Group homomorphisms as error correcting codes

Alan Guo*

CSAIL, Massachusetts Institute of Technology
Cambridge, MA, U.S.A.
aguo@mit.edu

Submitted: Apr 27, 2014; Accepted: Dec 10, 2014; Published: Jan 2, 2015
Mathematics Subject Classification: 20D10, 20D15

Abstract

We investigate the minimum distance of the error correcting code formed by the homomorphisms between two finite groups G and H. We prove some general structural results on how the distance behaves with respect to natural group operations, such as passing to subgroups and quotients, and taking products. Our main result is a general formula for the distance when G is solvable or H is nilpotent, in terms of the normal subgroup structure of G as well as the prime divisors of $|G|$ and $|H|$. In particular, we show that in the above case, the distance is independent of the subgroup structure of H. We complement this by showing that, in general, the distance depends on the subgroup structure of H.

1 Introduction

1.1 Error correcting codes

The theory of error correcting codes studies *codes*, which are subsets of Σ^n for some alphabet Σ and block length n. The distance between two strings of equal length is the number of coordinates in which they differ. The distance Δ of a code is simply the minimum distance between any pair of distinct codewords (elements of the code). Hamming [Ham50] identifies the distance of a code as the key parameter measuring the error correcting capability of the code. As long as the number of coordinates in which a codeword is corrupted is less than $\Delta/2$, one can uniquely recover the original codeword. Elias [Eli57] and Wozencraft [Woz58] proposed *list decoding*, in which one insists only on recovering a list, whose size is at most polynomial in n, which contains the original codeword. The Johnson bound [Joh62] shows that codes can list decode errors beyond $\Delta/2$. Codes with efficient list decoding algorithms include the Hadamard code [GL89], Reed-Solomon codes and variants thereof [Sud97, GS99, GR08, Gur11], Reed-Muller codes [GKZ08, Gop13], multiplicity/derivative codes [Kop12, GW11], and abelian group homomorphisms [GKS06, DGKS08]. For some of these codes, in particular

*Research supported in part by NSF grants CCF-0829672, CCF-1065125, and CCF-6922462, and an NSF Graduate Research Fellowship.

for carefully chosen subcodes the folded Reed-Solomon codes and multiplicity/derivative codes [DL12], the Reed-Muller codes, and abelian group homomorphisms, it was shown that for any constant $\epsilon > 0$ one can algorithmically list decode up to $\Delta - \epsilon n$ errors with a constant list size, depending only on $1/\epsilon$. For all of these codes, the codewords are interpreted as certain functions $f : A \to B$ from some domain A to codomain B. In this case, the coordinates of the codeword are indexed by A and the alphabet is B.

In a companion work [GS14], the author and Sudan show the analogous list decoding results for group homomorphisms between supersolvable groups. A technical obstacle which did not arise in the previous works of [GKS06, DGKS08] on list decoding abelian group homomorphisms is actually determining the distance of the code. This turns out to be a nontrivial problem and serves as the primary motivation of this paper.

1.2 Group homomorphisms

Let G and H be finite groups, with homomorphisms $\operatorname{Hom}(G, H)$. A function $\phi : G \to H$ is a (left) affine homomorphism if there exists $h \in H$ and $\phi_0 \in \operatorname{Hom}(G, H)$ such that $\phi(g) = h\phi_0(g)$ for every $g \in G$. The set of left affine homomorphisms from G to H by $\operatorname{aHom}(G, H)$. 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 $\operatorname{Eq}(f, g)$, is the set

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

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

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

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* $\operatorname{agr}(f, g)$ between two functions $f, g : G \to H$ to be the quantity

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

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

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

In Section 2, we study the structure of the equalizers of homomorphisms and prove some basic results that will be useful later. As we will see (Proposition 2.5), adding affine homomorphisms does not change the distance of this code. However, we include these functions in the code so that $\Lambda_{G,H}$ is well-defined when $|\operatorname{Hom}(G, H)| = 1$, as long as H is nontrivial.

1.3 Our results

Our main result is the following formula for $\Lambda_{G,H}$ when G is solvable or H is nilpotent.

Theorem 1.1. *Let G and H be finite groups. Define*

$$\mathcal{P}_{G,H} \triangleq \{p \mid p \textit{ is a prime divisor of } \gcd(|G|,|H|)\}$$

and

$$\mathcal{N}_G \triangleq \{m \mid G \textit{ has a proper normal subgroup of index } m\}.$$

If G is solvable or H is nilpotent, then

$$\Lambda_{G,H} = \begin{cases} 0 & \textit{if } \mathcal{P}_{G,H} \cap \mathcal{N}_G = \emptyset, \\ \frac{1}{\min \mathcal{P}_{G,H} \cap \mathcal{N}_G} & \textit{if } \mathcal{P}_{G,H} \cap \mathcal{N}_G \neq \emptyset. \end{cases}$$

In Section 3, we prove general facts about $\Lambda_{G,H}$, such as how it behaves with respect to group decompositions, subgroups, and quotients.

The proof of Theorem 1.1 is divided into two sections. Section 4 handles the case where H is nilpotent, and Section 5 handles the case where G is solvable.

In Section 6, we investigate $\Lambda_{G,H}$ when G is a non-abelian simple group, and in particular when $G = A_n$ is the alternating group on $n \geqslant 5$ objects. We show that the formula for $\Lambda_{G,H}$ for solvable G does not apply to non-abelian simple groups, and hence does not extend to arbitrary groups. We also see that, in general, $\Lambda_{G,H}$ depends not only on the prime divisors of $|G|$ and $|H|$ but also on the subgroup structure of H, in particular whether H contains isomorphic copies of G and how these copies are embedded in H.

2 Equalizers

We begin by observing that the equalizer of a set of (affine) homomorphisms is a (coset of a) subgroup of G.

Proposition 2.1. *Let G and H be finite groups. If $\Phi \subseteq \mathrm{Hom}(G,H)$, then $\mathrm{Eq}(\Phi)$ is a subgroup of G. If $\Phi' \subseteq \mathrm{aHom}(G,H)$ and $\mathrm{Eq}(\Phi') \neq \emptyset$, then there exists $\Phi \subseteq \mathrm{Hom}(G,H)$ with $|\Phi| = |\Phi'|$ such that $\mathrm{Eq}(\Phi')$ is a coset of $\mathrm{Eq}(\Phi)$.*

A basic question we would like to answer is the following: if $\phi, \psi \in \mathrm{Hom}(G,H)$, then must the index of $\mathrm{Eq}(\phi,\psi)$ divide $|H|$? Note that this is true when one of the homomorphisms, say ψ, is the trivial homomorphism mapping to 1_H, so that $\mathrm{Eq}(\phi,\psi) = \ker\phi$. This follows from the fact that $G/\ker\phi \cong \mathrm{im}\,\phi$ which is a subgroup of H, so $[G : \ker\phi] = |\mathrm{im}\,\phi|$ divides H. We will show in Proposition 2.6 that the more general statement holds when H is a p-group. Before doing so, we collect a few more basic facts that will be useful to us.

Proposition 2.2. *Let G and H be finite groups and let $\Phi \subseteq \mathrm{Hom}(G,H)$. For $h \in H$, if the set $\bigcap_{\phi\in\Phi} \phi^{-1}(h)$ is nonempty, then it is a coset of the subgroup $\bigcap_{\phi\in\Phi} \ker\phi$.*

Proposition 2.3. *Let G be a group with normal subgroups $N_1, \ldots, N_k \triangleleft G$. Then $N \triangleq \bigcap_{i=1}^k N_i$ is a normal subgroup of G and G/N is isomorphic to a subgroup of $\bigoplus_{i=1}^k (G/N_i)$.*

Proof. Consider the homomorphism $\phi : G \to \bigoplus_{i=1}^{k}(G/N_i)$ which is defined by $\phi(g) = (gN_1, \ldots, gN_k)$. Then $\ker\phi = \bigcap_{i=1}^{k} N_i = N$, which shows that N is a normal subgroup. Moreover, $\operatorname{im}\phi$ is a subgroup of $\bigoplus_{i=1}^{k}(G/N_i)$, and by the First Isomorphism Theorem, $G/N = G/\ker\phi \cong \operatorname{im}\phi$. □

Proposition 2.4. *Let G and H be finite groups, and let $\Phi \subseteq \operatorname{Hom}(G, H)$. Let $K \subseteq H$ be the set of $h \in H$ such that $\bigcap_{\phi\in\Phi} \phi^{-1}(h)$ is nonempty. Then*

$$|\operatorname{Eq}(\Phi)| = \left|\bigcap_{\phi\in\Phi} \ker\phi\right| \cdot |K|\,.$$

Proof. We decompose $\operatorname{Eq}(\Phi)$ into the disjoint union

$$\operatorname{Eq}(\Phi) = \bigcup_{h\in K}\left(\bigcap_{\phi\in\Phi}\phi^{-1}(h)\right).$$

The result then follows from the fact that each $\bigcap_{\phi\in\Phi}\phi^{-1}(h)$ is a coset of $\bigcap_{\phi\in\Phi}\ker\phi$, which follows from Proposition 2.2. □

The following proposition is simply the observation that the maximum agreement between two affine homomorphisms is achievable by two homomorphisms, which will allow us to reason about homomorphisms rather than affine homomorphisms in later proofs, without loss of generality.

Proposition 2.5. *If G and H are finite groups, then there exist $\phi, \psi \in \operatorname{Hom}(G, H)$ such that $\operatorname{agr}(\phi, \psi) = \Lambda_{G,H}$, so if $|\operatorname{Hom}(G, H)| > 1$, then*

$$\Lambda_{G,H} = \max_{\substack{\phi,\psi\in\operatorname{Hom}(G,H)\\ \phi\neq\psi}} \operatorname{agr}(\phi, \psi)$$

Proof. Let $\phi', \psi' \in \operatorname{aHom}(G, H)$ such that $\operatorname{agr}(\phi', \psi') = \Lambda_{G,H}$. By Proposition 2.1, there exist $\phi, \psi \in \operatorname{Hom}(G, H)$ such that $|\operatorname{Eq}(\phi, \psi)| = |\operatorname{Eq}(\phi', \psi')|$, hence $\operatorname{agr}(\phi, \psi) = \operatorname{agr}(\phi', \psi')$. □

Finally, we conclude this section by proving the following.

Proposition 2.6. *Let G be a finite group and let H be a finite p-group. If $\Phi \subseteq \operatorname{aHom}(G, H)$ and $\operatorname{Eq}(\Phi) \neq \emptyset$, then $[G : \operatorname{Eq}(\Phi)]$ is a power of p. In particular,*

$$\Lambda_{G,H} \leqslant \frac{1}{p}.$$

Proof. By Proposition 2.1, we may assume that $\Phi \subseteq \operatorname{Hom}(G, H)$. It follows from Proposition 2.3 that $G/\left(\bigcap_{\phi\in\Phi}\ker\phi\right)$ is isomorphic to a subgroup of $\bigoplus_{\phi\in\Phi}(G/\ker\phi) \cong \bigoplus_{\phi\in\Phi}\operatorname{im}\phi$. But the $\operatorname{im}\phi$ are subgroups of H, so they are p-groups, hence $\bigoplus_{\phi\in\Phi}\operatorname{im}\phi$ is a p-group, and so $G/\left(\bigcap_{\phi\in\Phi}\ker\phi\right)$ is a p-group, i.e.

$$\frac{|G|}{\left|\bigcap_{\phi\in\Phi}\ker\phi\right|} = p^k$$

for some k. By Proposition 2.4, there is some integer m such that

$$\frac{|G|}{|\operatorname{Eq}(\Phi)|} = \frac{|G|}{\left|\bigcap_{\phi\in\Phi}\ker\phi\right|\cdot m} = \frac{p^k}{m}.$$

By Proposition 2.1, $\operatorname{Eq}(\Phi)$ is a subgroup of G, and so by Lagrange's theorem, $\frac{p^k}{m} = \frac{|G|}{|\operatorname{Eq}(\Phi)|}$ is an integer, hence m divides p^k, therefore $\frac{p^k}{m}$ is a power of p. $\square$

3 General facts

In this section, we investigate general properties of $\Lambda_{G,H}$.

3.1 Subgroups and Quotients

Proposition 3.1. *If G and H are finite groups and $K \leqslant H$ is a subgroup, then*

$$\Lambda_{G,H} \geqslant \Lambda_{G,K}.$$

Proof. This follows from the fact that $\operatorname{aHom}(G,K) \subseteq \operatorname{aHom}(G,H)$. $\square$

Proposition 3.2. *If G, H are nontrivial finite groups and $N \triangleleft G$ is a normal subgroup, then*

$$\Lambda_{G,H} \geqslant \Lambda_{G/N,H}.$$

Proof. By Proposition 2.5, there exist $\phi_{G/N}, \psi_{G/N} \in \operatorname{Hom}(G/N, H)$ such that

$$\operatorname{agr}(\phi_{G/N}, \psi_{G/N}) = \Lambda_{G/N,H}.$$

Define $\phi, \psi : G \to H$ as follows. For $x \in G$, define $\phi(x) = \phi_{G/N}(xN)$ and $\psi(x) = \psi_{G/N}(xN)$. Then $\phi, \psi \in \operatorname{Hom}(G,H)$ since ϕ is the composition of $\phi_{G/N}$ with the natural quotient map $G \to G/N$, and similarly for ψ. It suffices to show that $\operatorname{agr}(\phi,\psi) = \operatorname{agr}(\phi_{G/N}, \psi_{G/N})$, for which it suffices to show that $|\operatorname{Eq}(\phi,\psi)| = |N| \cdot |\operatorname{Eq}(\phi_{G/N}, \psi_{G/N})|$. This follows from the fact that ϕ and ψ are constant on cosets, so $\operatorname{Eq}(\phi,\psi)$ is a disjoint union of cosets, and the cosets xN on which ϕ and ψ agree are exactly those for which $\phi_{G/N}(xN) = \psi_{G/N}(xN)$. $\square$

Proposition 3.3. *If G, H are nontrivial finite groups and $S \leqslant G$ is a subgroup of G such that $|\operatorname{Hom}(S,H)| = 1$, then $\operatorname{Hom}(G,H) \cong \operatorname{Hom}(G/N,H)$, where $N \trianglelefteq G$ is the smallest normal subgroup of G containing S. In particular,*

$$\Lambda_{G,H} = \Lambda_{G/N,H}.$$

Proof. Let $\phi \in \operatorname{Hom}(G,H)$. The restriction of ϕ to the domain S is a homomorphism in $\operatorname{Hom}(S,H)$, which is trivial by assumption. This means that $S \leqslant \ker\phi$. Since $\ker\phi \trianglelefteq G$, by minimality of N it follows that $N \leqslant \ker\phi$. In particular, $\phi = \phi' \circ \pi$ where $\phi' \in \operatorname{Hom}(G/N, H)$ and $\pi : G \to G/N$ is the natural quotient map. $\square$

3.2 Zappa-Szép products

Proposition 3.4. *If G and H are finite groups and $G = G_1 \bowtie G_2$ for some subgroups $G_1, G_2 \leqslant G$, then*

$$\Lambda_{G,H} \leqslant \max\{\Lambda_{G_1,H}, \Lambda_{G_2,H}\}.$$

Proof. If $|\operatorname{Hom}(G,H)| = 1$, then $\Lambda_{G,H} = 0$ and so the bound is trivial. Assume that $|\operatorname{Hom}(G,H)| > 1$. By Proposition 2.1, there exist $\phi, \psi \in \operatorname{Hom}(G,H)$ such that $\operatorname{agr}(\phi,\psi) = \Lambda_{G,H}$. First, we introduce some convenient notation. Denote by $\phi_{G_1} : G_1 \to H$ and $\phi_{G_2} : G_2 \to H$ the restrictions of ϕ to G_1 and G_2 respectively, and similarly for ψ_{G_1} and ψ_{G_2}. For $y \in G_2$, denote by $\phi_y : G_1 \to H$ the restriction $\phi_y(x) \triangleq \phi(xy)$. It is straightforward to verify that $\phi_{G_i}, \psi_{G_i} \in \operatorname{Hom}(G_i, H)$ for $i \in \{1,2\}$ and $\phi_y, \psi_y \in \operatorname{aHom}(G_1, H)$ for $y \in G_2$.

By averaging, there exists $y \in G_2$ such that $\operatorname{agr}(\phi_y, \psi_y) \geqslant \Lambda_{G,H}$. If $\phi_y \neq \psi_y$, then we are done since

$$\Lambda_{G,H} \leqslant \operatorname{agr}(\phi_y, \psi_y) \leqslant \Lambda_{G_1,H}.$$

Otherwise, suppose $\phi_y = \psi_y$. Then $\phi_{G_1} = \psi_{G_1}$, since for $x \in G_1$,

$$\phi(x) = \phi_y(x)\phi_y(1_G)^{-1} = \psi_y(x)\psi_y(1_G)^{-1} = \psi(x).$$

We claim that

$$\operatorname{Eq}(\phi,\psi) = G_1 \bowtie \operatorname{Eq}(\phi_{G_2}, \psi_{G_2}).$$

For the forward containment, observe that if $xz \in \operatorname{Eq}(\phi,\psi)$ with $x \in G_1$ and $z \in G_2$, then

$$\phi(z) = \phi(x)^{-1}\phi(xz) = \phi_{G_1}(x)^{-1}\phi(xz) = \psi_{G_1}(x)^{-1}\psi(xz) = \psi(x)^{-1}\psi(xz) = \psi(z)$$

and so $z \in \operatorname{Eq}(\phi_{G_2}, \psi_{G_2})$. Conversely, if $x \in G_1$ and $z \in \operatorname{Eq}(\phi_{G_2}, \psi_{G_2})$, then

$$\phi(xz) = \phi_{G_1}(x)\phi_{G_2}(z) = \psi_{G_1}(x)\psi_{G_2}(z) = \psi(xz)$$

and so $xz \in \operatorname{Eq}(\phi,\psi)$. This completes the proof of our claim. Moreover, since $\operatorname{Eq}(\phi,\psi) \neq G$, $\operatorname{Eq}(\phi_{G_2}, \psi_{G_2}) \neq G_2$, hence $\phi_{G_2} \neq \psi_{G_2}$. Therefore,

$$\Lambda_{G,H} = \frac{|\operatorname{Eq}(\phi,\psi)|}{|G|} = \frac{|\operatorname{Eq}(\phi_{G_2}, \psi_{G_2})|}{|G_2|} \leqslant \Lambda_{G_2,H}.$$

□

Proposition 3.5. *If G and H are finite groups and $G = G_1 \bowtie G_2$ for some subgroups $G_1, G_2 \leqslant G$ and $|\operatorname{Hom}(G_2, H)| = 1$, then every $\phi \in \operatorname{aHom}(G,H)$ is of the form $\phi(xy) = \psi(x)$ for some $\psi \in \operatorname{aHom}(G_1,H)$ and every $x \in G_1$ and $y \in G_2$. In particular,*

$$\Lambda_{G,H} \leqslant \Lambda_{G_1,H}$$

Proof. Suppose $\phi \in \operatorname{aHom}(G,H)$. Then there is some $a \in H$ and some $\phi_0 \in \operatorname{Hom}(G,H)$ such that $\phi(xy) = a\phi_0(x)\phi_0(y)$ for every $x \in G_1$ and $y \in G_2$. The restriction of ϕ_0 to G_2 is a homomorphism from $G_2 \to H$, which is trivial by assumption. The restriction of ϕ_0 to G_1 is also a homomorphism from $G_1 \to H$. Thus, $\phi(xy) = \psi(x)$ where $\psi \in \operatorname{aHom}(G_1,H)$ is defined by $\psi(x) = a\phi_0(x)$. □

3.3 Direct products

Proposition 3.6. *If G, H, G_1, G_2, H_1, H_2 are finite groups, then*

1. $\Lambda_{G,H_1\times H_2} = \max\{\Lambda_{G,H_1}, \Lambda_{G,H_2}\}$
2. $\Lambda_{G_1\times G_2,H} = \max\{\Lambda_{G_1,H}, \Lambda_{G_1,H}\}$

Proof. 1. Since H_1 is isomorphic to the subgroup $H_1 \times \{1_{H_2}\} \leqslant H_1 \times H_2$, it follows from Proposition 3.1 that $\Lambda_{G,H_1\times H_2} \geqslant \max\{\Lambda_{G,H_1}, \Lambda_{G,H_2}\}$. For the reverse bound, if $|\operatorname{Hom}(G, H_1 \times H_2)| = 1$, then it is trivial, so assume $|\operatorname{Hom}(G, H_1 \times H_2)| > 1$. By Proposition 2.5, there exist $\phi, \psi \in \operatorname{Hom}(G, H)$ with $\operatorname{agr}(\phi, \psi) = \Lambda_{G,H_1\times H_2}$. Write $\phi = (\phi_1, \phi_2)$ and $\psi = (\psi_1, \psi_2)$ where $\phi_i, \psi_i : G \to H_i$ for $i \in \{1, 2\}$. Then $\operatorname{agr}(\phi_1, \psi_1), \operatorname{agr}(\phi_2, \psi_2) \geqslant \operatorname{agr}(\phi, \psi) = \Lambda_{G,H_1\times H_2}$. Moreover, since $\phi \neq \psi$, we have $\phi_i \neq \psi_i$ for at least one of the $i \in \{1, 2\}$. Therefore, $\Lambda_{G,H_1\times H_2} \leqslant \operatorname{agr}(\phi_i, \psi_i) \leqslant \Lambda_{G,H_i} \leqslant \max\{\Lambda_{G,H_1}, \Lambda_{G,H_2}\}$.

2. Since direct products are Zappa-Szép products, it follows from Proposition 3.4 that $\Lambda_{G_1\times G_2,H} \leqslant \max\{\Lambda_{G_1,H}, \Lambda_{G_2,H}\}$. For the reverse bound, assume without loss of generality that $\Lambda_{G_1,H} \geqslant \Lambda_{G_2,H}$. If $|\operatorname{Hom}(G_1, H)| = 1$, then the bound is trivial, so assume $|\operatorname{Hom}(G_1, H)| > 1$. By Proposition 2.5, there exist $\phi_1, \psi_1 \in \operatorname{Hom}(G_1, H)$ such that $\operatorname{agr}(\phi, \psi) = \Lambda_{G_1,H}$. Define $\phi, \psi : G_1 \times G_2 \to H$ by $\phi(x, y) \triangleq \phi_1(x)$ and $\psi(x, y) \triangleq \psi_1(x)$. Then $\phi, \psi \in \operatorname{Hom}(G_1 \times G_2, H)$, so $\Lambda_{G_1\times G_2,H} \geqslant \operatorname{agr}(\phi, \psi) = \operatorname{agr}(\phi_1, \psi_1) = \Lambda_{G_1,H} \geqslant \max\{\Lambda_{G_1,H}, \Lambda_{G_2,H}\}$.

□

3.4 Key facts

Here we prove some key facts that will help us characterize $\Lambda_{G,H}$ when G is solvable.

Lemma 3.7. *If G and H are finite groups and p is the smallest prime divisor of $|G|$, then*

$$\Lambda_{G,H} \leqslant \frac{1}{p}.$$

Proof. Suppose $\phi, \psi \in \operatorname{aHom}(G, H)$ are distinct. By Proposition 2.1, $\operatorname{Eq}(\phi, \psi)$ is a coset of a subgroup S of G, and hence $|\operatorname{Eq}(\phi, \psi)| = |S|$. By Lagrange's theorem, $|G|/|S|$ is a divisor of $|G|$, and since $\phi \neq \psi$ it must be greater than 1, hence $|G|/|S| \geqslant p$, so $\operatorname{agr}(\phi, \psi) = \frac{|\operatorname{Eq}(\phi,\psi)|}{|G|} = \frac{|S|}{|G|} \leqslant \frac{1}{p}$. □

Lemma 3.8. *If G has a normal subgroup of index p and p divides $|H|$, then*

$$\Lambda_{G,H} \geqslant \frac{1}{p}.$$

Proof. Let $N \lhd G$ be a normal subgroup of index p. Let $\phi_1 : G \to G/N$ be the natural quotient homomorphism. Since p divides $|H|$, by Cauchy's theorem, there is an element $h \in H$ of order p. The subgroup $\langle h\rangle \leqslant H$ generated by h is isomorphic to $\mathbb{Z}_p$, and since G/N has order p, it is also isomorphic to $\mathbb{Z}_p$, hence there is an isomorphism $\phi_2 : G/N \to \langle h\rangle$. Define $\phi : G \to H$ to be the composition $\phi = \phi_2 \circ \phi_1$. Since ϕ_1, ϕ_2 are homomorphisms, ϕ is a homomorphism, and moreover since ϕ_2 is an isomorphism, $\ker \phi = \ker \phi_1 = N$. Therefore, $|\ker \phi| = |N| = |G|/p$. □

Proposition 3.9. *If G and H are finite groups and $\gcd(|G|, |H|) = 1$, then $\mathrm{aHom}(G, H)$ consists of constant functions. In particular,*

$$\Lambda_{G,H} = 0.$$

Proof. It suffices to show that the only homomorphism $\phi : G \to H$ is the trivial map 1_H. If $\phi \in \mathrm{Hom}(G, H)$, then $G/\ker\phi \cong \mathrm{im}\,\phi$. Moreover, since $\ker\phi \leqslant G$ and $\mathrm{im}\,\phi \leqslant H$, $|\mathrm{im}\,\phi| = |G|/|\ker\phi|$ divides both $|G|$ and $|H|$, hence $|\mathrm{im}\,\phi| = 1$ and so $\mathrm{im}\,\phi = \{1_H\}$. $\square$

4 Nilpotent codomain

In this section, we prove Theorem 1.1 when H is nilpotent.

We begin by considering the case where G has no normal subgroups of index p for any prime p dividing $\gcd(|G|, |H|)$. The following fact will be useful.

Proposition 4.1. *If G is a finite solvable group and $N \lhd G$ is a maximal normal subgroup, then N has prime index in G.*

We proceed to prove that $\Lambda_{G,H} = 0$. In fact, we prove it for the case where H is solvable.

Proposition 4.2. *Let G and H be finite groups, with H solvable. If G has no normal subgroup of index p for any prime p dividing $\gcd(|G|, |H|)$, then $|\mathrm{Hom}(G, H)| = 1$ and in particular*

$$\Lambda_{G,H} = 0.$$

Proof. Suppose $\phi \in \mathrm{Hom}(G, H)$ is nontrivial. Then $\ker\phi \lhd G$ is a proper normal subgroup of G, and $G/\ker\phi \cong \mathrm{im}\,\phi$ which is a subgroup of H, and hence solvable. Let $N \lhd G$ be a maximal proper normal subgroup of G containing $\ker\phi$. By the Lattice Theorem, $N/\ker\phi \lhd G/\ker\phi$ is a maximal proper normal subgroup, so by the Second Isomorphism Theorem and Proposition 4.1, $[G : N] = [G/\ker\phi : N/\ker\phi] = p$ for some prime p dividing $|G/\ker\phi| = |G|/|\ker\phi|$. In particular, p divides $|G|$. But $p = [G : N]$ divides $[G : \ker\phi] = |\mathrm{im}\,\phi|$, which divides $|H|$, so p divides $\gcd(|G|, |H|)$. The existence of N contradicts our hypothesis, so ϕ must be trivial. $\square$

This does not hold in general as, for instance, when $G = H = A_n$ for $n \geqslant 5$, which is a non-abelian simple group, G has no normal subgroups of prime index, yet there are certainly nontrivial homomorphisms $A_n \to A_n$.

Now we proceed to the case where G has a normal subgroup of index p for some prime p dividing $\gcd(|G|, |H|)$. We use the well-known fact that finite nilpotent groups are direct products of their Sylow subgroups [DF04, Ch 6, Theorem 3].

Theorem 4.3. *If G is a finite group, H is a finite nilpotent group, and p is the smallest prime divisor of $\gcd(|G|, |H|)$ such that G has a normal subgroup of index p, then*

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

Proof. The lower bound follows from Lemma 3.8 so it suffices to show the upper bound. Write $H = P_1 \times \cdots \times P_r$ where P_i is the Sylow p_i-subgroup of H, and the p_i are distinct. If $p_i < p$, then G has no normal subgroup of index p_i by assumption, so by Proposition 4.2 it follows that $\Lambda_{G,P_i} = 0$. On the other hand, if G has a normal subgroup of index p_i, then it follows from Proposition 2.6 and Lemma 3.8 that $\Lambda_{G,P_i} = \frac{1}{p_i}$. Therefore, by Proposition 3.6, it follows that $\Lambda_{G,H} = \max_i \Lambda_{G,P_i} = \frac{1}{p}$. □

5 Solvable domain

In this section, we prove Theorem 1.1 when G is solvable. As in Section 4, we begin by considering the case where G has no normal subgroups of index p for any prime p dividing $\gcd(|G|, |H|)$.

Proposition 5.1. *Let G be a finite solvable group and let H be any finite group. If G has no normal subgroup of index p for any prime p dividing $\gcd(|G|, |H|)$, then $|\operatorname{Hom}(G, H)| = 1$ and in particular*

$$\Lambda_{G,H} = 0.$$

Proof. Suppose $\phi \in \operatorname{Hom}(G, H)$ is nontrivial. Then $\ker\phi \lhd G$ is a proper normal subgroup of G, and $G/\ker\phi$ is isomorphic to a subgroup of H, by the First Isomorphism Theorem. In particular, $[G : \ker\phi]$ divides $|H|$. Let $N \lhd G$ be a maximal proper normal subgroup of G containing $\ker\phi$. By Proposition 4.1, $[G : N] = p$ for some prime p dividing $|G|$. But $p = [G : N]$ divides $[G : \ker\phi]$ which divides $|H|$, so p divides $\gcd(|G|, |H|)$. By our hypothesis, N cannot exist, so ϕ must be trivial. □

We proceed to the case where G has a normal subgroup of index p for some prime p dividing $\gcd(|G|, |H|)$. Let p be the minimal such prime, so that we wish to show $\Lambda_{G,H} = \frac{1}{p}$. We first consider the special case where every prime divisor of $|G|$ less than p also divides $|H|$. In this case, we show that G has no subgroups of index less than p, which yields the upper bound. To show this, we use the following fact, due to Berkovich, found as an exercise in [Isa08].

Proposition 5.2 ([Isa08, Exercise 3B.15])**.** *Let G be a finite solvable group. Suppose $H < G$ is a proper subgroup of G with smallest index. Then $H \lhd G$.*

We now prove the upper bound for the special case.

Lemma 5.3. *Suppose G is a finite solvable group, H is any group, and p is the smallest prime divisor of $\gcd(|G|, |H|)$ such that G has a normal subgroup of index p. If every prime less than p dividing $|G|$ also divides $|H|$, then*

$$\Lambda_{G,H} \leqslant \frac{1}{p}.$$

Proof. We claim that G has no subgroups of index less than p. Let S be the subgroup with smallest possible index. By Proposition 5.2, S is normal. Since S is a maximal normal subgroup, by Proposition 4.1 it follows that the index $[G : S] = q$ for some prime q dividing $|G|$. If $q < p$, then our hypotheses imply that q divides $|H|$, so G has a normal subgroup of prime index less than p dividing $|H|$, contradicting the minimality of p. Thus $[G : S] \geqslant p$, proving our claim.

By Lemma 3.8, $|\operatorname{Hom}(G, H)| > 1$, so by Proposition 2.5, there exist homomorphisms $\phi, \psi \in \operatorname{Hom}(G, H)$ such that $\operatorname{agr}(\phi, \psi) = \Lambda_{G,H}$. By Proposition 2.1, $\operatorname{Eq}(\phi, \psi)$ is a subgroup of G, so it follows that $\Lambda_{G,H} = \operatorname{agr}(\phi, \psi) = 1/[G : \operatorname{Eq}(\phi, \psi)] \leqslant 1/p$. □

We deal with the general case using the following theorem of Hall [Hal38] characterizing finite solvable groups as those with Sylow bases.

Theorem 5.4 ([Hal38])**.** *Let G be a finite group with order prime factorization $|G| = \prod_{i=1}^{m} p_i^{e_i}$. Then G is solvable if and only if it has Sylow p_i-subgroups P_i such that $G = P_1 \bowtie \cdots \bowtie P_m$.*

We use this decomposition to filter out all the prime divisors of $|G|$ not dividing $|H|$ to reduce to our special case.

Theorem 5.5. *If G is a finite solvable group, H is any group, and p is the smallest prime divisor of $\gcd(|G|, |H|)$ such that G has a normal subgroup of index p, then*

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

Proof. The lower bound follows from Lemma 3.8 so it suffices to show the upper bound. By Hall's theorem (Theorem 5.4), we can write $G = G_1 \bowtie G_2$ where $\gcd(|G_2|, |H|) = 1$ and every prime dividing $|G_1|$ divides $|H|$. By Proposition 3.9, $|\operatorname{Hom}(G_2, H)| = 1$. Let $N \lhd G$ be the smallest normal subgroup of G containing G_2. By Proposition 3.3, $\Lambda_{G,H} = \Lambda_{G/N,H}$, so it suffices to upper bound $\Lambda_{G/N,H}$.

Since $|G_2|$ divides $|N|$, it holds that $[G : N]$ divides $[G : G_2] = |G_1|$. In particular, every prime dividing $|G/N|$ divides $|H|$. Moreover, G/N has no normal subgroups of index $q < p$, for if it did, it would follow from the Lattice Theorem that G has a normal subgroup of index q, and moreover q divides $\gcd(|G|, |H|)$, contradicting the minimality of p. Thus, G/N has no normal subgroups of index less than p. Thus, by Lemma 5.3, it follows that $\Lambda_{G/N,H} \leqslant \frac{1}{p}$. □

The formula for $\Lambda_{G,H}$ for solvable G does not extend to arbitrary finite groups for the obvious reason that G may not have any normal subgroups of prime index. This holds, for instance, if G is any non-abelian simple group. One might then hope that the modified statement, where we drop the requirement that p be prime, holds. For simple G, this formula would be $\Lambda_{G,H} = \frac{1}{|G|}$. However, the following is a simple (pun intended) counterexample.

Let $G = H = A_5$. Consider the automorphisms which are conjugation by (123), and its inverse, conjugation by (132). Then these are distinct homomorphisms, since they disagree on (12) because $(132)(12)(123) = (13)$ while $(123)(12)(132) = (23)$. However, they agree on (45) since (45) is a fixed point. This shows that $\Lambda_{A_5,A_5} \geqslant \frac{1}{30} > \frac{1}{|G|}$. In fact, we show in Section 6 that $\Lambda_{A_5,A_5} = \frac{1}{10}$.

6 Non-abelian simple groups

We would like to determine $\Lambda_{G,H}$ for arbitrary finite groups G and H. We propose a two-part strategy for doing this. First, understand $\Lambda_{G,H}$ for simple groups G. Then, understand how to determine $\Lambda_{G,H}$ for arbitrary G by cleverly decomposing G. In Section 3, we proved some general facts about $\Lambda_{G,H}$ which could be useful (but far from complete) for the second part of this program. In this section, we explore the first part, namely we investigate $\Lambda_{G,H}$ for non-abelian simple groups G. A full investigation would entail using the classification of finite simple groups and considering each family of finite simple groups, which we do not do in this work. Instead, we prove some nontrivial lower bounds on $\Lambda_{G,H}$ for general non-abelian simple G. We then prove some lower and upper bounds on $\Lambda_{G,G}$ for the specific family $\{A_n\}_{n\geqslant 5}$ of alternating groups and pin down $\Lambda_{A_5,A_5} = \frac{1}{10}$ exactly. We highlight a major difficulty, which is that in the general setting, unlike in the setting where G is solvable, $\Lambda_{G,H}$ depends on *how* copies of G are embedded in H, not just on the prime divisors of $|G|$ and $|H|$ and the normal subgroup structure of G.

6.1 Domain and codomain are isomorphic

If H does not contain a subgroup isomorphic to G, then $\mathrm{Hom}(G,H)$ is trivial. Let us assume that $G = H$. Since G is simple, $\mathrm{Hom}(G,H) = \mathrm{Aut}(G) \cup \{g \mapsto 1_G\}$. For $\phi \in \mathrm{Aut}(G)$, $\ker\phi = \{1_G\}$, so clearly $\Lambda_{G,G} \geqslant \frac{1}{|G|}$. Can we achieve better agreement?

Better agreement must come from two automorphisms $\phi, \psi \in \mathrm{Aut}(G)$. Note that $\phi(g) = \psi(g)$ if and only if $(\phi^{-1} \circ \psi) \in \mathrm{Aut}(G)$ fixes g, so we wish to find a non-identity automorphism $\phi \in \mathrm{Aut}(G)$ which maximizes $|G^\phi|$, where

$$G^\phi \triangleq \{g \in G \mid \phi(g) = g\}$$

is the subset of G fixed by $\phi \in \mathrm{Aut}(G)$. Observe that the group $\mathrm{Aut}(G)$ naturally acts on the set G via $\phi \cdot g = \phi(g)$. Let $G/\mathrm{Aut}(G)$ denote the orbits of G under this group action. By Burnside's lemma,

$$|G/\mathrm{Aut}(G)| = \frac{1}{|\mathrm{Aut}(G)|} \sum_{\phi\in\mathrm{Aut}(G)} |G^\phi|.$$

Since $G^{\mathrm{id}} = G$, where $\mathrm{id} \in \mathrm{Aut}(G)$ is the identity automorphism,

$$|G/\mathrm{Aut}(G)| - \frac{|G|}{|\mathrm{Aut}(G)|} = \frac{1}{|\mathrm{Aut}(G)|} \sum_{\phi\in\mathrm{Aut}(G),\phi\neq\mathrm{id}} |G^\phi|,$$

or

$$\frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(G)|-1}\left(|G/\mathrm{Aut}(G)| - \frac{|G|}{|\mathrm{Aut}(G)|}\right) = \frac{1}{|\mathrm{Aut}(G)|-1} \sum_{\phi\in\mathrm{Aut}(G),\phi\neq\mathrm{id}} |G^\phi|.$$

By averaging, this implies that there is some non-identity automorphism $\phi \in \mathrm{Aut}(G)$ such that

$$|G^\phi| \geqslant \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(G)|-1}\left(|G/\mathrm{Aut}(G)| - \frac{|G|}{|\mathrm{Aut}(G)|}\right)$$

and thus, by dividing by $|G|$, we have

$$\Lambda_{G,G} \geqslant \frac{|\operatorname{Aut}(G)|}{|\operatorname{Aut}(G)|-1}\left(\frac{|G/\operatorname{Aut}(G)|}{|G|} - \frac{1}{|\operatorname{Aut}(G)|}\right).$$

6.2 Alternating groups

In this section, we prove the following.

Proposition 6.1. *For $n \geqslant 5$,*

$$\frac{2}{n(n-1)} \leqslant \Lambda_{A_n,A_n} \leqslant \frac{1}{n}.$$

When $n \neq 6$, the upper bound is strict.

For $n = 5$, the lower bound is tight, that is $\Lambda_{A_5,A_5} = \frac{|S_3|}{|A_5|} = \frac{1}{10}$. This is because the only subgroups of A_n larger than S_3, up to isomorphism, are the dihedral group D_{10} of order 10 generated by $(1\ 2\ 3\ 4\ 5)$ and $(2\ 5)(3\ 4)$, and A_4. One can check that no conjugation fixes all of A_4 nor all of D_{10}.

For the proof of Proposition 6.1, we use the following fact.

Claim 6.2. *Let $n \geqslant 3$. The subgroup $A_{n-1} \leqslant A_n$ is the unique subgroup (up to isomorphism) of A_n of smallest index. That is, there are no subgroups of A_n with index less than n, and any subgroup of index n is isomorphic to A_{n-1}.*

Proof. First, we show that there are no subgroups of index less than n. Suppose $H \leqslant A_n$ with $m \triangleq [A_n : H] < n$. The group A_n acts on the left cosets A_n/H by left multiplication, i.e. there is a homomorphism $\rho : A_n \to \operatorname{Perm}(A_n/H) \cong S_m$. This action is clearly nontrivial, and since A_n is simple, this means ρ is injective, so A_n embeds into S_m. This is impossible since $n > 2$ implies $|A_n| = \frac{n!}{2} > (n-1)! \geqslant m! = |S_m|$.

Now, we show uniqueness up to isomorphism. Let $H \leqslant A_n$ have index n. We will show that $H \cong A_{n-1}$. Again, consider the action ρ as defined above. We established that A_n acts faithfully on A_n/H. Observe that H acts on A_n/H by fixing the coset H and permuting the other $n-1$ cosets. Therefore, $\rho(H)$ is a subgroup of a copy of A_{n-1} inside $\operatorname{Perm}(A_n/H)$. Since ρ is injective, $|\rho(H)| = (n-1)!$, and so $\rho(H)$ is actually isomorphic to A_{n-1}. Moreover, H is isomorphic to $\rho(H)$ by the injectivity of ρ, so H is isomorphic to A_{n-1}. □

Proof of Proposition 6.1. For the lower bound, note that there is a twisted copy of S_{n-2} inside A_n, generated by the elements $(1\ 2\ \cdots\ n-2)$ and $(n-1\ n)$ when n is even, and by $(1\ 2\ \cdots\ n-1)$ and $(n-1\ n)$ when n is odd. In either case, the automorphism $\phi_\rho : \sigma \mapsto \rho\sigma\rho^{-1}$ with $\rho = (n-1\ n)$ fixes this copy of S_{n-2}.

The upper bound follows from the fact that A_{n-1} is the unique subgroup (up to isomorphism) of A_n of smallest index (Claim 6.2). For $n \neq 6$, every automorphism of A_n is conjugation by some $\sigma \in S_n$, but no $\sigma \in S_n$ fixes every element of A_{n-1}. □

6.3 Codomain contains copies of domain

If H contains a copy of G, then $\Lambda_{G,H} \geqslant \Lambda_{G,G}$, by Proposition 3.1. When G is solvable, it follows from Proposition 5.5 that this is an equality. One might hope to show that if G is non-abelian simple, then this is actually an equality, but this is not true. An easy counterexample is when $H = A_6$ with subgroups $\mathrm{Alt}(\{1,2,3,4,5\})$ and $\mathrm{Alt}(\{1,2,3,4,6\})$ (both isomorphic copies of A_5) with $G = \mathrm{Alt}(\{1,2,3,4,5\})$. Then $\phi_1 : G \to \mathrm{Alt}(\{1,2,3,4,5\})$ defined by $\phi_1(\sigma) = \sigma$ and $\phi_2 : G \to \mathrm{Alt}(\{1,2,3,4,6\})$ defined by $\phi_2(\sigma) = (5\ 6)\sigma(5\ 6)$ agree on $\mathrm{Alt}(\{1,2,3,4,5\}) \cap \mathrm{Alt}(\{1,2,3,4,6\}) = \mathrm{Alt}(\{1,2,3,4\}) \cong A_4$. Thus $\Lambda_{A_5,A_6} = \frac{|A_4|}{|A_5|} = \frac{1}{5} > \frac{1}{10} = \Lambda_{A_5,A_5}$.

Acknowledgements

The author thanks Madhu Sudan for inspiring discussions.

References

[DF04] David Steven Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & sons, Hoboken, NJ, 2004.

[DGKS08] Irit Dinur, Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Decodability of group homomorphisms beyond the Johnson bound. In Dwork [Dwo08], pages 275–284.

[DL12] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In Howard J. Karloff and Toniann Pitassi, editors, *STOC*, pages 351–358. ACM, 2012.

[Dwo08] Cynthia Dwork, editor. *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008.* ACM, 2008.

[Eli57] Peter Elias. List decoding for noisy channels. *Technical Report 335, Research Laboratory of Electronics, MIT*, 1957.

[GKS06] 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.

[GKZ08] Parikshit Gopalan, Adam R. Klivans, and David Zuckerman. List-decoding Reed-Muller codes over small fields. In Dwork [Dwo08], pages 265–274.

[GL89] 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.

[Gop13] Parikshit Gopalan. A Fourier-analytic approach to Reed-Muller decoding. *IEEE Transactions on Information Theory*, 59(11):7747–7760, 2013.

[GR08] 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.

[GS99] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[GS14] Alan Guo and Madhu Sudan. List decoding group homomorphisms between supersolvable groups. In Klaus Jansen, José D. P. Rolim, Nikhil R. Devanur, and Cristopher Moore, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2014, September 4-6, 2014, Barcelona, Spain*, volume 28 of *LIPIcs*, pages 737–747. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2014.

[Gur11] Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *IEEE Conference on Computational Complexity*, pages 77–85. IEEE Computer Society, 2011.

[GW11] 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.

[Hal38] Philip Hall. On the Sylow systems of a soluble group. *Proceedings of the London Mathematical Soceity*, s2-43(1):316–323, 1938.

[Ham50] Richard W. Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29:147–160, April 1950.

[Isa08] I. Martin Isaacs. *Finite Group Theory*. American Mathematical Society, 2008.

[Joh62] Selmer M. Johnson. A new upper bound for error-correcting codes. *IEEE Transactions on Information Theory*, 8:203–207, 1962.

[Kop12] Swastik Kopparty. List-decoding multiplicity codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:44, 2012.

[Sud97] Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *J. Complexity*, 13(1):180–193, 1997.

[Woz58] John M. Wozencraft. List Decoding. *Quarterly Progress Report, Research Laboratory of Electronics, MIT*, 48:90–95, 1958.