Local Decoding and Testing for Homomorphisms

Elena Grigorescu Swastik Kopparty Madhu Sudan

May 4, 2007

Abstract

Locally decodable codes (LDCs) have played a central role in many recent results in theoretical computer science. The role of finite fields, and in particular, low-degree polynomials over finite fields, in the construction of these objects is well studied. However the role of group homomorphisms in the construction of such codes is not as widely studied. Here we initiate a systematic study of local decoding of codes based on group homomorphisms. We give an efficient list decoder for the class of homomorphisms from any abelian group G to a fixed abelian group H. The running time of this algorithm is bounded by a polynomial in $\log |G|$ and an agreement parameter, where the degree of the polynomial depends on H. Central to this algorithmic result is a combinatorial result bounding the number of homomorphisms that have large agreement with any function from G to H. Our results give a new generalization of the classical work of Goldreich and Levin, and give new abstractions of the list decoder of Sudan, Trevisan and Vadhan. As a by-product we also derive a simple(r) proof of the local testability (beyond the Blum-Luby-Rubinfeld bounds) of homomorphisms mapping $\mathbb{Z}_p^n$ to $\mathbb{Z}_p$, first shown by M. Kiwi.

1 Introduction

Given a pair of finite groups $G = (G, +)$ and $H = (H, \cdot)$, the class of homomorphisms between G and H forms an "error-correcting code". Namely, for any two distinct homomorphisms $\phi, \psi : G \to H$, the fraction of elements $\alpha \in G$ such that $\phi(\alpha) = \psi(\alpha)$ is at most $1/2$. This observation has implicitly driven the quest for many "homomorphism testers" [3, 2, 8, 1, 13], which test to see if a function $f : G \to H$ given as an oracle is close to being a homomorphism. In this paper, we investigate the complementary "decoding" question: Given oracle access to a function $f : G \to H$ find all homomorphisms $\phi : G \to H$ that are close to f.

To define the questions we study more precisely, let $\text{agree}(f, g)$ denote the agreement between $f, g : G \to H$, i.e., the quantity $\Pr_{x \leftarrow_U G}[f(x) = g(x)]$. Let $\text{Hom}(G, H) = \{\phi : G \to H \mid \phi(x + y) = \phi(x)\phi(y)\}$ denote the set of homomorphisms from G to H. We consider the *combinatorial* question: Given G, H and $\epsilon > 0$, what is the largest

"list" of functions that can have ϵ-agreement with some fixed function, i.e, what is $\max_{f:G\to H} |\{\phi : G \to H | \phi \in \mathrm{Hom}(G,H), \mathrm{agree}(f,g) \geq \epsilon\}|$?

We also consider the algorithmic question: Given G, H, $\epsilon > 0$ and oracle access to a function $f : G \to H$, (implicitly) compute a list of all homomorphisms $\phi : G \to H$ that have agreement ϵ with f. (A formal definition of implicit decoding will be given later. For now, we may think of this as trying to compute the value of ϕ on a set of generators of G.) We refer to this as the "local decoding" problem for homomorphisms.

Local decoding of homomorphisms for the special case of $G = \mathbb{Z}_2^n$ and $H = \mathbb{Z}_2$ was the central technical problem considered in the seminal work of Goldreich and Levin [4]. They gave combinatorial bounds showing that for $\epsilon = \frac{1}{2} + \delta$, the list size is bounded by $\mathrm{poly}(1/\delta)$, and gave a local decoding algorithm with running time $\mathrm{poly}(n/\delta)$.

The work of Goldreich and Levin was previously abstracted as decoding the class of degree one n-variate polynomials over the field of two elements. This led Goldreich, Rubinfeld, and Sudan [5] to generalize the decoding algorithm to the case of degree one polynomials over any finite field. (In particular, this implies a decoding algorithm for homomorphisms from $G = \mathbb{Z}_p^n$ to $H = \mathbb{Z}_p$, that decodes from $\frac{1}{p} + \epsilon$ agreement and runs in time $\mathrm{poly}(n/\epsilon)$, where $\mathbb{Z}_p$ denotes the additive group of integers modulo a prime p.) Later Sudan, Trevisan, and Vadhan [11], generalized the earlier results to the case of higher degree polynomials over finite fields . This generalization, in turn led to some general reductions between worst-case complexity and average-case complexity.

Our work is motivated by the group-theoretic view of Goldreich and Levin, as an algorithm to decode group homomorphisms. While the group-theoretic view has been applied commonly to the complementary problem of "homomorphism testing", the decoding itself does not seem to have been examined formally before.

To motivate we start with a simple example.

Consider the case where $G = \mathbb{Z}_p^n$ and $H = \mathbb{Z}_p^m$. How many homomorphisms can have agreement $\frac{1}{p} + \delta$ with a fixed function $f : G \to H$? Most prior work in this setting used (versions) of the Johnson bound in coding theory. Unfortunately such a bound only works for agreement greater than $\frac{1}{\sqrt{p}}$ in this setting.[1] An ad-hoc counting argument gives a better bound on the list size of $\delta^{-O(m)}$. While better bounds ought to be possible, none are known, illustrating the need for further techniques. Our work exposes several such questions. It also sheds new light on some of the earlier algorithms.

[1]For those familiar with the application of the Johnson bound in the setting of $m = 1$, we point out that it relied crucially on the fact that the agreement of any pair of homomorphisms was $\frac{1}{|H|}$ which is no longer true when $m \neq 1$.

Our results. Our results are restricted to the case of abelian groups G and H. Let $\Lambda = \Lambda_{G,H}$ denote the maximum possible agreement between two homomorphisms from G to H. Our main algorithmic result is an efficient algorithm, with running time $\mathrm{poly}(\log|G|, \frac{1}{\epsilon})$ to decode all homomorphisms with agreement $\Lambda + \epsilon$ with a function $f : G \to H$ given as an oracle, for any *fixed* group H. Note that in such a case the polynomial depends on H. See Theorem 5 for full details.

Crucial to our algorithmic result is a corresponding combinatorial one showing that there are at most $\mathrm{poly}(\frac{1}{\epsilon})$ homomorphisms with agreement $\Lambda_{G,H} + \epsilon$ with any function $f : G \to H$, for any fixed group H. Once again, the polynomial in the bound depends on H. See Theorem 4 for details.

Finally, we also include a new proof of a result of Kiwi [8] on testing homomorphisms from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p$. This is not related to our main quests, but we include it since some of the techniques we use to decode homomorphisms yield a simple proof of this result. See Theorem **??**.

Techniques Our results are derived by reducing the case of general abelian groups to the case of *p-groups*, i.e., groups of the form $Z_{p^{a_1}}^{n_1} \times \cdots \times Z_{p^{a_k}}^{n_k}$. We reduce both the combinatorial problem and the algorithmic problem to the case where G is a p-group and H is of the form Z_{p^r}. Our main technical result is a combinatorial bound on the list-size for homomorphisms from a p-group G to the group Z_{p^r}. For p-groups, the maximal agreement between homomorphisms is $\frac{1}{p}$. We show that the number of homomorphisms with agreement $\frac{1}{p} + \epsilon$ with any function is at most $(2p)^{3r}\frac{1}{\epsilon^2}$. (See Lemma 10.) This result is proved by Fourier analysis.

The algorithmic results are abstractions of algorithms of Goldreich and Levin [4] and Sudan, Trevisan, and Vadhan [11]. In particular, we note that the [4] algorithm can be viewed as an extension of any decoding algorithm for the classes $\mathrm{Hom}(G_1, H)$ and $\mathrm{Hom}(G_2, H)$ to the class $\hom(G_1 \times G_2, H)$. While this result is useful for general groups, if both G_1 and G_2 are p-groups (and hence also G), then the technique from [11] can be extended directly to get more efficient decoding algorithms.

Organization of this paper. In Section 2 we present basic terminology and our main results. In Section 3 we exploit the decomposition theorem for abelian groups to reduce the proofs of the main theorems to the special case of p-groups. In Section 4 we tackle the combinatorial problem of the list-size for p-groups. In Section 6 we consider the corresponding algorithmic problem. Section **??** analyzes a homomorphism tester for functions from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p$ using some techniques of the previous sections.

2 Definitions and Main Results

Let G, H be abelian groups, and let $\mathrm{Hom}(G, H) = \{h : G \to H \mid h \text{ is a homomorphism}\}$. Note that $\mathrm{Hom}(G, H)$ forms a *code*. Indeed, if $f, g \in \mathrm{Hom}(G, H)$, then $G' = \{x \mid$

$f(x) = g(x)\}$ is a subgroup of G. Since the largest subgroup of G has size at most $\frac{|G|}{2}$, it follows that f and g differ in at least $\frac{1}{2}$ of the domain.
For two functions $f, g : G \to H$, define

$$\text{agree}(f, g) = \Pr_{x \in G}[f(x) = g(x)],$$

and

$$\Lambda_{G,H} = \max_{f,g \in \text{Hom}(G,H), f \neq g} \{\text{agree}(f,\ g)\}.$$

In the case when $\text{Hom}(G, H)$ contains only the zero homomorphism we define $\Lambda_{G,H} = 0$.

Definition 1 *[11] (List decodability) The code* $\text{Hom}(G, H)$ *is* (δ, l)**-list decodable** *if for every function* $f : G \to H$*, there exist at most* l *homomorphisms* $h \in \text{Hom}(G, H)$ *such that* $\text{agree}(f, h) \geq \delta$*.*

Definition 2 *A probabilistic algorithm* M γ**-computes** *a function* f *if for all* x *in the domain of* f*,*

$$\Pr[M(x) = f(x)] \geq \gamma.$$

where the probability is taken over the randomness of $M(x)$*.*

Definition 3 *[14](Local list decoding) A probabilistic oracle algorithm* $\mathcal{A}$ *is a* (δ, T) *local list decoder for* $\text{Hom}(G, H)$ *if, for any function* $f : G \to H$*, when* $\mathcal{A}$ *is given oracle access to* f*, (written* $\mathcal{A}^f$*), the following hold:*

1. *,* $\mathcal{A}^f$ *outputs a list of probabilistic oracle machines* $M_1, \ldots, M_L$ *s.t., for any homomorphism* $h \in \text{Hom}(G, H)$ *with* $\text{agree}(f, h) \geq \delta$*, with probability at least* $\frac{3}{4}$ *over the random choices of* $\mathcal{A}^f$*,* $\exists j \in [L]$ *such that* M_j^f $\frac{3}{4}$*-computes* h*.*

2. $\mathcal{A}$ *and each* M_j^f *run in time* T*.*

An abelian group G can be represented (see Sect. 3) by its cyclic decomposition $\mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}}$, where p_i's are prime. This allows us a convenient and simple method of representing elements of groups as $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, with $\alpha_i \in \mathbb{Z}_{p_i^{e_i}}$.

Our main results are the list decodability and local list decodability of group homomorphism codes.

Theorem 4 *Let* H *be a fixed finite abelian group. For all finite abelian groups* G*,* $\text{Hom}(G, H)$ *is* $\left(\Lambda_{G,H} + \epsilon, \text{poly}_{|H|}(\frac{1}{\epsilon})\right)$ *list decodable.*

Remark: The exact polynomial bound on the list size that our proof gives, in general, depends on the structure of the groups in an intricate way, but can nevertheless be uniformly bounded by $O\left(\frac{1}{\epsilon^{4 \log |H|}}|H|^5\right)$. Still, the precise bounds obtained by the proof are not optimal. For example, our proof gives that $\text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^2)$ is $(\frac{1}{2} + \epsilon, O(\frac{1}{\epsilon^4}))$ list decodable, while it can be shown (via alternate means) that it is $(\frac{1}{2} + \epsilon, O(\frac{1}{\epsilon^2}))$ list decodable.

Theorem 5 *Let H be a fixed finite abelian group. For all finite abelian groups G there is a $(\Lambda_{G,H} + \epsilon, \mathrm{poly}_{|H|}(\log |G|, \frac{1}{\epsilon}))$ local list decoder for* $\mathrm{Hom}(G, H)$.

3 Decomposition and Reduction

We will embark on our quest by first decomposing the groups involved into slightly smaller but better-behaved groups. In this section we will see how these decompositions can be done and thereby reduce our main theorems to statements about list decoding on "p-groups". These statements will be proved in the following two sections by some Fourier analytic machinery and by generalizing the STV-style list decoders.

The structure theorem for finite abelian groups states that every abelian group G is of the form $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$, where the p_i's are primes (not necessarily distinct) and the e_i's are positive integers. A *p-group* is a group of order p^r, for some positive integer r. The structure theorem implies that for any prime p, any finite abelian group G can be written as $G_p \times G'$, where G_p is a p-group and $\gcd(p, |G'|) = 1$ (take $G_p = \prod_{p_i = p} \mathbb{Z}_{p_i^{e_i}}$). This decomposition will play a crucial role in what follows.

Remark $\Lambda_{G,H}$ behaves well under direct product decomposition of G and H:

1. If $\gcd(|G|, |H|) = 1$ then $\mathrm{Hom}(G, H)$ contains only the zero homomorphism and therefore, $\Lambda_{G,H} = 0$.

2. Otherwise, let p be the smallest prime s.t. $p \mid \gcd(|G|, |H|)$. Then $\Lambda_{G,H} = \frac{1}{p}$. To see this, let $g, h : G \to H$ be distinct homomorphisms. Let $d = |\mathrm{image}\ (g-h)|$ and note that $d \mid |H|$. Since $G/\ker(g-h) \cong \mathrm{image}(g-h)$, we have that $d \mid |G|$. It follows that $\mathrm{agree}(g, h) = |\ker(g-h)|/|G| = 1/d \leq 1/p$, and thus $\Lambda_{G,H} \leq \frac{1}{p}$. In the other direction, if $G = \mathbb{Z}_{p^t} \times G'$, and $H = \mathbb{Z}_{p^r} \times H'$, then the homomorphism $h : G \to H$ definde by $h(a, b) = (ap^{r-1}, 0)$ satisfies $\mathrm{agree}(h, \mathbf{0}) = \frac{1}{p}$. Hence, $\Lambda_{G,H} = \frac{1}{p}$.

3. The above observations imply $\Lambda_{G_1 \times G_2, H} = \max\{\Lambda_{G_1,H}, \Lambda_{G_2,H}\}$ and $\Lambda_{G,H_1 \times H_2} = \max\{\Lambda_{G,H_1}, \Lambda_{G,H_2}\}$.

3.1 The decompositions $G \to H_1 \times H_2$ and $G_1 \times G_2 \to H$

The following two propositions say that list decoding questions for $Hom(G, H)$ can be reduced to list decoding questions on summands of G or H.

Proposition 6 *Let G, H_1, H_2 be abelian groups. Let $a_i = \Lambda_{G,H_i}$. Suppose for all $\epsilon > 0$, $\mathrm{Hom}(G, H_i)$ is $(a_i + \epsilon, \ell_i(\epsilon))$-list decodable, with $(a_i + \epsilon, T_i(\epsilon))$ local list decoders, for $i = 1, 2$. Then $\mathrm{Hom}(G, H_1 \times H_2)$ is $(\max\{a_1, a_2\} + \epsilon, \ell_1(\epsilon)\ell_2(\epsilon))$ list decodable and has a $(\max\{a_1, a_2\} + \epsilon, O((T_1(\epsilon)T_2(\epsilon)))$ local list decoder, for all $\epsilon > 0$.*

Proof Take an $f = (f_1, f_2) : G \to H_1 \times H_2$. Consider the list of high-agreement homomorphisms

$$\mathcal{L} = \{h = (h_1, h_2) \in \mathrm{Hom}(G, H_1 \times H_2) : \mathrm{agree}(f, h) \geq \max\{a_1, a_2\} + \epsilon\}.$$

Also consider the corresponding lists for the two components:

$$\mathcal{L}_i = \{h_i \in \mathrm{Hom}(G, H_i) : \mathrm{agree}(f_i, h_i) \geq \max\{a_1, a_2\} + \epsilon\}.$$

By assumption, $|\mathcal{L}_i| \leq \ell_i(\epsilon)$. Now, since $\mathrm{agree}(f, h) \leq \min\{\mathrm{agree}(f_1, h_1), \mathrm{agree}(f_2, h_2)\}$, we have

$$\mathcal{L} \subset \mathcal{L}_1 \times \mathcal{L}_2, \tag{1}$$

and so $|\mathcal{L}| \leq \ell_1(\epsilon)\ell_2(\epsilon)$, which proves the list decodability. The local list decoding algorithm, which follows immediately from Equation (1), simply runs the appropriate local list decoders for f_1 and f_2 and takes the product of the lists[2]. ■

Proposition 7 *Let G_1, G_2, H be abelian groups. Let $a_i = \Lambda_{G_i,H}$. Suppose for all $\epsilon > 0$, $\mathrm{Hom}(G_i, H)$ is $(a_i+\epsilon, \ell_i(\epsilon))$-list decodable, with a $(a_i+\epsilon, T_i(\epsilon))$ local list decoder, for $i = 1, 2$. Then $\mathrm{Hom}(G_1 \times G_2, H)$ is $(\max\{a_1, a_2\} + \epsilon, O(\frac{1}{\epsilon^2}\ \ell_1(\epsilon)\ell_2(\epsilon)\ |H|^2))$ list decodable, and has a $(\max\{a_1, a_2\} + \epsilon,\ O(\frac{|H|}{\epsilon^2}\ (T_1(\epsilon) + T_2(\epsilon)) + \ell_1(\epsilon)\ell_2(\epsilon)\ |H|^2)$ local list decoder, for all $\epsilon > 0$.*

Proof We shall first give the local list decoder. Its analysis will give the claimed bound on the list decodability of $\mathrm{Hom}(G, H)$. Let $\mathcal{A}_i$ be the $(a_i + \epsilon, T_i(\epsilon))$-local list decoders for $\mathrm{Hom}(G_i, H)$.

The decoder will be based on the observation that any $h \in \mathrm{Hom}(G_1 \times G_2, H)$ can be written as $h(x, y) = h((x, 0)) + h((0, y)) = h_1(x) + h_2(y),\ \forall x \in G_1, \forall y \in G_2$ where $h_1(x) = h(x, 0) \in \mathrm{Hom}(G_1, H)$, $h_2(y) = h(0, y) \in \mathrm{Hom}(G_2, H)$.
Our local list decoder $\mathcal{B}(x, y)$ for $\mathrm{Hom}(G_1 \times G_2, H)$ finds good candidates for h_1 and h_2. Accordingly, the oracle machines' output will be of the form $M_{g_1,g_2}(x, y) = g_1(x) + g_2(y)$, where $g_1 \in \mathrm{Hom}(G_1, H)$, and $g_2 \in \mathrm{Hom}(G_2, H)$.

The local list decoder $\mathcal{B}(x, y)$:
Repeat $\Theta(\frac{1}{\epsilon^2})$ times:
Step 1: Pick $(x_0, y_0) \in G_1 \times G_2$ uniformly at random.
Step 2: For each $\alpha \in H$, run $\mathcal{A}_1$ (for agreement $a_1 + \frac{\epsilon}{2}$) on the function $f(\cdot, y_0) - \alpha$, and get list $\mathcal{L}_1^\alpha$.
Step 3: For each $\beta \in H$, run $\mathcal{A}_2$ (for agreement $a_2 + \frac{\epsilon}{2}$) on the function $f(x_0, \cdot) - \beta$, and get list $\mathcal{L}_2^\beta$.
Step 4: If for some pair $(\alpha_0, \beta_0) \in H^2$ there exist homomorphisms $g_1 \in \mathcal{L}_1^{\alpha_0}$ and $g_2 \in \mathcal{L}_2^{\beta_0}$ s.t. $\alpha_0 = g_2(y_0)$ and $\beta_0 = g_1(x_0)$, then output M_{g_1,g_2}.

[2]By repeating and taking majority, one can convert an algorithm that (say) 9/16-computes a function to one that 3/4-computes it, with just an $O(1)$ factor increase in running time.

Analysis: Fix a homomorphism $h \in \mathrm{Hom}(G_1 \times G_2)$ with $\mu := \mathrm{agree}(f,h) \geq \max(a_1, a_2) + \epsilon$. Call $x_0 \in G_1$ *good* for h if $\Pr_{y \in G_2}[f(x_0,y) = h(x_0,y)] \geq \mu - \frac{\epsilon}{2}$. Similarly, call $y_0 \in G_2$ *good* for h if $\Pr_{x \in G_1}[f(x,y_0) = h(x,y_0)] \geq \mu - \frac{\epsilon}{2}$.

Claim 8 $\Pr_{x_0 \in G_1}[x_0$ *is good* $] \geq \frac{\epsilon}{2}$ *and* $\Pr_{y_0 \in G_2}[y_0$ *is good* $] \geq \frac{\epsilon}{2}$.

Proof We just discuss the case of x_0, the y_0 case being identical. Let $D(x_0) = \Pr_y[f(x_0,y) \neq h(x_0,y)]$. We have $\mathbb{E}_{x_0}[D(x_0)] = 1 - \mu$. By Markov's inequality,

$$\begin{aligned}\Pr_{x_0}[x_0 \text{ is not good}] &= \Pr_{x_0}[D(x_0) > 1 - \mu + \frac{\epsilon}{2}] \\ &\leq \frac{1-\mu}{1-\mu+\frac{\epsilon}{2}} = 1 - \frac{\frac{\epsilon}{2}}{1-\mu+\frac{\epsilon}{2}} \leq 1 - \frac{\epsilon}{2}.\end{aligned}$$

■

Claim 9 *(Correctness) If* $h \in \mathrm{Hom}(G_1 \times G_2, H)$ *is s.t.* $\mathrm{agree}(f,h) \geq \mu$ *then with probability* $> \frac{9\epsilon^2}{64}$ *in any one iteration, one of the oracle machines* M *that is output* $9/16$*-computes* h.

Proof $x_0 \in G_1$ and $y_0 \in G_2$ are both good for h with probability $> \frac{\epsilon^2}{4}$. In this case, setting $\alpha = h(0,y_0)$ and $\beta = h(x_0,0)$, with probability at least $(\frac{3}{4})^2$, algorithm $\mathcal{A}_1$ will output a machine in $\mathcal{L}_1^\alpha$ that $\frac{3}{4}$-computes $h(\cdot,0)$ and algorithm $\mathcal{A}_2$ will output a machine in $\mathcal{L}_2^\beta$ that $\frac{3}{4}$-computes $h(0,\cdot)$. Thus, with probability at least $\frac{9}{16}\frac{\epsilon^2}{4}$, the algorithm will, in Step 5, (with $\alpha_0 = \alpha, \beta_0 = \beta, g_1 = h(\cdot,0), g_2 = h(0,\cdot)$), $M_{h(\cdot,0),h(0,\cdot)}$ will be output, which $\frac{9}{16}$-computes h.

■

The above claim implies that (for suitable choice of implicit constants, and suitably amplifying, with $O(1)$ slowdown, the correctness of the oracle machines) with probability $> 3/4$, a machine $3/4$-computing h will appear in the output list. ■

3.2 Proof of the main theorems

Using the propositions proved in the previous section, our theorems will reduce to the main lemma given below, which will itself be proved in Section 4 .

Lemma 10 *Let* p *be a fixed prime and* $r > 0$ *be a fixed integer. Then for any abelian* p*-group* G, $\mathrm{Hom}(G, \mathbb{Z}_{p^r})$ *is* $\left(\frac{1}{p} + \epsilon, (2p)^{3r}\frac{1}{\epsilon^2}\right)$ *list decodable.*

In Section 6, we shall use it to prove the corresponding algorithmic version.

Lemma 11 *Let p be a fixed prime and $r > 0$ be a fixed integer. Then for any abelian p-group G,* $\mathrm{Hom}(G, \mathbb{Z}_{p^r})$ *is* $\left(\frac{1}{p} + \epsilon, \mathrm{poly}(\log |G|, \frac{1}{\epsilon})\right)$ *locally list decodable.*

Proof [of Theorem 4] If $|G|, |H|$ are relatively prime then the result is obvious. Otherwise, let $p(= \frac{1}{\Lambda_{G,H}})$ be the smallest prime dividing both $|G|$ and $|H|$. Let $H = \prod_{i=1}^{k} \mathbb{Z}_{p_i^{\beta_i}}$. Let $i \in \{1, \ldots, k\}$. If $\gcd(p_i, |G|) = 1$, then $\mathrm{Hom}(G, \mathbb{Z}_{p_i^{\beta_i}})$ is $(\epsilon, 1)$ list decodable. Otherwise, write G as $G_{p_i} \times G'$, where G_{p_i} is a p_i-group and $\gcd(p_i, |G'|) = 1$. Then by Lemma 10 and Proposition 7, $\mathrm{Hom}(G, \mathbb{Z}_{p_i^{\beta_i}})$ is $\left(\frac{1}{p_i} + \epsilon, O(\frac{1}{\epsilon^4}(2p_i)^{3\beta_i} p^{2\beta_i})\right)$ list decodable, and hence is also $\left(\frac{1}{p} + \epsilon, \frac{1}{\epsilon^4} p_i^{5\beta_i}\right)$ list decodable (since if $p_i || G|$, then $p \leq p_i$). Combining these for all $i \in \{1, \ldots, k\}$ by Proposition 6, $\mathrm{Hom}(G, H)$ is $\left(\frac{1}{p} + \epsilon, \prod_{p_i || G|} (\frac{1}{\epsilon^4}(2p_i)^{5\beta_i})\right)$ list decodable, as required. ■

Proof [of Theorem 5] The proof of this theorem is directly analogous to the previous proof, using Lemma 11 instead of Lemma 10. ■

4 Combinatorial bounds for p-groups

In this section we will prove our main lemma (Lemma 10). Recall that we wish to obtain a upper bound on the number of homomorphisms having agreement $\frac{1}{p} + \epsilon$ with a function $f : G \to \mathbb{Z}_{p^r}$, where G is a p-group. The starting point for our proof is the observation that $\mathbb{Z}_{p^r}$ is isomorphic to μ_{p^r}, the multiplicative group of complex p^rth roots of unity. This makes the tools of Fourier analysis available to us. We begin by introducing the necessary background on Fourier analysis on finite abelian groups that we will use.

4.1 Preliminaries on Fourier Analysis

Let G be a finite abelian group. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the multiplicative group of non-zero complex numbers.
Suppose $G = \prod_{i=1}^{k} \mathbb{Z}_{p_i^{r_i}}$. Let $\omega_i \in \mathbb{C}$ be a primitive $p_i^{r_i} th$ root of unity. For any $\alpha \in G$, we get an explicitly defined character χ_α of G given by

$$\chi_\alpha(x) = \prod_{i=1}^{k} \omega_i^{\alpha_i x_i},$$

where $x = (x_1, \ldots, x_k)$ and $\alpha = (\alpha_1, \ldots, \alpha_k)$ (written as elements of $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{r_i}}$). In fact, any character of G is of this form.
Some useful properties of characters are given below:

- $\chi_{\mathbf{0}}(x) = 1$, for all $x \in G$
- $\chi_\alpha(x)\chi_\beta(x) = \chi_{\alpha+\beta}(x)$, hence $\chi_\alpha^i(x) = \chi_{i\alpha}(x)$.
- $\overline{\chi}_\alpha(x) = \chi_{-\alpha}(x)$.
- $\mathbb{E}_x \chi_\alpha(x)\overline{\chi}_\beta(x) = \begin{cases} 0, & \text{if } \alpha \neq \beta \\ 1, & \text{otherwise.} \end{cases}$

Given a function $f : G \to \mathbb{C}$, the *Fourier coefficients* of f are given by $\widehat{f} : G \to \mathbb{C}$,

$$\widehat{f}(\alpha) = \mathbb{E}_{x \in G}\ f(x)\overline{\chi}_\alpha(x).$$

Parseval's identity states

$$\sum_{\alpha \in G} \left|\widehat{f}(\alpha)\right|^2 = 1.$$

We will need a notion of division in abelian groups. For χ_α a character of G and $i \in \mathbb{Z}$, define the "set of quotients"

$$\left[\frac{\chi_\alpha}{i}\right] := \{\chi_\beta : (\chi_\beta)^i = \chi_\alpha\}$$

For S a set of characters of G and $i \in \mathbb{Z}$, define

$$\left[\frac{S}{i}\right] := \bigcup_{\chi_\alpha \in S} \left[\frac{\chi_\alpha}{i}\right] = \{\chi_\beta : (\chi_\beta)^i \in S\}$$

For $i, d \in \mathbb{Z}$ and p a prime, we say $p^i \| d$, if $p^i \mid d$ and $p^{i+1} \not| d$.

4.2 Sketch of the argument

Let us first give a sketch of the proof at a very high level. We are given a function $f : G \to \mathbb{Z}_{p^r}$. We begin by giving a formula that expresses the agreement between our function and any given homomorphism in terms of Fourier coefficients of some functions related to f. This will imply that every homomorphism having high agreement with f "corresponds" to some large Fourier coefficient. Now Parseval's identity tells us that there can only be few large Fourier coefficients, and the end of the proof looks near. Unfortunately, it is possible that many distinct homomorphisms "correspond" to the same Fourier coefficients. We will nevertheless be able to quantify the failure of the above approach in terms of the number of homomorphisms in $Hom(G, \mathbb{Z}_{p^l})$ having high agreement with a related function $f' : G \to \mathbb{Z}_{p^l}$, for some $l < r$. Inducting on r, with the base case $r = 1$ being handled by the Johnson bound, we will arrive at the result.

We proceed with the details. Let μ_{p^r} be the multiplicative group of the complex $p^r th$ roots of unity. Note that the groups $\mathbb{Z}_{p^r}$ and μ_{p^r} are isomorphic, and henceforth

we restrict our attention to $\mathrm{Hom}(G, \mu_{p^r})$. By definition, any element of $\mathrm{Hom}(G, \mu_{p^r})$ is a character of G and hence

$$\mathrm{Hom}(G, \mu_{p^r}) \subset \{\chi_\alpha : \alpha \in G\}.$$

The following lemma expresses the agreement between a function and a homomorphism in terms of Fourier coefficients.

Lemma 12 *Let G be a p-group. For $f : G \to \mu_{p^r}$ and $\chi_\alpha \in \mathrm{Hom}(G, \mu_{p^r})$*

$$\mathrm{agree}(f, \chi_\alpha) = \mathbb{E}_{0 \le j < p^r} \widehat{f^j}(j\alpha)$$

Proof We have

$$\begin{aligned}
\mathrm{agree}(f, \chi_\alpha) &= \mathbb{E}_{x \in G} \mathbb{E}_{0 \le j < p^r} \left(f(x)\overline{\chi_\alpha}(x)\right)^j \\
&= \mathbb{E}_{0 \le j < p^r} \mathbb{E}_{x \in G} f^j(x)\overline{\chi_{j\alpha}}(x) \\
&= \mathbb{E}_{0 \le j < p^r} \widehat{f^j}(j\alpha).
\end{aligned}$$

■

Before we start the proof of the main lemma, we sketch a proof of a corollary to the Johnson bound that we use for the base case of the induction, as well as in Sect. **??**.

Lemma 13 *Let G be a p-group. Then*

1. *$\mathrm{Hom}(G, \mu_p)$ is $(\frac{1}{p} + \epsilon, \frac{1}{\epsilon^2})$ list decodable, for any $\epsilon > 0$.*
2. *Let $f : G \to \mu_p$ and $\rho_t = \mathrm{agree}(f, \chi_t)$ for $\chi_t \in \mathrm{Hom}(G, \mu_p)$, then*

$$\sum_{\chi_t \in \mathrm{Hom}(G, \mu_p)} \left(\rho_t - \frac{1}{p-1}(1 - \rho_t)\right)^2 \le 1.$$

Proof For any function $h : G \to \mu_p$, associate a vector $v_h \in \mathbb{R}^{(p-1)|G|}$ such that the following properties hold:

- v_f is unit length
- If $f, g : G \to \mu_p$ then

$$\langle v_f, v_g \rangle = \mathrm{agree}(f, g) - \frac{1}{p-1}\left(1 - \mathrm{agree}(f, g)\right)$$

  where $\langle \cdot, \cdot \rangle$ denotes the usual vector inner product.

Such an embedding is explicitly given in [6]. For any distinct $\chi_\alpha, \chi_\beta \in \mathrm{Hom}(G, \mu_p)$, $\mathrm{agree}(\chi_\alpha, \chi_\beta) = \frac{1}{p}$, and this implies that $\{v_{\chi_\alpha} \mid \chi_\alpha \in \mathrm{Hom}(G, \mu_p)\}$ is a set of orthonormal vectors in $\mathbb{R}^{(p-1)|G|}$.

Thus, by Bessel's inequality,

$$\sum_{t \in G} \langle v_f, v_{\chi_t} \rangle^2 = \sum_{t \in G} \left(\rho_t - \frac{1}{p-1}(1-\rho_t) \right)^2 \leq \langle v_f, v_f \rangle = 1.$$

To prove the other part, notice that if $\mathrm{agree}(f, \chi_t) \geq \frac{1}{p} + \epsilon$ then $\langle v_f, v_{\chi_t} \rangle \geq \frac{p}{p-1}\epsilon > \epsilon$, and therefore there are at most $\frac{1}{\epsilon^2}$ values of $\chi_t \in \mathrm{Hom}(G, \mu_p)$ satisfying the above inequality. ■

4.3 The proof

Lemma 10. *Let G be a p-group.*[3] *Then* $\mathrm{Hom}(G, \mathbb{Z}_{p^r})$ *is* $\left(\frac{1}{p} + \epsilon, (2p)^{3r}\frac{1}{\epsilon^2}\right)$ *list decodable.*

Proof As suggested earlier, we identify $\mathbb{Z}_{p^r}$ with μ_{p^r}. We proceed by induction on r. The case $r = 1$ was proved in Lemma 13.

Let $r > 1$. By induction, assume the result is true for $\mathrm{Hom}(G, \mu_{p^k})$, for $k = 1, \ldots, r-1$. Take any $f : G \to \mu_{p^r}$ and $\epsilon > 0$. We wish to bound the size of $\mathcal{L} = \{\chi_\alpha \in \mathrm{Hom}(G, \mu_{p^r}) : \mathrm{agree}(f, \chi_\alpha) \geq \frac{1}{p} + \epsilon\}$.

By Lemma 12 (after removing $j = 0$ from the expectation) we get that for any $\chi_\alpha \in \mathcal{L}$,

$$\mathbb{E}_{0<j<p^r} \widehat{f^j}(j\alpha) \geq \frac{p^r}{p^r - 1}\left(\frac{1}{p} - \frac{1}{p^r} + \epsilon\right) > \frac{1}{p} - \frac{1}{p^r} + \epsilon.$$

This implies that for all $\chi_\alpha \in \mathcal{L}$, $\exists j$, $0 < j < p^r$ such that $|\widehat{f^j}(j\alpha)| > \frac{1}{p} - \frac{1}{p^r} + \epsilon$.

This naturally leads us to consider the set $S_i = \{\chi_\beta \in \mathrm{Hom}(G, \mu_{p^r}) : |\hat{f}^i(\beta)| > \frac{1}{p} - \frac{1}{p^r} + \epsilon\}$.

The above discussion implies that

$$\mathcal{L} \subset \bigcup_{i=1}^{p^r-1} \left[\frac{S_i}{i}\right].$$

At this point one would be tempted to bound $|\mathcal{L}|$ by $\sum_i \left|\left[\frac{S_i}{i}\right]\right|$. However, this approach is doomed to failure because the size of $\left[\frac{S_i}{i}\right]$ can be very large when $p \mid i$.

Instead, we perform a subtler manipulation:

$$\mathcal{L} \subset \bigcup_{i=1}^{p^r-1} \left(\left[\frac{S_i}{i}\right] \cap \mathcal{L} \right) = \bigcup_{i=1}^{p^r-1} \bigcup_{\chi_\alpha \in S_i} \left(\left[\frac{\chi_\alpha}{i}\right] \cap \mathcal{L} \right) \tag{2}$$

[3] In fact, the lemma holds for any abelian group G, by the same proof. Here we state it only for p-groups as this is the case that is needed for the main algorithmic lemma.

It turns out that although $\left|\left[\frac{\chi_\alpha}{i}\right]\right|$ can be large, the induction hypothesis implies that $\left|\left[\frac{\chi_\alpha}{i}\right] \cap \mathcal{L}\right|$ cannot be large.

The following two statements formalize this and will be used to bound $|\mathcal{L}|$:

1. For each i, $|S_i| \leq 4p^2$:
   By Parseval's identity we know that

   $$\sum_{\beta \in G} |\hat{f}^i(\beta)|^2 = 1,$$

   and so

   $$1 \geq \sum_{\chi_\beta \in S_i} |\hat{f}^i(\beta)|^2 \geq |S_i| \left(\frac{1}{p} - \frac{1}{p^r} + \epsilon\right)^2,$$

   which proves the statement (recall that $r > 1$).

2. If $p^l \| i$, then for any $\alpha \in G$, $|[\,\frac{\chi_\alpha}{i}\,] \cap \mathcal{L}| \leq (2p)^{3l} \frac{1}{\epsilon^2}$:
   To prove this part, we shall find a function $g : G \to \mu_{p^l}$ and a one-to-one map $T : \left[\frac{\chi_\alpha}{i}\right] \cap \mathcal{L} \to \mathrm{Hom}(G, \mu_{p^l})$ such that for all $\chi_\beta \in \left[\frac{\chi_\alpha}{i}\right] \cap \mathcal{L}$, $\mathrm{agree}(T(\chi_\beta), g) \geq \frac{1}{p} + \epsilon$. Notice that this together with the induction hypothesis for $\mathrm{Hom}(G, \mu_{p^l})$, proves the statement.

   Let $\chi_{\beta_0} \in \left[\frac{\chi_\alpha}{i}\right]$. Define $g : G \to \mu_{p^l}$ by

   $$g(x) = \begin{cases} f(x)\overline{\chi_{\beta_0}}(x), & \text{if } f(x)\overline{\chi_{\beta_0}}(x) \in \mu_{p^l} \\ 1, & \text{otherwise} \end{cases}$$

   Define $T : \left[\frac{\chi_\alpha}{i}\right] \cap \mathcal{L} \to \mathrm{Hom}(G, \mu_{p^l})$ by

   $$T(\chi_\beta) = \chi_\beta \overline{\chi_{\beta_0}}.$$

   By construction, for all $x \in G$,

   $$(T(\chi_\beta)(x))^i = (\chi_{\beta-\beta_0}(x))^i = \chi_{i(\beta-\beta_0)}(x) = 1. \tag{3}$$

   Now since $T(\chi_\beta) \in \mathrm{Hom}(G, \mu_{p^r})$ and $p^l || i$, (3) implies that $T(\chi_\beta) \in \mathrm{Hom}(G, \mu_{p^l})$. T is injective since it is just multiplication by a non-zero function. Furthermore, if $f(x) = \chi_\beta(x)$, then $g(x) = T(\chi_\beta)(x)$, and so $\mathrm{agree}(g, T(\chi_\beta)) \geq \mathrm{agree}(f, \chi_\beta)$. Thus g and T have the required properties, and the statement follows.

The two facts above enable us to bound $|\mathcal{L}|$ as follows:

$$\begin{aligned}
|\mathcal{L}| &\leq \sum_i \sum_{\chi_\alpha \in S_i} \left| \left[\frac{\chi_\alpha}{i}\right] \bigcap \mathcal{L} \right| && \text{(by (2))} \\
&\leq \sum_{l=0}^{r-1} \sum_{\substack{0<i<p^r \\ p^l || i}} |S_i|(2p)^{3l}\frac{1}{\epsilon^2} && \text{(by statement 2 above)} \\
&\leq \sum_{l=0}^{r-1} (p^{r-l} - p^{r-l-1})(4p^2)(2p)^{3l}\frac{1}{\epsilon^2} && \text{(by statement 1 above)} \\
&\leq \frac{1}{\epsilon^2}(2p)^{3r}.
\end{aligned}$$

This completes the induction and the proof of our lemma. ■

5 Subgroups, Cosets and a Sampling Lemma

In this section we will introduce some terminology and prove some lemmas in preparation for the local list decoder for p-groups given in the next section.

Let G be an abelian p-group and let $T = p^d$ be the largest order of any element in G. For $z_1, \ldots, z_k \in G$, denote by $S_{z_1,\ldots,z_k}$ the subgroup of G generated by $z_1, \ldots, z_k$.

Let $R_{x,z_1,\ldots,z_k}$ be the set $x + S_{z_1-x,\ldots,z_k-x}$ (the "affine subspace" passing through $x, z_1, \ldots, z_k$). For a function $g : G \to H$, define the restriction $g|_{R_{x,z_1,\ldots,z_k}} : S_{z_1-x,\ldots,z_k-x} \to H$ by $g|_{R_{x,z_1,\ldots,z_k}}(y) = g(y + x)$. By this definition, if g is a homomorphism, then $g|_{R_{x,z_1,\ldots,z_k}}(y) = g(y + x) = g(y) + g(x)$, and thus $g|_{R_{x,z_1,\ldots,z_k}}$ is an *affine homomorphism*, i.e., a function of the form $h + b$ where h is a homomorphism and $b \in H$.

In general, for a fixed k, the cardinality of $S_{z_1,\ldots,z_k}$ could vary drastically, and consequently there is no simple and natural way of indexing its elements. All our dealings with $S_{z_1,\ldots,z_k}$ will be via the homomorphism

$$\pi_{z_1,\ldots,z_k} : \mathbb{Z}_T^k \to S_{z_1,\ldots,z_k}$$

given by[4]

$$\pi_{z_1,\ldots,z_k}(\bar{\alpha}) = \sum_{i=1}^{k} \alpha_i z_i.$$

By choice of T, this map is a surjection, and hence $S_{z_1,\ldots,z_k} \cong \mathbb{Z}_T^k/(\ker \pi_{z_1,\ldots,z_k})$. Further, for $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}_T^k$, we have that $\pi_{z_1,\ldots,z_k}(\bar{\alpha}) = \pi_{z_1,\ldots,z_k}(\bar{\beta})$ iff $\bar{\alpha} - \bar{\beta} \in \ker \pi_{z_1,\ldots,z_k}$. This easily implies the following proposition.

[4]Abusing notation, for $a \in \mathbb{Z}_T$ (which we interpret as a nonnegative integer $< T$) and $z \in G$, the "product" az represents z added to itself a times. By choice of T, the map $\mathbb{Z}_T \times G \to G$ given by $(a, z) \mapsto az$ is a group homomorphism in each variable.

Proposition 14 *For any* $z \in S_{z_1,\ldots,z_k}$,

$$\frac{|\pi^{-1}_{z_1,\ldots,z_k}(z)|}{T^k} = \frac{1}{|S_{z_1,\ldots,z_k}|}$$

.

The above proposition shows how one can use the map π for sampling elements from $R_{x,z_1,\ldots,z_k}$. The next lemma does a similar thing for list decoding.

Lemma 15 *Let* $g : S_{z_1-x,\ldots,z_k-x} \to H$ *be any function. For all* $\delta > 0$, *there is a one-to-one correspondence between the following sets:*

$$\mathcal{L}_1 = \{(h, b) \in \mathrm{Hom}(S_{z_1-x,\ldots,z_k-x}, H) \times H : \mathrm{agree}(h + b, g) \geq \frac{1}{p} + \delta\}$$
$$\mathcal{L}_2 = \{(h', b') :\in \mathrm{Hom}(\mathbb{Z}_T^k, H) \times H : \mathrm{agree}(h' + b', g \circ \pi_{z_1-x,\ldots,z_k-x}) \geq \frac{1}{p} + \delta\}$$

where $(h, b) \in \mathcal{L}_1$ *corresponds to* $(h \circ \pi_{z_1-x,\ldots,z_k-x}, b) \in \mathcal{L}_2$. *Furthermore, the corresponding agreements* $\mathrm{agree}(h + b, g)$ *and* $\mathrm{agree}((h + b) \circ \pi_{z_1-x,\ldots,z_k-x}, g \circ \pi_{z_1-x,\ldots,z_k-x})$ *are equal.*

Proof Define $\alpha : \mathcal{L}_1 \to \mathcal{L}_2$ by

$$\alpha(h, b) := (h \circ \pi_{z_1-x,\ldots,z_k-x}, b).$$

Proposition 14 implies that $\mathrm{agree}(h+b, g) = \mathrm{agree}(h \circ \pi_{z_1-x,\ldots,z_k-x} + b, g \circ \pi_{z_1-x,\ldots,z_k-x})$ (and hence the range of $\alpha(h, b)$ is indeed $\mathcal{L}_2$).

The following diagram is helpful in visualizing the setup.

$$\mathbb{Z}_T^k \xrightarrow{\pi_{z_1-x,\ldots,z_k-x}} S_{z_1-x,\ldots,z_k-x} \xrightarrow{g} H$$

Since $\pi_{z_1-x,\ldots,z_k-x}$ is onto, α is one-to-one. To show that α is onto, take $(h', b') \in \mathcal{L}_2$. Consider two cases:

- **Case 1:** $h'(\ker \pi_{z_1-x,\ldots,z_k-x}) = 0$
  Define $h : S_{z_1-x,\ldots,z_k-x} \to H$ by $h(z) = h'(z')$ for any $z' \in \pi^{-1}_{z_1-x,\ldots,z_k-x}(z)$. Since $h'(\ker \pi_{z_1-x,\ldots,z_k-x}) = 0$, the above definition does not depend on choice of z' and so h is well defined. It is easy to see that h is a homomorphism and that $\alpha(h, b') = (h', b')$.

- **Case 2:** $h'(\ker \pi_{z_1-x,\ldots,z_k-x}) \neq 0$
  In this case, since $h'(\ker \pi_{z_1-x,\ldots,z_k-x})$ is the homomorphic image of a p-group, $|h'(\ker \pi_{z_1-x,\ldots,z_k-x})| \geq p$. Furthermore, as z varies over $\ker \pi_{z_1-x,\ldots,z_k-x}$, the map $h'(z)$ assumes each value in $h'(\ker \pi_{z_1-x,\ldots,z_k-x})$ an equal number of times.

This implies that for any coset of $\ker \pi_{z_1-x,\ldots,z_k-x}$, the map $h' + b'$ equals any particular element in H on at most $\frac{1}{p}$ of the coset.

However $g \circ \pi_{z_1-x,\ldots,z_k-x}$ is constant on cosets of $\ker \pi_{z_1-x,\ldots,z_k-x}$. Therefore $\text{agree}(h' + b', g) \leq \frac{1}{p}$, and so this case cannot occur. [5]

Thus α is a bijection. ■

Remark The above lemma is, in general, *false* for $\delta = 0$.

5.1 The Sampling Lemma

We now prove our main sampling lemma.

Lemma 16 (Sampling Lemma) *Let G be an abelian p-group, let $A \subseteq G$, with $\mu = \frac{|A|}{|G|}$ and let $x, z_1, \ldots z_k \in G$ be picked uniformly at random. Then*

$$\Pr_{x,z_1,\ldots,z_k}\left[\left|\frac{|A \cap (x + S_{z_1,\ldots,z_k})|}{|S_{z_1,\ldots,z_k}|} - \mu\right| > \epsilon\right] \leq \frac{1}{\epsilon^2 p^k}.$$

Proof

We shall use the second moment method. The key is to find the right underlying random variables to study. Note that this could potentially be tricky since the size of $S_{z_1,\ldots z_k}$ can vary drastically. Proposition 14 will play a crucial role in dealing with this.

For $\bar{\alpha} \in \mathbb{Z}_T^k$, consider the random variable $Y_{\bar{\alpha}} = x + \pi_{z_1,\ldots,z_k}(\bar{\alpha})$. By Proposition 14, for any $\bar{\alpha} \in \mathbb{Z}_T^k$, $Y_{\bar{\alpha}}$ is uniformly distributed on G. The next claim identifies many pairwise-independent pairs of $Y_{\bar{\alpha}}$'s.

Claim 17 *Let $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}_T^k$ for which $\exists i \in [k]$ such that $p \not| \alpha_i - \beta_i$. Then $Y_{\bar{\alpha}}$ and $Y_{\bar{\beta}}$ are pairwise independent.*

[5] The situation can be summarized succinctly as follows. We have the exact sequence:

$$0 \longrightarrow \ker \pi \longrightarrow \mathbb{Z}_T^k \longrightarrow S_{z_1-x,\ldots,z_k-x} \longrightarrow 0.$$

Applying the left exact contravariant functor $\text{Hom}(-, H)$, we get the exact sequence,

$$0 \longrightarrow \text{Hom}(S_{z_1-x,\ldots,z_k-x}, H) \longrightarrow \text{Hom}(\mathbb{Z}_T^k, H) \longrightarrow \text{Hom}(\ker \pi, H),$$

and hence $h' \in \text{Hom}(\mathbb{Z}_T^k, H)$ is of the form $h \circ \pi$ iff $h'|_{\ker \pi} = 0$. The argument above implies that if $g : S_{z_1-x,\ldots,z_k-x} \to H$ is such that $\text{agree}(g \circ \pi, h') > \frac{1}{p}$, then $h'|_{\ker \pi} = 0$, and hence h' is of the form $h \circ \pi$.

Proof Without loss of generality, suppose $p \not| \alpha_1 - \beta_1$. Recall that this implies that for any $z' \in G$, there is exactly one $z'' \in G$ such that $(\alpha_1 - \beta_1)z'' = z'$. Now, for any $a, b \in G$

$$\begin{aligned}
\Pr_{x,z_1,\ldots,z_k}[Y_{\bar{\alpha}} = a \wedge Y_{\bar{\beta}} = b] &= \Pr_{x,z_1,\ldots,z_k}\left[\left(\sum_{i=1}^{k}(\alpha_i - \beta_i)z_i = b - a\right) \wedge (Y_{\bar{\beta}} = b)\right] \\
&= \Pr_{x,z_1,(z_2,\ldots,z_k)}\left[\left((\alpha_1 - \beta_1)z_1 = (b-a) - \sum_{i=2}^{k}(\alpha_i - \beta_i)z_i\right) \wedge \left(x = b - \sum_{i=1}^{k}\beta_i z_i\right)\right] \\
&= \frac{1}{|G|^2}
\end{aligned}$$

where the last step follows from the independence of x and z_1 and the above mentioned fact. ■

Define random variable $I_{\bar{\alpha}} = 1$ if $Y_{\bar{\alpha}} \in A$ and $I_{\bar{\alpha}} = 0$ otherwise. Thus $\mathbb{E}[I_{\bar{\alpha}}] = \mu$. Let $X = \frac{1}{T^k}\sum_{\bar{\alpha}\in\mathbb{Z}_T^k} I_{\bar{\alpha}}$. By Proposition 14, we have that

$$X = \frac{|A \cap (x + S_{z_1,\ldots,z_k})|}{|S_{z_1,\ldots,z_k}|} \tag{4}$$

We wish to bound $\Pr[|X - \mu| > \epsilon]$. Now $\mathbb{E}[X] = \mu$. Below we shall estimate the variance of X and complete the proof using Chebyshev's inequality.

$$\begin{aligned}
\mathbb{E}[X^2] = \frac{1}{T^{2k}}\mathbb{E}[(\sum_{\bar{\alpha}} I_{\bar{\alpha}})^2] &= \frac{1}{T^{2k}}\mathbb{E}[\sum_{\bar{\alpha},\bar{\beta}} I_{\bar{\alpha}} I_{\bar{\beta}}] \\
&= \frac{1}{T^{2k}}\mathbb{E}\sum_{\substack{\bar{\alpha},\bar{\beta} \\ \exists i,p|\alpha_i-\beta_i}} I_{\bar{\alpha}} I_{\bar{\beta}} + \frac{1}{T^{2k}}\mathbb{E}\sum_{\substack{\bar{\alpha},\bar{\beta} \\ \forall i,p|\alpha_i-\beta_i}} I_{\bar{\alpha}} I_{\bar{\beta}} \\
&= \frac{1}{T^{2k}}\sum_{\substack{\bar{\alpha},\bar{\beta} \\ \exists i,p|\alpha_i-\beta_i}} \mathbb{E}[I_{\bar{\alpha}}]\mathbb{E}[I_{\bar{\beta}}] + \frac{1}{T^{2k}}\sum_{\substack{\bar{\alpha},\bar{\beta} \\ \forall i,p|\alpha_i-\beta_i}} \mathbb{E}[I_{\bar{\alpha}} I_{\bar{\beta}}] \\
&\leq (1 - \frac{1}{p^k})\mu^2 + \frac{1}{p^k}.
\end{aligned}$$

The last step follows from Claim 17 and the fact that for each fixed $\bar{\alpha} \in G$ there are exactly $\frac{1}{p^k}T^k$ $\bar{\beta}$'s s.t. $p \mid (\alpha_i - \beta_i)$ for all $i \in [k]$. Therefore, $Var[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2 \leq (1 - \frac{1}{p^k})\mu^2 + \frac{1}{p^k} - \mu^2 \leq \frac{1}{p^k}$.

By Chebyshev's inequality, $\Pr_{\{x,(z_i)\}}[|X - \mu| > \epsilon] \leq \frac{1}{p^k\epsilon^2}$, and thus by (4), the lemma follows. ■

Proposition 18 *Let l, k be positive integers and let p be a prime. Let M be a $k \times k$ integer matrix. Then there exists a $k \times k$ integer matrix A such that $AM \equiv I \mod p^l$ (where I is the $k \times k$ identity matrix) iff $\det M \not\equiv 0 \mod p$.*

Proof The "only if" direction is clear. To prove the "if" part, we will use the Hensel lifting lemma. Suppose we are given a system of polynomials with integer coefficients $P_1(x_1, \ldots, x_m), \ldots, P_m(x_1, \ldots, x_m)$ and a point $a \in \mathbb{Z}^m$ such that:

- $P_i(a) \equiv 0 \mod p$ for $i \in [m]$.
- The Jacobian matrix at a, $J(a)$ (given by $J(a)_{ij} = \frac{\partial p_i}{\partial x_j}(a)$) is invertible mod p

Then the Hensel lifting lemma says that for any $l > 0$ there exists a point $b \in \mathbb{Z}^m$ such that

- $b \equiv a \mod p$.
- $P_i(b) \equiv 0 \mod p^l$ for $i \in [m]$.

Suppose $\det M \not\equiv 0 \mod p$. For an indeterminate $k \times k$ matrix X, consider the expression $P(X) = XM - I$. This is a system of k^2 polynomials in k^2 unknowns. Setting $X = M^{-1}$ (the inverse of M over the field $\mathbb{Z}_p$), we get $P(X) \equiv 0 \mod p$. Further, from the form of these polynomials it can be checked that $\det J(X) = (\det M)^k \neq 0$. Thus by Hensel's lifting lemma, there exists an integer matrix A such that $AM \equiv I \mod p^l$. ■

Lemma 19 *Let $z_1, \ldots, z_k \in G$. Let $y_1, \ldots, y_k$ be picked uniformly at random from $S_{z_1,\ldots,z_k}$. Then*

$$\Pr_{y_1,\ldots,y_k}[S_{y_1,\ldots,y_k} = S_{z_1,\ldots,z_k}] > \frac{1}{10}.$$

Proof Pick $\bar{\alpha}_1, \ldots, \bar{\alpha}_k$ uniformly at random from $\mathbb{Z}_T^k$. By Proposition 14, the distribution of $(y_1, \ldots, y_k)$ is identical to the distribution of $(\pi_{z_1,\ldots,z_k}(\bar{\alpha}_1), \ldots, \pi_{z_1,\ldots,z_k}(\bar{\alpha}_k))$. Thus we can (and do) assume that the y_i are generated in this manner, i.e., $y_i = \pi_{z_1,\ldots,z_k}(\bar{\alpha}_i)$.

It is clear that if $\bar{\alpha}_1, \ldots, \bar{\alpha}_k$ generate $\mathbb{Z}_T^k$, then $y_1, \ldots, y_k$ generate $S_{z_1,\ldots,z_k}$ and hence $S_{y_1,\ldots,y_k} = S_{z_1,\ldots,z_k}$. Thus it suffices to prove that

$$\Pr_{\bar{\alpha}_1,\ldots,\bar{\alpha}_k}\left[\bar{\alpha}_1, \ldots, \bar{\alpha}_k \text{ generate } \mathbb{Z}_T^k\right] > \frac{1}{10}.$$

Now, $\bar{\alpha}_1, \ldots, \bar{\alpha}_k$ generate $\mathbb{Z}_T^k$ iff $\exists a_{ij} \in \mathbb{Z}$ such that for all $i \in [k]$, $\sum_{j=1}^k a_{ij}\bar{\alpha}_j = \bar{e}_i$ (here $\bar{e}_i$ is the element of $\mathbb{Z}_T^k$ with 1 in the i^{th} coordinate and 0 in all the other coordinates). This is equivalent to saying that there is a $k \times k$ matrix A with entries in $\mathbb{Z}$ such that $AM \equiv I \mod T$, where M is the $k \times k$ matrix with $M_{jl} = (\bar{\alpha}_j)_l$, and

I is the $k \times k$ identity matrix. Thus, by Proposition 18 (recalling that T is a power of p), it suffices to show that

$$\Pr_{\alpha_1,\ldots,\alpha_k}[\det M \not\equiv 0 \mod p] > \frac{1}{10}.$$

Since $\det M \mod p$ depends only on the values $\mod p$ of the entries of M, this is clearly equivalent to showing that at least $\frac{1}{10}$ of all $k \times k$ matrices with entries in $\mathbb{Z}_p$ are non-singular.

But the fraction of $k \times k$ $\mathbb{Z}_p$-matrices that are nonsingular can be written explicitly as

$$\prod_{i=1}^{k}\left(1 - \frac{1}{p^i}\right).$$

This quantity is bounded from below by

$$\left(1 - \frac{1}{p}\right)\left(1 - \sum_{i=2}^{\infty}\frac{1}{p^i}\right) > \frac{1}{10}$$

for all primes p, as required. ■

6 Algorithmic results for p-groups

Here we will show Lemma 11 stated in Section 3.

Lemma 11. *Let p be a fixed prime and $r > 0$ be a fixed integer. Then for any abelian p-group G, $Hom(G, \mathbb{Z}_{p^r})$ is $\left(\frac{1}{p} + \epsilon, \mathrm{poly}(\log|G|, \frac{1}{\epsilon})\right)$ locally list decodable.*

We will provide an algorithm which, given access to a function $f : G \to \mathbb{Z}_{p^r}$, with G a p-group, outputs an implicit representation of the homomorphisms that agree in a $\frac{1}{p} + \epsilon$ with f.

6.1 The generalized STV algorithm

Proposition 20 (Self-Correctors [3]) *For any $g : G \to H$, there is a randomized procedure $Corr^g : G \to H$ running in time $\mathrm{poly}(\log|G|)$ satisfying the following property: if there is some homomorphism $h : G \to H$ with $\mathrm{agree}(g, h) > 7/8$, then $Corr^g$ $\frac{3}{4}$-computes h.*

To illustrate the strategy underlying the list decoder, consider the following scenario. Suppose $f : G \to H$ agrees with homomorphism $h : G \to H$ on $\frac{1}{p} + \epsilon$ points. Now if we pick $z_1, \ldots, z_k \in G$ randomly and independently, by the Sampling Lemma

with high probability for most x, $f|_{R_{x,z_1,\ldots,z_k}}$ and $h|_{R_{x,z_1,\ldots,z_k}}$ (which is an affine homomorphism) will have agreement at least $\frac{1}{p}+\epsilon/2$. Thus in order to find the value of $h(x)$, it seems like the following would be a reasonable strategy: List decode $f|_{R_{x,z_1,\ldots,z_k}}$ for all affine homomorphisms that have agreement $\frac{1}{p}+\frac{\epsilon}{2}$ with it. $R_{x,z_1,\ldots,z_k}$ being a coset of group generated by few elements, should be easier to list decode on. Finally, by the combinatorial bound, the list size is small, and at a crucial juncture of the analysis we will utilize this bound to disambuguate the list and systematically select and ! collate the affine homomorphisms on $R_{x,z_1,\ldots,z_k}$ that arise as restrictions of global homomorphisms. Assembling these ideas into the framework of local list decoding, we arrive at our local list decoder.

The oracle $M^f_{z_1,\ldots,z_k,a_1,\ldots,a_k}(x)$**:**
For $b \in H$, define $m_b : \mathbb{Z}_T^k \to H$ by $m_b(\bar{\alpha}) = b + \sum \alpha_i(a_i - b)$.
1: For each b in H, estimate [6] (by random sampling)
$l_b := \text{agree}(m_b, f|_{R_{x,z_1,\ldots,z_k}} \circ \pi_{z_1-x,\ldots,z_k-x})$.
2: If there is exactly one b with $l_b > \frac{1}{p} + \frac{\epsilon}{4}$ then output b, else fail.

The local list decoder:
Repeat $O(1)$ times:
1: Pick $z_1, \ldots, z_k \in G$ uniformly and independently at random, where $k = c \log_p \frac{1}{\epsilon}$.
2: For each $(a_1, \ldots, a_k) \in H^k$, output $Corr^{M^f_{z_1,\ldots,z_k,a_1,\ldots,a_k}}$.

6.2 Analysis

Lemma 21 *If $h : G \to H$ is a homomorphism such that* $\text{agree}(h, f) \geq \frac{1}{p} + \epsilon$ *then*

$$\Pr_{z_1,\ldots,z_k}\left[\Pr_x[M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x) = h(x)] \geq 7/8\right] \geq 3/4.$$

Proof The following two claims prove that certain events occur with low probability. As we shall see, these are the events that prevent $M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x) = h(x)$.

Claim 22 *There is a constant c_1, such that for $k > c_1 \log_p \frac{1}{\epsilon}$ we have*

$$\Pr_{x,z_1,\ldots,z_k}[M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x) \text{ finds } l_{h(x)} < \frac{1}{p} + \frac{\epsilon}{2}] \leq \frac{1}{100}.$$

Proof By definition, $l_{h(x)} = \text{agree}(m_h(x), f|_{R_{x,z_1,\ldots,z_k}} \circ \pi_{z_1-x,\ldots,z_k-x})$. We have

$$\begin{aligned} m_{h(x)}(\bar{\alpha}) &= h(x) + \sum_i \alpha_i(h(z_i) - h(x)) \\ &= h(x) + \sum_i (\alpha_i h(z_i - x)) \\ &= h|_{R_{x,z_1,\ldots,z_k}} \circ \pi_{z_1-x,\ldots,z_k-x}(\bar{\alpha}). \end{aligned}$$

As noted earlier, $h|_{R_{x,z_1,\ldots,z_k}}$ is an affine homomorphism. Therefore, by Lemma 15, $l_{h(x)} \geq \frac{1}{p} + \frac{\epsilon}{2}$ iff $\text{agree}(h|_{R_{x,z_1,\ldots,z_k}}, f|_{R_{x,z_1,\ldots,z_k}}) \geq \frac{1}{p} + \frac{\epsilon}{2}$. Setting $A = \{x : f(x) = h(x)\}$,

$$\text{agree}(h|_{R_{x,z_1,\ldots,z_k}}, f|_{R_{x,z_1,\ldots,z_k}}) = \frac{|A \cap R_{x,z_1,\ldots,z_k}|}{|R_{x,z_1,\ldots,z_k}|} = \frac{|A \cap (x + S_{z_1-x,\ldots,z_k-x})|}{|S_{z_1-x,\ldots,z_k-x}|}.$$

Thus, by the Sampling Lemma, for suitable c_1,

$$\Pr\left[l_{h(x)} < \frac{1}{p} + \frac{\epsilon}{2}\right] = \Pr\left[\frac{|A \cap (x + S_{z_1-x,\ldots,z_k-x})|}{|S_{z_1-x,\ldots,z_k-x}|} < \frac{1}{p} + \frac{\epsilon}{2}\right] = \frac{4}{\epsilon^2 p^k} < \frac{1}{100}$$

■

Let $\mathcal{L}(x, z_1, \ldots, z_k)$ be the list of all affine homomorphisms $g : S_{z_1-x,\ldots,z_k-x} \to H$ such that

$$\text{agree}(g, f|_{R_{x,z_1,\ldots,z_k}}) > \frac{1}{p} + \frac{\epsilon}{8}.$$

Let $B(x, z_1, \ldots, z_k)$ denote the event:
There exist $g_1, g_2 \in \mathcal{L}(x, z_1, \ldots, z_k)$ with $g_1 \neq g_2$, such that for all $j \in [k]$, $g_1(z_j) = g_2(z_j)$.

Claim 23 *There is a constant c_2 such that for any $k \geq c_2 \log_p \frac{1}{\epsilon}$, we have*

$$\Pr_{x,z_1,\ldots,z_k}[B(x, z_1, \ldots, z_k)] < \frac{1}{100}.$$

Proof

We shall show that for some $c_2 > 0$, with k as above, the following stronger estimate holds: For all $x \in G$, for all $\zeta_1, \ldots, \zeta_k \in G$, setting $R = R_{x,\zeta_1,\ldots,\zeta_k}$:

$$\Pr_{z_1,\ldots,z_k}[B(x, z_1, \ldots, z_k) | R_{x,z_1,\ldots,z_k} = R] < \frac{1}{100}.$$

Averaging this over all possible choices of R gives us the claim.

Fix $\zeta_1, \ldots, \zeta_k \in G$. Pick $y_1, \ldots, y_k$ independently and uniformly at random from $R_{x,\zeta_1,\ldots,\zeta_k}$. Let E be the event that $y_1 - x, \ldots, y_k - x$ generate $S_{\zeta_1-x,\ldots,\zeta_k-x}$ (as a group). The key observation is that the distribution of $(z_1, \ldots, z_k)$ given $R_{x,z_1,\ldots,z_k} = R$ is identical to the distribution of $(y_1, \ldots, y_k)$ given E.

Notice that $R_{x,z_1,\ldots,z_k} = R$ implies that $\mathcal{L}(x, z_1, \ldots, z_k) = \mathcal{L}(x, \zeta_1, \ldots, \zeta_k)$. Fix $g_1 \neq g_2 \in \mathcal{L}(x, \zeta_1, \ldots, \zeta_k)$. Since they are both affine homomorphisms, $\Pr_{y \in R}[g_1(y) = g_2(y)] \leq \frac{1}{p}$. Let $C_{g_1,g_2} = \{y \in R : g_1(y) = g_2(y)\}$.

The key observation above gives us

$$\Pr_{z_1,\ldots,z_k}[\forall j, g_1(z_j) = g_2(z_j) | R_{x,z_1,\ldots,z_k} = R] = \Pr_{y_1,\ldots,y_k}[(y_1, \ldots, y_k) \in C^k_{g_1,g_2} | E]. \quad (5)$$

Our strategy will be to bound $\Pr[(y_1,\ldots,y_k)\in C^k_{g_1,g_2}|E]$ by relating it to $\Pr[(y_1,\ldots,y_k)\in C^k_{g_1,g_2}]$. To this end, write

$$\Pr[(y_1,\ldots,y_k)\in C^k_{g_1,g_2}|E]\Pr[E]+\Pr[(y_1,\ldots,y_k)\in C^k_{g_1,g_2}|\bar{E}]\Pr[\bar{E}]$$
$$=\Pr[(y_1,\ldots,y_k)\in C^k_{g_1,g_2}]=\frac{1}{p^k}.$$

Lemma 19 tells us that $\Pr[E]\geq\frac{1}{10}$. So,

$$\Pr[(y_1,\ldots,y_k)\in C^k_{g_1,g_2}|E]\leq\frac{1}{p^k\Pr[E]}<\frac{10}{p^k}.$$

Thus (5) gives us that for any particular $g_1,g_2\in\mathcal{L}(x,\zeta_1,\ldots,\zeta_k)$,

$$\Pr_{z_1,\ldots,z_k}[\forall j,g_1(z_j)=g_2(z_j)|R_{x,z_1,\ldots,z_k}=R]\leq\frac{10}{p^k}$$

Applying the above estimate to each pair $g_1,g_2\in\mathcal{L}(x,\zeta_1,\ldots,\zeta_k)$ (setting $L=|\mathcal{L}(x,\zeta_1,\ldots,\zeta_k)|$), and combining with the union bound,

$$\Pr_{z_1,\ldots,z_k}[B(x,z_1,\ldots,z_k)|R_{x,z_1,\ldots,z_k}=R]\leq\frac{10\binom{L}{2}}{p^k}.$$

By the combinatorial list decoding bound, Lemma 10, we have that $L\leq O(p^r(2p)^{3r}\frac{1}{\epsilon^2})$ (remember these are affine homomorphisms, not just homomorphisms).

Therefore, there exists a constant c_2 s.t. for $k\geq c_2\log_p(\frac{1}{\epsilon})$ we have the desired probability $<\frac{5L^2}{p^k}<\frac{1}{100}$. ■

By the above claims, with probability $<\frac{1}{100}$, $M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x)$ estimates $l_{h(x)}\leq\frac{1}{p}+\frac{\epsilon}{2}$, and with probability $\leq\frac{1}{100}$, it finds at least two values of b for which $l_b>\frac{1}{p}+\frac{\epsilon}{8}$. In the absence of these two events, $M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x)$ estimates $l_{h(x)}>\frac{1}{p}+\frac{\epsilon}{2}$ and $h(x)$ is the unique such b, i.e., in this case oracle $M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x)$ outputs $h(x)$. Thus,

$$\Pr_{x,z_1,\ldots,z_k}[M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x)=h(x)]\geq 49/50.$$

By Markov's inequality, we conclude that

$$\Pr_{z_1,\ldots,z_k}[\ \Pr_x[M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}(x)=h(x)]\geq 7/8]\geq\frac{3}{4}.$$

■

Proof of Lemma 11

Let h be a homomorphism that agrees with f on a $\frac{1}{p}+\epsilon$ fraction of points. Consider the oracle $M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}$ (i.e., the a_i are "consistent" with h). By Lemma 21, with probability at least $3/4$ over the choice of $z_1,\ldots,z_k$, the oracle machine $M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}$ correctly computes h on at least $\frac{7}{8}$ of the $x \in G$. Therefore, the self-corrected version $Corr^{M^f_{z_1,\ldots,z_k,h(z_1),\ldots,h(z_k)}}$ $\frac{3}{4}$-computes h on all of G with probability at least $\frac{3}{4}$, as required. It is easily seen that the local list decoder and the oracles both run in time at most $\mathrm{poly}(\log|G|, \frac{1}{\epsilon})$.

7 Linearity testing over finite fields

In this section we will prove a result of Kiwi using techniques related to Section 4.

We shall work on the finite field $\mathbb{F}_q$, where $q = p^r$ is a power of the prime p. Given $f : \mathbb{F}_q^n \to \mathbb{F}_q$. We consider the following linearity test:

- Pick $x, y \in \mathbb{F}_q^n$, $\alpha, \beta \in \mathbb{F}_q^*$ uniformly at random
- Accept if $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$, else reject.

Kiwi [8] analyzed this test to get the following theorem.

Theorem 24 *Suppose f is acceptd by the above test with probability δ, then f has agreement at least δ with some linear function*[7] *in* $\mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q)$.

His proof uses the MacWilliams identities and properties of the Krawtchouk polynomials. Here we give a simple proof of the above theorem using elementary Fourier analysis.

First some generalities on finite fields (see [**?**]).

For $t \in \mathbb{F}_q^n$, let the linear function $h_t : \mathbb{F}_q^n \to \mathbb{F}_q$ be defined by

$$h_t(x) = t \cdot x.$$

These are clearly all the $\mathbb{F}_q$-linear functions.

Recall the definition of the trace function, the $\mathbb{F}_p$-linear function $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$,

$$\mathrm{Tr}(x) = \sum_{i=0}^{r-1} x^{p^i}.$$

The trace will play a crucial role in our proofs because we can explicitly describe all the characters of $\mathbb{F}_q^n$ in terms of this function. For $t \in \mathbb{F}_q^n$, let character $\chi_t : \mathbb{F}_q^n \to \mathbb{C}$ be defined by

$$\chi_t(x) = \omega^{\mathrm{Tr}(h_t(x))}$$

[7] In this section, the linear functions we consider are *vector space homomorphisms*, i.e., functions that are $\mathbb{F}_q$-linear.

where ω is a primitive p^{th} root of unity. The χ_t are all the characters of $\mathbb{F}_q^n$ and hence we can use them to do Fourier analysis.

It will also be useful to introduce twisted complex-embedded versions of f. For $c \in \mathbb{F}_q$, define $f_c : \mathbb{F}_q^n \to \mathbb{C}$ by $f_c(x) = \omega^{\mathrm{Tr}(cf(x))}$.

Proof The proof is modeled along the general lines of the argument in [2] (i.e., expressing everything in terms of Fourier coefficients and comparing).

For $\eta \in \mathbb{F}_q$, define $\mathcal{S}(\eta) = \mathbb{E}_{c \in \mathbb{F}_q^*}[\omega^{\mathrm{Tr}(c\eta)}]$. From the equidistribution properties of the trace function, it can be seen that:

$$\mathcal{S}(\eta) = \begin{cases} 1, & \text{if } \eta = 0 \\ \frac{-1}{q-1}, & \text{otherwise} \end{cases}$$

For $t \in \mathbb{F}_q^n$ let ρ_t be the agreement of f with h_t. We shall prove that $\delta \leq \max_{t \in \mathbb{F}_q^n} \rho_t$. This will prove the result.

We begin by finding an explicit formula for ρ_t in terms of the Fourier coefficients of the f_c (this is essentially Lemma 12).

$$\rho_t - \frac{1}{q-1}(1-\rho_t) = \mathbb{E}_{x \in \mathbb{F}_q^n}[S(f(x) - h_t(x))] = \mathbb{E}_{x \in \mathbb{F}_q^n, c \in \mathbb{F}_q^*}[\omega^{\mathrm{Tr}(cf(x))}\omega^{-\mathrm{Tr}(ch_t(x))}] \quad (6)$$

$$= \mathbb{E}_{c \in \mathbb{F}_q^*}\mathbb{E}_{x \in \mathbb{F}_q^n}[f_c(x)\overline{\chi_{ct}}(x)] = \mathbb{E}_{c \in \mathbb{F}_q^*}[\hat{f}_c(ct)] \quad (7)$$

We now find a similar formula for δ and perform some manipulations that allow us to relate it to our formula for ρ_t.

$$\delta - \frac{1}{q-1}(1-\delta) = \mathbb{E}_{x,y \in \mathbb{F}_q^n}\mathbb{E}_{\alpha,\beta \in \mathbb{F}_q^*}\left[S\left(\alpha f(x) + \beta f(y) - f(\alpha x + \beta y)\right)\right] \quad (8)$$

$$= \mathbb{E}_{x,y \in \mathbb{F}_q^n}\mathbb{E}_{\alpha,\beta \in \mathbb{F}_q^*}\left[\mathbb{E}_{c \in \mathbb{F}_q^*}[\omega^{\mathrm{Tr}(c\alpha f(x))}\omega^{\mathrm{Tr}(c\beta f(y))}\omega^{\mathrm{Tr}(-cf(\alpha x+\beta y))}]\right] \quad (9)$$

$$= \mathbb{E}_{x,y}\mathbb{E}_{\alpha,\beta}\mathbb{E}_c\left[f_{c\alpha}(x)f_{c\beta}(y)f_{-c}(\alpha x + \beta y)\right] \quad (10)$$

$$= q^n\mathbb{E}_{x,y,z}\mathbb{E}_{\alpha',\beta',\gamma'}\left[f_{\alpha'}(x)f_{\beta'}(y)f_{\gamma'}(z)\mathbf{1}(\alpha'x + \beta'y + \gamma'z = 0)\right] \quad (11)$$

$$(12)$$

where we substituted $\alpha' = c\alpha, \beta' = c\beta, \gamma' = -c, z = \alpha x + \beta y$ (and one verifies that $z = \alpha x + \beta y$ is equivalent to $\alpha' x + \beta' y + \gamma' z = 0$). Note that since $\gamma' \in \mathbb{F}_q^*$, the probability that a random $z \in \mathbb{F}_q^n$ is such that $\alpha' x + \beta' y + \gamma' z = 0$ is $\frac{1}{q^n}$.

$$\begin{aligned}
(12) &= q^n\mathbb{E}_{x,y,z}\mathbb{E}_{\alpha',\beta',\gamma'}\left[f_{\alpha'}(x)f_{\beta'}(y)f_{\gamma'}(z)\mathbb{E}_{t \in \mathbb{F}_q^n}[\overline{\chi_t}(\alpha'x + \beta'y + \gamma'z)]\right] \\
&= q^n\mathbb{E}_t\left[\mathbb{E}_{\alpha',\beta',\gamma'}\mathbb{E}_x\left[f_{\alpha'}(x)\overline{\chi_{\alpha' t}}(x)\right]\mathbb{E}_y\left[f_{\beta'}(y)\overline{\chi_{\beta' t}}(y)\right]\mathbb{E}_z\left[f_{\gamma'}(z)\overline{\chi_{\gamma' t}}(z)\right]\right] \\
&= \sum_t\left[\mathbb{E}_{\alpha',\beta',\gamma'}\left[\hat{f_{\alpha'}}(\alpha' t)\hat{f_{\beta'}}(\beta' t)\hat{f_{\gamma'}}(\gamma' t)\right]\right] \\
&= \sum_t\left(\mathbb{E}_{\alpha' \in \mathbb{F}_q^*}[\hat{f_{\alpha'}}(\alpha' t)]\right)^3
\end{aligned}$$

By (7), this is equal to

$$\sum_t \left(\rho_t - \frac{1}{q-1}(1-\rho_t)\right)^3$$

which

$$\leq \max_t \left(\rho_t - \frac{1}{q-1}(1-\rho_t)\right) \sum_t \left(\rho_t - \frac{1}{q-1}(1-\rho_t)\right)^2 \leq \max_t \left(\rho_t - \frac{1}{q-1}(1-\rho_t)\right)$$

The last step follows from Lemma 13.
So

$$\delta - \frac{1}{q-1}(1-\delta) \leq \max_t \left(\rho_t - \frac{1}{q-1}(1-\delta)\right)$$

and therefore

$$\delta \leq \max_t \rho_t.$$

■

Acknowledgments

Thanks to Amir Shpilka for many valuable discussions.

References

[1] Michael Ben-Or, Don Coppersmith, Michael Luby, Ronitt Rubinfeld, Non-Abelian Homomorphism Testing, and Distributions Close to their Self-Convolutions. RANDOM 2004.

[2] Mihir Bellare and Don Coppersmith and Johan Håstad and Marcos Kiwi and Madhu Sudan. Linearity testing over characteristic two. *IEEE Transactions on Information Theory*, 42(6), 1781-1795, 1996.

[3] Manuel Blum and Michael Luby and Ronitt Rubinfeld. Self-Testing/Correcting with Applications to Numerical Problems. *Journal of Computer and System Sciences*, 47(3), 549-595, 1993.

[4] Oded Goldreich and Leonid Levin. A hard-core predicate for all one-way functions. *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, 25–32, 1989

[5] Oded Goldreich and Ronitt Rubinfeld and Madhu Sudan. Learning polynomials with queries: The highly noisy case. *SIAM Journal on Discrete Mathematics,* 13(4):535-570, 2000.

[6] Venkatesan Guruswami and Madhu Sudan. List decoding algorithms for certain concatenated codes. *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, 181-190, 2000.

[7] Marcos Kiwi , Frédéric Magniez , Miklos Santha. Exact and approximate testing/correcting of algebraic functions: A survey. *Theoretical Aspects of Computer Science,* Teheran, Iran, Springer-Verlag, LNCS 2292, 30-83, 2002.

[8] Marcos Kiwi. Testing and weight distributions of dual codes. *Theoretical Computer Science*, 299(1–3):81-106, 2003.

[9] Eyal Kushilevitz and Yishay Mansour. Learning decision trees using the Fourier spectrum. SIAM Journal on Computing 22(6):1331-1348, 1993.

[10] Dana Moshkovitz, Ran Raz. Sub-Constant Error Low Degree Test of Almost Linear Size, STOC 2006.

[11] Madhu Sudan and Luca Trevisan and Salil Vadhan. Pseudorandom generators without the XOR lemma, *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* 537-546, 1999.

[12] Madhu Sudan. Algorithmic Introduction to Coding Theory. Lecture Notes, 2001.

[13] Amir Shpilka and Avi Wigderson. Derandomizing Homomorphism Testing in General Groups. *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 427-435, 2004.

[14] L. Trevisan. Some Applications of Coding Theory in Computational Complexity. Survey Paper. *Quaderni di Matematica* 13:347-424, 2004