# Expanders Meet Reed-Muller: Easy Instances of Noisy k-XOR

Jarosław Błasiok* Paul Lou† Alon Rosen‡ Madhu Sudan§

April 11, 2026

**Abstract**

In the noisy $k$-XOR problem, one is given $y \in \mathbb{F}_2^M$ and must distinguish between $y$ uniform and $y = Ax + e$, where $A$ is the adjacency matrix of a $k$-left-regular bipartite graph with $N$ variables and $M$ constraints, $x \in \mathbb{F}_2^N$ is random, and $e$ is noise with rate $\eta$. Lower bounds in restricted computational models such as Sum-of-Squares and low-degree polynomials are closely tied to the expansion of $A$, leading to conjectures that expansion implies hardness. We show that such conjectures are false by constructing an explicit family of graphs with near-optimal expansion for which noisy $k$-XOR is solvable in polynomial time.

Our construction combines two powerful directions of work in pseudorandomness and coding theory that have not been previously put together. Specifically, our graphs are based on the lossless expanders of Guruswami, Umans and Vadhan (JACM 2009). Our key insight is that by an appropriate interpretation of the vertices of their graphs, the noisy XOR problem turns into the problem of decoding Reed-Muller codes from random errors. Then we build on a powerful body of work from the 2010s correcting from large amounts of random errors. Putting these together yields our construction.

Concretely, we obtain explicit families for which noisy $k$-XOR is polynomial-time solvable at constant noise rate $\eta = 1/3$ for graphs with $M = 2^{O(\log^2 N)}$, $k = (\log N)^{O(1)}$, and $(N^{1-\alpha}, 1 - o(1))$-expansion. Under standard conjectures on Reed-Muller codes over the binary erasure channel, this extends to families with $M = N^{O(1)}$, $k = (\log N)^{O(1)}$, expansion $(N^{1-\alpha}, 1 - o(1))$ and polynomial-time algorithms at noise rate $\eta = N^{-c}$.

## 1 Introduction

Noisy $k$-XOR is a canonical hypothesis-testing problem for sparse random linear systems and a central example in the study of statistical-computational gaps. A widely held intuition attributes such gaps to expansion properties of an associated graph. We show that this intuition fails in general by providing an explicit counterexample.

This serves as a cautionary tale: near-optimal expansion does not, by itself, imply hardness for noisy $k$-XOR. While many prior works focus on the case of constant $k$, for example $k = 3$, our results apply when $k$ is polylogarithmic in the number of variables. We are not aware of any compelling reason to expect this regime to be algorithmically easier than the constant-$k$ setting.

*Bocconi University. jaroslaw.blasiok@unibocconi.it.
†Bocconi University, BIDSA. paul.lou@unibocconi.it.
‡Bocconi University, BIDSA. alon.rosen@unibocconi.it.
§Harvard University. madhu@cs.harvard.edu.

### 1.1 The Noisy $k$-XOR Problem

Given a vector $y \in \mathbb{F}_2^M$, one must distinguish between $y$ being sampled from the null distribution where $y$ is uniform random and the planted distribution where $y = A_H \cdot x + e$ that we now describe. In the planted distribution, we consider matrices $A_H \in \mathbb{F}_2^{M \times N}$ where every row is of Hamming weight $k$, a uniform random $x \in \mathbb{F}_2^N$, and a sparse noise vector $e \in \mathbb{F}_2^M$. Viewing $A_H$ as the adjacency matrix of a $k$-left regular bipartite graph $H$ where each of the $M$ rows corresponds to a constraint and each of the $N$ columns corresponds to a variable, we have the following definition.

**Definition 1** (Noisy k-XOR Distinguishing Problem)**.** *In the $\eta$-noisy XOR distinguishing problem associated with a constraint graph $H$, we are given a vector $y \in \mathbb{F}_2^M$, with a promise that either*

- *(Null case): $y \sim \mathrm{Unif}(\mathbb{F}_2^M)$,*
- *(Planted case): $y = A_H \cdot x + e$, where $x \in \mathbb{F}_2^N$ is a uniform random vector, and each element of the noise vector $e \in \mathbb{F}_2^M$ is independently 1 with probability $\eta$ (and 0 otherwise).*

*The goal of the algorithm is to distinguish between those two distributions. For example, an algorithm $\mathcal{A}$ is said to succeed in the distinguishing task, if*

$$\left| \Pr_{y \sim \mathrm{Unif}\mathbb{F}_2^M} [\mathcal{A}(y) = 1] - \Pr_{\substack{x \sim \mathbb{F}_2^N \\ e \sim \mathsf{Ber}(\eta)^M}} [\mathcal{A}(A_H \cdot x + e) = 1] \right| > 1/10.$$

When $M \leq N$, the planted and the null distributions are typically identical (as long as the adjacency matrix $A_H$ is of full rank), so the problem is not well-posed. We therefore only consider the setting where $M > N$. In this setting, the columns of the matrix $A_H$ span a linear code in $\mathbb{F}_2^M$, and the problem is essentially equivalent to deciding whether $y$ is a randomly corrupted codeword (through a binary symmetric channel with noise level $\eta$), or a random word from $\mathbb{F}_2^M$.

### 1.2 Statistical-Computational Gap and Expansion Properties

When $H$ is a random *dense* graph, or equivalently when $A_H$ is a random linear code, the problem is the classical Learning Parity with Noise (LPN) problem, which is conjectured to remain subexponentially hard even with subexponentially many samples [Blu+93; Ale03].

In the *sparse* regime, a large body of work has studied random $k$-left-regular constraint graphs $H$. This includes hardness and cryptographic formulations of sparse noisy parity/$k$-LIN/XOR-code problems [Ale03; BSV19; BRT25], as well as algorithmic work on planted and random CSPs [FPV15; Bas+25]. The sparse regime is believed to exhibit a statistical-computational gap: the problem becomes polynomial-time solvable beyond a known computational threshold, but is conjectured to remain hard below it. Some of this line of work was motivated by Feige's reduction from refuting random $k$-SAT to refuting random $k$-XOR [Fei02; FKO06].

Closely related, though somewhat orthogonal to the noisy $k$-XOR distinguishing problem itself, is a line of work on local pseudorandom generators, Goldreich-type functions, and algebraic attacks, often instantiated using sparse random or expanding graphs [MST06; BQ12; ABR16; AL18; App13].

Positive results in this setting provide a polynomial-time algorithm when $M \gtrsim N^{k/2}$. For these values of parameters, the polynomial-time distinguisher between planted and null distributions is trivial (the birthday paradox implies that with decent probability there are two equations on exactly the same set of variables, and one can just check if those two have the same value), and a non-trivial algorithm can either recover a planted solution, or refute a random instance [CGL07; BM16; AOW15; RRS17; GKM23].

Moreover, some evidence for computational hardness is provided by the means of lower bounds in the restricted models of computation (Sum-of-Squares, Statistical Queries, low degree polynomials) for both the distinguishing and refutation versions of the problem [Gri01; ABW10; FPV15; Kot+17; Bar+23; Gho+25].

The connection between graph expansion properties of the constraint graph $H$ and the conjectured hardness of noisy $k$-XOR associated with $H$ is most transparent in terms of low-weight linear dependencies in the matrix $A_H$, or equivalently small even covers. Graph expansion rules out the existence of small even covers, implying local pseudorandomness, lower bounds for low-degree distinguishers, and SoS lower bounds (see Section 2). These results, together with the lack of efficient algorithms for sparse instances, suggest the intuition that expansion may be the *only* structural source of hardness for noisy $k$-XOR. This intuition can be formalized into a mathematical conjecture in several ways, among which one of the strongest we provide below.

**Conjecture 2.** *There is a constant $\alpha \in (1/2, 1)$, such that for every $k$-left regular bipartite graph $H = ([M] \cup [N], E_H)$ that is $(T, \alpha)$-expanding, any circuit $C$ that succeeds in distinguishing the $\eta$-noisy $k$-XOR distinguishing problem with the constraint graph $H$, for $\eta \cdot T \gtrsim \log(M)$ has size at least $2^{\Omega(T)}$.*

**Remark 3.** *See Lemma 7 for more discussion on why condition $\eta \gtrsim \log(M)/T$ is needed for the conjectured hardness.*

The belief that the corresponding noisy version of the $k$-XOR distinguishing problem is hard for every sufficiently expanding graph $H$ seems to go back at least to the work of Alekhnovich [Ale03, Remark 1] who proposes two YES and NO distributions in the spirit of our YES and NO distribution and says (in our notation) that "We believe that (...), and if $H$ is an expander (which occurs with probability $1 - O(1/n)$) then the distributions of YES and NO are indistinguishable."[1]

The exact conjecture that the $k$-XOR distinguishing problem as in Definition 1 is hard for every expanding graph $H$ was reiterated by Barak in [Bar14, Page 39], although without specifying a concrete setting of parameters.

A version of this conjecture with a more concrete realization of the parameters was suggested in [Gho+25], albeit in the case of larger field $\mathbb{F}_p$ for $p = N^{\Omega(1)}$, instead of $\mathbb{F}_2$ as below (see Conjecture 4.3 therein). They used this conjecture, together with the planted-clique conjecture as a security basis for a Public-Key Encryption protocol. Their conjecture is the following.

**Conjecture 4.** *There is a constant $\alpha \in (1/2, 1)$, such that for every $k$-left regular bipartite graph $H = ([M] \cup [N], E_H)$ if it is $(T, \alpha)$-expanding, then every circuit that can solve the $\eta$-noisy $k$-XOR distinguishing problem must have size $M^{\omega(1)}$, where, with $n \coloneqq \log_2 N$,*

- *$k = \Omega(n)$,*
- *$T = \exp(n^\gamma)$ for some $\gamma \in (0, 1)$,*
- *$\eta = n^{-\zeta}$ for some constant $\zeta$.*

### 1.3 Our Results

In our work, we first refute Conjecture 2 by showing the following.

[1] See Remark 18 for a description of actual YES and NO instances suggested by Alekhnovich, and a sketch of how our approach can be used to distinguish them.

**Main Theorem 1** (See Theorem 37)**.** *For every constant $\alpha > 0$ there is an infinite family of $k$-left regular constraint graphs $G = ([M] \cup [N], E)$, where $M = 2^{\Theta(\log^2 N)}$, and $k = (\log N)^{\Theta(1/\alpha)}$, which is $(N^{1-\alpha}, 1 - o(1))$-expanding and there is an algorithm with running time* $\mathrm{poly}(M)$ *to solve the $\eta$-noisy $k$-XOR distinguishing problem for those graphs, with constant noise rate $\eta = 1/3$.*

Then, under a standard assumption that Reed-Muller codes efficiently achieve capacity for the binary erasure channel (BEC) (see Conjecture 14 and a short discussion thereafter), we provide a construction with polynomial number of constraints.

**Main Theorem 2** (Informal, see Theorem 38)**.** *Assume Reed-Muller codes efficiently achieve capacity for the BEC. Then, for every $\alpha, c > 0$ there is an infinite family of $k$-left-regular constraint graphs $H = ([M] \cup [N], E)$ such that*

$$M = N^{\Theta(1)}, \qquad k = (\log N)^{\Theta(1/\alpha)},$$

*the graph is $(N^{1-\alpha}, 1 - o(1))$-expanding, and there is an algorithm running in time* $\mathrm{poly}(M)$ *that solves the $\eta$-noisy $k$-XOR distinguishing problem on these graphs for $\eta = N^{-c}$.*

In fact, we prove the conclusion of Theorem 2 under a significantly weaker conjecture on Reed-Muller codes: for some constants $\gamma, C > 0$, Reed-Muller codes of blocklength $M$ and rate $1 - \varepsilon$ for $\varepsilon \gtrsim M^{-\gamma}$ can efficiently recover from $O(\varepsilon^C)$ random erasures (see Conjecture 16).

### 1.4 Our Techniques

Our counterexample to expansion-based hardness in the context of the noisy XOR problem combines two previously separate lines of work. Namely, we combine explicit lossless expander constructions from the pseudorandomness community with Reed-Muller decoding from random errors.

At a high level, the noisy XOR problem is naturally coding-theoretic, so using a decoding algorithm for a linear error-correcting code to disprove a conjecture about the hardness of recognizing a noisy XOR system is not surprising. In particular, error correcting codes have been used to (weakly) refute other conjectures in the statistical-computational gap setting, most notably the low-degree conjecture in [HW21; Buh+25]. Yet, despite this obvious connection, to the best of our knowledge such conjectures on expansion-based hardness for noisy XOR have not previously been refuted in any nontrivial parameter regime.

The first obstacle is that the encoding matrix of an error-correcting code is hard to realize as the adjacency matrix of a sparse constraint graph. Our transformation exploits some simple but specific properties of Reed-Muller codes to achieve this effect. Namely, we observe that Reed-Muller decoding applies whenever the constraint graph is a *coset graph*, that is, when it has additional algebraic structure such that every constraint defines an affine subspace (equivalently, a coset).

After establishing this connection, we draw on a powerful body of work from the 2010s showing that Reed-Muller codes can decode random errors far beyond their minimum distance [ASW14; SSV15; Kud+16]. However, even then it is *a priori* unclear how to ensure that the resulting graph is an expander. Indeed, we leave open the question of whether a random subspace construction of coset graphs is expanding.

To overcome the second obstacle, namely ensuring that the encoding matrix comes from an expander, we turn to the explicit constructions of Guruswami, Umans, and Vadhan, who built lossless expanders from Parvaresh-Vardy codes [PV05; GUV09]. We show that their lossless expanders can be interpreted as coset graphs, allowing us to obtain expansion while retaining the ability to apply Reed-Muller decoding from random errors.

### 1.5 Related Work on Hardness and Graph Expansion

Perhaps the earliest work in the deterministic[2] noise setting that explicitly connects computational hardness and graph expansion properties is Goldreich's proposal of a candidate one-way function (OWF) in which a local predicate is evaluated on an expanding constraint graph and whose hardness heuristically depends on graph expansion [Gol00; Gol11]. The same construction idea for longer output lengths immediately gives a candidate pseudorandom generator (PRG). Subsequently Oliveira, Santhanam, and Tell refuted this general conjecture by constructing a family of expander graphs such that instantiating Goldreich's PRG with this family is insecure even for reasonable predicate families [OST19]. In their work, they critically use the fact that the neighborhood function of the graph is of low complexity, e.g. affine or $\mathsf{AC}^0[\oplus]$. Our counterexample is incomparable with theirs for two reasons. First, their counterexamples concern the deterministic noise setting while ours concern the random noise setting. Secondly, while our construction also falls into a low-complexity regime because our neighbor function is affine, our algorithm for distinguishing noisy k-XOR proceeds through decoding from random erasures rather than complexity theoretic techniques.

A connection between graph expansion and hardness in the random noise setting was proposed in the work of Alekhnovich [Ale03]. Alekhnovich conjectured that the noisy 3-XOR with exact error weight $w$ is indistinguishable from noisy 3-XOR with exact error weight $w+1$ when the matrix $A$ is *any* expander. Our work morally refutes the conjecture (see Remark 18).

Applebaum, Barak, Wigderson construct public-key encryption (PKE) from various combinations of three combinatorial assumptions whose hardness is related to expansion properties [App13]. These constructions, however, use *random* graphs that are expanders with high probability. Similarly, a follow-up by Bogdanov, Kothari, Rosen combines ideas from the prior work to construct a PKE scheme whose security is based on Goldreich's PRG, thereby also using random graphs [BKR23]. Our counterexample has no immediate implications for either of these works.

More recently, the work of Ghosal, Hair, Jain, Sahai constructs PKE from the conjectured hardness of the planted clique problem and the noisy $k$-XOR over expander problem over large fields (see Conjecture 4) [Gho+25]. The reason they use such a strong conjecture is that their PKE scheme constructs a *structured* expander graph from a random $G(n, 1/2)$ graph. While our counterexample does not address the case of large fields nor their specific structured expander family, it is cautionary counter evidence to statements such as their second assumption.

### 1.6 Low degree method

The *low degree method* is a powerful heuristic that is gaining significant attention in the algorithmic learning community, widely employed to shed a light into computational complexity of concrete learning tasks. A raising number of non-trivial algorithms in computational statistics is either accompanied, or followed by a "matching" lower bound against low-degree polynomials or algorithms in the statistical query model; and a lack of such lower bound is often a motivation to look for more efficient algorithms.

While low-degree lower bounds themselves are often mathematically interesting, and provide deeper understanding of a structure of a problem at hand, the intuition that for "natural" and "noisy enough" problems the predictions provided by low-degree method should match the complexity of actual algorithms is sporadically challenged. One concrete example of this is the low-degree conjecture by Hopkins [Hop18], a formal mathematical statement attempting to capture the intuition that every "symmetric enough" and "noisy enough" distribution, which is hard to distinguish from

[2]The nonlinear predicate for locally computing output bits produces noise that is a deterministic function of the input. In the noisy $k$-XOR setting we add *random* Bernoulli error independently of the input.

uniform by low-degree polynomials should be also hard to distinguish by all efficient algorithms. This conjecture has recently been weakly refuted in [Buh+25].

Our construction does not satisfy the symmetry requirement of the low-degree conjecture, but it can be treated as providing a new example of a "noisy" problem for which low-degree predictions suggest exponential hardness, while a polynomial-time algorithm exists.

# 2 Technical Overview

We begin by reviewing how graph expansion implies lower bounds in several restricted computational models, e.g. SoS and low-degree polynomials. This motivates our community's current belief that an expanding constraint graph $H$ should imply the computational hardness of the associated noisy $k$-XOR problem. Then, we overview the construction of our counterexample, demonstrating that expansion cannot be the only explanation of hardness.

## 2.1 Expansion Implies Lower Bounds

We review explicitly the connection between graph expansion and known lower bounds. These relations establish why the community has believed that graph expansion alone implies hardness for the noisy $k$-XOR problem.

**Definition 5.** *In a bipartite graph $H = ([M] \cup [N], E_H)$, we say that a set of left-vertices $C \subset [M]$ is an even cover if every right vertex $x \in [N]$ has an even number of neighbors in $C$.*

This can be related to the standard notion of cycle in a graph $G$ in the following way. From a graph $G$ we build a 2-left regular bipartite graph $H = (E(G) \cup V(G), E_H)$ in which the left-vertices are the edges of $G$, and the right-vertices are the vertices of $G$ (in $H$ a left vertex $e$ is connected with a right vertex $v$ if $v$ lies on the edge $e$ in $G$). In this case, any minimal even cover of $H$ corresponds exactly to a collection of edges forming a simple cycle in $G$.

Note that equivalently, in terms of linear algebra, an even cover $C$ can be thought of as a subset of rows that add up to a zero vector, or $y \in \mathbb{F}_2^M$ such that $y^T A_H = 0$.

**Observation 6.** *If the constraint graph $H$ has an even cover $z \in \mathbb{F}_2^M$ of size $\mathrm{wt}(z) \ll 1/\eta$, then the planted and null distributions are easy to distinguish.*

*Proof.* Given vector $y$, consider $\langle z, y\rangle$. In the null distribution $\Pr[\langle z, y\rangle = 1] = \frac{1}{2}$, whereas in the planted distribution we have $\langle z, y\rangle = z^T(A_H x + e) = \langle z, e\rangle$. Now by union bound $\Pr[\langle z, e\rangle = 1] \leq \mathrm{wt}(z)\eta$. □

We can improve this bound by a logarithmic factor, if we have many disjoint even covers of small weight.

**Lemma 7.** *If we have $S$ disjoint even covers $z_1, \dots z_S$, each of weight at most $t$, we can distinguish planted from null distribution with noise level $\eta \lesssim \log(S)/t$.*

*Proof Sketch.* If $z$ is an even cover, then $z^T y = z^T e$ is a sum (over $\mathbb{F}_2$) of $t := \mathrm{wt}(z)$ independent random variables, each with $\mathrm{Bern}(\eta)$ distribution. We can interpret that $\mathrm{Bern}(\eta)$ random variable instead, as a variable that's 0 with probability $(1-2\eta)$, and uniformly random with probability $2\eta$.

The sum $\langle z, e\rangle$ is zero with probability $(1-2\eta)^t \approx \exp(-2\eta t)$, and uniformly random with the remaining probability. If we had $\exp(4\eta t)$ independent samples (i.e. corresponding to disjoint even covers ), we could distinguish the planted from the null distribution. □

Note that by simple linear algebra, every constraint graph $H = ([M] \cup [N], E_H)$ has $\Omega(M/N)$ pairwise disjoint even covers of length at most $N+1$. As such, the noise level $\eta \leq \frac{\log(M/N)}{N}$ can be considered trivial.

The size of minimum even cover is relevant, when attempting to use the so-called *low-degree heuristic* to understand the complexity of the noisy $k$-XOR problem: for any graph without small even cover the planted and null distributions are indistinguishable by low-degree polynomials. In particular, if the smallest cover is of size at least $T+1$, the planted distribution is $T$-wise independent and fools all degree $T$-polynomials over the reals.

Notably, a simple counting argument shows every sufficiently expanding constraint graph $H$ does not have small even covers.

**Definition 8.** *A set $S \subset [M]$ of left vertices in a $k$-left-regular graph $H = ([M] \cup [N], E_H)$ is said to be $\alpha$-expanding if*

$$|N(S)| \geq \alpha k |S|.$$

*A $k$-left-regular graph $H$ is an $(T, \alpha)$-expander if for every set $S \subset [M]$ of size at most $T$ is $\alpha$-expanding.*

**Lemma 9.** *If a graph $H$ is $(T, \alpha)$-expander for $\alpha > 1/2$, then every even cover in $H$ is larger than $T$.*

*Proof.* Consider any set $S$ of size $|S| \leq T$. Since $H$ is an expander, $N(S) > k|S|/2$.

Consider an induced subgraph on $S \cup N(S)$. Clearly, adding up the degrees of left vertices, the total number of edges in this subgraph is just $k|S|$.

If every vertex in $N(S)$ had at least two neighbors in $S$, we can count the total number of edges in this graph by adding up the right-degrees of vertices in $N(S)$. We would have $|E[S \cup N(S)]| \geq 2|N(S)| > 2k|S|/2 = k|S|$, a contradiction. □

The relevance of expansion is highlighted as a determining factor for a sum-of-squares lower bound for the noisy $k$-XOR problem. Concretely, Grigoriev showed that for a random $k$-regular constraint graph $H$, low-degree sum-of-squares cannot solve the $k$-XOR distinguishing problem [Gri01]. Later, Barak [Bar14, Lemma 3.4] observed that in the Grigoriev's lower-bound proof, the only relevant property of a random $k$-regular constraint graph, was its expansion (see also [BS16, Chapter 3.2]). That is, he showed the following.

**Theorem 10** ([Bar14])**.** *For every constraint graph $H$ which is $(T, \alpha)$-expander, with $\alpha > 1/2$, Sum-of-Squares of degree much smaller than $T/100$ cannot distinguish between $A_H \cdot x$ (i.e. planted distribution with noise level $\eta = 0$) and the null distribution* $\mathrm{Unif}(\mathbb{F}_2^M)$.

From this perspective, the Grigoriev's lower bound for a random $k$-XOR can be interpreted as a corollary of Theorem 10 together with a standard fact that a random $k$-regular graph is highly expanding with high probability.

This expansion can also be used to prove lower bounds in various other restricted models of computation.

**Definition 11** ($\delta$-biased)**.** *A distribution $D$ over $\{0,1\}^m$ is said to be $\delta$-biased if for every nonzero $a \in \mathbb{F}_2^m$,*

$$\left| \mathbb{E}_{y \sim D} \left[ (-1)^{\langle a, y \rangle} \right] \right| \leq \delta.$$

**Theorem 12** (Imported from [App13], see Theorem 9.1 therein)**.** *Let $A_H \in \mathbb{F}_2^{M\times N}$ be a $k$-sparse[3] matrix, and let $H = ([M] \cup [N], E)$ be its associated bipartite graph. Assume that $H$ is a $(T, 0.51)$-expander. Let $y = A_H \cdot x + e$, where $x$ is uniform in $\{0,1\}^N$ and $e \in \{0,1\}^M$ has independent $\mathsf{Ber}(\eta)$ coordinates. Then the distribution of $y$ satisfies:*

1. *it is $T$-wise independent;*
2. *it is $\delta$-biased, where $\delta = \frac{1}{2}(1-2\eta)^T$;*
3. *for every Boolean function $f : \{0,1\}^M \to \{0,1\}$ representable by a degree-$t$ polynomial over $\mathbb{F}_2$,*
$$|\Pr[f(y) = 1] - \Pr[f(u) = 1]| \leq 8 \cdot (1-2\eta)^{T/2^t - 1},$$
*where $u$ is uniform in $\{0,1\}^M$.*

Through a known result, this $T$-wise independence implies lower bounds against $\mathsf{AC}^0$ circuits [Bra08].

Finally, since random $k$-left regular graphs are optimally expanding with large probability, all the lower bounds above can be used to deduce similar hardness for a random noisy $k$-XOR.

**Lemma 13** ([GRS12, Theorem 11.2.3])**.** *There exists a universal constant $c$, such that the following holds. For every $M, N$, where $M \leq N^{ck}$, let us consider a random $k$-left regular graph with $M$ left vertices and $N$-right vertices. With probability $1 - o(1)$ this graph is a $(T, 3/4)$-expander, where $T \gtrsim \Omega(M/k)$.*

## 2.2 Our Results

First, combining our construction based on GUV expanders ([GUV09]) with the reduction from decoding RM-codes over Binary symmetric channel (BSC) to decoding a (higher degree) code over binary erasure channel (BEC) [SSV15] and the result that RM codes achieve capacity over BEC in the constant rate regime [Kud+16], we obtain the following theorem.

**Main Theorem 1** (See Theorem 37)**.** *For every constant $\alpha > 0$ there is an infinite family of $k$-left regular constraint graphs $G = ([M] \cup [N], E)$, where $M = 2^{\Theta(\log^2 N)}$, and $k = (\log N)^{\Theta(1/\alpha)}$, which is $(N^{1-\alpha}, 1 - o(1))$-expanding and there is an algorithm with running time $\mathrm{poly}(M)$ to solve the $\eta$-noisy $k$-XOR distinguishing problem for those graphs, with constant noise rate $\eta = 1/3$.*

This theorem statement refutes Conjecture 2. In the proof of this statement, we use a result of Kudekar, Kumar, Mondelli, Pfister, Şaşoğlu and Urbanke that RM codes achieve capacity over BEC, i.e. they recover from erasure rate $\varepsilon - o_M(1)$ where $\varepsilon \coloneqq 1 - \mathsf{Rate}$ [Kud+16] [4]. To get a result for a polynomial number of equations in the number of variables we need much faster rate of convergence to capacity than is currently known. We say that Reed-Muller codes efficiently achieve capacity for the binary erasure channel, if there is a constant $\gamma > 0$, such that any Reed-Muller codeword in $\mathrm{RM}(m, r)$ over $\mathbb{F}_2$ with rate $R = 1 - \varepsilon$ can be recovered with probability $1 - o(1)$ from independent random erasures with erasure rate $\varepsilon - O(1/M^\gamma)$. The constant $1/\gamma$ is known in the coding theory literature as a *scaling exponent*.

[3] That is, every row has weight $k$.

[4] Following closely the proof in [Kud+16], it is possible to extract an explicit upper bound on the *gap to capacity* $o_M(1)$: RM codes of rate $1 - \varepsilon$ can recover from $\varepsilon - O(1/\log\log M)$ fraction of random erasures; see [Rao21] for an expository YouTube talk proving this bound.

**Conjecture 14** (Reed-Muller Codes Efficiently Achieve Capacity for BEC)**.** *There exists a constant $\gamma$, such that for every $m, r \in \mathbb{N}$ such that $\mathrm{RM}(m,r)$ has rate at most $1-\epsilon$, a random erasure pattern sampled from $(\mathsf{Ber}(\eta))^{2^m}$ is recoverable with probability $1-o(1)$ provided that $\eta < \varepsilon - \frac{1}{M^\gamma}$, where $M = 2^m$ is the blocklength of the underlying code.*

The question of the gap-to-capacity results for RM codes for symmetric channels has been explicitly raised in [AY19, Section V], [Has+18; MHU14], and in [ASY21].

Note that this type of gap-to-capacity behavior is true and relatively simple to show for random codes, with a scaling exponent $1/\gamma = 2$, but it is much more challenging to prove for any explicit code with an efficient decoding algorithm. The breakthrough results [GX15; HAU14] showed that polar codes efficiently achieve capacity for binary symmetric channels (i.e. have finite scaling exponent), and variants of polar codes can achieve $1/\gamma \to 2$ [GRY22].

**Remark 15.** *Consider a linear space $\mathbb{F}_2[X]_{\le r}$ of low-degree polynomials with dimension $(1-\varepsilon)M$, and a random subset $S$ of $(1-\varepsilon)M + M^{1-\gamma}$ locations on the hypercube $\mathbb{F}_2^m$. Conjecture 14 is equivalent to a statement that with probability $1-o(1)$ there is no non-zero polynomial in $\mathbb{F}_2[X]_{\le r}$ that happens to vanish on all points of $S$.*

In fact, a plausibly simpler-to-prove conjecture suffices to derive a counterexample to the noisy-XOR distinguishing problem where the number of constraints $M$ is polynomial in the number of variables $N$.

**Conjecture 16** (Weak Random Erasure Recovery)**.** *There exist constants $\gamma > 0$ and $\zeta \ge 1$, such that for every $m, r \in \mathbb{N}$ if $\mathrm{RM}(m,r)$ has rate at most $1-\epsilon$ for $M^{-\gamma} < \varepsilon < 1/2$, a random erasure pattern sampled from $(\mathsf{Ber}(\eta))^{2^m}$ is recoverable with probability $1-o(1)$ provided that $\eta < \varepsilon^\zeta$, where $M = 2^m$ is the blocklength of the underlying code.*

**Remark 17.** *Conjecture 16 is implied by Conjecture 14. Therefore, we state the following theorem only assuming Conjecture 16.*

Either of these conjectures holding would imply the following counterexample, in which the number of constraints $M$ is polynomially related to the number of variables $N$, but the noise-rate is inverse polynomial.

**Main Theorem 2** (Informal, see Theorem 38)**.** *Assume Reed-Muller codes efficiently achieve capacity for the BEC. Then, for every $\alpha, c > 0$ there is an infinite family of $k$-left-regular constraint graphs $H = ([M] \cup [N], E)$ such that*

$$M = N^{\Theta(1)}, \qquad k = (\log N)^{\Theta(1/\alpha)},$$

*the graph is $(N^{1-\alpha}, 1-o(1))$-expanding, and there is an algorithm running in time $\mathrm{poly}(M)$ that solves the $\eta$-noisy $k$-XOR distinguishing problem on these graphs for $\eta = N^{-c}$.*

Therefore, under Conjecture 14 or Conjecture 16, we obtain an even stronger refutation of Conjecture 2, in which we refute the setting where the number of constraints and variables are polynomially related, as opposed to quasi-polynomially related.

**Remark 18.** *The inverse-polynomial noise rate $\eta = N^{-c}$ was already suggested as a regime potentially hard for every expander $H$ in [Ale03]. The YES and NO distributions suggested there are slightly different: YES instances consist of vectors $A_H x + e$ where $e$ is a random vector with sparsity exactly $t := \lfloor \eta M \rfloor$, where NO distributions are given by vectors $A_H x + e$ where $e$ is a random $t+1$-sparse vector.*

*Since the algorithm we propose for planted instances $y = A_H x + e$ actually recovers the solution $x$, our approach can be used to distinguish Alekhnovich's distributions as well. Specifically, upon receiving a vector $y$, we can independently flip each coordinate with probability somewhat larger than $\eta$, to obtain a vector $y' = A_H x + e + e'$. Now $e + e'$ is statistically close to a random vector with i.i.d. entries, hence with high probability we can correctly recover $A_H x$ from $y'$, and check if the Hamming distance between $A_H x$ and $y$ is $t$ or $t + 1$.*

# 3 Preliminaries

We begin by recalling facts that relate the Hamming ball volume to the binary entropy function. These facts will be used to prove correctness of our distinguisher.

**Fact 19.** *Let*

$$\binom{n}{\leq d} := \sum_{k \leq d} \binom{n}{k}.$$

*Then for $d \leq n/2$, we have*

$$nH_2(d/n) - o(n) \leq \log_2 \binom{n}{\leq d} \leq nH_2(d/n),$$

*where*

$$H_2(p) := p \log(1/p) + (1-p) \log(1/(1-p))$$

*is the binary entropy function.*

Now we recall standard asymptotic bounds on the binary entropy function.

**Fact 20** (Standard Entropy Bounds)**.** *Let $H_2$ be the binary entropy function. Then*

1. *For $\varepsilon \to 0$,*
$$H_2(\varepsilon) = O(\varepsilon \log(1/\varepsilon)).$$
2. *For $\varepsilon \to 0$,*
$$H_2\left(\frac{1}{2} - \varepsilon\right) = 1 - \Theta(\varepsilon^2).$$

Finally, we recall the Berry-Esséen Theorem. It allows us to obtain more precise lower bounds on $1 - R$ for the rate $R$ of a $(m, r)$ Reed-Muller code where $r > m/2$.

**Theorem 21** (Berry-Esséen Theorem [Tao23])**.** *Let $X$ have mean zero, variance one and finite third moment. Let $X_1, \ldots, X_n$ be i.i.d. copies of $X$, and let $S_n := (X_1 + \cdots + X_n)/\sqrt{n}$. Then,*

$$\Pr[S_n < a] \leq \Pr[Z < a] + \frac{K \cdot \mathbb{E}\left[|X|^3\right]}{\sqrt{n}}$$

*uniformly for all $a \in \mathbb{R}$ where $Z \sim N(0,1)$ and $K$ is some absolute constant.*

# 4 Our Counterexample

We will discuss a generic construction of a family of graphs for which $A_H \cdot x$ is a Reed-Muller codeword; as such, in some noise range the distinguishing problem can be solved in polynomial time by the known results for decoding Reed-Muller codewords from random errors.

What remains to be shown is that there is a graph in this class which is a $(T, 3/4)$-expander for some decent value of $T$.

### 4.1 Graphs with Reed-Muller decoding

In order to use the theory of Reed-Muller codes for the distinguishing problem, we will use an additional structure of a constraint graph.

**Definition 22** (Coset graph)**.** *Given $k$ matrices $A_1, \dots A_k \in \mathbb{F}_2^{d \times m}$ (where $d < m$), the $(m, k, d)$-coset graph associated with $(A_1, \dots A_k)$ is the following:*

- *The set of left vertices $[M]$ is identified with points on a hypercube $\mathbb{F}_2^m$.*
- *The set of right vertices $[N]$ is identified with $[k] \times \mathbb{F}_2^d$*
- *Left vertex $v \in \mathbb{F}_2^m$ is connected with the right vertex $(i, u) \in [k] \times \mathbb{F}_2^d$ if $A_i \cdot v = u$.*

*Alternatively, for a collection $(V_1, \dots V_k)$ of subspaces of dimension at least $m-d$ in $\mathbb{F}_2^m$, the $(m, k, d)$ coset graph associated with $(V_1, \dots V_k)$ is the $(m, k, d)$-coset graph associated with $(A_1, \dots A_k)$ where matrices $A_i$ are such that $\ker A_i = V_i$ (the coset graph does not depend on the choice of matrices $A_i$, only on the subspaces $V_i$).*

We now observe that the code generated by the columns of the matrix $A_H$ forms a subcode of the Reed-Muller code $\mathrm{RM}(m, d)$.

**Lemma 23** (Coset Graphs give RM Subcodes)**.** *Let $H$ be an $(m, k, d)$-coset graph and let $A_H \in \mathbb{F}_2^{2^m \times k \cdot 2^d}$ be the adjacency matrix. Then the column space $\mathsf{Im}(A_H) \subseteq \mathbb{F}_2^{2^m}$ is a subcode of $\mathrm{RM}(m, d)$.*

*Proof.* We will show that every column of $A_H$ is a $\mathrm{RM}(m, d)$ codeword, i.e. an evaluation vector of a multilinear polynomial of degree at most $d$ on all of $\mathbb{F}_2^m$. Every column of $A_H$ corresponds to a right vertex of $H$ given by a pair $(i, u)$ with $i \in [k]$ and $u \in \mathbb{F}_2^d$. Its neighborhood of left vertices is given by the affine subspace

$$W_{i,u} \coloneqq \{v \in \mathbb{F}_2^m : A_i \cdot v = u\}.$$

where by the definition of the $(m, k, d)$-coset graph, we have $\mathsf{rank}(A_i) \leq d$. In the adjacency matrix $A_H$, for every $v \in \mathbb{F}_2^m$, the $v$-th entry of the $(i, u)$-column of $A_H$ is 1 if and only if $A_i \cdot v = u$. Observe that this subspace can be characterized by at most $d$ many affine constraints of the following form for linear functions $\ell_j : \mathbb{F}_2^M \to \mathbb{F}_2$, given by the $j$-th row of $A_i$, and scalar values $u_j$ over $\mathbb{F}_2$:

$$\{\ell_j(X) + u_j = 0\}_{j \in [\mathsf{rank}(A_i)]}.$$

Therefore, the evaluation vector is exactly that of a degree $\mathsf{rank}(A_i) \leq d$ indicator polynomial for the subspace $W_{i,u}$:

$$\mathbf{1}_{i,u}(X) = \prod_{j \in [\mathsf{rank}(A_i)]} (\ell_j(X) + u_j + 1).$$

Since every column of $A_H$ is a codeword of $\mathrm{RM}(m, d)$, the column span $\mathsf{Im}(A_H)$ is contained in $\mathrm{RM}(m, d)$. □

Therefore, if we can decode the Reed-Muller code up to the $\eta$ fraction of random errors, we can distinguish the $A_H \cdot x + e$ vector from a random one for any coset graph $H$.

Let us first see what we can obtain using the unique decoding of the RM codes.

**Fact 24.** *The distance of the Reed-Muller code $\mathrm{RM}(m, r)$ is $\Delta = 2^{m-r}$. Relative distance is $\delta = 2^{-r}$.*

Since we can uniquely decode RM codes up to an error rate $\delta/2$, we have the following.

**Corollary 25.** *For every $(m, k, d)$-coset graph, the associated XOR-distinguishing problem can be solved in polynomial time when $\eta < \delta/2 \approx \frac{k}{N}$.*

Note that the largest $\alpha$-expanding set is in a $k$-left regular bipartite graph on $[M] \cup [N]$ is of size proportional to $N/k$. Even in the most optimistic scenario with respect to the expansion of random $(m, k, d)$-coset graphs, this falls (barely) short of disproving the Conjecture 2, as we would prefer the noise rate to be at least larger by a $\log(N)$ factor. This is not particularly helpful; we can try to improve on that in the following way.

### 4.2 Known Results in RM Decoding from Random Erasures

The approach for distinguishing a randomly corrupted codeword from a uniformly random string will leverage the fact that corruptions are introduced at random. Several prior works [ASW14; SSV15; SS18] have studied decoding Reed-Muller codes with random errors (see also [ASY21] for an exposition of recent results on Reed-Muller codes). Concretely, [SSV15] provides an algorithmic result for decoding Reed-Muller codes from random errors of a rate vastly exceeding the distance of the code. Specifically, they show the following.

**Theorem 26** ([SSV15])**.** *There is an efficient*[5] *algorithm that corrects a pattern $P \subset [M]$ of corruptions in* $\mathrm{RM}(m, r)$ *codeword, if the corresponding codeword can be recovered from the same pattern of* erasures *$P$ in a Reed-Muller code of higher degree* $\mathrm{RM}(m, \frac{m+r}{2})$.

This reduces the question of efficient correction of random corruptions, to a purely analytical question of understanding what fraction of erasures the Reed-Muller code can reconstruct under the binary erasure channel. To this end, the work of Kudekar et al. implies the following theorem statement.

**Theorem 27** (Random Erasure Recovery [Kud+17])**.** *For every $m, r \in \mathbb{N}$ such that* $\mathrm{RM}(m, r)$ *has rate at most $1-\epsilon$, a random erasure pattern sampled from $(\mathsf{Ber}(\eta))^{2^m}$ is recoverable*[6] *with probability $1 - o(1)$ provided that $\eta < \varepsilon - o(1)$.*

Armed with these two theorems, we are ready to prove that this decoder leads to a distinguisher. Before doing so in Section 5, we first identify an exact expanding family of coset graphs.

### 4.3 GUV Expander from PV Codes

We will use a brilliant construction of [GUV09] of an unbalanced expander graph from Parvaresh-Vardy codes. First, we will show that this expander graph family is a $(m, k, d)$ coset graph, giving a Reed-Muller subcode. Then, we will give two parameter regimes of interest—the first case being when $d = O(\sqrt{m})$ and the second being when $d = O(m)$. These two settings correspond respectively to the settings of a quasi-polynomial number of constraints and polynomial number of constraints.

For fixed $E \in \mathbb{F}_Q[X]_{=r+1}$ an irreducible polynomial of degree $r + 1$, and a prime power $Q$, we define a $(E, Q, r, s, h)$-GUV graph as follows:

- The set of left vertices is identified with the set of all polynomials over $\mathbb{F}_Q$ of degree at most $r$: $\mathbb{F}_Q[X]_{\leq r} \approx \mathbb{F}_Q^{(r+1)}$.

[5] By efficient, we mean polynomial time in the block length $2^m$.

[6] By recoverable we mean that the codeword is information-theoretically determined. For any linear code this also implies that it can be efficiently recovered by solving a linear system.

- The set of right vertices is identified with $\mathbb{F}_Q \times \mathbb{F}_Q^s$.
- Each left-vertex has exactly $Q$ neighbors: one in each $\{y\} \times \mathbb{F}_Q^s$ for every $y \in \mathbb{F}_Q$.
- Specifically, for a polynomial $f$, and $y \in \mathbb{F}_Q$, the $y$ neighbor of $f$ is $(y, f_0(y), \dots f_{s-1}(y))$ where $f_i := f^{h^i} \bmod E$.

Note that when $h$ and $Q = 2^q$ are powers of two, we can identify $\mathbb{F}_Q^{(r+1)}$ with $\mathbb{F}_2^{q(r+1)}$ while preserving the additive structure. In this sense $f \mapsto f^{2^i}$ is $\mathbb{F}_2$ linear and $f \mapsto f \pmod E$ is $\mathbb{F}_Q$ linear (hence, also $\mathbb{F}_2$ linear), as is the evaluation map $f \mapsto f(y)$, so the composition from $\mathbb{F}_2^{q(r+1)} \to \mathbb{F}_2^{(s+1)q}$ sending $f$ to $(y, f_0(y), \dots f_{s-1}(y))$ is $\mathbb{F}_2$ linear: a preimage of a point is an affine subspace of codimension at most $(s+1)q$.

**Fact 28.** *Let $Q = 2^q$ and $h = 2^t$ be powers of two for $q, t \geq 1$. Then every $(E, Q, r, s, h)$-GUV graph is an $(m, k, d)$-coset graph with $m = (r+1)q$, $k = Q$ and $d = s \cdot q$.*

*Proof.* Fix an $\mathbb{F}_2$-basis of $\mathbb{F}_Q$ where we view $\mathbb{F}_Q \cong \mathbb{F}_2^q$ as a $\mathbb{F}_2$-vectorspace. Then the set $\mathbb{F}_Q[X]_{\leq r}$ is a $\mathbb{F}_2$-vectorspace of dimension $m := (r+1)q$. Consider the map

$$L_y : \mathbb{F}_Q[X]_{\leq r} \to \mathbb{F}_Q^s, \qquad f \mapsto (f_0(y), \dots, f_{s-1}(y))$$

where $f_i := f^{h^i} \bmod E$. Then the GUV graph has edges between left vertex $f \in \mathbb{F}_Q[X]_{\leq r}$ and right vertex $(y \in \mathbb{F}_Q, z \in \mathbb{F}_Q^s)$ if and only if $L_y(f) = z$.

Observe that $f \mapsto f^{h^i}$ is $\mathbb{F}_2$-linear because for any integer $\ell \geq 0$ the following holds in characteristic two field arithmetic:

$$\begin{aligned}(f+g)^{2^\ell} &= f^{2^\ell} + \left(\sum_{i=1}^{2^\ell - 1} \binom{2^\ell}{i} f^{2^\ell - i} g^i\right) + g^{2^\ell} \\ &= f^{2^\ell} + g^{2^\ell}.\end{aligned}$$

Then recall that modular reduction by irreducible $E$ and evaluation at a fixed point $y$ are both $\mathbb{F}_Q$-linear, therefore $\mathbb{F}_2$-linear. Therefore, we can represent $L_y$ by a binary matrix $A_y \in \mathbb{F}_2^{s \cdot q \times m}$. Then, for any left vertex $f$ written in $\mathbb{F}_2^{(r+1)q}$ representation and right vertex $z$ written in $\mathbb{F}_2^{s \cdot q}$ representation, we have the edge condition above given exactly by the condition $A_y \cdot f = z$. These matrices $\{A_y\}_{y \in \mathbb{F}_2^q}$ define a coset graph with $m = (r+1)q, k = Q$, $d = s \cdot q$. □

The expansion of GUV graphs has been famously analyzed by [GUV09] (see also [Vad12, Theorem 5.35]).

**Theorem 29** ([GUV09])**.** *Every $(E, Q, r, s, h)$-GUV graph is an $(T, \alpha)$-expander for $T = h^s$ and $\alpha = 1 - \frac{r \cdot s \cdot h}{Q}$.*

**Corollary 30.** *For every $\alpha \in (0,1)$ and $\gamma \in (0,1)$, there is an infinite family of explicit $(m, k, d)$-coset graphs, with $d = \gamma m + \Theta(\log m)$ and $k = (m / \lg m)^{\Theta(1/\alpha)}$, each of which is $(T, 1 - o(1))$-expanding with $T = 2^{(1-\alpha)d}$.*

*Proof.* Fix constants $\alpha, \gamma \in (0,1)$. Define parameter $D \in \mathbb{N}$ that serves as an index for the infinite family of coset graphs. Let $C > 2$ be a constant and define the following parameters:

$$\begin{aligned} q &\coloneqq \left\lceil \frac{C}{\alpha} \lg D \right\rceil, & Q &\coloneqq 2^q, \\ m &\coloneqq qD, & M &\coloneqq 2^m, \\ n &\coloneqq \lfloor \gamma D \rfloor, & N &\coloneqq 2^{(n+1)q}, \\ t &\coloneqq \left\lceil \frac{(n+1)(1-\alpha)}{n} \cdot q \right\rceil, & h &\coloneqq 2^t. \end{aligned}$$

For field size $Q$ and for any degree $D$ irreducible polynomial $E(X) \in \mathbb{F}_Q[X]$, we have a $(E, Q, D-1, n+1, h)$-GUV graph with $M$ left nodes and $N$ right nodes with $Q$ left regular degree. By Fact 28, this GUV graph is a $(m, Q, \log N)$-coset graph where

$$\log N = (n+1) \cdot q = \gamma \cdot \log M + \Theta(\log \log M).$$

Moreover, we have $m = \Theta\left(\frac{D \lg D}{\alpha}\right)$, implying that $D = \Theta(\alpha m / \lg m)$. Therefore,

$$Q = D^{\Theta(1/\alpha)} = (m/\lg m)^{\Theta(1/\alpha)}.$$

Now consider the expansion factor. First observe that our choice of $q$ directly implies that $Q^\alpha \geq D^C$ for $C > 2$. Then, observe $h = Q^{1-\alpha+o(1)}$ which together with the above implies that

$$\frac{(D-1) \cdot (n+1) \cdot h}{Q} = O(D^2 \cdot Q^{-\alpha+o(1)}) = o(1).$$

Finally, observe that our choice of $t$ gives $h^n \geq N^{1-\alpha}$. By Theorem 29, this coset graph is $(N^{1-\alpha}, 1 - o(1))$ expanding. □

**Remark 31.** *For rational $\gamma$ and appropriate choices of $D$ such that $D\gamma$ is integral, we can sharpen the theorem statement to $d = \gamma m$, removing the additive $\Theta(\log m)$ term.*

**Remark 32.** *The same theorem statement holds for an infinite family of explicit $(m, k, d)$-coset graphs with $d = c_\beta \cdot \sqrt{m}$ and $k = (m/\lg m)^{\Theta(1/\alpha)}$ where $c_\beta$ can be an arbitrarily small constant that depends on a constant parameter $\beta$. To see this, observe that the proof above holds when the parameter $n = \left\lfloor \beta \cdot \sqrt{D/\log D} \right\rfloor$ where $D$ was the index for the infinite family and $\beta$ is any constant of our choice.*

## 5 Distinguisher for the Noisy $k$-XOR Problem on Coset Graphs

We directly combine the two known theorems, Theorem 26 and Theorem 27, to construct a distinguisher running in polynomial time in the blocklength $M = 2^m$ for the setting in which the error rate $\eta$ has a $o(1)$ gap to the capacity. The distinguisher proceeds in two steps. First, it uses Reed-Muller decoding to recover a candidate codeword. Then, it checks if the corresponding error is of the expected weight. The following result is unconditional.

**Theorem 33.** *For any constant $c \in (0,1)$, for any $d = d(m) < m$ such that $m + d$ is an even integer and such that $p = d/m < c$ for all sufficiently large $m$, let $\varepsilon_{m,d} \coloneqq 1 - \mathsf{Rate}\left(\mathrm{RM}\left(m, \frac{m+d}{2}\right)\right)$. For any $\eta = \eta(m)$ satisfying $\eta < \varepsilon_{m,d} - o(1)$ and*

$$\eta \cdot 2^m \lesssim 2^{m \cdot H_2((1-p)/2)},$$

*for every $k = (\log N)^{O(1)}$, for any $(m, k, d)$-coset graph $H$, there exists an algorithm running in time polynomial in the blocklength $M = 2^m$, that solves the $\eta$-noisy XOR distinguishing problem for $H$ with distinguishing advantage $1 - o(1)$.*

*Proof.* For convenience, let $M \coloneqq 2^m$. By Theorem 26, any error pattern that is recoverable from erasures in $\mathrm{RM}\left(m, \frac{m+d}{2}\right)$ is also decodable from errors in $\mathrm{RM}(m, d)$. By Theorem 27, if

$$\eta < \varepsilon_{m,d} - o(1)$$

then a random erasure pattern sampled from $(\mathsf{Ber}(\eta))^M$ is (possibly inefficiently) decodable in $\mathrm{RM}\left(m, \frac{m+d}{2}\right)$ with probability $1 - o(1)$. Therefore by Theorem 26, there is an algorithm $\mathcal{A}_{\mathrm{RM}}$ that runs in time polynomial in the block length $2^m$ such that for every $c \in \mathrm{RM}(m, d)$,

$$\Pr_{e \sim (\mathsf{Ber}(\eta))^M} [\mathcal{A}_{\mathrm{RM}}(c + e) = c] = 1 - o(1)$$

Let $H$ be an $(m, k, d)$-coset graph, and define the subspace

$$C_H \coloneqq \mathsf{Im}(A_H) \subseteq \mathbb{F}_2^M.$$

By Lemma 23, we have $C_H \subseteq \mathrm{RM}(m, d)$ is a subcode. Therefore, for every $c \in C_H$,

$$\Pr_{e \sim (\mathsf{Ber}(\eta))^M} [\mathcal{A}_{\mathrm{RM}}(c + e) = c] = 1 - o(1).$$

Define the distinguisher $\mathsf{Dist}$ as follows. On input $y \in \mathbb{F}_2^M$:

1. Compute $\hat{c} \leftarrow \mathcal{A}_{\mathrm{RM}}(y)$.
2. Output 1 if and only if $\mathrm{wt}(y - \hat{c}) \le t$ and $\hat{c} \in C_H$.

where $t = (1 + \delta)\eta M$ for a small constant $\delta > 0$ is such that standard tail bounds imply that

$$\Pr_{e \sim (\mathsf{Ber}(\eta))^M} [\mathrm{wt}(e) \le t] = 1 - o(1).$$

This distinguisher is polynomial-time because $A_{\mathrm{RM}}$ is a polynomial-time algorithm and the codeword check can be done via linear algebra.

In the planted case, $y = c + e$ for a uniformly random $c \in C_H$ and $e \sim (\mathsf{Ber}(\eta))^M$. With probability $1 - o(1)$ over the choice of $e$, the decoder returns $\hat{c} = c$ and $\mathrm{wt}(e) \le t$. Hence

$$\Pr[\mathsf{Dist}(y) = 1] = 1 - o(1).$$

Now consider the null case where the input is $y \sim \mathrm{Unif}(\mathbb{F}_2^M)$. We'll show the probability that $\mathsf{Dist}$ accepts such an input is $o(1)$. If $\mathsf{Dist}(y) = 1$, then by definition of $\mathsf{Dist}$, there exists some codeword $\hat{c} \in \mathrm{RM}(m, d)$ with $\mathrm{wt}(y - \hat{c}) \le t$ such that $\hat{c} \in C_H$. Let $\mathsf{Vol}(M, t) \coloneqq \binom{M}{\le t}$ denote the Hamming ball of radius $t$ in dimension $M$. By a union bound over all codewords of $C_H$, the probability that $y$ is within $t$ Hamming weight of any codeword in $C_H$ is

$$\Pr\left[d(y, C_H) \le t\right] \le \frac{|C_H| \cdot \mathsf{Vol}(M, t)}{2^M}.$$

First observe that since $k = (\log N)^{O(1)}$,

$$\lg(|C_H|) = \mathsf{rank}(A_H) \le k2^d = M^{p + o(1)} \le M^c = o(M).$$

Then recall that $t$ can be taken to be $(1+\delta)\cdot\eta\cdot M$ for any arbitrarily small constant $\delta$. Since $p \in (0,c)$ for $c<1$ and $\eta\cdot M \lesssim 2^{m\cdot H_2((1-p)/2)}$, we have that $t = o(M)$. Then, $H_2(t/M) = o(1)$ and Fact 19 implies

$$\lg(\mathsf{Vol}(M,t)) \le M\cdot H_2(t/M) = o(M).$$

Therefore,

$$\Pr\left[d(y,C_H)\le t\right] = 2^{-M+o(M)} = o(1).$$

Thus, we conclude that

$$\Pr_{y\sim\mathrm{Unif}(\mathbb{F}_2^M)}[\mathsf{Dist}(y)=1] = o(1),$$

so $\Pr[\mathsf{Dist}(y)=0] = 1-o(1)$ in the null case. □

As previously, we can inspect the consequences of this in range $d=\gamma m$ and $d=(1-\gamma)m$ for small constant $\gamma$ —this theorem leads to the same range of parameters as the distinguishing one discussed in the previous section, but with a dual guarantee.

**Corollary 34.** *When $d=(1-\gamma)m$, the bound in Theorem 33 simplifies to*

$$2^m\eta \lesssim 2^{mH_2(\gamma/2)} = (2^{m-d})^{\Omega(\log 1/\gamma)} = \Delta^{\Omega(\log 1/\gamma)}$$

*for $\gamma\to 0$ and where $\Delta = 2^{m-d}$ is the distance of the underlying code.*

*Proof.* Recall the fact that for $\gamma\to 0$,

$$H_2(\gamma) = \gamma\log(1/\gamma) + (1-\gamma)\log(1/(1-\gamma)) = \Theta(\gamma\log(1/\gamma)).$$

Then observe that $\Delta = 2^{\gamma\cdot m}$ and the rest follows directly by substitution. □

**Corollary 35.** *When $d=\gamma m$, the bound in Theorem 33 simplifies to*

$$\eta \lesssim 2^{-\Omega(\gamma^2 m)} = \delta^{\Omega(\gamma)}$$

*for $\gamma\to 0$, where $\delta = 2^{-\gamma m}$ is the relative distance of the underlying code.*

*Proof.* Observe that $(1-p)/2 = (1-(d/m))/2 = (1/2)-(\gamma/2)$. Taking the Taylor expansion of the binary entropy function around $1/2$ gives $H_2((1/2)-(\gamma/2)) = 1-\Theta(\gamma^2)$. Substitution then gives the desired result. □

The best possible expanding set is of size $N/k = 1/\delta$. If we had $(T,3/4)$-expanding coset graph with $T=(N/k)^{1-\alpha}$ (as we could hope from the PV codes), this leads to $T\eta \approx \delta^{-1+\alpha+\Omega(\gamma)}$. As long as $\alpha + C\gamma \le 1/2$, this noise rate is enough to solve the conjectured one.

**Theorem 36.** *Assume Conjecture 16. Let $\xi>0$ and $\zeta\ge 1$ be the constants from that conjecture. For any constant $c\in(0,1)$, for any $d=d(m)<m$ such that $m+d$ is an even integer and such that $p \coloneqq d/m < c$ for all sufficiently large $m$, let*

$$\varepsilon_{m,d} \coloneqq 1-\mathsf{Rate}\left(\mathrm{RM}\left(m,\frac{m+d}{2}\right)\right), \qquad M\coloneqq 2^m.$$

*If $M^{-\xi} < \varepsilon_{m,d} < \frac{1}{2}$, then, for any $\eta=\eta(m)$ satisfying*

$$\eta < \varepsilon_{m,d}^{\zeta} \qquad \text{and} \qquad \eta M \lesssim M^{H_2((1-p)/2)},$$

*for every $k=(\log N)^{O(1)}$, for any $(m,k,d)$-coset graph $G$, there exists a $\mathrm{poly}(M)$ time algorithm that solves the $\eta$-noisy XOR distinguishing problem for $G$ with distinguishing advantage $1-o(1)$.*

*Proof.* The proof is identical to that of Theorem 33, with Conjecture 16 replacing Theorem 27 in the proof of Theorem 33. □

# 6 Putting Decoding and Expansion Together

We now restate and prove our main theorems. Our first main theorem is for the case where the number of constraints is quasi-polynomial in the number of variables and holds unconditionally with constant error rate.

**Theorem 37** (Main Theorem 1)**.** *For every constant $\alpha > 0$ there is an infinite family of $k$-left regular constraint graphs $G = ([M] \cup [N], E)$, where $M = 2^{\Theta(\log^2 N)}$, and $k = (\log N)^{\Theta(1/\alpha)}$, which is $(N^{1-\alpha}, 1 - o(1))$-expanding and there is an algorithm with running time $\mathrm{poly}(M)$ to solve the $\eta$-noisy $k$-XOR distinguishing problem for those graphs with distinguishing advantage $1 - o(1)$, with constant noise rate $\eta = 1/3$.*

*Proof.* Applying Remark 32 to Corollary 30, there is an infinite family of explicit $(m, k, d)$-coset graphs

$$G_m = ([M] \cup [N], E_m)$$

that is $(N^{1-\alpha}, 1 - o(1))$-expanding with the following relation on parameters:

- $M = 2^m$,
- $d = c \cdot \sqrt{m}$ for $c = 0.1$ (chosen specifically for $\eta = 1/3$). Observe that $c$ satisfies two conditions:

$$\Pr[Z \le c/2] < 0.6, \tag{1}$$

  for a standard normal $Z \sim N(0, 1)$ and

$$c^2 < -\ln(1/3)/2 \tag{2}$$

- $k = (m/\log m)^{\Theta(1/\alpha)}$.

First, we claim that $M = 2^{\Theta(\log^2 N)}$, and $k = (\log N)^{\Theta(1/\alpha)}$. Since $G_m$ is an $(m, k, d)$-coset graph, its right side has size $N = k \cdot 2^d$. Because $d = \Theta(\sqrt{m})$ and $\log k = O(\log m)$, we have $\log N = d + \log k = \Theta(\sqrt{m})$, implying $m = \Theta\left(\log^2 N\right)$. Therefore,

$$M = 2^m = 2^{\Theta(\log^2 N)}.$$

Also, since $m = \log M$, the left degree satisfies[7]

$$k = (m/\log m)^{\Theta(1/\alpha)} = (\log N)^{\Theta(1/\alpha)}.$$

Now we check that our choice of parameters satisfy the hypotheses in the statement of Theorem 33, which constructs a $\mathrm{poly}(M)$-time distinguisher. First, we compute the rate $R$ of the $\mathrm{RM}\left(m, \frac{m+d}{2}\right)$. For convenience, let $r = \frac{m+d}{2}$.

We rewrite the rate as the probability that a binomial random variable with parameters $(m, 1/2)$ is at most $r$:

$$R = 2^{-m} \cdot \sum_{i=0}^{r} \binom{m}{i} = \Pr[\mathrm{Bin}(m, 1/2) \le r].$$

Then, consider the normalized random variable $S \coloneqq (\mathrm{Bin}(m, 1/2) - (m/2)) / (\sqrt{m}/2)$. The equivalent event of interest in terms of $S$ is when $S \le 2 \cdot (r - (m/2))/\sqrt{m} = c/2$, that is,

$$\Pr[\mathrm{Bin}(m, 1/2) \le r] = \Pr[S \le c/2],$$

[7]Since $m = \Theta(\log^2 N)$, for any constant $\varepsilon > 0$ and sufficiently large $N$, $(\log N)^{(2-\varepsilon)/\alpha} \le m/\log m \le (\log N)^{2/\alpha}$.

where we recall that $c$ is the constant such that $d = c\sqrt{m}$. Since the absolute centered third moment of the $\mathsf{Ber}(1/2)$ random variable is $1/8$, the Berry-Esséen Theorem (see Theorem 21) gives

$$\Pr[S \le c/2] = \Pr\left[Z \le c/2\right] + O\left(\frac{1}{\sqrt{m}}\right),$$

for $Z \sim N(0,1)$. Any $c$ satisfying Equation (1) implies that $1 - R \ge 0.4 + O\left(\frac{1}{\sqrt{m}}\right)$ so that $\eta = 1/3 \le 1 - R + O(1/\log m)$.

For the other hypothesis, we need to show that $\eta \cdot 2^m \le 2^{m \cdot H_2((1-(d/m))/2)}$ for sufficiently large $m$. Observe that $d/m = c/\sqrt{m}$. By the Taylor expansion of $H_2$ around $1/2$, we have that

$$m \cdot H_2((1-(d/m))/2) = m \cdot \left(1 - \frac{2}{\ln 2} \cdot \left(\frac{c}{\sqrt{m}}\right)^2 + O(m^{-2})\right) = m - \frac{2c^2}{\ln 2} + O(m^{-1}).$$

Therefore, as long as $(1/3) \le 2^{-2c^2/(\ln 2)}$, any $c$ satisfying Equation (2) we have

$$(1/3) \cdot M \lesssim 2^{m \cdot H_2((1-(d/m))/2)}.$$

Since both hypotheses are satisfied, Theorem 33 implies that there exists an algorithm with running time $\mathrm{poly}(M)$ that solves the $\eta$-noisy $k$-XOR distinguishing problem with constant noise rate $\eta = 1/3$. □

### 6.1 The Setting of Polynomially Many Constraints

Assuming Reed-Muller codes efficiently achieve capacity of the BEC allows us to obtain a stronger theorem statement in which the number of constraints is polynomially related to the number of variables. As mentioned before, a weaker conjecture (Conjecture 16) leads to the same conclusion.

**Theorem 38** (Main Theorem 2)**.** *Assume Conjecture 16. Then for every $\alpha, c > 0$ there exists an infinite family of $k$-left-regular constraint graphs $G = ([M] \cup [N], E)$ such that*

$$M = N^{\Theta(1)}, \qquad k = (\log N)^{O(1/\alpha)},$$

*the graph is $(N^{1-\alpha}, 1 - o(1))$-expanding, and there is an algorithm running in time $\mathrm{poly}(M)$ that solves the $\eta$-noisy $k$-XOR distinguishing problem on these graphs for $\eta = N^{-c}$.*

*Proof.* Fix constants $\alpha, c > 0$. Let $\xi > 0, \zeta \ge 1$ be constants given by Conjecture 16. Let

$$\lambda(\beta) \coloneqq 1 - H_2\left(\frac{1-\beta}{2}\right)$$

for a value of $\beta$ we will choose shortly. By the Taylor expansion of $H_2$ around $1/2$, as $\beta \to 0$ we have

$$\lambda(\beta) = \frac{\beta^2}{2\ln 2} + O(\beta^4).$$

Let $\gamma_0 \coloneqq \frac{c \cdot \beta}{2}$, and choose a sufficiently small constant $\beta \in (0,1)$ such that

$$\lambda(\beta) < \min\left(\xi,\ \frac{c \cdot \beta}{4\zeta}\right) < \gamma_0. \tag{3}$$

By Corollary 30, there is an infinite family of explicit $(m, k, d)$-coset graphs

$$G_m = ([M] \cup [N], E_m)$$

which is $(N^{1-\alpha}, 1 - o(1))$-expanding with

- $M = 2^m$,
- $d = \beta m + \Theta(\log m)$,
- $k = (m/\log m)^{\Theta(1/\alpha)}$.

We claim that $M = N^{\Theta(1)}$ and that $k = (\log N)^{\Theta(1/\alpha)}$. Since $G_m$ is an $(m, k, d)$-coset graph, its right side has size $N = k \cdot 2^d$. Because $d = \beta m + \Theta(\log m)$ and $\log k = O(\log m)$, we have

$$\log N = d + \log k = \beta m + \Theta(\log m) = (\beta + o(1)) \cdot m,$$

implying immediately that

$$N = M^{\beta + o(1)}. \tag{4}$$

and implying immediately that $m = \Theta(\log N)$ so that

$$\boxed{M = 2^m = N^{\Theta(1)}.}$$

Also, since $m = \Theta(\log N)$, the left degree satisfies

$$\boxed{k = (m/\log m)^{\Theta(1/\alpha)} = (\log N)^{\Theta(1/\alpha)}.}$$

We now verify the hypotheses of Theorem 36. First observe that,

$$p \coloneqq d/m = \beta + \Theta\left(\frac{\log m}{m}\right) = \beta + o(1).$$

For convenience let $r \coloneqq \frac{m+d}{2}$. Using the continuity of the binary entropy function

$$H_2\left(\frac{1-p}{2}\right) = H_2\left(\frac{1-\beta}{2}\right) + o(1) = 1 - \lambda(\beta) + o(1). \tag{5}$$

For convenience let $r \coloneqq \frac{m+d}{2}$. We now show the first hypothesis holds for Theorem 36, namely that for sufficiently large $m$,

$$M^{-\xi} < \varepsilon_{m,d} < 1/2.$$

Observe that

$$\varepsilon_{m,d} \coloneqq 1 - \mathsf{Rate}\left(\mathrm{RM}\left(m, \frac{m+d}{2}\right)\right) = 2^{-m} \sum_{i < \frac{m-d}{2}} \binom{m}{i}.$$

By applying the standard Hamming ball asymptotics and then applying Equation (5), we have

$$\varepsilon_{m,d} = 2^{-m(1 - H_2((1-p)/2)) + o(m)} = M^{-\lambda(\beta) + o(1)}. \tag{6}$$

This quantity is less than $1/2$ for all sufficiently large $m$ since $M = 2^m$. Then recall that $\beta$ was chosen so that $\lambda(\beta) < \xi$. Therefore, for sufficiently large $m$, we have the desired property

$$\boxed{M^{-\xi} < \varepsilon_{m,d} < 1/2.}$$

Now we show that $\eta = N^{-c}$ satisfies $\eta < \varepsilon_{m,d}^{\zeta}$. Equation (4) implies $\eta = M^{-c \cdot \beta + o(1)}$. Equation (6) implies

$$\varepsilon_{m,d}^{\zeta} = M^{-\zeta \cdot \lambda(\beta) + o(1)}.$$

Equation (3) implies $\frac{\lambda(\beta)}{\beta} < \frac{c}{\zeta}$, which implies the desired statement that for sufficiently large $m$,

$$\boxed{\eta < \varepsilon_{m,d}^{\zeta}.}$$

Finally we show that $\eta \cdot M \lesssim M^{H_2((1-p)/2)}$. Since $\eta = N^{-c}$, Equation (4) implies that

$$\eta \cdot M = M^{1-c\cdot\beta+o(1)}.$$

Equation (5) implies that

$$M^{H_2((1-p)/2)} = M^{1-\lambda(\beta)+o(1)}.$$

Equation (3) implies that $1 - c \cdot \beta < 1 - \lambda(\beta)$ since $\lambda(\beta) < c \cdot \beta/4$ (since $\zeta \geq 1$). Therefore we conclude that

$$\boxed{\eta \cdot M \lesssim M^{H_2((1-p)/2)}.}$$

Since all hypotheses of Theorem 36 hold, there exists a $\mathrm{poly}(M)$ time algorithm that solves the $\eta$-noisy XOR distinguishing problem for $G_m$ with distinguishing advantage $1 - o(1)$. □

## Acknowledgements

We thank Andrej Bogdanov for helpful discussions. PL and AR are supported by European Research Council (ERC) under the EU's Horizon 2020 research and innovation programme (Grant agreement No. 101019547). PL is additionally supported by Stellar Foundation grant and AR by Cariplo CRYPTONOMEX grant. MS is supported in part by a Simons Investigator Award and NSF Award CCF 2152413. Part of MS's work done while visiting Bocconi University.

## References

[ABR16] Benny Applebaum, Andrej Bogdanov, and Alon Rosen. "A Dichotomy for Local Small-Bias Generators". In: *J. Cryptol.* 29.3 (2016), pp. 577–596. DOI: 10.1007/S00145-015-9202-8. URL: https://doi.org/10.1007/s00145-015-9202-8.

[ABW10] Benny Applebaum, Boaz Barak, and Avi Wigderson. "Public-key cryptography from different assumptions". In: *Proceedings of the forty-second ACM symposium on Theory of computing*. 2010, pp. 171–180.

[AL18] Benny Applebaum and Shachar Lovett. "Algebraic Attacks against Random Local Functions and Their Countermeasures". In: *SIAM J. Comput.* 47.1 (2018), pp. 52–79. DOI: 10.1137/16M1085942. URL: https://doi.org/10.1137/16M1085942.

[Ale03] Michael Alekhnovich. "More on Average Case vs Approximation Complexity". In: *44th Symposium on Foundations of Computer Science, FOCS 2003, Cambridge, MA, USA, October 11-14, 2003, Proceedings*. IEEE Computer Society, 2003, pp. 298–307. DOI: 10.1109/SFCS.2003.1238204. URL: https://doi.org/10.1109/SFCS.2003.1238204.

[AOW15] Sarah R. Allen, Ryan O'Donnell, and David Witmer. *How to refute a random CSP*. 2015. arXiv: 1505.04383 [cs.CC]. URL: https://arxiv.org/abs/1505.04383.

[App13] Benny Applebaum. "Pseudorandom Generators with Long Stretch and Low Locality from Random Local One-Way Functions". In: *SIAM J. Comput.* 42.5 (2013), pp. 2008–2037. DOI: 10.1137/120884857. URL: https://doi.org/10.1137/120884857.

[ASW14] Emmanuel Abbe, Amir Shpilka, and Avi Wigderson. "Reed-Muller codes for random erasures and errors". In: *CoRR* abs/1411.4590 (2014). arXiv: 1411.4590. URL: http://arxiv.org/abs/1411.4590.

[ASY21] Emmanuel Abbe, Amir Shpilka, and Min Ye. "Reed-Muller Codes: Theory and Algorithms". In: *IEEE Trans. Inf. Theory* 67.6 (2021), pp. 3251–3277. DOI: 10.1109/TIT.2020.3004749. URL: https://doi.org/10.1109/TIT.2020.3004749.

[AY19] Emmanuel Abbe and Min Ye. *Reed-Muller codes polarize*. 2019. arXiv: 1901.11533 [cs.IT]. URL: https://arxiv.org/abs/1901.11533.

[Bar+23] Boaz Barak, Benjamin L. Edelman, Surbhi Goel, Sham Kakade, Eran Malach, and Cyril Zhang. *Hidden Progress in Deep Learning: SGD Learns Parities Near the Computational Limit*. 2023. arXiv: 2207.08799 [cs.LG]. URL: https://arxiv.org/abs/2207.08799.

[Bar14] Boaz Barak. "Sum of squares upper bounds, lower bounds, and open questions". In: *Lecture notes* (2014).

[Bas+25] Arpon Basu, Jun-Ting Hsieh, Andrew D. Lin, and Peter Manohar. "Solving Random Planted CSPs below the $n^{k/2}$ Threshold". In: *CoRR* abs/2507.10833 (2025). DOI: 10.48550/ARXIV.2507.10833. arXiv: 2507.10833. URL: https://doi.org/10.48550/arXiv.2507.10833.

[BKR23] Andrej Bogdanov, Pravesh K. Kothari, and Alon Rosen. "Public-Key Encryption, Local Pseudorandom Generators, and the Low-Degree Method". In: *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part I*. Ed. by Guy N. Rothblum and Hoeteck Wee. Lecture Notes in Computer Science. Springer, 2023, pp. 268–285. DOI: 10.1007/978-3-031-48615-9_10. URL: https://doi.org/10.1007/978-3-031-48615-9%5C_10.

[Blu+93] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. "Cryptographic Primitives Based on Hard Learning Problems". In: *13th Annual International Cryptology Conference, CRYPTO 1993*. 1993, pp. 278–291. DOI: 10.1007/3-540-48329-2_24. URL: https://doi.org/10.1007/3-540-48329-2%5C_24.

[BM16] Boaz Barak and Ankur Moitra. *Noisy Tensor Completion via the Sum-of-Squares Hierarchy*. 2016. arXiv: 1501.06521 [cs.LG]. URL: https://arxiv.org/abs/1501.06521.

[BQ12] Andrej Bogdanov and Youming Qiao. "On the security of Goldreich's one-way function". In: *Comput. Complex.* 21.1 (2012), pp. 83–127. DOI: 10.1007/S00037-011-0034-0. URL: https://doi.org/10.1007/s00037-011-0034-0.

[Bra08] Mark Braverman. "Polylogarithmic independence fools AC 0 circuits". In: *Journal of the ACM (JACM)* 57.5 (2008), pp. 1–10.

[BRT25] Andrej Bogdanov, Alon Rosen, and Kel Zin Tan. "Sample Efficient Search to Decision for kLIN". In: *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part I*. Lecture Notes in Computer Science. Springer, 2025, pp. 203–220.

[BS16] Boaz Barak and David Steurer. *Proofs, beliefs, and algorithms through the lens of sum-of-squares*. 2016.

[BSV19] Andrej Bogdanov, Manuel Sabin, and Prashant Nalini Vasudevan. "XOR Codes and Sparse Learning Parity with Noise". In: *Proceedings of 2019 ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 2019, pp. 986–1004. DOI: 10.1137/1.9781611975482.61. eprint: https://epubs.siam.org/doi/pdf/10.1137/1.9781611975482.61. URL: https://epubs.siam.org/doi/abs/10.1137/1.9781611975482.61.

[Buh+25] Rares-Darius Buhai, Jun-Ting Hsieh, Aayush Jain, and Pravesh K. Kothari. "The Quasi-Polynomial Low-Degree Conjecture is False". In: *66th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2025, Sydney, Australia, December 14-17, 2025*. IEEE, 2025, pp. 2577–2590. DOI: 10.1109/FOCS63196.2025.00134. URL: https://doi.org/10.1109/FOCS63196.2025.00134.

[CGL07] Amin Coja-Oghlan, Andreas Goerdt, and André Lanka. "Strong Refutation Heuristics for Random k-SAT". In: *Combinatorics, Probability and Computing* 16.1 (2007), pp. 5–28. DOI: 10.1017/S096354830600784X.

[Fei02] Uriel Feige. "Relations between average case complexity and approximation complexity". In: *Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*. 2002, pp. 534–543.

[FKO06] Uriel Feige, Jeong Han Kim, and Eran Ofek. "Witnesses for non-satisfiability of dense random 3CNF formulas". In: *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*. 2006, pp. 497–508. DOI: 10.1109/FOCS.2006.78.

[FPV15] Vitaly Feldman, Will Perkins, and Santosh S. Vempala. "Subsampled Power Iteration: a Unified Algorithm for Block Models and Planted CSP's". In: *Advances in Neural Information Processing Systems 28: Annual Conference on Neural Information Processing Systems 2015, December 7-12, 2015, Montreal, Quebec, Canada*. Ed. by Corinna Cortes, Neil D. Lawrence, Daniel D. Lee, Masashi Sugiyama, and Roman Garnett. 2015, pp. 2836–2844. URL: https://proceedings.neurips.cc/paper/2015/hash/9597353e41e6957b5e7aa79214fcb256-Abstract.html.

[Gho+25] Riddhi Ghosal, Isaac M. Hair, Aayush Jain, and Amit Sahai. "Using the Planted Clique Conjecture for Cryptography: Public-Key Encryption from Planted Clique and Noisy k-LIN over Expanders". In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. STOC '25. Prague, Czechia: Association for Computing Machinery, 2025, pp. 1921–1932. ISBN: 9798400715105. DOI: 10.1145/3717823.3718306. URL: https://doi.org/10.1145/3717823.3718306.

[GKM23] Venkatesan Guruswami, Pravesh K. Kothari, and Peter Manohar. *Algorithms and Certificates for Boolean CSP Refutation: "Smoothed is no harder than Random"*. 2023. arXiv: 2109.04415 [cs.CC]. URL: https://arxiv.org/abs/2109.04415.

[Gol00] Oded Goldreich. "Candidate One-Way Functions Based on Expander Graphs". In: *Electron. Colloquium Comput. Complex.* TR00, TR00-090 (2000). ECCC: TR00-090. URL: https://eccc.weizmann.ac.il/eccc-reports/2000/TR00-090/index.html.

[Gol11] Oded Goldreich. "Candidate One-Way Functions Based on Expander Graphs". In: *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation - In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman*. Ed. by Oded Goldreich. Lecture Notes in Computer Science. Springer, 2011, pp. 76–87. DOI:

10.1007/978-3-642-22670-0_10. URL: https://doi.org/10.1007/978-3-642-22670-0%5C_10.

[Gri01] Dima Grigoriev. "Complexity of Positivstellensatz proofs for the knapsack". In: *Comput. Complex.* 10.2 (2001), pp. 139–154. DOI: 10.1007/S00037-001-8192-0. URL: https://doi.org/10.1007/s00037-001-8192-0.

[GRS12] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. *Essential Coding Theory*. Draft available online, 2012. URL: http://www.cse.buffalo.edu/atri/courses/coding-theory/book.

[GRY22] Venkatesan Guruswami, Andrii Riazanov, and Min Ye. "Arıkan Meets Shannon: Polar Codes With Near-Optimal Convergence to Channel Capacity". In: *IEEE Transactions on Information Theory* 68.5 (2022), pp. 2877–2919. DOI: 10.1109/TIT.2022.3146786.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. "Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes". In: *J. ACM* 56.4 (July 2009). ISSN: 0004-5411. DOI: 10.1145/1538902.1538904. URL: https://doi.org/10.1145/1538902.1538904.

[GX15] Venkatesan Guruswami and Patrick Xia. "Polar Codes: Speed of Polarization and Polynomial Gap to Capacity". In: *IEEE Transactions on Information Theory* 61.1 (2015), pp. 3–16. DOI: 10.1109/TIT.2014.2371819.

[Has+18] Hamed Hassani, Shrinivas Kudekar, Or Ordentlich, Yury Polyanskiy, and Rüdiger Urbanke. *Almost Optimal Scaling of Reed-Muller Codes on BEC and BSC Channels*. 2018. arXiv: 1801.09481 [cs.IT]. URL: https://arxiv.org/abs/1801.09481.

[HAU14] Seyed Hamed Hassani, Kasra Alishahi, and Rüdiger L Urbanke. "Finite-length scaling for polar codes". In: *IEEE Transactions on Information Theory* 60.10 (2014), pp. 5875–5898.

[Hop18] Samuel Hopkins. *Statistical inference and the sum of squares method*. Cornell University, 2018.

[HW21] Justin Holmgren and Alexander S. Wein. "Counterexamples to the Low-Degree Conjecture". In: *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, Virtual Conference, January 6-8, 2021*. Ed. by James R. Lee. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 75:1–75:9. DOI: 10.4230/LIPICS.ITCS.2021.75. URL: https://doi.org/10.4230/LIPIcs.ITCS.2021.75.

[Kot+17] Pravesh K. Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. "Sum of squares lower bounds for refuting any CSP". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*. Ed. by Hamed Hatami, Pierre McKenzie, and Valerie King. ACM, 2017, pp. 132–145. DOI: 10.1145/3055399.3055485. URL: https://doi.org/10.1145/3055399.3055485.

[Kud+16] Shrinivas Kudekar, Santhosh Kumar, Marco Mondelli, Henry D. Pfister, Eren Sasoglu, and Rüdiger L. Urbanke. "Reed-Muller codes achieve capacity on erasure channels". In: *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*. Ed. by Daniel Wichs and Yishay Mansour. ACM, 2016, pp. 658–669. DOI: 10.1145/2897518.2897584. URL: https://doi.org/10.1145/2897518.2897584.

[Kud+17] Shrinivas Kudekar, Santhosh Kumar, Marco Mondelli, Henry D. Pfister, Eren Sasoglu, and Rüdiger L. Urbanke. "Reed-Muller Codes Achieve Capacity on Erasure Channels". In: *IEEE Trans. Inf. Theory* 63.7 (2017), pp. 4298–4316. DOI: 10.1109/TIT.2017.2673829. URL: https://doi.org/10.1109/TIT.2017.2673829.

[MHU14] Marco Mondelli, S Hamed Hassani, and Rüdiger L Urbanke. "From polar to Reed-Muller codes: A technique to improve the finite-length performance". In: *IEEE Transactions on Communications* 62.9 (2014), pp. 3084–3091.

[MST06] Elchanan Mossel, Amir Shpilka, and Luca Trevisan. "On epsilon-biased generators in $NC^0$". In: *Random Struct. Algorithms* 29.1 (2006), pp. 56–81. DOI: 10.1002/RSA.20112. URL: https://doi.org/10.1002/rsa.20112.

[OST19] Igor Carboni Oliveira, Rahul Santhanam, and Roei Tell. "Expander-Based Cryptography Meets Natural Proofs". In: *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, San Diego, California, USA, January 10-12, 2019*. Ed. by Avrim Blum. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, 18:1–18:14. DOI: 10.4230/LIPICS.ITCS.2019.18. URL: https://doi.org/10.4230/LIPIcs.ITCS.2019.18.

[PV05] Farzad Parvaresh and Alexander Vardy. "Correcting Errors Beyond the Guruswami-Sudan Radius in Polynomial Time". In: *46th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2005, Pittsburgh, PA, USA, October 23-25, 2005, Proceedings*. IEEE Computer Society, 2005, pp. 285–294. DOI: 10.1109/SFCS.2005.29. URL: https://doi.org/10.1109/SFCS.2005.29.

[Rao21] Anup Rao. *Reed-Muller codes achieve capacity on the erasure channel*. YouTube. Dec. 2021. URL: https://www.youtube.com/watch?v=V9HCmPPz110.

[RRS17] Prasad Raghavendra, Satish Rao, and Tselil Schramm. "Strongly refuting random CSPs below the spectral threshold". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*. Ed. by Hamed Hatami, Pierre McKenzie, and Valerie King. ACM, 2017, pp. 121–131. DOI: 10.1145/3055399.3055417. URL: https://doi.org/10.1145/3055399.3055417.

[SS18] Ori Sberlo and Amir Shpilka. *On the Performance of Reed-Muller Codes with respect to Random Errors and Erasures*. 2018. arXiv: 1811.12447 [cs.IT]. URL: https://arxiv.org/abs/1811.12447.

[SSV15] Ramprasad Saptharishi, Amir Shpilka, and Ben Lee Volk. "Decoding high rate Reed-Muller codes from random errors in near linear time". In: *CoRR* abs/1503.09092 (2015). arXiv: 1503.09092. URL: http://arxiv.org/abs/1503.09092.

[Tao23] Terence Tao. *Topics in random matrix theory*. Vol. 132. American Mathematical Society, 2023.

[Vad12] Salil P Vadhan. "Pseudorandomness". In: *Foundations and Trends® in Theoretical Computer Science* 7.1-3 (2012), pp. 1–336.