Approximate Polymorphisms[*]

Gilad Chase
Technion — Israel Institute of
Technology
The Henry & Marilyn Taub Faculty of
Computer Science
Haifa, Israel
giladchase@gmail.com

Yuval Filmus
Technion — Israel Institute of
Technology
The Henry & Marilyn Taub Faculty of
Computer Science
Haifa, Israel
yuvalfi@cs.technion.ac.il

Dor Minzer
Massachusetts Institute of Technology
Department of Mathematics
Cambridge, MA, USA
minzer.dor@gmail.com

Elchanan Mossel
Massachusetts Institute of Technology
Mathematics and IDSS
Cambridge, MA, USA
elmos@mit.edu

Nitin Saurabh
Indian Institute of Technology
Hyderabad
Department of Computer Science and
Engineering
Sangareddy, Telangana, India
nitin@cse.iith.ac.in

ABSTRACT

For a function $g\colon \{0,1\}^m \to \{0,1\}$, a function $f\colon \{0,1\}^n \to \{0,1\}$ is called a g-polymorphism if their actions commute. The function f is called an approximate g-polymorphism if this equality holds with probability close to 1, when Z is sampled uniformly. A pair of functions $f_0, f_1\colon \{0,1\}^n \to \{0,1\}$ are called a skew g-polymorphism if $f_0(g(\mathrm{row}_1(Z)), \ldots, g(\mathrm{row}_n(Z))) = g(f_1(\mathrm{col}_1(Z)), \ldots, f_1(\mathrm{col}_m(Z)))$ for all $Z \in \{0,1\}^{n \times m}$.

We study the structure of exact polymorphisms as well as approximate polymorphisms. Our results include a proof that an approximate polymorphism f must be close to an exact *skew* polymorphism, and a characterization of exact skew polymorphisms, which shows that besides trivial cases, only the functions AND, XOR, OR, NAND, NOR, XNOR admit non-trivial exact skew polymorphisms.

We also study the approximate polymorphism problem in the list-decoding regime (i.e., when the probability equality holds is not close to 1, but is bounded away from some value). We show that if $f(x \wedge y) = f(x) \wedge f(y)$ with probability larger than $s_\wedge \approx 0.815$ then f correlates with some junta, and $s_\wedge$ is the optimal threshold for this property.

Our result generalize the classical linearity testing result of Blum, Luby and Rubinfeld, that in this language showed that the approximate polymorphisms of $g = $ XOR are close to XOR's, as well as a recent result of Filmus, Lifshitz, Minzer and Mossel, showing that the approximate polymorphisms of AND can only be close to AND functions.

CCS CONCEPTS

• **Mathematics of computing** → *Probability and statistics*; • **Theory of computation** → *Randomness, geometry and discrete structures*.

KEYWORDS

property testing, social choice theory, polymorphisms

1 INTRODUCTION

Let $m \in \mathbb{N}$ be thought of as a constant, $n \in \mathbb{N}$ be thought of as large, and let $g\colon \{0,1\}^m \to \{0,1\}$ be any function. We say that $f\colon \{0,1\}^n \to \{0,1\}$ is a *polymorphism* of g if their operations commute. More precisely, defining the functions $f \circ g^n, g \circ f^m\colon \{0,1\}^{n \times m} \to \{0,1\}$ as

$$(f \circ g^n)(Z) = f(g(\mathrm{row}_1(Z)), \ldots, g(\mathrm{row}_n(Z))),$$
$$(g \circ f^m)(Z) = g(f(\mathrm{col}_1(Z)), \ldots, f(\mathrm{col}_m(Z))),$$

we say that f is a polymorphism of g if $f \circ g^n = g \circ f^m$. See Figure 1 for an illustration.

More generally, for a parameter $\delta > 0$, we say that f is a δ-*approximate polymorphism* if

$$\Pr_Z[(f \circ g^n)(Z) \neq (g \circ f^m)(Z)] \leqslant \delta;$$

here and throughout, the distribution over Z is uniform over $\{0,1\}^{n \times m}$. We note that for any function g, one always has dictatorship functions as polymorphisms. Namely, for each $j \in [n]$, it is easily seen that the function $f(x) = x_j$ is a polymorphism of g as

$$(f \circ g^n)(Z) = g(\mathrm{row}_j(Z)) = (g \circ f^m)(Z).$$

Dictatorship polymorphisms will thus be referred to as *trivial polymorphisms* of g. If g possesses a mild structural property, then
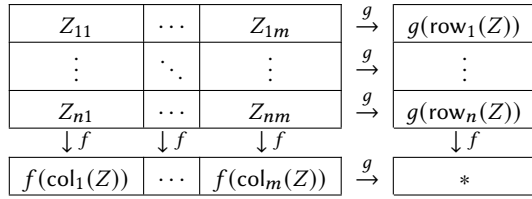
Gilad Chase, Yuval Filmus, Dor Minzer, Elchanan Mossel, and Nitin Saurabh

Figure 1: f is a polymorphism of g, in symbols $f \circ g^n = g \circ f^m$, if applying g to the bottom row produces identical results to applying f to the rightmost column.

there are additional trivial polymorphisms: when g is odd, anti-dictatorships also form polymorphisms; if $g(b, \ldots, b) = b$, then the constant function $f(x) = b$ also forms a polymorphism. What can be said about the structure of functions g that have non-trivial polymorphisms? More generally, what can be said about functions g that have approximate polymorphisms that are far from being trivial? Furthermore, can we classify the structure of the approximate polymorphisms in these cases?

The problem of studying the structure of polymorphisms as well as approximate polymorphisms has appeared in several different contexts throughout theoretical computer science:

(1) **Universal algebra and the complexity of constraint satisfaction problems.** In this context, the function g is allowed to be a predicate rather than a function, and a polymorphism is a function f that takes satisfying assignments to g, ordered as rows in the matrix $Z \in \{0, 1\}^n$, and produces a satisfying assignment for g in the form $f^m(Z)$ (i.e., somewhat of a one-sided version of the above equation). In this context, the existence of non-trivial polymorphisms is strongly linked to the complexity of the constraint satisfaction problem corresponding to the predicate g (see for example [2]).

(2) **Property testing.** Perhaps the most basic problem in property testing, the linearity testing problem [3, 4], can be cast in the language of approximate polymorphisms. Here, one takes $m = 2$ and the function $g(x, y) = x \oplus y$, in which case a function f is an δ approximate polymorphism if $f(x \oplus y) = f(x) \oplus f(y)$ with probability $\geqslant 1 - \delta$, where x and y are sampled uniformly and independently from $\{0, 1\}^n$. This question, as well as its $1/2 + \delta$ list-decoding variant have been well studied and are useful in the study of PCP's [9].

(3) **Social choice theory.** In this context, one thinks of the functions f, g as voting rules, and then the above functions $f \circ g^n, g \circ f^m$ can be thought of as two ways of aggregating these voting rules in order to reach a final outcome. Due to this interpretation, it makes sense to also consider the "cross" version of the problem, wherein we have multiple functions f, say $f_0, \ldots, f_m$, and we replace the above equation by

$$(f_0 \circ g^n)(Z) = g(f_1(\text{col}_1(Z)), \ldots, f_m(\text{col}_m(Z))).$$

The interpretation here is that there are n voters that cast their yes/no opinion on each one of m topics; notationally, the vector $\text{row}_i(Z)$ represents the opinions of voter i. The goal is to aggregate these opinions about the topic to reach a

final conclusion, and naturally this can be done in one of two ways: first, one may aggregate the opinion of each voter, and then aggregate the final conclusion of each voter. This way of aggregation is represented by $(f_0 \circ g^n)(Z)$. Another way to aggregate these opinions is to first reach a final conclusion regarding each topic, which is $f_j(\text{col}_j(Z))$ in the above notation, and then aggregate those; this is represented by the function $g(f_1(\text{col}_1(Z)), \ldots, f_m(\text{col}_m(Z)))$. Thus, in this interpretation, the question asks for which aggregation rules g and f_i does it hold that the two natural ways of aggregating the votes are essentially equivalent.

The case where g is an AND function is a prominent example that has been studied in this context. In particular, the fact that $f =$ Majority does not yield equivalent rules is known as the *Doctrinal paradox*, which raised the question of what are all f's in this case that yield equivalent rules. This problem has been addressed by Nehama [17] in the context of social choice theory and by Parnas, Ron and Samorodnitsky [18] from the property testing point of view, and both works establishing partial results. A recent work [7] has improved these results, showing that in this case the approximate polymorphisms of g can only be functions that are close to AND functions.

With this in mind, it makes sense to ask what is the most general result one can prove when g is a general function on constantly many coordinates. Indeed, answering this question is the main goal of this paper:

> Determine all pairs f, g which are *approximate polymorphisms*:
> $$\Pr[f \circ g^n = g \circ f^m] \geqslant 1 - \delta.$$

1.1 The Structure of Exact Polymorphisms

The exact polymorphisms variant of this problem, i.e. the case that $\delta = 0$, has been previously studied by Dokow and Holzman [5]. They manage to give the following tight classification of all possible pairs f, g in which f is a polymorphism of g:

(1) One of f, g is constant, a dictator (x_i), or an anti-dictator $(\neg x_i)$.
(2) f, g are XORs or their negation.
(3) f, g are ANDs.
(4) f, g are ORs.

Stated otherwise, the only g's that have non-trivial polymorphisms are AND's, OR's, XOR's and NXOR's. It is interesting to note that in each one of these cases, the answer to the approximate polymorphisms problem has already been resolved; the case g is an XOR or an NXOR is linearity testing [3, 4], and it is well-known that f must be close to an XOR or its negation. When g is an AND, it was shown in [7] that f is close to zero or to an AND, and the case where g is an OR is similar.

Thus, it would be natural to guess that the only g's that have non-trivial approximate polymorphisms would be exactly the g's found by Dokow and Holzman. Furthermore, we would expect that if g is not an XOR, NXOR, AND, or OR, and f is an approximate

polymorphism, then f must be trivial, i.e. close to a constant, a dictator, or an anti-dictator. Here and throughout, closeness is measured with respect to the Hamming distance over the uniform measure on $\{0,1\}^n$.

1.2 Main Results

1.2.1 Approximate Polymorphisms. In this language, our main result reads:

Theorem 1.1. *Fix* $g\colon \{0,1\}^m \to \{0,1\}$. *For every* $\varepsilon > 0$ *there exists* $\delta > 0$ *(depending on both g and ε) such that for every n, if* $f\colon \{0,1\}^n \to \{0,1\}$ *satisfies*

$$\Pr_Z[(f \circ g^n)(Z) = (g \circ f^m)(Z)] \geqslant 1 - \delta,$$

then either:

(1) *f is ε-close to a constant, dictator, anti-dictator or an exact polymorphism of g;*

(2) *g is either an NOR or an NAND, and f is ε-close to an OR or an AND (respectively).*

Naively, one may have hoped that the first item in the theorem must always hold, however as we explain next, it is necessary to include the second item as well. Suppose that g is unbalanced, so that $p = \mathbb{E}[g]$ is at least 2^{-m}-far from $1/2$. Suppose we have functions f_0 and f_1 satisfying $f_0 \circ g^n = g \circ f_1^m$. Given such f_0, f_1, we may construct a function f agreeing with f_1 around the middle slice and with f_0 around the pn-slice, and have that $f \circ g^n \approx g \circ f^m$. All new solutions in Theorem 1.1 arise from such *skew polymorphisms.*

Dokow and Holzman in fact solved the more general cross version of the problem defined above. Namely, they managed to classify all solutions to the equation $f_0 \circ g^n = g \circ (f_1, \ldots, f_m)$. Our main result extends to this setting as well, and we prove an analog of Theorem 1.1 for it as well:

Theorem 1.2. *Fix* $g\colon \{0,1\}^m \to \{0,1\}$. *For every* $\varepsilon > 0$ *there exists* $\delta > 0$ *(depending on both g and ε) such that for every n, if* $f_0, \ldots, f_m\colon \{0,1\}^n \to \{0,1\}$ *satisfy*

$$\Pr_Z[(f_0 \circ g^n)(Z) = (g \circ (f_1, \ldots, f_m))(Z)] \geqslant 1 - \delta,$$

then $f_0, \ldots, f_m$ are ε-close to functions $F_0, \ldots, F_m\colon \{0,1\}^n \to \{0,1\}$ satisfying $F_0 \circ g^n = g \circ (F_1, \ldots, F_m)$. (In the case of f_0, F_0, closeness is with respect to the biased measure μ_p, where $p = \Pr[g = 1]$.)

In the context of Theorem 1.1, we have $f_0 = \cdots = f_m = f$. While we can guarantee that $F_1 = \cdots = F_m$, it is not necessarily the case that $F_0 = F_1$. This is the reason for the second option in the statement of Theorem 1.1.

We also provide an alternative proof of the classification of Dokow and Holzman [5], using Boolean function analysis. To illustrate the merits of this proof technique, we classify all solutions of the slightly more general equation

$$f_0 \circ g^n = h \circ (f_1, \ldots, f_m).$$

1.2.2 The List Decoding Regime. As discussed earlier, the linearity testing problem, which constitutes one example of the approximate polymorphisms problem, can be studied in several different regimes:

(1) Exact regime: If $\Pr[f(x \oplus y) = f(x) \oplus f(y)] = 1$ then f is an XOR.

(2) Approximate regime: If $\Pr[f(x \oplus y) = f(x) \oplus f(y)] \geqslant 1 - \delta$ then f is $O(\delta)$-close to an XOR.

(3) List decoding regime: If $\Pr[f(x \oplus y) = f(x) \oplus f(y)] \geqslant 1/2 + \delta$ then f is $\Omega(\delta)$-correlated with some XOR.

In this language, Dokow and Holzman extended the exact regime to arbitrary functions g (in linearity testing, $g(x, y) = x \oplus y$), and Theorem 1.1 extends the approximate regime to arbitrary functions g. Our second main result extends the list decoding regime to arbitrary functions g.

Theorem 1.3. *Fix* $g\colon \{0,1\}^m \to \{0,1\}$ *which is not an XOR or an NXOR. There exists a constant $s_g < 1$ such that the following holds:*

(1) *For every $\varepsilon > 0$ there exist $L, \delta > 0$ such that for every n, if*

$$\Pr_Z[(f \circ g^n)(Z) = (g \circ f^m)(Z)] \geqslant s_g + \delta$$

then f is ε-correlated with some Boolean L-junta h, that is, $\Pr[f = h] \geqslant 1/2 + \varepsilon$.
(Without loss of generality, we can take h to be an XOR.)

(2) *For every sufficiently small $\delta > 0$, there exists large enough n and a function $f\colon \{0,1\}^n \to \{0,1\}$ such that the correlation of f with any $(1/\delta)$-junta is at most δ, and*

$$\Pr_Z[(f \circ g^n)(Z) = (g \circ f^m)(Z)] \geqslant s_g - \delta.$$

A similar result also holds if g is an XOR or an NXOR *of at least two variables,* with the following difference: instead of guaranteeing that f correlates with a junta, all we can show is that it is correlated with an XOR (which is also all we can hope for, since XORs are exact polymorphism of XOR).

Computing the value of s_g may be a challenging task in general. When g is an XOR, one has $s_g = 1/2$. When $g(x, y) = x \wedge y$, one may have expected s_g to be equal to $3/4$ (as was conjectured by [7]). It turns out that it is actually higher, about 0.814975.

1.2.3 Comparison to Previous Work. Our main theorems generalize classical work on linearity testing [3, 4], which is the special case of $g = $ XOR.

This work was prompted by recent work [7] which proved Theorem 1.1 in the special case of $g = $ AND. Theorem 1.1 and Theorem 1.3 answer two of the three open questions posed in [7].

Several other results in the literature can be seen as analogs of Theorem 1.1 in the more general case of predicates:

(1) **Arrow's theorem.** The NAE_3 predicate is a predicate on triples of bits which holds whenever the three bits are not all equal. Arrow's theorem [1] for three candidates states, in our language, that the only polymorphisms of NAE_3 satisfying $f(0, \ldots, 0) = 0$ and $f(1, \ldots, 1) = 1$ are dictators. Wilson [20] improved this, showing that the only polymorphisms of NAE_3 are dictators and anti-dictators.

Mossel [14], improving on earlier work of Kalai [11], showed that approximate polymorphisms of NAE_3 are close to dictators or to anti-dictators. Mossel's result is more general, allowing for more than three candidates.[1] Mossel's work was subsequently improved quantitatively by Keller [12].

---

[1]Mossel's result is even more general, classifying also exact and approximate *multipolymorphisms,* in which different f's are allowed for different columns.

Gilad Chase, Yuval Filmus, Dor Minzer, Elchanan Mossel, and Nitin Saurabh

(2) **Intersecting families.** An intersecting family is the same as a polymorphism of the binary predicate NAND_2 on pairs of bits. We define approximate polymorphisms of NAND_2 with respect to the unique distribution $\mu_{p,p}$ supported on the support of NAND_2 whose marginals are μ_p.

Friedgut and Regev [8] proved, in our language, that when $p < 1/2$, any approximate polymorphism of NAND_2 is close to an exact polymorphism of NAND_2.

1.3 Techniques: Theorem 1.1

The proof of Theorem 1.1 is composed of two parts. First, we show that f is close to a junta. Second, we use this to reduce the approximate question to an *exact* question.

We can assume without loss of generality that g depends on all coordinates. If g is an XOR or an NXOR then Theorem 1.1 reduces to linearity testing (except for the trivial cases $m = 0$ and $m = 1$), and so we can assume that g is not an XOR or an NXOR. This implies that g has an input α with a nonsensitive coordinate j, that is, $g(\alpha) = g(\alpha^{\oplus j})$, where $\alpha^{\oplus j}$ results from flipping the jth coordinate. To simplify notation, we assume that $j = m$.

1.3.1 Showing That f is Close to a Junta.

The basic argument. In this part, we assume that $(f \circ g^n)(Z) = (g \circ f^m)(Z)$ with probability at least $1 - \eta$. Later on, we will choose δ as a function of both η and the size of the junta.

Suppose first that all variables in f have small influence. In this case, we will show that f is ε-close to a constant function. We do this by assuming that f is ε-far from constant and reaching a contradiction.

The idea is to construct two correlated inputs Z, W, each individually uniformly random, such that

$$(f \circ g^n)(Z) = (f \circ g^n)(W)$$

with probability 1. To sample such Z, W, we use the input α. Namely, we form W by resampling the mth coordinate of each row whose first $m - 1$ coordinates agree with α. Thus, by the approximate polymorphism condition, it follows that $(g \circ f^m)(Z) = (g \circ f^m)(W)$ with probability $\geqslant 1 - 2\eta$; as we argue next, this last fact will tell us that f must be close to constant.

Since g depends on all coordinates, there is an input β such that $g(\beta) \neq g(\beta \oplus e_m)$; suppose without loss of generality that $g(\beta_1, \ldots, \beta_{m-1}, x_m) = x_m$. By assumption, f is ε-far from constant, and so with probability at least ε^{m-1}, if we evaluate f on the first $m - 1$ columns of Z (which are identical to the corresponding columns of W) then we obtain $\beta_1, \ldots, \beta_{m-1}$. When this happens,

$$(g \circ f^m)(Z) = f(\mathrm{col}_m(Z)) \text{ and } (g \circ f^m)(W) = f(\mathrm{col}_m(W)),$$

and we get that $f(\mathrm{col}_m(Z)) = f(\mathrm{col}_m(W))$ with probability $\geqslant 1 - 2\eta$. To analyze this event, we consider the following equivalent way of sampling $z = \mathrm{col}_m(Z)$ and $w = \mathrm{col}_m(W)$:

(1) Sample a subset $R \subseteq [n]$ by including each element with probability $2^{-(m-1)}$; these are the rows whose first $m - 1$ columns agree with α.
(2) Sample $z_j = w_j$ for each $j \notin R$.
(3) Sample z_j, w_j independently for each $j \in R$.

The first two steps define a random restriction, and to reach a contradiction we would like to argue that this random restriction

still has a significant variance with high probability (so that we will in fact have $f(z) \neq f(w)$ with significant probability). Indeed, this is true provided the variance of f is significant and all of the (low-degree) influences of f are small; this is the so-called "It Ain't Over Till It's Over" theorem from [15]. A bit more precisely, this result asserts that provided the influences of f are small, it is extremely likely (the failure probability is smaller than $\varepsilon^{m-1}/2$) that f is γ-far from constant even after the random restriction, where $\gamma(\varepsilon, m) > 0$. This gives us that

$$\Pr[(g \circ f^m)(Z) \neq (g \circ f^m)(W)] \geqslant \left(\varepsilon^{m-1} - \frac{\varepsilon^{m-1}}{2} \right) \cdot 2\gamma(1 - \gamma).$$

Thus, choosing η so that 2η is smaller than this expression, we reach a contradiction. This contradiction thus implies that if all of the influences of f are small, then the only way for f to be an approximate polymorphism of g is that f is close to a constant.

Lifting the small low-degree influences assumption. An arbitrary function f could potentially have variables with large low-degree influence. To generalize our argument to this case, we make use of a regularity lemma [10] by Jones. This lemma asserts that one may find a small set of variables T such that randomly restricting them in f, one gets a function with no significant low-degree influences with probability close to 1. Thus, we first perform this random restriction, and then use a variant of the above argument to argue that under such restrictions, f must be in fact close to a constant. Overall, we obtain that f is close to a junta.

1.3.2 Deducing Theorem 1.1. The previous part shows that f is close to a junta F, say depending on the first L coordinates. We split the input Z accordingly to two matrices: $Z^{(1)}$ consists of the first L rows, and $Z^{(2)}$ consists of the remaining rows. Thus with probability $1 - \delta$,

$$f(g(\mathrm{row}_1(Z^{(1)})), \ldots, g(\mathrm{row}_L(Z^{(1)})),$$
$$g(\mathrm{row}_1(Z^{(2)})), \ldots, g(\mathrm{row}_{n-L}(Z^{(2)}))) =$$
$$g(f(\mathrm{col}_1(Z^{(1)}), \mathrm{col}_1(Z^{(2)})), \ldots, f(\mathrm{col}_m(Z^{(1)}), \mathrm{col}_m(Z^{(2)}))).$$

If we fix $Z^{(2)}$ then we can find functions $f_0, \ldots, f_m : \{0, 1\}^L \to \{0, 1\}$ such that the left-hand side becomes $f_0 \circ g$, and the right-hand side becomes $g \circ (f_1, \ldots, f_m)$.

For a typical $Z^{(2)}$, the functions $f_1, \ldots, f_m$ are all close to F and so to each other, and furthermore

$$\Pr[f_0 \circ g^n \neq g \circ (f_1, \ldots, f_m)] \leqslant \delta.$$

We choose $\delta < \min(\eta, 2^{-mL})$, and so this implies that in fact,

$$f_0 \circ g^n = g \circ (f_1, \ldots, f_m).$$

Since the functions $f_1, \ldots, f_m$ are close to each other, the classification of all solutions to the equation $f_0 \circ g = g \circ (f_1, \ldots, f_m)$ implies that $f_1 = \cdots = f_m$ (except for some corner cases), and so $f_0 \circ g = g \circ f_1$. This completes the proof, since both f_1 and f are close to F.

1.4 Techniques: Theorem 1.3

We illustrate the proof of the theorem in the special case of the AND function. It will be more convenient to switch from $\{0, 1\}$ to

$\{-1, 1\}$, and to consider $g(x_1, x_2) = x_1 \wedge x_2 = \min(x_1, x_2)$ (which is one possible interpretation of AND).

We prove the theorem in contrapositive: assuming that all low-degree Fourier coefficients are small (which is equivalent to having small correlation with all XORs), we will bound $\Pr[f(x \wedge y) = f(x) \wedge f(y)]$, or rather $\mathbb{E}[f(x \wedge y)(f(x) \wedge f(y))]$ (this is one reason to switch to $\{-1, 1\}$).

The main idea is to apply the invariance principle in order to switch to a problem in Gaussian space. For this, we need f to have small low-degree influences, as well as low degree. We can assume that f has small low-degree influences by appealing to Jones' regularity lemma. In order to reduce the degree of f, we apply a small amount of noise. An expansion argument of Mossel [13] shows that the noise doesn't affect the expectation by much, essentially since given x and $x \wedge y$ there is some uncertainty regarding y.

What do we get in Gaussian space? The vector

$$\frac{(x \wedge y) + 1/2}{\sqrt{3/4}}, x, y$$

has expectation zero and covariance matrix

$$\Sigma = \begin{pmatrix} 1 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & 1 & 0 \\ \frac{1}{\sqrt{3}} & 0 & 1 \end{pmatrix}.$$

This shows that for some functions $q, p \colon \mathbb{R}^n \to \mathbb{R}$,

$$\mathbb{E}[f(x \wedge y)(f(x) \wedge f(y))] \approx \mathbb{E}[q(\mathcal{G}_0)(p(\mathcal{G}_1) \wedge p(\mathcal{G}_2))],$$

where $(\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2)$ is a multivariate Gaussian with expectation zero and covariance Σ, and $p(\mathcal{G}_1) \wedge p(\mathcal{G}_2) = (-1 + p(\mathcal{G}_1) + p(\mathcal{G}_2) + p(\mathcal{G}_1)p(\mathcal{G}_2))/2$ is the multilinear extension of $\wedge$. Due to the degree-reducing noise, p depends mostly on the behavior of f around the middle slice, and q depends mostly on its behavior around the quarter slice. A standard truncation argument lets us assume that q, p attain values in $[-1, 1]$, and a further rounding argument lets us assume that they attain values in $\{-1, 1\}$.

The assumption that f has no large low-degree Fourier coefficients translates to $\mathbb{E}[p] \approx 0$.[2] We do not have control over $\mathbb{E}[q]$, since it is controlled by the low-degree Fourier coefficients of f with respect to the $\{-1, 1\}$-analog of $\mu_{1/4}$. Applying a generalization of Borell's theorem due to Neeman [16], this is enough to show that the optimal choice for p is the one-dimensional sign function. By calculating the corresponding optimal choice for q, we obtain

$$\Pr[f(x \wedge y) = f(x) \wedge f(y)] \lesssim 0.814975356673002.$$

Here is a matching construction: take f to be the majority function for inputs x such that $\frac{1}{n} \sum_i x_i \approx 0$, and an appropriate threshold function elsewhere. The construction exploits the fact that random points $x, y \in \{-1, 1\}^n$ satisfy $\frac{1}{n} \sum_i x_i, \frac{1}{n} \sum_i y_i \approx 0$ while $\frac{1}{n} \sum_i (x_i \wedge y_i) \approx -\frac{1}{2}$. Choosing the optimal threshold gives a function f with

$$\Pr[f(x \wedge y) = f(x) \wedge f(y)] \gtrsim 0.814975356673002.$$

---

[2]Due to the application of Jones' regularity lemma, we are actually working with restrictions of f rather than f itself. In order to ensure that these restrictions have expectation close to zero, we need to assume that f has small lower-degree Fourier coefficients.

Explicitly, the following function f works, for $\alpha \approx 0.78670616285939$:

$$f(x_1, \dots, x_n) = \begin{cases} +1 & \text{if } \mathbb{E}[x] \geqslant 0, \\ -1 & \text{if } -\frac{1}{4} \leqslant \mathbb{E}[x] < 0, \\ +1 & \text{if } -\frac{1}{2} - \frac{\alpha}{\sqrt{n}} \leqslant \mathbb{E}[x] < -\frac{1}{4}, \\ -1 & \text{if } \mathbb{E}[x] < -\frac{1}{2} - \frac{\alpha}{\sqrt{n}}, \end{cases}$$

where $\mathbb{E}[x] = \frac{1}{n} \sum_i x_i$.

1.5 Techniques: Classifying Exact (Multi-)polymorphisms

Dokow and Holzman [5] classified all exact multi-polymorphisms, that is, all exact solutions to the equation $f_0 \circ g^n = g \circ (f_1, \dots, f_m)$, using combinatorial arguments. We present an alternative proof using Boolean function analysis in the full version of the paper. For the sake of the proof, we switch from $\{0, 1\}$ to $\{-1, 1\}$.

The proof proceeds in two main steps. In the first step, we determine all multilinear polynomials $g, h \colon \{-1, 1\}^m \to \mathbb{R}$ and $f_0, \dots, f_m \colon \{-1, 1\}^n \to \mathbb{R}$ which solve the equation

$$f_0(g(z_{11}, \dots, z_{1m}), \dots, g(z_{n1}, \dots, z_{nm})) = $$
$$h(f_1(z_{11}, \dots, z_{n1}), \dots, f_m(z_{1m}, \dots, z_{nm})),$$

where the functions $f_0, \dots, f_m, g, h$ are extended to $\mathbb{R}^n$ or $\mathbb{R}^m$ multilinearly. Except for some corner cases, these solutions all involve functions of the form

$$A \prod_{i \in S} (x_i + \kappa_i) - B.$$

In the second step, we observe that a function of the form above is Boolean iff it corresponds to either XOR, NXOR, AND, or OR, which completes the classification.

The first step is itself composed of two substeps. In the first substep, we relate the supports of the Fourier expansions of g, h and $f_0, \dots, f_m$ to that of $f_0 \circ g$ and $g \circ (f_1, \dots, f_m)$, and conclude that except for some corner cases, and after possibly removing irrelevant coordinates, $\deg g = \deg h = m$ and $\deg f_0 = \deg f_1 = \cdots = \deg f_m = n$. In the second step, we show that up to affine shifts, the only solution to $f_0 \circ g^n = h \circ (f_1, \dots, f_m)$ is $g(y) = h(y) = \prod_{j=1}^m y_j$ and $f_0(x) = f_1(x) = \cdots = f_m(x) = \prod_{i=1}^n x_i$.

2 LIST DECODING REGIME

A polymorphism of g is a function f satisfying $f \circ g^n = g \circ f^m$. There are two ways to relax this definition:

- The 99% regime: study functions f satisfying $f \circ g^n = g \circ f^m$ for most inputs. Theorem 1.1 shows that such functions are close to exact polymorphisms.
- The 1% regime: study functions f satisfying $f \circ g^n = g \circ f^m$ with *significant* probability. We would like to say that such functions are *structured*.

When g is the XOR function, the classic analysis of linearity testing [3] shows that if $\Pr[f(x \oplus y) = f(x) \oplus f(y)] \geqslant 1/2 + \varepsilon$, then f is correlated with some character, that is, for some $S \subseteq [n]$,

$$\Pr\left[f(x) = \bigoplus_{i \in S} x_i\right] \geqslant \frac{1}{2} + \varepsilon.$$

Conversely, if f is a random function then $\Pr[f(x \oplus y) = f(x) \oplus f(y)] \approx 1/2$, showing that $1/2$ is the correct threshold for this kind of structure.

What happens for other g? Let us take the AND function as a test case. If we choose f at random then $\Pr[f(x \wedge y) = f(x) \wedge f(y)] \approx 1/2$, and so one could conjecture that when $\Pr[f(x \wedge y) = f(x) \wedge f(y)] \geq 1/2 + \varepsilon$ then f is correlated with some character. The Majority function refutes this conjecture, since it satisfies $\Pr[f(x \wedge y) = f(x) \wedge f(y)] \approx 3/4$ but is not correlated with any character.

The threshold $3/4$ is natural, since it corresponds to the following "almost-random" construction: choose f at random for inputs whose Hamming weight is close to $n/2$ (where n is the input size), and choose f to be 0 elsewhere. However, it is not the correct threshold: if we choose f to be Majority for inputs whose Hamming weight is close to $n/2$, and a *biased* majority for other inputs, then $\Pr[f(x \wedge y) = f(x) \wedge f(y)] \approx 0.814975$; the exact definition of f appears below, as part of the statement of Theorem 2.7.

Our main result shows that 0.814975 is the correct threshold for AND: if $\Pr[f(x \wedge y) = f(x) \wedge f(y)] \geq 0.814975 + \varepsilon$ then f is correlated with some character. Moreover, we can guarantee that this character has low degree.

The idea of the proof is to translate the question about Boolean variables to a question on Gaussian space. To this end, we define a Gaussian analog of the distribution $(g(x), x)$. It will be convenient to switch from $\{0, 1\}$ to $\{-1, 1\}$.

Definition 2.1. Let $g: \{-1, 1\}^m \to \{-1, 1\}$ be non-constant. The distribution $\mathcal{N}_g$ is an $(m+1)$-variate Gaussian distribution $(\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_m)$ given by:

- Each coordinate is a standard Gaussian.
- The Gaussians $\mathcal{G}_1, \ldots, \mathcal{G}_m$ are independent.
- For each $j \in [m]$,

$$\mathbb{E}[\mathcal{G}_0 \mathcal{G}_j] = \frac{\hat{g}(\{j\})}{\sqrt{1 - \hat{g}(\emptyset)^2}}.$$

Our main result states that if $\Pr[f \circ g^n = g \circ f^m]$ exceeds a certain threshold, then f is correlated with a low-degree character. The result applies to any function other than XOR or NXOR; analogous results for these functions (in which the character need not be low-degree) follow from a generalization of the arguments in [3].

Definition 2.2. Fix a function $g: \{-1, 1\}^m \to \{-1, 1\}$. Let s_g be the infimum over all s for which the following holds.

For every $\varepsilon > 0$ there exist $\delta > 0$ and $L \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, if $f: \{-1, 1\}^n \to \{-1, 1\}$ satisfies

$$\Pr[f \circ g^m = g \circ f^m] \geq s + \varepsilon$$

then f has correlation at least δ with some character of degree at most L, that is, there exists $S \subseteq [n]$, of size at most L, such that

$$\left| \mathbb{E}\left[f(x) \prod_{i \in S} x_i \right] \right| \geq \delta.$$

Theorem 2.3. *Fix a function $g: \{-1, 1\}^m \to \{-1, 1\}$ which depends on all coordinates and is not $\pm \prod_{i=1}^m x_i$.*

If $\mathbb{E}[g] \neq 0$ then let s_g^U be the supremum of

$$\frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{x \sim \mathcal{N}(0,1)^n} \left[\left| \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g^n} [g(q_1(\mathcal{G}_1), \ldots, q_m(\mathcal{G}_m)) \mid \mathcal{G}_0 = x] \right| \right]$$

over all $n \in \mathbb{N}$ and all functions $q_1, \ldots, q_m: \mathbb{R}^n \to \{-1, 1\}$ satisfying $\mathbb{E}[q_1] = \cdots = \mathbb{E}[q_m] = 0$.

If $\mathbb{E}[g] = 0$, instead let s_g^U be the supremum of

$$\frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g^n} [q_0(\mathcal{G}_0) g(q_1(\mathcal{G}_1), \ldots, q_m(\mathcal{G}_m))]$$

over all $n \in \mathbb{N}$ and all functions $q_0, \ldots, q_m: \mathbb{R}^n \to \{-1, 1\}$ satisfying $\mathbb{E}[q_0] = \cdots = \mathbb{E}[q_m] = 0$.

Then $s_g \leq s_g^U$.

We can show that $s_g^U < 1$ for all functions g covered by the theorem.

Lemma 2.4. *If $g: \{-1, 1\}^m \to \{-1, 1\}$ depends on all coordinates and is not $\pm \prod_{i=1}^m x_i$ then $s_g^U < 1$.*

If we take the supremum in Theorem 2.3 with the additional constraint that the functions $q_1, \ldots, q_m$ coincide, then the resulting value is a lower bound on s_g.

Lemma 2.5. *Fix a function $g: \{-1, 1\}^m \to \{-1, 1\}$ which depends on all coordinates and is not $\pm \prod_{i=1}^m x_i$.*

If $\mathbb{E}[g] \neq 0$ then let s_g^L be the supremum of

$$\frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{x \sim \mathcal{N}(0,1)^n} \left[\left| \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g^n} [g(q(\mathcal{G}_1), \ldots, q(\mathcal{G}_m)) \mid \mathcal{G}_0 = x] \right| \right]$$

over all $n \in \mathbb{N}$ and all functions $q: \mathbb{R}^n \to [-1, 1]$ satisfying $\mathbb{E}[q] = 0$.

If $\mathbb{E}[g] = 0$, instead let s_g^L be the supremum of

$$\frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g^n} [q(\mathcal{G}_0) g(q(\mathcal{G}_1), \ldots, q(\mathcal{G}_m))]$$

over all $n \in \mathbb{N}$ and all functions $q: \mathbb{R}^n \to [-1, 1]$ satisfying $\mathbb{E}[q] = 0$.

There exists a sequence of functions $f_N: \{-1, 1\}^N \to \{-1, 1\}$, with $N \to \infty$, such that

$$\Pr[f_N \circ g^N = g \circ f_N^m] \longrightarrow s_g^L,$$

and for each $\delta > 0$ and $L \in \mathbb{N}$, for large enough N the functions f_N do not have correlation at least δ with any character of degree at most L.

Consequently, $s_g \geq s_g^L$.

We do not know whether $s_g^U > s_g^L$ holds for some g, that is, whether there is any advantage in allowing $q_1, \ldots, q_m$ to be different.

When $\mathbb{E}[g] \neq 0$, for any function q satisfying $\mathbb{E}[q] = 0$ we have

$$\mathop{\mathbb{E}}_{x \sim \mathcal{N}(0,1)^n} \left[\left| \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g^n} [g(q(\mathcal{G}_1), \ldots, q(\mathcal{G}_m)) \mid \mathcal{G}_0 = x] \right| \right] \geq$$

$$\left| \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g^n} [g(q(\mathcal{G}_1), \ldots, q(\mathcal{G}_m))] \right| = |\mathbb{E}[g]|,$$

and so

$$s_g^L \geq \frac{1}{2} + \frac{1}{2} |\mathbb{E}[g]|.$$

This corresponds to the trivial construction in which f is chosen randomly around the middle slice, and $\text{sign}(\mathbb{E}[g])$ elsewhere. The following result, proved by taking $n = 1$ and $q = \text{sign}$, shows that we can improve it if all Fourier coefficients of g on the first level are non-zero.

Lemma 2.6. *If $g: \{-1, 1\}^m \to \{-1, 1\}$ satisfies $\mathbb{E}[g] \neq 0$ and $\hat{g}(\{x_j\}) \neq 0$ for all $j \in [m]$ then $s_g^L > \frac{1}{2} + \frac{1}{2}|\mathbb{E}[g]|$.*

When g is an AND function, we can show that s_g^U is attained by $n = 1$ and $q_1(x) = \cdots = q_m(x) = \text{sign}(x)$. In view of Lemma 2.5, this gives an expression for s_g.

THEOREM 2.7. *Let $m \geqslant 2$, and let $g(x_1, \ldots, x_m) = \min(x_1, \ldots, x_m)$. Then*

$$s_g = \frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{x \sim \mathcal{N}(0,1)} \left[\left| \mathop{\mathbb{E}}_{\mathcal{G} \sim \mathcal{N}_g} [g(\text{sign}(\mathcal{G}_1), \ldots, \text{sign}(\mathcal{G}_m)) \mid \mathcal{G}_0 = x] \right| \right].$$

In particular, when $m = 2$, we obtain

$$s_\wedge \approx 0.814975356673002,$$

where $\wedge$ denotes the binary AND function $g(a, b) = a \wedge b = \min(a, b)$. Moreover, this is realized by the functions

$$f(x_1, \ldots, x_n) = \begin{cases} \text{sign}\left(\sum_i x_i\right) & \text{if } \sum_i x_i \geqslant -\frac{n}{4}, \\ \text{sign}\left(\sum_i x_i + \frac{n}{2} - \theta\sqrt{\frac{3}{4}n}\right) & \text{if } \sum_i x_i < -\frac{n}{4}, \end{cases}$$

where $\theta \approx 0.9084100298000161$.

Remark 2.8. If $g \colon \{-1, 1\}^m \to \{-1, 1\}$ is of the form $\pm \prod_{i=1}^m x_i$ for $m \geqslant 2$ and $\Pr[f \circ g^n = g \circ f^m] \geqslant \frac{1}{2} + \varepsilon$, then the classical analysis of linearity testing shows that f has correlation $\Omega(\varepsilon^{1/(m-1)})$ with *some* character. In contrast to Theorem 2.3, we cannot guarantee correlation with a low-degree character.

3 OPEN QUESTIONS

Our work suggests many open questions. Here are some of them.

OPEN QUESTION 1. *Can Theorem 1.1 be extended to polymorphisms of predicates? That is, given a function $g \colon \{0, 1\}^m \to \{0, 1\}$, what we can say about functions $f \colon \{0, 1\}^n \to \{0, 1\}$ satisfying*

$$\Pr[(g \circ f^m)(Z) = 1 \mid g(\text{row}_i(Z)) = 1 \text{ for all } i \in [n]] \geqslant 1 - \varepsilon?$$

As mentioned in the introduction, Kalai [11] proved a version of Theorem 1.1 for the predicate NAE_3, and Friedgut and Regev proved a version of Theorem 1.1 for the predicate NAND_2.

OPEN QUESTION 2. *What is the optimal dependence between ε and δ in Theorem 1.1? Does it depend on g?*

In our current proof, the dependence is not polynomial. In fact, due to the use of Jones' regularity lemma, the dependence is of tower type. This can be dramatically improved by using a different regularity lemma, which approximates the function by a decision tree rather than by a junta. The dependence now becomes only doubly exponential. We sketch this argument in the full version of the paper.

For many specific g we can prove a version of Theorem 1.1 in which δ is polynomial in ε. This is the case for linearity testing, and also for Maj_3, the majority function on three inputs, as we sketch in the full version of the paper.

OPEN QUESTION 3. *Can we extend Theorem 1.1 to larger alphabets, replacing $\{0, 1\}$ with an arbitrary finite set?*

One issue is that, to the best of our knowledge, a complete classification of multi-polymorphisms for larger alphabets is not currently known, though some preliminary results appear in [6, 19]. Moreover, while the complete classification of polymorphism of binary

predicates is known (it is given by Post's lattice), the situation for larger alphabets is known to be much wilder.

Nevertheless, it might be possible to show that every approximate polymorphism is close to a skew polymorphism, even without classifying the latter.

OPEN QUESTION 4. *Can we extend Theorem 1.1 to tensors? For example, what can we say about Boolean functions f, g, h satisfying $f \circ (g \circ h^m)^n = g \circ (h \circ f^p)^m$ with probability $1 - \delta$?*

Section 2 gives an upper bound s_g^U and a lower bound s_g^L on s_g which are similar but not identical.

OPEN QUESTION 5. *Is $s_g^U = s_g^L$? Is the optimum always achieved in one-dimensional Gaussian space?*

Another interesting question concerns an analog of "approximation resistance". When g is unbalanced, we trivially have $s_g \geqslant \max(\mathbb{E}[g], 1 - \mathbb{E}[g])$ by taking f to be random around the middle slice, and constant around the $\mathbb{E}[g]$-slice; and when g is balanced, we trivially have $s_g \geqslant 1/2$ by taking f to be a random function.

OPEN QUESTION 6. *For which functions g is $s_g > \max(\mathbb{E}[g], 1 - \mathbb{E}[g])$?*

Lemma 2.6 shows that the strict inequality holds for unbalanced g whenever all Fourier coefficients on the first level are non-zero. Conversely, when all Fourier coefficients on the first level vanish, Theorem 2.3 shows that equality holds.

Finally, it would be nice to extend the classification of exact solutions to the case in which we are allowed not only multiple f's, but also multiple g's.

OPEN QUESTION 7. *Classify all solutions $f_0, \ldots, f_m \colon \{0, 1\}^n \to \{0, 1\}$ and $g_0, g_1, \ldots, g_n \colon \{0, 1\}^m \to \{0, 1\}$ to the equation*

$$f_0 \circ (g_1, \ldots, g_n) = g_0 \circ (f_1, \ldots, f_m).$$

REFERENCES

[1] Kenneth J. Arrow. 1950. A Difficulty in the Concept of Social Welfare. *Journal of Political Economy* 58, 4 (1950), 328–346. https://doi.org/10.1086/256963 arXiv:https://doi.org/10.1086/256963
[2] Libor Barto, Andrei Krokhin, and Ross Willard. 2017. Polymorphisms, and how to use them. In *Dagstuhl Follow-Ups*, Vol. 7. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
[3] Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos Kiwi, and Madhu Sudan. 1996. Linearity testing in characteristic two. *IEEE Trans. Inform. Theory* 42, 6, part 1 (1996), 1781–1795. https://doi.org/10.1109/18.556674 Codes and complexity.
[4] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. 1990. Self-Testing/Correcting with Applications to Numerical Problems. In *STOC*. 73–83.
[5] Elad Dokow and Ron Holzman. 2009. Aggregation of binary evaluations for truth-functional agendas. *Soc. Choice Welf.* 32, 2 (2009), 221–241. https://doi.org/10.1007/s00355-008-0320-1

[6] Elad Dokow and Ron Holzman. 2010. Aggregation of non-binary evaluations. *Adv. in Appl. Math.* 45, 4 (2010), 487–504. https://doi.org/10.1016/j.aam.2010.02.005

[7] Yuval Filmus, Noam Lifshitz, Dor Minzer, and Elchanan Mossel. 2020. AND testing and robust judgement aggregation. In *52nd ACM Symposium on Theory of Computing (STOC'20)*.

[8] Ehud Friedgut and Oded Regev. 2018. Kneser graphs are like Swiss cheese. *Discrete Anal.* (2018), Paper No. 2, 18. https://doi.org/10.19086/da

[9] Johan Håstad. 2001. Some optimal inapproximability results. *J. ACM* 48, 4 (2001), 798–859. https://doi.org/10.1145/502090.502098

[10] Chris Jones. 2016. A Noisy-Influence Regularity Lemma for Boolean Functions. *CoRR* abs/1610.06950 (2016). arXiv:1610.06950 http://arxiv.org/abs/1610.06950

[11] Gil Kalai. 2002. A Fourier-theoretic perspective on the Condorcet paradox and Arrow's theorem. *Adv. in Appl. Math.* 29, 3 (2002), 412–426. https://doi.org/10.1016/S0196-8858(02)00023-4

[12] Nathan Keller. 2012. A tight quantitative version of Arrow's impossibility theorem. *J. Eur. Math. Soc. (JEMS)* 14, 5 (2012), 1331–1355. https://doi.org/10.4171/JEMS/334

[13] Elchanan Mossel. 2010. Gaussian bounds for noise correlation of functions. *Geom. Funct. Anal.* 19, 6 (2010), 1713–1756. https://doi.org/10.1007/s00039-010-0047-x

[14] Elchanan Mossel. 2012. A quantitative Arrow theorem. *Probab. Theory Related Fields* 154, 1-2 (2012), 49–88. https://doi.org/10.1007/s00440-011-0362-7

[15] Elchanan Mossel, Ryan O'Donnell, and Krzysztof Oleszkiewicz. 2010. Noise stability of functions with low influences: Invariance and optimality. *Annals of Mathematics* 171, 1 (2010), 295–341.

[16] Joe Neeman. 2014. A multidimensional version of noise stability. *Electron. Commun. Probab.* 19 (2014), no. 72, 10. https://doi.org/10.1214/ECP.v19-3005

[17] Ilan Nehama. 2013. Approximately classic judgement aggregation. *Ann. Math. Artif. Intell.* 68, 1-3 (2013), 91–134. https://doi.org/10.1007/s10472-013-9358-6

[18] Michal Parnas, Dana Ron, and Alex Samorodnitsky. 2002. Testing basic Boolean formulae. *SIAM J. Disc. Math.* 16, 1 (2002), 20–46.

[19] Mario Szegedy and Yixin Xu. 2015. Impossibility Theorems and the Universal Algebraic Toolkit. Unpublished note.

[20] Robert Wilson. 1972. Social choice theory without the Pareto principle. *J. Econom. Theory* 5, 3 (1972), 478–486. https://doi.org/10.1016/0022-0531(72)90051-8