell = O(\epsilon^{-1}\log\log M)$ and $\eta' = O(\epsilon k^{-3}\ell^{-3})$, is

$$O(\log^6 M (\log\log M)^5 \epsilon^{-6} \log(1/c)).$$

Clearly if S is an abelian group, there will be no failure, and the tester always accepts. Let us now suppose that $\mathsf{Edit}(S, \mathcal{F}) > \epsilon$. Then from (iv) of Theorem 4 it follows that for a random $\bar{\gamma} \in \bar{\Gamma}$ with probability at least 1/2 at least one of the inequalities (14)–(21) does not hold. Since the number of inequalities is less than $8kl$ and $\eta' = \eta/16kl$, Markov's inequality implies that at least one of the inequalities (31)–(38) does not hold either. It follows from standard Chernoff bound arguments [1] that T will find with probability at least $1 - c$ a frequency of failure greater than $\eta'/2$ for the corresponding event, and therefore will reject with at least that probability. $\square$

ACKNOWLEDGMENTS

The authors are grateful to Lajos Rónyai and Csaba Schneider for their useful remarks and suggestions.

6. REFERENCES

[1] N. Alon and J. Spencer. The probabilistic method. John Wiley & Sons, 1992.

[2] M. Bellare, D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan. Linearity testing in characteristic two. *IEEE Transactions on Information Theory*, 42(6), pp. 1781–1795, 1996.

[3] M. Bellare, S. Goldwasser, C. Lund and A. Russell. Efficient probabilistically checkable proofs and applications to approximations. In *Proceedings of 25th ACM STOC*, pp. 294–304, 1993.

[4] M. Bellare and M. Sudan. Improved non-approximability results. In *Proceedings of 26th ACM STOC*, pp. 184–193, 1994.

[5] M. Ben-Or, D. Coppersmith, M. Luby and R. Rubinfeld. Non-abelian homomorphism testing, and distributions close to their self-convolutions. In *Proceedings of 8th RANDOM, LNCS vol. 3122*, pp. 273–285, 2004.

[6] H. Buhrman, L. Fortnow, I. Newman and H. Röhrig, Quantum property testing, In *Proceedings of the 14th ACM-SIAM SODA*, pp. 480–488, 2003.

[7] E. Ben-Sasson, M. Sudan, S. Vadhan and A. Wigderson. Randomness-efficient Low Degree Tests and Short PCPs via Epsilon-Biased Sets. In *Proceedings of 35th ACM STOC*, pp. 612-621, 2003.

[8] M. Blum, M. Luby, and R. Rubinfeld. Self–testing/correcting with applications to numerical problems. *J. of Computer and System Sciences*, 47(3), pp. 549–595, 1993.

[9] K. Cheung and M. Mosca. Decomposing finite Abelian groups, *Quantum Information and Computation*, 1(3), pp. 26–32, 2001.

[10] F. Ergün, S. Kannan, R. Kumar, R. Rubinfeld and M. Viswanathan. Spot-Checkers. *J. of Computer and System Sciences*, 60(3), pp. 717–751, 2000.

[11] O. Goldreich. Combinatorial property testing — A survey. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, vol. 43, pp. 45–60, 1998.

[12] J. Håstad and A. Wigderson. Simple analysis of graph tests for linearity and PCP. *Random Structures and Algorithms*, vol. 22, no. 2, pp. 139-160, 2003.

[13] M. Kiwi, F. Magniez and M. Santha. Exact and approximate testing/correcting of algebraic functions: A survey. In *Proceedings of 1st Summer School on Theoretical Aspects of Computer Science*, LNCS vol. 2292 pp. 30–83, 2000.

[14] R. Lipton. New directions in testing. *Series in Discrete Mathematics and Theoretical Computer Science*, ACM/AMS, Vol. 2, pp. 191–202, 1991.

[15] S. Rajagopalan and L. Schulman. Verification of Identities. *SIAM J. Computing*, 29(4), pp. 1155-1163, 2000.
[16] M. Mosca and A. Ekert, The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer, In *Proceedings of the 1st NASA Int. Conf. on Quantum Computing and Quantum Communication, (QCQC'98), LNCS vol. 1509,* pp. 174–188, 1999.
[17] D. Ron. Property testing (A tutorial). *Handbook on Randomized Computing*, Kluwer Press, 2001.
[18] A. Samorodnitsky and L. Trevisan. A PCP characterisation of NP with optimal amortized query complexity. In *Proceedings of 32nd ACM STOC*, pp. 191–199, 2000.
[19] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. on Computing*, vol. 26(5), pp. 1484–1509, 1997.
[20] A. Shpilka and A. Wigderson. Derandomizing homomorphism testing in general groups. In *Proceedings of 36th ACM STOC*, pp. 427–435, 2004.

APPENDIX

Proof of Theorem 3

We start by proving a few claims. One of our main tool will be the following well-known fact.

FACT 1 (HALVING PRINCIPLE). *Let Ω and S denote finite sets such that $S \subseteq \Omega$, and let ψ be a boolean function defined over Ω. Then,*

$$\mathop{\mathbf{Pr}}_{x\in S}[\psi(x)] \leq \frac{|\Omega|}{|S|} \mathop{\mathbf{Pr}}_{x\in\Omega}[\psi(x)].$$

If Ω is twice the size of S, then $\mathbf{Pr}_{x\in\Omega}[\psi(x)]$ is at least one half of $\mathbf{Pr}_{x\in S}[\psi(x)]$. This motivates the choice of the name.

We define the relation E_D over $D_{4N} \times D_{4N}$, an approximate version of the earlier binary relation $E(x, y)$ as follows:

$$E_D(x, y) \Leftrightarrow \mathop{\mathbf{Pr}}_{u\in D_{4N}}[f(x+u) = f(y+u)] \geq 1/2.$$

Our first claim states that the majority is actually overwhelming.

CLAIM 4. *Let $x, y \in D_{4N}$. Then either*

$$\mathop{\mathbf{Pr}}_{u\in D_{4N}}[f(x+u) = f(y+u)] \geq 1 - 24\eta$$

or

$$\mathop{\mathbf{Pr}}_{u\in D_{4N}}[f(x+u) \neq f(y+u)] \geq 1 - 24\eta.$$

PROOF. The halving principle and (11) implies that

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u+v) = f(x+u)\cdot f(v)] \geq 1 - 4\eta,$$

and similarly

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(y+u+v) = f(y+u)\cdot f(v)] \geq 1 - 4\eta.$$

Therefore

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u+v) = f(y+u+v) \iff f(x+u)\cdot f(v) = f(y+u)\cdot f(v)] \geq 1 - 8\eta.$$

Again the halving principle and approximate invertibility (12) give

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u+v) = f(y+u+v) \iff f(x+u) = f(y+u)] \geq 1 - 12\eta.$$

Symmetrically

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u+v) = f(y+u+v) \iff f(x+v) = f(y+v)] \geq 1 - 12\eta,$$

so

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u) = f(y+u) \iff f(x+v) = f(y+v)] \geq 1 - 24\eta.$$

Rewriting the left hand side gives

$$\mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u) = f(y+u)]^2 + \mathop{\mathbf{Pr}}_{u,v\in D_{4N}}[f(x+u) \neq f(y+u)]^2 \geq 1 - 24\eta.$$

From this the statement follows because one of the inequalities

$$\mathop{\mathbf{Pr}}_{u\in D_{4N}}[f(x+u) = f(y+u)] \geq 1 - 24\eta,$$

and

$$\mathop{\mathbf{Pr}}_{u\in D_{twoENN}}[f(x+u) \neq f(y+u)]\} \geq 1 - 24\eta$$

must hold.

□

CLAIM 5. *E is an equivalence relation on D_{4N}.*

PROOF. Reflexivity is trivial, and S is symmetric because its definition is symetric. For the transitivity, $E_D(x, y) = 1$ and $E_D(y, z) = 1$, by Claim 4 implies that

$$\mathop{\mathbf{Pr}}_{u\in D_{4N}}[f(x+u) = f(z+u)] \geq 1 - 48\eta.$$

Therefore S is equivalence relation. □

CLAIM 6. *If $E_D(x_1, y_1)$ and $E_D(x_2, y_2)$ holds for some $x_1, y_1, x_2, y_2 \in D_{2N}$ then $E_D(x_1 + x_2, y_1 + y_2)$*

PROOF. We show first that the special case, when $x_2 = y_2$ is true. This will imply the claim, since from $E_D(x_1, y_1)$ follows that $E_D(x_1+x_2, y_1+x_2)$ and similarly from $E_D(x_2, y_2)$ follows that $E_D(y_1+x_2, y_1+y_2)$ and by transitivity $E_D(x_1+x_2, y_1+y_2)$.

We now prove the special case that is $E_D(x, y)$ implies $E_D(x+z, y+z) = 1$ when $x, y, z \in D_{2N}$. By Claim 4, $\mathbf{Pr}_{u\in D_{4N}}[f(x+u) = f(y+u)] \geq 1 - 24\eta$. Since the size of the intersection of D_{4N} and $z+D_{4N}$ is at least $6N$ and therefore $\mathbf{Pr}_{u\in D_{4N}}[f(x+z+u) = f(y+z+u)] \geq 3/4 - 24\eta \geq 1/2$. The claim follows from the definition of $E_D(x+z, y+z)$. □

We say that an element $x \in D_{4N}$ is *well-behaving* if

$$\mathop{\mathbf{Pr}}_{u\in D_{2N}}[f(x+u) = f(x)\cdot f(u)] \geq 4/5$$

and

$$\Pr_{u \in D_{2N}}[(f(x) \cdot f(u)) \cdot f(-u) = f(x)] \geq 4/5.$$

For $x \in D_{4N}$ its equivalence class on D_{4N} is denoted by $[x]$. We say that the element $x \in D_{4N}$ is *good* if it is well-behaving and $f(x) = \mathrm{Maj}_{y \in [x]}(f(y))$.

Claim 7. *Let $x_1, x_2 \in D_{4N}$ well-behaving elements. Then $[x_1] = [x_2]$ iff $f(x_1) = f(x_2)$.*

Proof. Because the x_i are well-behaving,

$$\Pr_{u \in D_{2N}}[f(x_i + u) = f(x_i) \cdot f(u)] \geq 4/5$$

and

$$\Pr_{u \in D_{2N}}[f(x_i + u) \cdot f(-u) = f(x_i)] \geq 4/5.$$

If $f(x_1) = f(x_2)$ then $\mathbf{Pr}_{u \in D_{2N}}[f(x_1 + u) = f(x_2 + u)] \geq 3/5$, so the classes $[x_1]$ and $[x_2]$ are the same.

On the other hand when $[x_1] = [x_2]$, by Claim 4 and the halving principle $\mathbf{Pr}_{u \in D_{2N}}[f(x_1 + u) = f(x_2 + u)] \geq 1 - 48\eta$, therefore $\mathbf{Pr}_{u \in D_{2N}}[f(x_1) = f(x_2)] \geq 1 - 48\eta - 4/5 > 0$. □

Claim 8. $\mathbf{Pr}_{x \in D_{2N}}[x \text{ \emph{non well-behaving} }] \leq 80\eta$.

Proof. The halving principle and (11) imply that

$$\Pr_{x,u \in D_{2N}}[f(x + u) \neq f(x) \cdot f(u)] \leq 16\eta$$

Now if we had that $\mathbf{Pr}_{x \in D_{2N}}[x \text{ non well-behaving }] > 80\eta$ then $\mathbf{Pr}_{x,u \in D_{2N}}[f(x + u) \neq f(x) \cdot f(u)] > 16\eta$. □

Claim 9. $\mathbf{Pr}_{x \in D_{2N}}[x \text{ \emph{bad} }] \leq 160\eta$.

Proof. We show that

$$\Pr_{x \in D_{2N}}[x \text{ bad and well-behaving }] \leq \Pr_{x \in D_{2N}}[x \text{ non well-behaving }].$$

In fact we show the stronger statement that this inequality holds when the probability is taken on a set E_D where E_D is the restriction of an equivalence class to D_{2N}. We know that the function is constant on the well-behaving elements of E_D (by Claim 7). Since the bad well-behaving elements do not form the majority inside E_D, the number of non well-behaving elements must be greater. □

Let us now finish the proof of Theorem 3. From Claim 9 follows by the halving principle that

$$\Pr_{x \in D_{\lceil N/2d \rceil}}[x \text{ good }] \geq 1 - 640d\eta > 1/2.$$

Therefore the number of good elements in $D_{\lfloor N/2d \rfloor}$ is greater than $|\Gamma|$, so by the pigeonhole principle there are two distinct good elements $x_1, x_2 \in D_{\lfloor N/2d \rfloor}$ such that $f(x_1) = f(x_2)$. Claim 7 implies that $[x_1] = [x_2]$. If we set $q = x_1 - x_2 \in D_{\lfloor N/d \rfloor}$ then, by Claim 6, $[q] = [0]$. Let m be an integer multiple of q such that $N/2d < m \leq N/d$. Again, Claim 6 implies that $[0] = [\pm m]$ and $[x + t_1 m] = [x + t_2 m]$ for every $x \in \mathbb{Z}_m$ and $|t_1|, |t_2| < \lfloor 2N/m \rfloor$. Now from Claim 7, Claim 8 and the halving principle follows (13).