List decoding group homomorphisms between supersolvable groups*

Alan Guo[1] and Madhu Sudan[2]

1 **CSAIL,**
Massachusetts Institute of Technology,
32 Vassar Street, Cambridge, MA, USA.
aguo@mit.edu

2 **Microsoft Research**
One Memorial Drive, Cambridge, MA, USA
madhu@mit.edu

Abstract

We show that the set of homomorphisms between two supersolvable groups can be locally list decoded up to the minimum distance of the code, extending the results of Dinur et al who studied the case where the groups are abelian. Moreover, when specialized to the abelian case, our proof is more streamlined and gives a better constant in the exponent of the list size. The constant is improved from about 3.5 million to 105.

1998 ACM Subject Classification F.2.2 Computation on Discrete Structures

Keywords and phrases Group theory, error-correcting codes, locally decodable codes

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

It is well-known that for any pair of groups G and H with G being finite, the set of homomorphisms from G to H form an error-correcting code with $\omega(1)$ distance (since any two distinct homomorphisms agree on a subgroup of G which has size a constant factor smaller than that of G). The most classical example of such a setting is when G is the additive group over $\mathbb{F}_2^n$ and $H = \mathbb{F}_2$ (where $\mathbb{F}_q$ denotes the finite field of size q). The seminal work of Goldreich and Levin [3] gave an "efficient local list-decoding" algorithm for this particular setting. Such an algorithm has oracle access to a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and given $\epsilon > 0$, reports all homomorphisms ϕ that agree with f on $1/2 + \epsilon$ fraction of the points in time $\mathrm{poly}(\log |G|, \log |H|, 1/\epsilon)$.

A natural question, given the centrality of the Goldreich-Levin algorithm in coding theory and learning theory, is to ask what is the most general setting in which it works. In particular, one abstraction of the (original) Goldreich-Levin algorithm is that it uses coding theory (in particular, the Johnson bound of coding theory) to get a combinatorial bound on the list size, namely the number of functions that may have agreement $1/2+\epsilon$ with the function f. It then uses some decomposability properties of the domain $\mathbb{F}_2^n$ to get an algorithm for the list-decoding. Grigorescu et al. [7] and Dinur et al. [1], extended this abstraction to the more general setting of abelian groups. They first analyze $\delta_{G,H}$, the minimum possible distance between two homomorphisms from G to H. They then consider the task of recovering all

* The first author was partially supported by NSF grants CCF-0829672, CCF-1065125, and CCF-6922462, and an NSF Graduate Research Fellowship.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 1–12
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

homomorphisms at distance $\delta_{G,H} - \epsilon$ from a given function f. Roughly they show that the "decomposability" used in the algorithmic step of Goldreich and Levin can be generalized to the case of direct sum of abelian groups, so if $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$ and each G_i is small and also if H is small, then the algorithmic step can be extended. This reduces the list-decoding question to the combinatorial one. Here the standard bounds from coding theory are insufficient, however one can use decompositions of the group H into prime cyclic groups to show that the list size is at most $\mathrm{poly}(1/\epsilon)$.

In this work, we take this line of work a step further and explore this algorithm in the setting where G and H are not abelian. In this setting decompositions of G and H turn out to be more complex, and indeed even the question of determining $\delta_{G,H}$ turns out to be non-trivial. This question is explored in a companion work by the first author [8], where $\delta_{G,H}$ is determined explicitly for a broad class of groups, including the case of "supersolvable" groups which we study here. To describe the groups we consider we recall some basic group-theoretic terminology.

A subset $N \subseteq G$ is a subgroup of G, denote $N \leq G$, if N is closed under the group operation. A subgroup $N \leq G$ is said to be normal in G, denoted $N \lhd G$, if $aN = Na$ for all $a \in G$, where $aN = \{an | n \in N\}$ and $Na = \{na | n \in N\}$. If $N \lhd G$, then the set of cosets of N in G form a group under the operation $(aN)(bN) = (abN)$. This group is denoted G/N. G is *solvable* if there exists a series of groups $\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$ such that G_i/G_{i-1} is abelian for every i. We refer to the sequence $\langle 1_G = G_0, G_1, \ldots, G_k = G\rangle$ as the solvability chain of G. G is *supersolvable* if it has a solvability chain $\langle 1_G = G_0, G_1, \ldots, G_k = G\rangle$ where $G_i \lhd G$ and G_i/G_{i-1} is cyclic for every i.

1.1 Our results

Our main results, stated somewhat informally, are the following:

- **(Combinatorial list decodability)** There exists a constant $C \approx 105$ such that if G and H are *supersolvable* groups, then for any $f : G \to H$, the number of (affine) homomorphisms from G to H disagreeing with f on less than $\delta_{G,H} - \epsilon$ fraction of G is at most $(1/\epsilon)^C$. (See Theorem 3.4.)
- **(Algorithmic list decodability)** Let G be a solvable group and H be any group such that the set of homomorphisms from G to H have nice combinatorial list-decodability, i.e., the number of homomorphisms from G to H that have distance $\delta_{G,H} - \epsilon$ from a fixed function f is at most $(1/\epsilon)^C$. Then, the set of homomorphisms from G to H can be locally list decoded up to $\delta_{G,H} - \epsilon$ errors in $\mathrm{poly}(\log |G|, \log |H|, \frac{1}{\epsilon})$ time assuming oracle access to the multiplication table of H.[1] (See Theorem 4.2.)

Putting the two ingredients together we get efficient list-decoding algorithms up to radius $\delta_{G,H} - \epsilon$ whenever G and H are supersolvable.

1.1.0.1 Potential extensions and limits.

The case of solvable groups appears to be a natural limit to the nature of results given above, but we are not able achieve even this limit due to technical limitations which only

[1] For the group G we only need to be able sample its elements in a specific way, and compute f on elements sampled in such a way. Using the (super)solvability of G, we can guarantee that such a sampling oracle of size $\mathrm{poly}\log |G|$ can be provided for every G. For H we are not aware of a similar result which allows for a presentation of its elements, and providing access to the group operation with size $\mathrm{poly}\log |H|$. Hence we are forced to make this an explicit assumption.

allows us to deal with the case where the quotient group of successive members in the solvability chain are cyclic. It seems possible to go slightly beyond the results mentioned above though. Say that a group G is k-supersolvable if $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$ where G_i/G_{i-1} is supersolvable for every i. It seems likely that our techniques extend immediately to show that for every k there exists a constant C_k such that for every $\epsilon > 0$ there are at most ϵ^{-C_k} homomorphisms that disagree with any function $f : G \to H$ on $\delta_{G,H} - \epsilon$ fraction of inputs, provided G is k-supersolvable and H is solvable. If so, an algorithmic result would also follow. We hope to report on these extensions in a fuller version of this paper. Finally, if G and H are not solvable then it appears that we have much poorer understanding of the set of homomorphisms as codes. Indeed the behavior of $\delta_{G,H}$ is no longer clean. For example, when G and H are solvable $\delta_{G,H} = 1 - 1/p$ for some prime p. But Guo [8] shows that this is no longer necessarily true if the groups are not solvable. In particular $\delta_{A_5,A_5} = 9/10$ where A_5 is the alternating group on 5 elements.

1.2 Motivation and Contributions

The study of list-decoding of homomorphisms is motivated by a few objectives. First, an abstraction of the list-decoding algorithm highlights the minimal assumptions needed to make it work. Here our work extends the understanding in terms of reducing the dependence on commutativity (and so in principle can apply to the decoding of matrix-valued functions).

A second motivation, emerging from the works of [7, 1], is to extend combinatorial analyses of list-decoding to settings beyond those where the Johnson bound is applicable. Specifically the previous works used the Johnson bound when the target group was $\mathbb{Z}_p$ for prime p and then used the group-theoretic framework to extend the analysis first to the case of cyclic groups of prime power (so $H = \mathbb{Z}_{p^k}$ for prime p and integer k) and then to the case of general abelian groups. Each one of these steps lost in the exponent. Specifically [1] gave a function $C : \mathbb{R} \to \mathbb{R}$ such that the list size grew as $(1/\epsilon)^{C(2)}$ when $H = \mathbb{Z}_{p^k}$ and $(1/\epsilon)^{C(C(2))}$ for general groups. They didn't calculate the exponents explicitly, but $C(2) \approx 105$ and $C(C(2)) \approx 3.5 \times 10^6$. Our more general abstraction ends up cleaning up their proof significantly, and even improves their exponent significantly. Specifically, we are able to apply the inductive analysis implicit in previous works directly to the solvability chain of H (rather than working with the product structure) and this allows us to merge the two steps in previous works to get a list-size bound of $(1/\epsilon)^{C(2)}$ for all supersolvable groups. Thus the abstraction and generalization improves the list-size bounds even in the abelian case. Our analysis shows that the list-decoding radius is as large as the distance. We note that there are relatively few cases of codes that are known to be list-decodable up to their minimum distance. This property is shown to be true for folded Reed-Solomon codes [10, 9], derivative/multiplicity codes [11, 12], Reed-Muller codes [6, 4], homomorphisms between abelian groups [7, 1], and codes obtained by tensor products of any of the above [5].

Finally, a potential objective would be to get new codes with better list-decodability than existing codes. Unfortunately, this hope remains unrealized in this work as well as in [7, 1].

1.3 Overview of proof

We first prove the combinatorial bound on the list size by following the framework developed by [1], which works as follows. First, find groups $\{1\} = H_{(0)}, H_{(1)}, \ldots, H_{(m)} = H$ in such a way that any homomorphism $\phi \in \mathrm{Hom}(G, H)$ naturally induces a homomorphism

$\phi^{(i)} \in \mathrm{Hom}(G, H_{(i)})$. This gives a natural notion of "extending" a homomorphism $\psi \in \mathrm{Hom}(G, H_{(i)})$: ϕ extends ψ if $\phi^{(i)} = \psi$. One then shows inductively that if $\psi \in \mathrm{Hom}(G, H_{(i)})$ has significant agreement with $f^{(i)}$, then there are not too many $\phi \in \mathrm{Hom}(G, H)$ extending ψ with significant agreement with f. In [1], H is abelian and is decomposed as $H = \mathbb{Z}_{{p_1}^{r_1}}^{e_1} \oplus \cdots \oplus \mathbb{Z}_{{p_r}^{r_m}}^{e_m}$. One may take $H_{(i)}$ to be the direct sum of all but the last i summands. Then every $f : G \to H$ is naturally written as $f = (f_1, \ldots, f_m)$ where $f_i : G \to \mathbb{Z}_{{p_i}^{r_i}}^{e_i}$, and thus $f^{(i)} = (f_1, \ldots, f_{m-i})$. Now, to show the inductive claim for H, they reduce to the special cases where $H = \mathbb{Z}_p^r$ and where $H = \mathbb{Z}_{p^r}$, and go through the same approach for the special cases too. This goes through the "special intersecting family" theorem of [1] twice, resulting in a huge blowup in the exponent of the list size. Our proof differs from that of [1] as we prove the full inductive claim directly, without reducing to any special cases, resulting in a much smaller exponent. However, for technical reasons, we only manage to use this approach when the smallest prime divisor of $|G|$ also divides $|H|$. In the general case, we reduce to the previous case by decomposing G as a semidirect product.

The algorithmic results are a straightforward generalization of those of [1]. In particular, one merely needs to find the correct way to generalize the algorithms (replacing the direct product presentation of G with a polycyclic presentation) and verifying that the same analysis goes through.

2 Preliminaries

2.1 Group homomorphisms

Let G and H be finite groups, with homomorphisms $\mathrm{Hom}(G, H)$. A function $\phi : G \to H$ is a (left) affine homomorphism if there exists $h \in H$ and $\phi_0 \in \mathrm{Hom}(G, H)$ such that $\phi(g) = h\phi_0(g)$ for every $g \in G$. We use $\mathrm{aHom}(G, H)$ to denote the set of left affine homomorphisms from G to H. Note that the set of left affine homomorphisms equals the set of right affine homomorphisms, since

$$h\phi_0(g) = (h\phi_0(g)h^{-1})h$$

and $\psi_0(g) \triangleq h\phi_0(g)h^{-1}$ is a homomorphism.

The *equalizer* of two functions $f, g : G \to H$, denoted $\mathrm{Eq}(f, g)$, is the subset of G on which f and g agree, i.e.

$$\mathrm{Eq}(f, g) \triangleq \{x \in G \mid f(x) = g(x)\}.$$

More generally, if $\Phi \subseteq \{f : G \to H\}$ is a collection of functions, then the *equalizer* of Φ is the set

$$\mathrm{Eq}(\Phi) \triangleq \{x \in G \mid f(x) = g(x) \quad \forall f, g \in \Phi\}.$$

In the theory of error correcting codes, the usual measure of distance between two strings is the relative Hamming distance, which is the fraction of symbols on which they differ. In the context of group homomorphisms, we find it more convenient to study the complementary notion, the fractional agreement. We define the *agreement* $\mathrm{agr}(f, g)$ between two functions $f, g : G \to H$ to be the quantity

$$\mathrm{agr}(f, g) \triangleq \frac{|\mathrm{Eq}(f, g)|}{|G|}.$$

The *maximum agreement* of the code $\mathrm{aHom}(G, H)$, denoted by $\Lambda_{G,H}$, is defined as

$$\Lambda_{G,H} \triangleq \max_{\substack{\phi,\psi \in \mathrm{aHom}(G,H) \\ \phi \neq \psi}} \mathrm{agr}(\phi, \psi)$$

Recall that a group H is said to be *nilpotent* if it has a series of subgroups $\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_k = G$ such that for each i the commutator subgroup $[G, G_i]$, generated by all $g^{-1}h^{-1}gh$ for $g \in G$ and $h \in G_i$, is a subgroup of G_{i-1}. such that for each i, the commutator subgroup $[G, G_i]$ is a subgroup of G_{i-1}. The following theorem gives the value of $\Lambda_{G,H}$ when G is solvable or H is nilpotent.

▶ **Theorem 2.1** ([8]). *Suppose G and H are finite groups and G is solvable or H is nilpotent. Then*

$$\Lambda_{G,H} = \frac{1}{p}$$

where p is the smallest prime divisor of $\gcd(|G|, |H|)$ such that G has a normal subgroup of index p. If no such p exists, then $|\mathrm{Hom}(G, H)| = 1$; in particular, $\Lambda_{G,H} = 0$.

We also need the following proposition relating $\Lambda_{G.H}$ and $\Lambda_{N,H}$ when $N \triangleleft G$ and G can be written as a semidirect product of N with some other group G_1. (Recall that the semidirect product of two groups A and B, denoted $A \rtimes B$, is defined when elements of B act on the elements of A. The elements of $A \rtimes B$ are pairs (a, b) with $a \in A$ and $b \in B$ and $(a, b) \cdot (c, d) = ((a \cdot c^b, b \cdot d).)$

▶ **Proposition 2.2.** *If G and H are finite groups and $G = N \rtimes G_1$ for some normal subgroup $N \triangleleft G$ and subgroup $G_1 \leq G$ and $|\mathrm{Hom}(G_1, H)| = 1$, then every $\phi \in \mathrm{aHom}(G, H)$ is of the form $\phi(xy) = \psi(x)$ for some $\psi \in \mathrm{aHom}(N, H)$ and every $x \in N$ and $y \in G_1$. In particular,*

$$\Lambda_{G,H} \leq \Lambda_{N,H}$$

2.2 Some facts about supersolvable groups

▶ **Proposition 2.3.** *If G is a finite supersolvable group and $|G| = p_1 \cdots p_k$, where $p_1 \geq \cdots \geq p_k$ are primes, then G has a normal cyclic series*

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_k = G$$

where each $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$.

The following proposition allows us to decompose a finite supersolvable group as a semidirect product whose components have coprime orders.

▶ **Proposition 2.4.** *Let G be a finite supersolvable group and $|G| = p_1^{r_1} \cdots p_m^{r_m}$, where $p_1 > \cdots > p_m$ are prime. For any $k \in [m]$, G has a normal subgroup $N_k \triangleleft G$ such that $|N_k| = p_1^{r_1} \cdots p_k^{r_k}$, $|G/N_k| = p_{k+1}^{r_{k+1}} \cdots p_m^{r_m}$, and $G = N_k \rtimes G/N_k$.*

2.3 Special intersecting families

▶ **Definition 2.5** (Special intersecting family). Fix an ambient set X. For any subset $S \subseteq X$, define the *density of S in X* to be

$$\mu(S) = \frac{|S|}{|X|}.$$

A collection $S_1, \ldots, S_\ell \subseteq X$ of subsets is a (ρ, τ, c)-*special intersecting family* if the following hold:

1. $\mu(S_i) \geq \rho$ for each i;
2. $\mu(S_i \cap S_j) \leq \rho$ whenever $i \neq j$;
3. $\sum_{i=1}^{\ell} (\mu(S_i) - \rho)^c \leq 1$;
4. If $J \subseteq I \subseteq [\ell]$, $|J| \geq 2$, and $\mu(S_I) > \tau$, then $S_I = S_J$, where $S_K = \cap_{i \in K} S_i$ for any $K \subseteq [\ell]$;

For our bounds on the combinatorial list-decodability, we use the same outline as that of [1]. In particular, this involves analyzing the agreement sets of homomorphisms with the given function and showing that they form a special intersecting family. The following result of [1] allows us to deduce bounds on the sizes of the agreement sets in terms of the size of the union.

▶ **Theorem 2.6** ([1, Theorem 3.2]). *For every $c < \infty$, there exists $C = C(c) < \infty$ such that the following holds: if $S_1, \dots, S_\ell$ form a (ρ, ρ^2, c)-special intersecting family, with $\mu(S_i) = \rho + \alpha_i$ and $\mu(\cup_i S_i) = \rho + \alpha$, then*

$$\alpha^C \geq \sum_{i=1}^{\ell} \alpha_i^C. \tag{1}$$

In fact, one can take $C(c) = 2c \cdot (c+1)(4 + (c+1)\log_2 3)$.

We refer to $C(c)$ as the *special intersecting number for c*.

We will also use the following q-ary Johnson bound (see the appendix of [1] for a proof).

▶ **Proposition 2.7** (q-ary Johnson Bound). *Let $f, \phi_1, \dots, \phi_\ell : [n] \to [q]$ be functions satisfying the following properties:*

1. $\mathrm{agr}(f, \phi_i) = \frac{1}{q} + \alpha_i$ *for $\alpha_i \geq 0$*
2. $\mathrm{agr}(\phi_i, \phi_j) \leq \frac{1}{q}$ *for every $i \neq j$.*

Then $\sum_{i=1}^{\ell} \alpha_i^2 \leq 1$.

3 List-decoding radius for supersolvable groups

3.1 Preliminary notation and definitions

If H is supersolvable, we may write

$$H = H_0 \triangleright H_1 \triangleright \dots \triangleright H_m = \{1\}$$

where $H_{i-1}/H_i \cong \mathbb{Z}_{p_i}$. For $k \in [m]$, define $H_{(k)} \triangleq H/H_k$, which is a group since H_k is normal in H. In particular, $H_{(0)} = \{1\}$ and $H_{(m)} = H$.

Given $f : G \to H$ and $k \in [m]$, define $f^{(k)} : G \to H_{(k)}$ and $f^{(-k)} : G \to H_k$ as follows. Define $f^{(k)} : G \to H_{(k)}$ to be f composed with the natural quotient map, sending $x \in G$ to the coset $f(x)H_k$ of H_k. Therefore, $f^{(k)}$ is an (affine) homomorphism if f is. To define the latter map, we need to choose, for each $i \in [0, m-1]$, an element $y_i \in H_i \setminus H_{i+1}$. Then each k-tuple $(a_0, \dots, a_{k-1})$, where $0 \leq a_j \leq p - 1$, corresponds to a distinct coset $y_0^{a_0} \cdots y_{k-1}^{a_{k-1}} H_k$. If $f(x)H_k = y_0^{a_0} \cdots y_{k-1}^{a_{k-1}} H_k$, then define $f^{(-k)}(x) \triangleq y_{k-1}^{-a_{k-1}} \cdots y_0^{-a_0} f(x)$. Note that $f^{(-k)}(x) \in H_k$ but $f^{(-k)}$ may not be a homomorphism in general (even if f is). Also, note that f is determined by $f^{(k)}$ and $f^{(-k)}$: if $f^{(k)}(x) = y_0^{a_0} \cdots y_{k-1}^{a_{k-1}} H_k$, then $f(x) = y_0^{a_0} \cdots y_{k-1}^{a_{k-1}} f^{(-k)}(x)$.

If $i < j$ and $\phi : G \to H_{(i)}$ and $\psi : G \to H_{(j)}$, then ψ *extends* ϕ if $\psi^{(i)} = \phi$. Here, $\psi^{(i)}$ makes sense, because $H_j < H_i$, and so we get a chain $H_0/H_j \triangleright H_1/H_j \triangleright \dots \triangleright H_j/H_j = \{1\}$ induced by the original chain for H, and so $\psi^{(i)}$ is just ψ composed by modding out by H_i/H_j. One can then define $\psi^{(-i)}$ to make sense too.

3.2 Combinatorial bounds for agreement $\Lambda_{G,H} + \epsilon$

We begin with the case where the smallest prime divisor of $|G|$ also divides $|H|$.

▶ **Theorem 3.1.** *There exists a universal constant $C < \infty$ such that whenever G and H are finite supersolvable groups and the smallest prime divisor p of $|G|$ also divides $|H|$, then for any $f : G \to H$ and $\epsilon > 0$, there are at most $(1/\epsilon)^C$ affine homomorphisms $\phi \in \mathrm{aHom}(G, H)$ such that $\mathrm{agr}(\phi, f) \geq \frac{1}{p} + \epsilon$.*

Proof. We prove the theorem for $C = C(2)$ where $C(c)$ denotes the special intersecting number of c, as given by Theorem 2.6. Henceforth let $C = C(2)$. Let $p_1 \leq \cdots \leq p_m$ be primes such that $|H| = p_1 \cdots p_m$. By Proposition 2.3, H has a normal cyclic series

$$H = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = \{1_H\}$$

where $H_{i-1}/H_i \cong \mathbb{Z}_{p_i}$ for each i.

▶ Claim 3.2. For $k \in [0, m]$, if $\phi \in \mathrm{aHom}(G, H_{(k)})$ satisfies $\mathrm{agr}(\phi, f^{(k)}) = \frac{1}{p} + \alpha$ for some $\alpha \geq \epsilon$, then the number of $\psi \in \mathrm{aHom}(G, H)$ extending ϕ with $\mathrm{agr}(\psi, f) \geq \frac{1}{p} + \epsilon$ is at most $(\alpha/\epsilon)^C$.

Proof. We induct backwards on k. The base case $k = m$ is trivial. Now suppose $k < m$ and the claim holds for $k+1$. Let $\phi_1, \ldots, \phi_\ell \in \mathrm{aHom}(G, H_{(k+1)})$ be all the homomorphisms extending ϕ with $\mathrm{agr}(\phi_i, f^{(k+1)}) \geq \frac{1}{p} + \epsilon$. Define $\alpha_i \triangleq \mathrm{agr}(\phi_i, f^{(k+1)}) - \frac{1}{p}$. Define $S_i \triangleq \mathrm{Eq}(\phi_i, f^{(k+1)})$. We claim that $S_1, \ldots, S_\ell$ form a $\left(\frac{1}{p}, \frac{1}{p^2}, 2\right)$-special intersecting family. Before we prove this, we show how it implies the claim. By Theorem 2.6, $(\alpha')^C \geq \sum_{i=1}^{\ell} \alpha_i^C$, where $\alpha' = \mu(\cup_i S_i) - \frac{1}{p}$. But $\cup_i S_i \subseteq \mathrm{Eq}(\phi, f)$, so $\alpha \geq \alpha'$, and thus $\alpha^C \geq \sum_{i=1}^{\ell} \alpha_i^C$. Moreover, every $\psi \in \mathrm{aHom}(G, H)$ extending ϕ with $\mathrm{agr}(\psi, f) \geq \frac{1}{p} + \epsilon$ must extend one of the ϕ_i. By induction, there are at most $(\alpha_i/\epsilon)^C$ such ψ extending ϕ_i. Hence, there are at most $\sum_{i=1}^{\ell} (\alpha_i/\epsilon)^C \leq (\alpha/\epsilon)^C$ such ψ extending ϕ.

Now, we show that $S_1, \ldots, S_\ell$ form a $\left(\frac{1}{p}, \frac{1}{p^2}, 2\right)$-special intersecting family. We verify the four properties:

(1) By definition, we have $\mu(S_i) = \frac{1}{p} + \alpha_i \geq \frac{1}{p}$.
(2) If $i \neq j$, then since $\phi_i, \phi_j \in \mathrm{aHom}(G, H_{(k+1)})$, we have $S_i \cap S_j \subseteq \mathrm{Eq}(\phi_i, \phi_j)$ and therefore $\mu(S_i \cap S_j) \leq \mathrm{agr}(\phi_i, \phi_j) \leq \Lambda_{G, H_{(k+1)}} \leq \Lambda_{G,H} \leq \frac{1}{p}$.
(3) Define $g \triangleq (f^{(k+1)})^{(-k)} : G \to H_k/H_{k+1} \cong \mathbb{Z}_{p_{k+1}}$ and define $\psi_i \triangleq \phi^{(-k)} : G \to H_k/H_{k+1} \cong \mathbb{Z}_{p_{k+1}}$. If $\phi_i(x) = f^{(k+1)}(x)$, then $\psi_i(x) = g(x)$, so certainly $\mathrm{agr}(g, \psi_i) \geq \mathrm{agr}(f^{(k+1)}, \phi_i) = \frac{1}{p} + \alpha_i$. Moreover, if $i \neq j$, since ϕ_i, ϕ_j both extend ϕ, then $\phi_i(x) = \phi_j(x)$ if and only if $\psi_i(x) = \psi_j(x)$, so $\mathrm{agr}(\psi_i, \psi_j) = \mathrm{agr}(\phi_i, \phi_j) \leq \Lambda_{G, H_{(k+1)}} \leq \Lambda_{G,H} = \frac{1}{p}$.
(4) Suppose $J \subseteq I$, $|J| \geq 2$, and $\mu(S_I) > 1/p^2$. Define $\Phi_I \triangleq \{\phi_i \mid i \in I\}$ and define Φ_J similarly. Then $S_I \subseteq \mathrm{Eq}(\Phi_I)$ and $S_J \subseteq \mathrm{Eq}(\Phi_J)$, and since $|J| \geq 2$, we have $1/p^2 < \mu(\mathrm{Eq}(\Phi_I)) \leq \mu(\mathrm{Eq}(\Phi_J)) \leq 1/p$. But $\mu(\mathrm{Eq}(\Phi_J))/\mu(\mathrm{Eq}(\Phi_I))$ divides $|G|$ and p is the smallest prime divisor of $|G|$, so it must be that $\mu(\mathrm{Eq}(\Phi_I)) = \mu(\mathrm{Eq}(\Phi_J))$, and hence $\mathrm{Eq}(\Phi_I) = \mathrm{Eq}(\Phi_J)$. Fix any $j \in J$. Then $S_I = S_j \cap \mathrm{Eq}(\Phi_I) = S_j \cap \mathrm{Eq}(\Phi_J) = S_J$.

◀

The theorem follows by taking $k = 0$ in the claim. ◀

Before we prove the general case, we first prove a useful lemma. In what follows, for any code $\mathcal{C} \subseteq \Sigma^n$ and agreement parameter $a \in [0,1]$, define $\ell(\mathcal{C}, a)$ to be the quantity

$$\ell(\mathcal{C}, a) \triangleq \max_{w \in \Sigma^n} |\{c \in \mathcal{C} \mid \mathrm{agr}(c, w) \geq a\}|.$$

▶ **Lemma 3.3.** *Let $\mathcal{C} \subseteq \Sigma^n$ be a code. If $s > r \geq 1$, and $\mathcal{C}_r \triangleq \{(\underbrace{c, \ldots, c}_{r}) \in \Sigma^{rn} \mid c \in \mathcal{C}\}$ and $\mathcal{C}_s \triangleq \{((\underbrace{c, \ldots, c}_{s})) \in \Sigma^{sn} \mid c \in \mathcal{C}\}$, then for any $a \in [0,1]$,*

$$\ell(\mathcal{C}_r, a) \leq \ell(\mathcal{C}_s, \lfloor s/r \rfloor (r/s) \cdot a).$$

Proof. Let $w \in \Sigma^{rn}$ such that $|\{(\underbrace{c, \ldots, c}_{r}) \in \mathcal{C}_r \mid \mathrm{agr}((\underbrace{c, \ldots, c}_{r}), w) \geq a\}| = \ell(\mathcal{C}_r, a)$. Define $w' \in \Sigma^{sn}$ by $w' = (\underbrace{w, \ldots, w}_{\lfloor s/r \rfloor}, w'')$, where $w'' \in \Sigma^{(s - \lfloor s/r \rfloor r)n}$ is defined arbitrarily. Then for each $c \in \mathcal{C}$ such that $\mathrm{agr}((\underbrace{c, \ldots, c}_{r}), w) \geq a$,

$$\begin{aligned}
\mathrm{agr}((\underbrace{c, \ldots, c}_{s}), w') &\geq \frac{1}{sn}\left(\lfloor s/r \rfloor \cdot rn \cdot \mathrm{agr}((\underbrace{c, \ldots, c}_{r}), w)\right) \\
&\geq \left\lfloor \frac{s}{r} \right\rfloor \frac{r}{s} \cdot a.
\end{aligned}$$

◀

▶ **Theorem 3.4.** *There exists a universal constant $C < \infty$ such that whenever G and H are finite supersolvable groups, then for any $f : G \to H$ and $\epsilon > 0$, there are at most $(1/\epsilon)^C$ affine homomorphisms $\phi \in \mathrm{aHom}(G, H)$ such that $\mathrm{agr}(\phi, f) \geq \Lambda_{G,H} + \epsilon$.*

Proof. We prove the theorem for $C = C(2)$, in particular using the fact that Theorem 2.6 holds for this constant. Let p be the smallest prime divisor of $\gcd(|G|, |H|)$ such that G has a normal subgroup of index p, so that $\Lambda_{G,H} = \frac{1}{p}$ (Theorem 2.1). If p is the smallest prime divisor of $|G|$, then the result follows from Theorem 3.1, so suppose p is not the smallest prime divisor of $|G|$. By Proposition 2.4, we can write $G = N \rtimes G'$ for some proper normal subgroup $N \lhd G$ where p is the smallest prime divisor of $|N|$ and every prime dividing $|G'|$ is smaller than p, and therefore $\gcd(|G'|, |H|) = 1$. By Proposition 2.2, every $\phi \in \mathrm{aHom}(G, H)$ is of the form $\phi(x, y) = \psi(x)$ for $x \in N$ and $y \in G'$. Thus, $\mathrm{aHom}(G, H)$ is isomorphic to the code

$$\mathcal{C}_r \triangleq \{(\underbrace{\psi, \ldots, \psi}_{r}) \mid \psi \in \mathcal{C}\}$$

where $\mathcal{C} = \mathrm{aHom}(N, H)$ and $r = |G'|$. Let $q > \max\{|G|, |H|\}$ be a prime and consider the group $G'' \triangleq N \oplus \mathbb{Z}_q$, which is supersolvable. Then $\mathrm{aHom}(G'', H)$ is isomorphic to the code

$$\mathcal{C}_q \triangleq \{(\underbrace{\psi, \ldots, \psi}_{q}) \mid \psi \in \mathcal{C}\}.$$

Letting $a \triangleq \frac{1}{p} + \epsilon$, applying Lemma 3.3 and Theorem 3.1 (using the fact that the smallest prime divisor of $|G''|$ also divides $|H|$), we get an upper bound of

$$\left(\frac{1}{(\lfloor q/|G'| \rfloor (|G'|/q) - 1)\frac{1}{p} + \lfloor q/|G'| \rfloor (|G'|/q) \cdot \epsilon}\right)^C \leq \left(\frac{1}{\left(1 - \frac{|G'|}{q}\right)\epsilon - \frac{|G'|}{q}\frac{1}{p}}\right)^C$$

affine homomorphisms $\phi \in \mathrm{aHom}(G, H)$ with $\mathrm{agr}(\phi, f) \geq \frac{1}{p} + \epsilon$. By taking $q \to \infty$, the above upper bound approaches $(1/\epsilon)^C$. ◀

3.3 Exponential list size for agreement $\Lambda_{G,H}$

We conclude this section by showing that if G is solvable, then the list size for agreement $\Lambda_{G,H}$ can be exponential in $\log |G| + \log |H|$, showing that the list-decoding distance we achieve is optimal. In other words, we have identified the list-decoding radius for $\mathrm{aHom}(G, H)$ when G and H are supersolvable.

In fact, we observe that the list size can be $\Omega(|G| \cdot |H|)$ even just for abelian G and H, when $\Lambda_{G,H} = \frac{1}{p}$ is fixed. Let $G = \mathbb{Z}_p^n$ and $H = \mathbb{Z}_p^m$, so that $\Lambda_{G,H} = \frac{1}{p}$. Consider the maps $\phi_{a,b}$, where $a \in \mathbb{Z}_p^n$ and $b \in \mathbb{Z}_p^m$ are nonzero vectors, defined by

$$\phi_{a,b}(x_1, \ldots, x_n) = (a_1 x_1 + \cdots + a_n x_n) b.$$

Note that $\mathrm{agr}(\phi_{a,b}, 0) = \frac{1}{p}$. Moreover, there are $p^n - 1$ choices for a and $p^m - 1$ choices for b, and $\phi_{a,b} = \phi_{c,d}$ if and only if there exists $\lambda \in \mathbb{Z}_p^*$ such that $c = \lambda a$ and $b = \lambda d$. So the number of distinct homomorphisms agreeing with the zero function is $\frac{(p^n-1)(p^m-1)}{p-1} = \Omega(|G| \cdot |H|) = \exp(\log |G| + \log |H|)$.

4 Algorithm for supersolvable G

In this section we give a local list-decoding algorithm for the set of homomorphisms from G to H whenever G and H are supersolvable.

▶ **Definition 4.1.** A probabilistic oracle algorithm $\mathcal{A}$ for list decoding homomorphisms takes as input two groups G and H and has oracle access to a function $f : G \to H$. The algorithm $\mathcal{A}$ is a (λ, T)-local list decoder for $\mathrm{aHom}(G, H)$ if, for every function $f : G \to H$, $\mathcal{A}^f$ runs in time T and outputs a list $L \subset \mathrm{aHom}(G, H)$ such that with probability at least 3/4, it holds that if $\phi \in \mathrm{aHom}(G, H)$ and $\mathrm{agr}(f, \phi) \geq \lambda$, then $\phi \in L$.

▶ **Theorem 4.2.** *There exists an algorithm $\mathcal{A}$ such that for every pair of finite groups G, H where G is solvable and H is supersolvable, and every $\epsilon > 0$, $\mathcal{A}$ is a $(\Lambda_{G,H} + \epsilon, \mathrm{poly}(\log |G|, \log |H|, \frac{1}{\epsilon}))$-local list decoder for $\mathrm{aHom}(G, H)$, provided that $\mathcal{A}$ has oracle access to the multiplication table of H and $\mathrm{aHom}(G, H)$ has a list-size bound of $(1/\epsilon)^{O(1)}$.*

4.1 Algorithm

Let

$$G = G_k \triangleright G_{k-1} \triangleright \cdots \triangleright G_0 = \{1_G\}$$

be a subnormal cyclic series, with $G_i/G_{i-1} \cong \mathbb{Z}_{p_i}$, $p_1 \geq p_2 \geq \cdots \geq p_k$ and representatives $g_i \in G_i \setminus G_{i-1}$. Our main algorithm is Algorithm 1, which uses Algorithms 2 and 3 as subroutines.

The analysis is the same as in [1].

Algorithm 1 List decode

```
procedure ListDecode(f,G,H)
    L ← ∅
    repeat
        S_0 ← ∅
        for i = 1 to k do
            S'_i ← Extend(i, S_{i−1})
            S_i ← Prune(i, S'_i)
        end for
        for all φ ∈ S_k do
            B ← FrequentValues(x ↦ f(x)φ(x)^{−1}, Λ_{G,H} + ε/2)
            L ← L ∪ {x ↦ bφ(x) | b ∈ B}
        end for
    until C log (1/ε) times
end procedure
```

Algorithm 2 Extend

```
procedure Extend(i,S)
    S' ← ∅
    for all φ ∈ S do
        repeat
            Pick (α_{i+1}, ..., α_k) ∈ Z_{p_{i+1}} ⊕ ··· ⊕ Z_{p_k} uniformly at random
            s ← g_k^{α_k} ··· g_{i+1}^{α_{i+1}}
            Pick y_1, y_2 ∈ G_{i−1} and c_1, c_2 ∈ Z_{p_i} uniformly at random
            if c_1 − c_2 is invertible modulo p_1 ··· p_i then
                γ ← (c_1 − c_2)^{−1} ∈ Z^⊕ p_1 ··· p_i
                a ← (φ(y_2) f(s g_i^{c_2} y_2)^{−1} f(s g_i^{c_1} y_1) φ(y_1)^{−1})^γ
                Define θ : G_i → H by θ(g_i^c x) = a^c φ(x)
                S' ← S' ∪ {θ}
            end if
        until (log |G| log |H| (1/ε))^4 times
    end for
    return S'
end procedure
```

Algorithm 3 Prune

procedure PRUNE(i,S)
  $S' \leftarrow \emptyset$
  repeat
    Pick $(\alpha_{i+1}, \ldots, \alpha_k) \in \mathbb{Z}_{p_{i+1}} \oplus \cdots \oplus \mathbb{Z}_{p_k}$ uniformly at random
    $s \leftarrow g_k^{\alpha_k} \cdots g_{i+1}^{\alpha_{i+1}}$
    for all $\phi \in S$ **do**
      $B \leftarrow$ FREQUENTVALUES$(x \mapsto f(sx)\phi(sx)^{-1}, \Lambda_{G,H} + \epsilon/2)$
      if $|B| \geq 1$ **then**
        $S' \leftarrow S' \cup \{\phi\}$
      end if
    end for
  until $(\log |G| \log |H| \frac{1}{\epsilon})^2$ times
  if $|S'| > (\log |G| \log |H| \frac{1}{\epsilon})^{2C}$ **then**
    return error
  end if
  return S'
end procedure

References

1 Irit Dinur, Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Decodability of group homomorphisms beyond the Johnson bound. In Dwork [2], pages 275–284.

2 Cynthia Dwork, editor. *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. ACM, 2008.

3 Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In David S. Johnson, editor, *STOC*, pages 25–32. ACM, 1989.

4 Parikshit Gopalan. A Fourier-analytic approach to Reed-Muller decoding. *IEEE Transactions on Information Theory*, 59(11):7747–7760, 2013.

5 Parikshit Gopalan, Venkatesan Guruswami, and Prasad Raghavendra. List decoding tensor products and interleaved codes. *SIAM Journal on Computing*, 40(5):1432–1462, 2011.

6 Parikshit Gopalan, Adam R. Klivans, and David Zuckerman. List-decoding Reed-Muller codes over small fields. In Dwork [2], pages 265–274.

7 Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Local decoding and testing for homomorphisms. In Josep Díaz, Klaus Jansen, José D. P. Rolim, and Uri Zwick, editors, *APPROX-RANDOM*, volume 4110 of *Lecture Notes in Computer Science*, pages 375–385. Springer, 2006.

8 Alan Guo. Group homomorphisms as error correcting codes. Technical report, April 2014. http://arxiv.org/abs/1404.3447.

9 Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *IEEE Conference on Computational Complexity*, pages 77–85. IEEE Computer Society, 2011.

10 Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.

11 Venkatesan Guruswami and Carol Wang. Optimal rate list decoding via derivative codes. In Leslie Ann Goldberg, Klaus Jansen, R. Ravi, and José D. P. Rolim, editors, *APPROX-RANDOM*, volume 6845 of *Lecture Notes in Computer Science*, pages 593–604. Springer, 2011.

12 Swastik Kopparty. List-decoding multiplicity codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:44, 2012.