

# Low-Degree Polynomials Extract from Local Sources

Omar Alrabiah  
 UC Berkeley  
 oalrabiah@berkeley.edu

Eshan Chattopadhyay\*  
 Cornell University  
 eshan@cs.cornell.edu

Jesse Goodman\*  
 Cornell University  
 jpmgoodman@cs.cornell.edu

Xin Li†  
 Johns Hopkins University  
 lixints@cs.jhu.edu

João Ribeiro‡  
 Carnegie Mellon University  
 jlourenc@cs.cmu.edu

## Abstract

We continue a line of work on extracting random bits from weak sources that are generated by simple processes. We focus on the model of locally samplable sources, where each bit in the source depends on a small number of (hidden) uniformly random input bits. Also known as local sources, this model was introduced by De and Watson (TOCT 2012) and Viola (SICOMP 2014), and is closely related to sources generated by  $AC^0$  circuits and bounded-width branching programs. In particular, extractors for local sources also work for sources generated by these classical computational models.

Despite being introduced a decade ago, little progress has been made on improving the entropy requirement for extracting from local sources. The current best explicit extractors require entropy  $n^{1/2}$ , and follow via a reduction to affine extractors. To start, we prove a barrier showing that one cannot hope to improve this entropy requirement via a black-box reduction of this form. In particular, new techniques are needed.

In our main result, we seek to answer whether low-degree polynomials (over  $\mathbb{F}_2$ ) hold potential for breaking this barrier. We answer this question in the positive, and fully characterize the power of low-degree polynomials as extractors for local sources. More precisely, we show that a random degree  $r$  polynomial is a low-error extractor for  $n$ -bit local sources with min-entropy  $\Omega(r(n \log n)^{1/r})$ , and we show that this is tight.

Our result leverages several new ingredients, which may be of independent interest. Our existential result relies on a new reduction from local sources to a more structured family, known as local non-oblivious bit-fixing sources. To show its tightness, we prove a “local version” of a structural result by Cohen and Tal (RANDOM 2015), which relies on a new “low-weight” Chevalley-Waring theorem.

---

\*Supported by NSF CAREER Award 2045576.

†Supported by NSF CAREER Award CCF-1845349.

‡Research supported in part by the NSF grants CCF-1814603 and CCF-2107347 and by the following grants of Vipul Goyal: the NSF award 1916939, DARPA SIEVE program, a gift from Ripple, a DoE NETL award, a JP Morgan Faculty Fellowship, a PNC center for financial services innovation award, and a Cylab seed funding award.

# 1 Introduction

Randomness is a fundamental resource in many areas of computer science, such as algorithm design and cryptography. However, such tasks often assume access to a source of independent and uniform bits, while real-world physical processes (e.g., electromagnetic noise, timings of user keystrokes) generate randomness that is far from perfect. This state of affairs motivates the problem of *randomness extraction*. The goal is to design a deterministic function, called an *extractor*, that can distill a (nearly) uniform bit from any source belonging to a certain family.<sup>1</sup>

**Definition 1** (Extractor). *A function  $\text{Ext} : \{0, 1\}^n \rightarrow \{0, 1\}$  is an extractor for a family of distributions  $\mathcal{X}$  over  $\{0, 1\}^n$  with error  $\varepsilon$  if, for every  $\mathbf{X} \in \mathcal{X}$ ,*

$$\left| \Pr[\text{Ext}(\mathbf{X}) = 1] - \frac{1}{2} \right| \leq \varepsilon.$$

*We also call  $\text{Ext}$  an  $\varepsilon$ -extractor for  $\mathcal{X}$ .*

Besides their practical motivation, randomness extractors (and other related pseudorandom objects such as dispersers, condensers, and expander graphs) have deep connections to coding theory, combinatorics, and complexity theory.

In order to construct an extractor for a family  $\mathcal{X}$  of sources, the most general assumption one can make about  $\mathcal{X}$  is that each  $\mathbf{X} \in \mathcal{X}$  has some “randomness.” Here, it is typical to measure the randomness of a source  $\mathbf{X}$  by its min-entropy  $H_\infty(\mathbf{X}) := -\log \max_x \Pr[\mathbf{X} = x]$ . However, even if we assume each  $\mathbf{X} \in \mathcal{X}$  has a very high amount of this very strong notion of entropy, extraction is still impossible: indeed, one cannot hope to extract from  $\mathcal{X}$  even if each source  $\mathbf{X} \in \mathcal{X}$  is guaranteed to have min-entropy  $k \geq n - 1$  [CG88]. To enable extraction, one must make additional assumptions on the structure of each  $\mathbf{X} \in \mathcal{X}$ .

**Extractors for local sources,  $\text{AC}^0$  sources, and small-space sources.** In a seminal work, Trevisan and Vadhan [TV00] initiated the study of randomness extraction from sources that can be sampled by “simple” processes. In addition to the generality of such sources, it can be argued that they serve a reasonable model of randomness that might actually be found in nature.

More formally, Trevisan and Vadhan studied sources that can be sampled by polynomial size circuits that are given uniform bits as input. However, extracting randomness from this class of sources requires strong computational hardness assumptions. This motivated De and Watson [DW12] and Viola [Vio14] to consider *unconditional* extraction from sources sampled by more restricted, but still natural, circuit families. To this end, they introduced the notion of *local sources*. Intuitively, a local source  $\mathbf{X}$  is one that can be sampled by a low-depth circuit with bounded fan-in (a low-complexity process).

**Definition 2** (Local source [DW12, Vio14]). *A distribution  $\mathbf{X} \sim \{0, 1\}^n$  is a  $d$ -local source if  $\mathbf{X} = g(\mathbf{U}_m)$ , where  $\mathbf{U}_m$  is the uniform distribution over  $m$  bits (for some  $m$ ), and  $g : \{0, 1\}^m \rightarrow \{0, 1\}^n$  is a function where each output bit depends on at most  $d$  input bits.*

Local sources are closely connected to other models of sources sampled by simple processes. Viola [Vio14] proved that every source generated by  $\text{AC}^0$  circuits is (close to) a convex combination of local sources with small locality and slightly lower min-entropy. More recently, Chattopadhyay

---

<sup>1</sup>In general, one would actually like to distill (from the source) as many uniform bits as possible. However, we focus here on the simpler goal of obtaining just a single uniform bit, as there remain significant barriers even in this most basic setting.

and Goodman [CG21] showed a similar result for sources generated by bounded-width branching programs [KRVZ11]. Thus, extractors for local sources also work for sources generated by these classical computational models. In fact, the current state-of-the-art extractors for sources generated by  $AC^0$  circuits and bounded-width branching programs are extractors for 1-local sources.

**A barrier at  $\sqrt{n}$  min-entropy.** Despite the applications above and being introduced over a decade ago, little progress has been made on constructing extractors for local sources [DW12, Vio14, Li16]. In particular, all known constructions require min-entropy at least  $\sqrt{n}$ , and follow via a reduction to extractors for affine sources (i.e., sources that are uniform over affine subspaces of  $\mathbb{F}_2^n$ ). Thus, there appears to be a “barrier” at  $\sqrt{n}$  min-entropy, at least when using affine extractors [Vio20]. It is natural to ask how we might break this  $\sqrt{n}$  barrier, which raises the question:

*Can affine extractors be used to extract from local sources with min-entropy  $k \ll \sqrt{n}$ ?*

As motivation, we start by providing strong evidence that the answer to the above question is negative. In particular, we prove the following.

**Theorem 0** (Barrier result). *It is not possible to extract randomness from 2-local sources with min-entropy  $k \geq \sqrt{n}$  by applying an affine extractor in a black-box manner.*

Thus, if we would like to construct extractors for local sources with min-entropy significantly below  $\sqrt{n}$ , new techniques are needed.

**Towards breaking the  $\sqrt{n}$  barrier using low-degree polynomials.** While explicit extractors that break the  $\sqrt{n}$  min-entropy barrier for local sources are the end goal, these still seem beyond reach. We believe that the next best thing are non-explicit extractors that are of “low complexity.” Our hope is that such extractors may help us eventually construct truly explicit extractors, as non-explicit extractors are more likely to be easier to derandomize if they belong to a low complexity class. At the same time, such non-explicit extractors may have applications in complexity theory (i.e., since the current state-of-the-art circuit lower bounds are against extractors [LY21]). There is a long line of work [Vio05, GVW15, CL18, Lu04, Vad04, BG13, CL18, DY21, HIV21, CT15] on the power of low-complexity computational models for extracting from various families of sources.

We choose to study the class of *low-degree  $\mathbb{F}_2$ -polynomials* as our low-complexity computational model. In particular, we ask whether (non-explicit) low-degree polynomials can help break the  $\sqrt{n}$  barrier for extracting from local sources, and more generally we seek to answer the following question:

**Question 1.** *How powerful are low-degree  $\mathbb{F}_2$ -polynomials as extractors for local sources?*

Beyond being a natural algebraic class, low-degree  $\mathbb{F}_2$ -polynomials have a natural combinatorial interpretation. We can represent a degree-2  $\mathbb{F}_2$ -polynomial  $f$  as a graph  $G_f$  on  $n$  vertices, with edges representing monomials included in  $f$ . Then,  $f$  being a good extractor for local sources translates into a parity constraint on the number of edges in certain induced subgraphs of  $G_f$ . Likewise, a degree-3  $\mathbb{F}_2$ -polynomial can be represented as a 3-hypergraph, and so on. Given the correspondence between low-degree polynomials and hypergraphs with small edge sizes, we hope that tools from combinatorics can be leveraged to make our constructions explicit and break the  $\sqrt{n}$  min-entropy barrier for extracting from local sources (which would also give improved extractors for small-space sources).

Our motivation to study low-degree polynomials as our “low complexity” model also comes from the work of Cohen and Tal [CT15], which studied the same question in the context of *affine* sources. In their

work, they showed that there exist degree- $r$   $\mathbb{F}_2$ -polynomials that extract from affine sources with min-entropy  $O(rn^{\frac{1}{r-1}})$ , and that this is tight. In order to answer [Question 1](#), we aim to provide a local source analogue of this result.

## 1.1 Summary of our results

In this paper, we fully characterize the power of low-degree polynomials as extractors for local sources, answering [Question 1](#) and proving a local-source analogue of Cohen-Tal. Along the way, we rely on several new ingredients which may be of independent interest. We present these results in [Section 1.1.1](#) and [Section 1.1.2](#), respectively.

### 1.1.1 Main result

Our main result gives a tight characterization of the power of low-degree polynomials as extractors for local sources. We state it formally, below.

**Theorem 1 (Main result).** *For every  $d \in \mathbb{N}$  and  $r \geq 2$ , there are constants  $C, c > 0$  such that the following holds. For every  $n \in \mathbb{N}$  there exists a (not necessarily explicit) degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  that is a  $(2^{-ck})$ -extractor for  $d$ -local sources with min-entropy*

$$k \geq C(n \log n)^{1/r},$$

*but for every degree  $\leq r$  polynomial  $g \in \mathbb{F}_2[x_1, \dots, x_n]$  there exists a  $d$ -local source with min-entropy*

$$k \geq c(n \log n)^{1/r}$$

*on which it is constant.*

[Theorem 1](#) implies that degree-3 polynomials are already enough to extract from min-entropy  $k = O((n \log n)^{1/3})$ , which (non-explicitly) breaks the  $\sqrt{n}$  min-entropy barrier of previous techniques ([Theorem 0](#)). Furthermore, given known reductions from  $\text{AC}^0$  sources and small-space sources to local sources [[Vio14](#), [CG21](#)], it also follows that low-degree polynomials can be used to break the current min-entropy barriers for extracting from these other models of weak sources. Finally, [Theorem 1](#) can be viewed as a generalization of a result by Viola [[Vio16](#)], who showed the existence of quadratic functions  $f$  such that  $\text{AC}^0$  cannot sample  $(\mathbf{U}_n, f(\mathbf{U}_n))$ : our result shows that there exist degree  $\leq r$  polynomials such that  $\text{AC}^0$  cannot sample  $(\mathbf{X}, f(\mathbf{X}))$ , where  $\mathbf{X}$  can be *any* distribution with min-entropy  $k \geq Cn^{1/r+\delta}$  for a large enough  $C$  and arbitrarily small  $\delta > 0$ .

While [Theorem 1](#) is stated for constant locality  $d$  and constant degree  $r$ , we actually prove stronger results that hold for superconstant  $d, r$ . In particular, [Theorem 1](#) follows immediately from the following two results, which provide upper and lower bounds on the entropy required to extract from  $d$ -local sources using a degree  $\leq r$  polynomials (where  $d, r$  need not be constant).

**Theorem 1.1 (Technical version of [Theorem 1](#), Upper Bound).** *There are universal constants  $C, c > 0$  such that for all  $n, d, r \in \mathbb{N}$ , the following holds. With probability at least 0.99 over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , it holds that  $f$  is an  $\varepsilon$ -extractor for  $d$ -local sources with min-entropy  $k$ , for any*

$$k \geq C2^d d^2 r \cdot (2^d n \log n)^{1/r},$$

*where  $\varepsilon = 2^{-\frac{ck}{r^3 2^d d^2}}$ .*

**Remark 1** (Informal version of [Theorem 6](#)). *If instead of extractors we aim to construct dispersers,<sup>2</sup> then we are able to improve [Theorem 1.1](#) to hold for min-entropy  $k \geq Cd^3r \cdot (n \log n)^{1/r}$ .*

**Theorem 1.2** (Technical version of [Theorem 1](#), Lower Bound). *There exists a universal constant  $c > 0$  such that for all  $n, d, r \in \mathbb{N}$  with  $2 \leq r \leq c \log(n)$  and  $d \leq n^{\frac{1}{r-1}-2^{-10r}} / \log(n)$ , the following holds. For any degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , there is a  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy at least*

$$k \geq cr(dn \log n)^{1/r}$$

such that  $f(\mathbf{X})$  is constant.

### 1.1.2 Key new ingredients

Our main result follows from a collection of new ingredients, which may be of independent interest. In order to prove our upper bound on min-entropy ([Theorem 1.1](#)), we prove a new reduction from  $d$ -local sources to  $d$ -local non-oblivious bit fixing (NOBF) sources. Informally, a  $d$ -local NOBF source  $\mathbf{X} \sim \{0, 1\}^n$  of min-entropy  $k'$  is a source that has  $k'$  uniform independent bits, with all other bits depending on at most  $d$  of the  $k'$  bits.

**Theorem 2** (Reduction from  $d$ -local sources to  $d$ -local NOBF sources). *There exists a universal constant  $c > 0$  such that for any  $n, k, d \in \mathbb{N}$ , the following holds. Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $\geq k$ . Then  $\mathbf{X}$  is  $\varepsilon$ -close to a convex combination of  $d$ -local NOBF sources with min-entropy  $\geq k'$ , where  $\varepsilon = 2^{-ck'}$  and*

$$k' = \frac{ck}{2^d d^2}.$$

The family of  $d$ -local NOBF sources, introduced in [\[CGGL20\]](#), is a significant specialization of  $d$ -local sources. The above reduction shows that, at least for constant locality  $d$ , we can just focus on extracting from this simpler class - even in future explicit constructions.

To prove our lower bound on min-entropy ([Theorem 1.2](#)), we actually prove this lower bound for the special class of  $d$ -local sources known as  $d$ -local affine sources: such a source  $\mathbf{X} \sim \mathbb{F}_2^n$  is uniform over a  $d$ -local affine subspace  $X \subseteq \mathbb{F}_2^n$ , which is a special type of affine subspace that admits a basis  $v_1, \dots, v_k \in \mathbb{F}_2^n$  where each coordinate  $i \in [n]$  holds the value 1 in at most  $d$  of these vectors. For this special class of sources, our lower bound is actually tight, and can be viewed as a “local” version of a result by Cohen and Tal [\[CT15\]](#).

**Theorem 3** (Local version of Cohen-Tal). *There exist universal constants  $C, c > 0$  such that for every  $n, r, d \in \mathbb{N}$  such that  $2 \leq r \leq c \log(n)$  and  $d \leq n^{\frac{1}{r-1}-2^{-10r}} / \log(n)$ , the following holds. For any degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , there exists a  $d$ -local affine subspace  $X \subseteq \mathbb{F}_2^n$  of dimension*

$$k \geq cr(dn \log n)^{1/r}$$

on which  $f$  is constant.

*This is tight: there exists a degree  $\leq r$  polynomial  $g \in \mathbb{F}_2[x_1, \dots, x_n]$  which is an extractor for  $d$ -local affine sources of dimension  $k \geq Cr(dn \log n)^{1/r}$ , which has error  $\varepsilon = 2^{-ck/r}$ .*

---

<sup>2</sup>A function  $\text{Disp} : \{0, 1\}^n \rightarrow \{0, 1\}$  is a disperser for a class of sources  $\mathcal{C}$  if the support of  $\text{Disp}(\mathbf{X})$  is  $\{0, 1\}$  for all sources  $\mathbf{X} \in \mathcal{C}$ .

We prove [Theorem 3](#) by extending the techniques of Cohen and Tal [[CT15](#)], while leveraging a key new ingredient: a “low-weight” Chevalley-Waring theorem. This result, which may be of independent interest, shows that any small system of low-degree polynomials admits a (nontrivial) solution of low Hamming weight.

**Theorem 4** (Low-weight Chevalley-Waring). *Let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  be a set of polynomials with linear degree<sup>3</sup> at most  $D$  and nonlinear degree<sup>4</sup> at most  $\Delta$ , such that  $0$  is a common solution and  $D + \Delta < n$ . Then there is a common solution  $x \neq 0$  with Hamming weight*

$$w \leq 8\Delta + 8D/\log(n/D) + 8.$$

## 1.2 Open problems

Our work leaves open several interesting avenues for future work. We highlight three of them here:

- For any constant  $r \geq 2$ , construct an explicit  $\mathbb{F}_2$ -polynomial of degree  $\leq r$  that extracts from 2-local sources of min-entropy  $o(n)$ .
- In [Theorem 2](#), we showed a reduction from  $d$ -local sources of min-entropy  $k$  to  $d$ -local non-oblivious bit fixing (NOBF) sources of min-entropy  $\Omega(k/(2^d d^2))$ . It would be interesting to show a reduction from a  $d$ -local source of min-entropy  $k$  to a  $d$ -local NOBF source of min-entropy  $\Omega(k/\text{poly}(d))$  (or show that such a reduction is impossible).
- [Theorem 4](#) shows that if a collection of low-degree  $n$ -variate polynomials of linear degree  $D$  and nonlinear degree  $\Delta$  has the zero vector as a solution (and  $D + \Delta < n$ ), then there exists a nonzero solution of weight at most  $O(\Delta + D/\log(n/D))$ . When  $\Delta = 0$ , this becomes asymptotically tight by the Hamming bound. Moreover, when  $D = 0$ , this will also be tight by picking the polynomial  $f(x) = \sum_{1 \leq |S| \leq \Delta} \prod_{i \in S} x_i$ . However, if we had  $\Delta/2$  quadratic polynomials, will the upper bound of  $O(\Delta)$  still be tight?

## 2 Overview of our techniques

In this section, we provide an overview of the techniques that go into our three main results:

- An entropy *upper bound* for low-degree extraction from local sources ([Theorem 1.1](#)).
- An entropy *lower bound* for low-degree extraction from local sources ([Theorem 1.2](#)).
- A *barrier* for extracting from local sources using black-box affine extractors ([Theorem 0](#)).

Along the way, we will overview the several new key ingredients ([Theorems 2, 3, and 4](#)) that go into these main results.

### 2.1 Upper bounds

We begin by discussing our entropy upper bounds for low-degree extraction from local sources. By this, we mean that we upper bound the entropy *requirement* for extracting from  $d$ -local sources using degree  $\leq r$  polynomials. In other words, we show that low-degree polynomials extract from local sources.

<sup>3</sup>The *linear degree*  $D$  is the sum of the degrees of the  $f_i$ 's which have degree 1.

<sup>4</sup>The *nonlinear degree* is the sum of the degrees of the  $f_i$ 's which have degree at least 2.

### 2.1.1 Low-degree extractors for local sources

We start by sketching the techniques behind our main upper bound ([Theorem 1.1](#)), which shows that most degree  $\leq r$  polynomials are low-error extractors for  $d$ -local sources with min-entropy at least

$$k = O(2^d d^2 r \cdot (2^d n \log n)^{1/r}).$$

**A strawman application of the probabilistic method.** A natural first attempt at proving our result would use a standard application of the probabilistic method, which looks something like the following. First, let  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  be a uniformly random polynomial of degree  $\leq r$ , meaning that each monomial of size  $\leq r$  is included in  $f$  with probability  $1/2$ . Then, we let  $\mathcal{X}$  be the family of  $d$ -local sources over  $\{0, 1\}^n$ , each with min-entropy at least  $k$ . To prove that most of these polynomials are low-error extractors for this family, a standard application of the probabilistic method would suggest that we:

1. Prove that  $f$  is an extractor for a single  $\mathbf{X} \in \mathcal{X}$  with extremely high probability.
2. Show that the family  $\mathcal{X}$  does not contain too many sources.
3. Conclude, via the union bound, that  $f$  is an extractor for *every*  $\mathbf{X} \in \mathcal{X}$  with high probability.

It is not too hard to complete Steps 2 and 3 in the above framework, but Step 1 turns out to be much more challenging. To see why, let us consider an arbitrary  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy at least  $k$ . By definition of  $d$ -local source, there exists some  $m \in \mathbb{N}$  and functions  $g_1, \dots, g_n : \{0, 1\}^m \rightarrow \{0, 1\}$  such that each  $g_i$  depends on just  $d$  of its inputs, and such that given a uniform  $\mathbf{Y} \sim \{0, 1\}^m$ , we have

$$\mathbf{X} = (g_1(\mathbf{Y}), g_2(\mathbf{Y}), \dots, g_n(\mathbf{Y})).$$

Now, we want to argue that a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  is a low-error extractor for  $\mathbf{X}$ . To do so, consider the function  $F : \{0, 1\}^m \rightarrow \{0, 1\}$  defined as

$$F(y_1, \dots, y_m) := (f \circ g)(y_1, \dots, y_m) = f(g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m)).$$

Notice that by the definition of  $\mathbf{X}$  and by [Definition 1](#) of extractor, we know that  $f$  is an extractor for  $\mathbf{X}$  with error  $\varepsilon$  if

$$|\text{bias}(F)| := \left| \Pr_{y \sim \mathbf{U}_m} [F(y) = 1] - \Pr_{y \sim \mathbf{U}_m} [F(y) = 0] \right| \leq 2\varepsilon.$$

Thus, to argue that a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  is a low-error extractor for  $\mathbf{X}$ , it suffices to argue that the function  $F = f \circ g$  has low bias (with high probability over the selection of  $f$ ).

Of course, the question now becomes: how can we ensure that  $F$  has low bias? We can start by noticing some properties of  $F$ . First, we know  $F = f \circ g$ , where  $f$  is a random degree  $\leq r$  polynomial and  $g$  is a fixed function where each output bit depends on  $\leq d$  input bits. Thus, it is not hard to argue that  $F$  will have degree  $\leq rd$ . Furthermore, since  $f$  is random and  $g$  is fixed, one may hope to argue that  $F$  is a *uniformly random* polynomial of degree  $\leq rd$ : in this case we would be done, since it is well-known that uniformly random low-degree polynomials have extremely low bias (with extremely high probability) [[BHL12](#)].

Unfortunately, it is too much to hope that  $F$  is a uniformly random low-degree polynomial. Indeed, it is not hard to see that the distribution of  $F$  over degree  $\leq rd$  polynomials depends heavily on the exact selection of  $g$ . Furthermore, for most selections of  $g$ , the random function  $F$  is *not* uniformly distributed over degree  $\leq t$  polynomials for *any*  $t$ .

Thus, there is no obvious way to apply [BHL12] in order to argue that  $F$  will have low bias. To proceed, it seems like we will somehow need to argue that the distribution of  $F$  over low-degree polynomials is guaranteed to have some specific *structure*, and then somehow argue that a random polynomial from any such structured distribution is guaranteed to have low-bias. Each of these steps seems quite challenging.

**Reductions to the rescue.** As it turns out, there is a simple trick we can use to greatly simplify the above approach. The key idea is to *reduce* local sources to a simpler class of sources. Given two families  $\mathcal{X}, \mathcal{Y}$  of distributions over  $\{0, 1\}^n$ , we say that  $\mathcal{X}$  *reduces* to  $\mathcal{Y}$  if each  $\mathbf{X} \in \mathcal{X}$  is (close to) a convex combination of  $\mathbf{Y} \in \mathcal{Y}$ .<sup>5</sup> Reductions are extremely useful, because of the following well-known fact: if  $\mathcal{X}$  reduces to  $\mathcal{Y}$ , and  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  is an extractor for  $\mathcal{Y}$ , then  $f$  is also an extractor for  $\mathcal{X}$ .

Thus, in order to show that low-degree polynomials extract from  $d$ -local sources, a key new ingredient we use is a reduction from  $d$ -local sources to a simpler class of sources called  *$d$ -local non-oblivious bit-fixing (NOBF) sources* [CGGL20]. Using the above discussion, it then suffices to show that low-degree polynomials extract from  $d$ -local NOBF sources. Thus, we proceed by:

1. Defining local NOBF sources, and showing how we can appropriately tailor our previous attempt at the probabilistic method so that it works for local NOBF sources.
2. Providing a new reduction from local sources to local NOBF sources.

**Low-degree extractors for local NOBF sources.** A  *$d$ -local NOBF source*  $\mathbf{X} \sim \{0, 1\}^n$  is a natural specialization of a  $d$ -local source where the entropic bits of the source must show up “in plain sight” somewhere in the source.<sup>6</sup> More formally, a  $d$ -local NOBF source with min-entropy  $k$  is a random variable  $\mathbf{X} \sim \{0, 1\}^n$  for which there exist functions  $g_1, \dots, g_n : \{0, 1\}^k \rightarrow \{0, 1\}$  such that the following holds: each  $g_i, i \in [n]$  depends on  $\leq d$  input bits; for every  $i \in [k]$  there is some  $i' \in [n]$  such that  $g_{i'}(y) = y_i$ ; and for uniform  $\mathbf{Y} \sim \{0, 1\}^k$  we have

$$\mathbf{X} = (g_1(\mathbf{Y}), g_2(\mathbf{Y}), \dots, g_n(\mathbf{Y})).$$

In other words, some  $k$  “good” bits in  $\mathbf{X}$  are uniform, and the remaining  $n - k$  “bad” bits are  $d$ -local functions of the good bits.

We must now show that a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  extracts from  $d$ -local NOBF sources with entropy  $k$ . As in our strawman application of the probabilistic method, consider an arbitrary  $d$ -local NOBF source  $\mathbf{X} = (g_1(\mathbf{Y}), \dots, g_n(\mathbf{Y}))$  and let  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  be a uniformly random degree  $\leq r$  polynomial. To show that  $f$  extracts from all  $d$ -local NOBF sources, recall that we just need to show that the function  $F : \{0, 1\}^k \rightarrow \{0, 1\}$  defined as

$$F(y) := (f \circ g)(y) = f(g_1(y), \dots, g_n(y))$$

has extremely low bias with extremely high probability. Furthermore, recall that if we can show that  $F$  itself is a uniformly random low-degree polynomial, then we know via [BHL12] that this is true.

It is still too much to hope that  $F$  is a uniform low-degree polynomial, but  $F$  is now “close enough in structure” to one so that we can make this work. To see why, we can first assume without loss of generality

<sup>5</sup>By this we mean that each  $\mathbf{X} \in \mathcal{X}$  can be written in the form  $\mathbf{X} = \sum_i p_i \mathbf{Y}_i$ , where each  $\mathbf{Y}_i \in \mathcal{Y}$ ,  $\sum_i p_i = 1$ , and  $\mathbf{X}$  samples from  $\mathbf{Y}_i$  with probability  $p_i$ .

<sup>6</sup>The relationship between local sources and local NOBF sources is not dissimilar to the relationship between error-correcting codes and *systematic* error-correcting codes.

(by definition of local NOBF source) that  $g_1(y) = y_1, \dots, g_k(y) = y_k$ . Thus, we can define  $c_S \sim \{0, 1\}$  as an independent uniform bit (for each  $S \subseteq [n]$  of size  $\leq r$ ) and write

$$F(y) = \sum_{S \subseteq [k]: |S| \leq r} c_S \prod_{i \in S} g_i(y) + \sum_{S \subseteq [n]: |S| \leq r, S \not\subseteq [k]} c_S \prod_{i \in S} g_i(y) = A(y) + B(y),$$

where  $A \in \mathbb{F}_2[y_1, \dots, y_k]$  is a uniformly random polynomial of degree  $\leq r$ , and  $B \in \mathbb{F}_2[y_1, \dots, y_k]$  is a random polynomial whose selection of monomials is *not uniformly random*, but is nevertheless *independent* of the selections made by  $A$ .

Thus, to show that  $F$  has extremely low bias, it suffices to show that  $A + B$  has extremely low bias. And to show that  $A + B$  has extremely low bias, it suffices to show that  $A + B'$  has low bias for any fixed polynomial  $B'$  induced by fixing the random monomials selected by  $B$ .

To conclude, we actually show something stronger: recalling that  $A \in \mathbb{F}_2[y_1, \dots, y_k]$  is a uniformly random polynomial of degree  $\leq r$ , we show that: for *any* fixed function  $B^* : \{0, 1\}^k \rightarrow \{0, 1\}$ , it holds that  $A + B^*$  has low bias. This does not follow immediately from the result [BHL12] that a random low-degree polynomial has low bias: indeed, it is more general, since [BHL12] is the special case where  $B^* = 0$ . However, it *does* follow immediately from known upper bounds on the list size of Reed-Muller codes [KLP12].

In the language we are using here, an upper bound on the list size of a Reed-Muller code is equivalent to saying that for any fixed function  $D \in \mathbb{F}_2[x_1, \dots, x_k]$ ,  $A$  will differ from  $D$  on many inputs, with very high probability. Thus, such bounds tell us that  $A$  differs from  $B^*$  on many inputs with very high probability, and  $A$  differs from  $1 + B^*$  (or rather, *equals*  $B^*$ ) on many inputs with very high probability. In other words,  $A$  is completely uncorrelated with  $B^*$ , meaning that  $\text{bias}(A + B^*)$  is extremely small, as desired.

Thus a random low-degree polynomial  $f$  extracts from the  $d$ -local NOBF source  $\mathbf{X}$  with min-entropy  $k$  with very high probability. In other words, it fails to do so with some very small probability  $\delta = \delta(k)$  which decreases rapidly as  $k$  grows. By applying the union bound, we get that  $f$  extracts from the entire family  $\mathcal{X}$  of  $d$ -local NOBF sources, provided  $\delta(k) \cdot |\mathcal{X}| \ll 1$ . All that remains is to upper bound the size of  $\mathcal{X}$ , which can easily be done using the  $d$ -locality of the sources.

**A reduction to local NOBF sources.** Above, we saw that random low-degree polynomials extract from *local NOBF sources*. To complete the proof that they also extract from more general *local sources*, recall that we need to provide a reduction from local sources to local NOBF sources. In other words, we need to show that every  $d$ -local source with min-entropy  $k$  is (close to) a convex combination of  $d$ -local NOBF sources with min-entropy  $k' \approx k$ . This is the main key ingredient in our result that low-degree polynomials extract from local sources ([Theorem 1.1](#)).

Our reduction works as follows. First, pick an arbitrary  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy  $k$ . Let  $k'$  be a parameter which is slightly smaller than  $k$ , which will be picked later. We start by arguing that  $\mathbf{X}$  is (close to) a convex combination of  $d$ -local NOBF sources where there are  $k'$  good bits, but the good bits may be biased (but not constant).

Towards this end, recall that  $\mathbf{X} = (g_1(\mathbf{Y}), \dots, g_n(\mathbf{Y}))$  for some  $d$ -local functions  $g_1, \dots, g_n : \{0, 1\}^m \rightarrow \{0, 1\}$  and uniform  $\mathbf{Y} \sim \{0, 1\}^m$ . The key idea is to consider the *largest possible set*  $T \subseteq [n]$  of “good bits,” i.e., such that  $\{\mathbf{X}_i\}_{i \in T}$  are independent (and none are constants). Then, we let  $T' \subseteq [m]$  be the bits of  $\mathbf{Y}$  on which  $\{\mathbf{X}_i\}_{i \in T}$  depend. The key observation is that *every* bit in  $\mathbf{X}$  depends on *some* bit in  $\{\mathbf{Y}_i\}_{i \in T'}$ , by the maximality of  $T$ . Using this observation, there are *two possible cases*, over which we perform a *win-win analysis*.

First, it is possible that  $T$  contains  $\geq k'$  bits. In this case, we consider fixing all bits  $\{\mathbf{Y}_i\}_{i \notin T'}$ . It is then not too hard to show that  $\mathbf{X}$  becomes a source which contains  $\geq k'$  good bits (which are mutually independent and not constants), and the remaining bad bits in  $\mathbf{X}$  are deterministic  $d$ -local functions of these good bits.<sup>7</sup> Thus in this case, we get that  $\mathbf{X}$  is a convex combination of NOBF sources of the desired type.

Second, it is possible that  $T$  contains  $< k'$  bits. In this case, we consider fixing all bits  $\{\mathbf{Y}_i\}_{i \in T'}$ . But since all bits in  $\mathbf{X}$  depend on *some* bit in this set, this fixing *decrements* the locality  $d \rightarrow d - 1$ . And furthermore, since this fixes  $|T'| \leq d|T| < dk'$  bits, the entropy only decreases from  $k \rightarrow k - dk'$  by the entropy chain rule. We then recurse until we hit the first case, or until we hit  $d = 1$ . If we eventually hit the first case, we already know that  $\mathbf{X}$  is a convex combination of NOBF sources of the desired type. On the other hand, it is easy to show that a 1-local source is actually a 1-local NOBF source! Thus we will always arrive at a (biased)  $d'$ -local NOBF source with  $d' \leq d$ , proving that  $\mathbf{X}$  is always convex combination of NOBF sources of the desired type. Depending on when this recursion stops, we will arrive at an NOBF source with the number of good bits equal to at least

$$\min\{k', k - dk', k - d(d-1)k', \dots, k - k' \prod_{i \in [d]} i\} \geq \min\{k', k - d^2 k'\},$$

which is always at least  $k'$  provided  $k' \leq \frac{k}{2d^2}$ .

Thus we see that any  $d$ -local source with min-entropy  $k$  can be written as a convex combination of  $d$ -local NOBF source with  $\Omega(k/d^2)$  good bits, where the good bits are mutually independent (and nonconstant), but they may be heavily biased. So all that remains is to show that such biased  $d$ -local NOBF sources can be written as a convex combination of *unbiased*  $d$ -local NOBF sources (as they were originally defined). This step is not difficult, by applying a standard Chernoff bound. However, since each good bit depends on up to  $d$  bits, each such good bit  $\mathbf{X}_i$  may have  $|\text{bias}(\mathbf{X}_i)| = 1 - 2 \cdot 2^{-d}$ . As a result, we end up with  $\Omega(\frac{k}{d^2 2^d})$  unbiased good bits.

This completes the reduction from local to local NOBF sources. Given our earlier proof sketch that low-degree polynomials extract from local NOBF sources, we finally get that low-degree polynomials also extract from local sources, as desired.

### 2.1.2 Low-degree dispersers for local sources

We now proceed to sketch the proof of [Remark 1](#), which shows that most degree  $\leq r$  polynomials are dispersers for  $d$ -local sources with min-entropy at least

$$k = O(d^3 r \cdot (n \log n)^{1/r}).$$

This improves our min-entropy requirement for extractors (which was  $k = O(2^d d^2 r \cdot (2^d n \log n)^{1/r})$ ) by removing two terms of the form  $2^d$ . We use a different key idea to remove each  $2^d$  term. While the outer exponential term  $2^d$  is the more dramatic one to remove, it turns out that it is also the easier one. To do this, we simply note that for dispersers, we can forego the last step in our local to local NOBF reduction, which incurs a factor of  $2^d$  by making the biased local NOBF source into an unbiased one. This improves the entropy requirement for dispersers from

$$k = O(2^d d^2 r \cdot (2^d n \log n)^{1/r}) \rightarrow k = O(d^2 r \cdot (2^d n \log n)^{1/r}).$$

---

<sup>7</sup>Technically, we need to fix a little more randomness to make this happen, but this can be done without much trouble by invoking some standard tricks from the extractor literature.

**Removing the inner exponential term.** Next, we focus on improving the entropy requirement for dispersers from

$$k = O(d^2 r \cdot (2^d n \log n)^{1/r}) \rightarrow k = O(d^3 r \cdot (n \log n)^{1/r}),$$

turning the inner exponential term  $2^d$  into an outer linear term  $d$ . This improvement is more challenging: while our first improvement relied on improving the local to local-NOBF reduction, this improvement relies on improving the entropy requirement for dispersing from local NOBF sources.

In order to show that low-degree polynomials extract from local NOBF sources, recall that we: (1) showed that a random low-degree polynomial extracts from an arbitrary local NOBF source with extremely high probability; and (2) used a union bound over the family  $\mathcal{X}$  of local NOBF sources to conclude that it extracts from *all* local NOBF sources with high probability. To get our second improvement on the min-entropy requirement for dispersers, we get improved upper bounds on the size of  $\mathcal{X}$ , so that our union bound is over fewer terms.

Towards this end, the key new idea is to show that in order to disperse from the family of  $d$ -local NOBF sources  $\mathcal{X}$ , it actually suffices to disperse from the much smaller family  $\mathcal{X}'$  of so-called  *$d$ -local, degree  $\leq r$  NOBF sources*.<sup>8</sup> This source family is the exact same as  $d$ -local NOBF sources, except it has the added restriction that the bad bits (which still depend on  $\leq d$  good bits each) can each be written as a degree  $\leq r$  polynomials. However, this family is significantly smaller: natural estimates on the sizes of  $\mathcal{X}, \mathcal{X}'$  give

$$\begin{aligned} |\mathcal{X}| &\leq \binom{n}{k} \cdot \left( \binom{k}{d} \cdot 2^{2^d} \right)^{n-k}, \\ |\mathcal{X}'| &\leq \binom{n}{k} \cdot \left( \binom{k}{d} \cdot 2^{\binom{d}{\leq r}} \right)^{n-k}. \end{aligned}$$

After plugging in these improved size bounds, it is straightforward calculation to see that the inner  $2^d$  term from the entropy requirement drops out. So all that remains is to show the above claim that a disperser for  $d$ -local, degree  $\leq r$  NOBF sources automatically works for the more general family of  $d$ -local NOBF sources.

The key ingredient that goes into this claim is a simple lemma on polynomial decomposition. We show the following: for any function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , any degree  $\leq r$  polynomials  $a_1, \dots, a_n : \{0, 1\}^k \rightarrow \{0, 1\}$ , and any polynomials  $b_1, \dots, b_n : \{0, 1\}^k \rightarrow \{0, 1\}$  that have no monomials of size  $\leq r$ , the following holds. There exists a polynomial  $h : \{0, 1\}^k \rightarrow \{0, 1\}$  with no monomials of size  $\leq r$  such that

$$f(a_1(y) + b_1(y), \dots, a_n(y) + b_n(y)) = f(a_1(y), \dots, a_n(y)) + h(y).$$

Then, given an arbitrary  $d$ -local NOBF source  $\mathbf{X} \sim \{0, 1\}^n$ , the idea is to write it in the form

$$\mathbf{X} = (a_1(\mathbf{Y}) + b_1(\mathbf{Y}), \dots, a_n(\mathbf{Y}) + b_n(\mathbf{Y})),$$

where  $\mathbf{Y} \sim \{0, 1\}^k$  is uniform and  $a_i, b_i$  are as before. Using our polynomial decomposition lemma, it then (roughly) holds that  $f$  is a disperser for  $\mathbf{X}$  if  $f$  is a disperser for the simpler class of  $d$ -local, degree  $\leq r$  NOBF sources. More precisely, we actually require from  $f$  a property that is ever-so-slightly stronger than being a disperser: we require that for any  $d$ -local, degree  $\leq r$  NOBF source  $\mathbf{X}' = (a_1(\mathbf{Y}), \dots, a_n(\mathbf{Y}))$ , it holds that the polynomial  $f(a_1, \dots, a_n)$  has a monomial of degree  $\leq r$ . Our polynomial decomposition lemma then guarantees that  $f$  will also have this property for the more general  $d$ -local source, since the

<sup>8</sup>Technically, we require something slightly stronger than dispersion from such sources, but this does not make a huge difference. We will go into more details below.

polynomial  $h$  in our decomposition lemma does not have any monomials of degree  $\leq r$ . Intuitively,  $h$  is not able to “destroy” the monomial of degree  $\leq r$  guaranteed to pop out of  $f(a_1(y), \dots, a_n(y))$ .

Thus, it suffices to “disperse” from  $d$ -local, degree  $\leq r$  NOBF sources in order to disperse from more general  $d$ -local NOBF sources, meaning that we can leverage our improved bound on the size of  $\mathcal{X}'$  to get our claimed improvement on the disperser’s entropy requirement.

## 2.2 Lower bounds

We now discuss our entropy lower bounds for low-degree extraction from local sources. By this, we mean that for every degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  we can find a  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  with relatively high min-entropy  $k$  on which  $f$  is constant. In other words, we show that in order to disperse (and thus extract) from  $d$ -local sources, they must have min-entropy exceeding this value  $k$ .

We show that every degree  $r \leq \Omega(\log n)$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  must admit a  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  of min-entropy at least

$$k = \Omega(r(dn \log n)^{1/r})$$

on which it is constant. That is, we sketch the proof of our lower bound ([Theorem 1.2](#)).

In order to prove this result, we actually prove a slightly stronger result: we show that we can find a  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  with the above parameters such that it is also *affine*.

Our starting point is a tight result of Cohen and Tal [[CT15](#)], which shows that any degree  $\leq r$  polynomial  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  admits a subspace  $V \subseteq \mathbb{F}_2^n$  of dimension  $\Omega(rn^{1/(r-1)})$  on which it is constant. Here, we obtain a (tight) “local” version of their result, and show that any degree  $\leq r$  polynomial  $f$  admits a  $d$ -local subspace  $X \subseteq \mathbb{F}_2^n$  of dimension  $k = \Omega(r(dn \log n)^{1/r})$  on which it is constant. Here, we say that  $V$  is *d-local* if  $V$  has a basis  $v_1, \dots, v_k \in \mathbb{F}_2^n$  such that for any index  $i \in [n]$ , at most  $d$  of these basis vectors equal 1 at this index. It is straightforward to verify that the uniform distribution  $\mathbf{X}$  over  $V$  is a  $d$ -local source with min-entropy  $k$ , so we focus now on proving the existence of such a  $V$ .

At a high level, the proof of Cohen and Tal proceeds by iteratively growing a subspace  $V$  on which  $f$  is constant. At each phase, they define a set  $A \subseteq \mathbb{F}_2^n$  such that  $f$  is constant over  $\text{span}(V, x)$  for every  $x \in A$ . They note that if  $|A|$  has size  $> 2^{\dim(V)}$ , then of course there is some  $x \in A \setminus V$  and furthermore we already know that  $f$  is constant on  $\text{span}(V, x)$ . Thus, they can grow their monochromatic subspace by one dimension.

In order to get a lower bound on  $|A|$ , they note that this set can be defined as the common solutions to a small collection of low-degree polynomials. A classical result known as the *Chevalley-Warning theorem* ([Theorem 11](#)) then shows that  $|A| \geq 2^{n-t}$ , where  $t$  is the sum of degrees across the collection of polynomials. To complete their proof, they grow their subspace  $V$  until they are no longer able to show  $|A| > 2^{\dim(V)}$ .

In our lower bound, we show that  $f$  is monochromatic on a *d-local subspace*. To prove this, we start with the same approach as Cohen and Tal. However, at each phase, we add extra constraints to  $A$  which guarantee the following: if we take any  $x \in A$  and add it to our current subspace  $V$  (with basis, say,  $v_1, \dots, v_{|\dim(V)|}$ ), then the location of the 1s appearing in vectors  $x, v_1, \dots, v_{|\dim(V)|}$  satisfy the  $d$ -locality constraint defined above. Again, as long as  $A$  is large enough, we can find some  $x \in A$  that grows the dimension of our  $d$ -local subspace.

In order to ensure that  $A$  remains large for as many iterations as possible, we would like to minimize the impact of the new “locality” constraints that we have added to  $A$ . Given the description of these constraints above, we observe that these constraints are minimized if we grow  $V$  by carefully selecting vectors that have the lowest possible Hamming weight. However, we now need an upper bound on the Hamming weight of

the lightest (nontrivial) common solution to a system of polynomial equations. Thus, our key new ingredient will be a result of this type, which we call a “low-weight Chevalley-Warning theorem.”

**A low-weight Chevalley-Warning theorem.** Above, we saw how the classical Chevalley-Warning theorem is critical in lower bounding the size of  $A$ , thereby showing that there is some (nontrivial) vector  $v \in A$  by which we can grow our monochromatic subspace. Now, we need an additional guarantee that there is such a  $v \in A$  that also has low Hamming weight. We prove such a result, and call it a *low-weight Chevalley-Warning theorem*. Our theorem roughly says the following. Given a collection  $\{f_i\}$  of polynomials that have cumulative degree  $D$  (and a common solution 0), if most of these polynomials have degree  $\leq 1$  then they admit a nontrivial solution of Hamming weight at most

$$w = O(D/\log(n/D)).$$

In order to prove our result, our key observation is that for any large enough subset  $A$  of common solutions to  $\{f_i\}$ , it holds that  $A + A$  also contains a (nontrivial) common solution to  $\{f_i\}$ . As it turns out, this observation follows quite readily from the CLP lemma [CLP17] - a result which was instrumental in the recent resolution of the cap set conjecture. Furthermore, given the above observation, we obtain an elementary proof of our low-weight Chevalley-Warning theorem, as follows. First, we let  $Q$  denote the set of common solutions to our collection of polynomials, and then:

1. We assume for contradiction that there is no nontrivial solution  $q \in Q$  of weight  $\leq w$ .
2. We use our key observation to conclude that every Hamming ball of radius  $w/2$  cannot have too many elements of  $Q$  in it, which implies that  $Q$  is a list-decodable code with small list size at radius  $w/2$ .
3. Using the list-decoding properties of  $Q$ , we use the Hamming bound (for list-decodable codes) to get an *upper bound* on its size.
4. Using the fact that  $Q$  holds the common solutions to a small set of low-degree polynomials, we use the classical Chevalley-Warning theorem to get a *lower bound* on its size.
5. We observe that the lower bound is greater than the upper bound, which yields a contradiction.

Equipped with our low-weight Chevalley-Warning theorem, our entropy lower bound for low-degree extraction from  $d$ -local affine spaces follows immediately via the proof sketch described above.

### 2.3 A barrier

To conclude our overview, we provide a proof sketch of our barrier result (**Theorem 0**), which shows that affine extractors (applied in a black-box manner) cannot extract from local sources with min-entropy  $k = \Omega(\sqrt{n})$ , even if the locality is 2. More formally, to show that an affine extractor also extracts from a different family  $\mathcal{Q}$  of distributions with min-entropy  $k$ , the standard technique is to show that each source  $\mathbf{Q} \in \mathcal{Q}$  with min-entropy  $k$  is (close to) a convex combination of affine sources with min-entropy slightly less than  $k$ . Here, we show that this is simply not possible for local sources with min-entropy  $\sqrt{n}$ . In particular, we show that there is a very simple 2-local source  $\mathbf{Q} \sim \{0, 1\}^n$  with min-entropy  $\Omega(\sqrt{n})$  that has statistical distance *exponentially close to 1* from any convex combination of affine sources with min-entropy  $k'$ .

In more detail, we consider the 2-local “clique” source  $\mathbf{Q} \sim \{0, 1\}^n$  defined as follows: first, pick any  $\ell \in \mathbb{N}$  and set  $n := \ell + \binom{\ell}{2}$ . Then, pick uniform and independent bits  $\mathbf{q}_1, \dots, \mathbf{q}_\ell \sim \{0, 1\}$  and set  $\mathbf{Q}$  to be

the concatenation of all  $\mathbf{q}_i$  over  $1 \leq i \leq n$  and  $\mathbf{q}_i \cdot \mathbf{q}_j$  over  $1 \leq i < j \leq \ell$ . Now, let  $\mathbf{X} \sim \{0, 1\}^n$  be a convex combination of affine sources, each with min-entropy  $\ell'$ . We argue that  $|\mathbf{Q} - \mathbf{X}| \geq 1 - 2^{-\Omega(\ell')}$  by showing that for any  $\ell'$ -dimensional affine  $\mathbb{F}_2$ -subspace  $S \subseteq \{0, 1\}^n$ , it holds that  $|\text{support}(\mathbf{Q}) \cap S|/|S| \leq 2^{-\Omega(\ell')}$ . That is, we wish to show that  $Q = \text{support}(\mathbf{Q})$  is *subspace-evasive*.

To show that cliques are subspace-evasive, we use the following key observation: For any nonempty set  $Q' \subseteq Q$  of cliques, the set  $Q' + Q' := \{u + v : u \in Q', v \in Q', u \neq v\}$  (where the sum is over  $\mathbb{F}_2^n$ ) has a ‘‘Sidon property:’’ each element  $x$  in  $Q' + Q'$  has a unique pair  $u, v \in Q'$  such that  $x = u + v$ . This observation is proven by noticing that by making another copy of each coordinate of the form  $\mathbf{q}_i \cdot \mathbf{q}_j$ , the set  $Q$  will correspond precisely to the symmetric rank-1 matrices of  $\mathbb{F}_2^{\ell \times \ell}$ . Thus all the elements in  $Q' + Q'$  would correspond to symmetric  $\mathbb{F}_2^{\ell \times \ell}$  matrices of rank at most 2. Hence by looking at the row space of  $x \in Q' + Q'$ , we can precisely find its symmetric rank-1 decomposition. That is, we can find  $u, v \in Q'$  such that  $x = u + v$ . Now, pick  $Q' = Q \cap S$ . Since addition is closed in  $S$ , we see that  $Q' + Q' \subseteq S$ . Thus  $|S| \geq |Q' + Q'| \geq \binom{|Q'|}{2} \geq \Omega(|Q \cap S|^2)$ . Hence we find that  $|Q \cap S|/|S| \leq O(\sqrt{|S|}/|S|) = O(1/\sqrt{|S|})$ , which is  $2^{-\Omega(\ell')}$  as  $|S| = 2^{\ell'}$ .

### 3 Preliminaries

We outline some basic notation, definitions, and facts that will be used throughout the paper.

#### 3.1 Notation

We let  $\mathbb{N} := \{1, 2, \dots\}$  denote the natural numbers, and for any  $n \in \mathbb{N}$ , we define  $[n] := \{1, 2, \dots, n\}$ . Throughout, we use  $\log$  to denote the base-2 logarithm, and we write  $\binom{n}{\leq r} := \sum_{i=0}^r \binom{n}{i}$ . For a bitstring  $x \in \{0, 1\}^n$ , we let  $x_i \in \{0, 1\}$  denote the bit it holds at coordinate  $i$ , and for a set  $S \subseteq [n]$  we let  $x_S \in \{0, 1\}^{|S|}$  denote the concatenation of bits  $x_i, i \in S$  in increasing order of  $i$ . On the other hand, we define  $x^S := \prod_{i \in S} x_i$ , and let  $x^\emptyset := 1$ .

We define the *support* of  $x \in \{0, 1\}^n$  as the set of coordinates  $i$  where  $x_i = 1$ .

For any  $n \in \mathbb{N}$ , we let  $0^n$  denote the string of  $n$  0s in a row, and we let  $1^n$  denote the string of  $n$  1s in a row. Given a set  $S \subseteq [n]$ , we write  $\bar{S}$  to denote its complement. We let  $\mathbb{F}_2$  denote the finite field of size 2, and we let  $\mathbb{F}_2^n$  denote the  $n$ -dimensional vector space over  $\mathbb{F}_2$ . Given sets  $A, B \subseteq \mathbb{F}_2^n$ , we let  $A + B$  denote the *sumset* of  $A$  and  $B$ :

$$A + B := \{a + b : a \in A, b \in B\}.$$

#### 3.2 Probability theory

We now overview some basic notions from (discrete) probability theory. First, random variables are denoted by boldface letters such as  $\mathbf{X}$ , and we let  $\text{support}(\mathbf{X})$  denote its support. For a set  $S$ , we write  $\mathbf{X} \sim S$  to denote that  $\mathbf{X}$  is supported on a subset of  $S$ . Next, the uniform distribution over  $\{0, 1\}^m$  is denoted by  $\mathbf{U}_m$ , and whenever  $\mathbf{U}_m$  appears multiple times in the same expression or formula, this represents multiple copies of the *same* random variable. For example, the random variable  $(\mathbf{U}_m, \mathbf{U}_m)$  hits each string  $(x, x) \in \{0, 1\}^m \times \{0, 1\}^m$  with probability  $2^{-m}$ .

Throughout, we will measure ‘‘randomness’’ of a random variable by its min-entropy:

**Definition 3** (Min-entropy). *The min-entropy of a random variable  $\mathbf{X}$  supported on a set  $S$ , denoted by  $H_\infty(\mathbf{X})$ , is defined as*

$$H_\infty(\mathbf{X}) = -\log \max_{x \in S} \Pr[\mathbf{X} = x].$$

The following lemma about min-entropy is not difficult to show, but is extremely useful.

**Lemma 1.** *Suppose  $\mathbf{X}$  and  $\mathbf{Y}$  are arbitrary random variables such that  $\mathbf{Y}$  is uniformly distributed over its support. Then, for every  $y \in \text{support}(\mathbf{Y})$ , it holds that*

$$H_\infty(\mathbf{X}|\mathbf{Y} = y) \geq H_\infty(\mathbf{X}) - \log |\text{support}(\mathbf{Y})|.$$

We measure the similarity of two random variables (or, rather, their distributions) via statistical distance.

**Definition 4** (Statistical distance). *The statistical distance between two random variables  $\mathbf{X}$  and  $\mathbf{Y}$  supported on a set  $S$ , denoted by  $\Delta(\mathbf{X}, \mathbf{Y})$ , is defined as*

$$\Delta(\mathbf{X}, \mathbf{Y}) = \max_{T \subseteq S} |\Pr[\mathbf{X} \in T] - \Pr[\mathbf{Y} \in T]| = \frac{1}{2} \sum_{s \in S} |\Pr[\mathbf{X} = s] - \Pr[\mathbf{Y} = s]|.$$

Moreover, we say  $\mathbf{X}, \mathbf{Y}$  are  $\varepsilon$ -close, denoted  $\mathbf{X} \approx_\varepsilon \mathbf{Y}$ , if  $\Delta(\mathbf{X}, \mathbf{Y}) \leq \varepsilon$ .

On the other hand, if  $\Delta(\mathbf{X}, \mathbf{Y}) \geq \varepsilon$ , we say that  $\mathbf{X}, \mathbf{Y}$  are  $\varepsilon$ -far.

Next, we say that  $\mathbf{X}$  is a *convex combination* of distributions  $\{\mathbf{Y}_i\}$  if there exist probabilities  $\{p_i\}$  summing to 1 such that  $\mathbf{X} = \sum_i p_i \mathbf{Y}_i$ , meaning that  $\mathbf{X}$  samples from  $\mathbf{Y}_i$  with probability  $p_i$ . The following standard fact about convex combinations is extremely useful in extractor research, and is straightforward to show.

**Fact 1.** *Let  $\text{Ext} : \{0, 1\}^n \rightarrow \{0, 1\}$  be an extractor for a family of distributions  $\mathcal{X}$  over  $\{0, 1\}^n$  with error  $\varepsilon$ . Then  $\text{Ext}$  also extracts with error  $\varepsilon$  from any  $\mathbf{X}$  which is a convex combination of distributions from  $\mathcal{X}$ .*

For the easier setting of dispersers, it is easy to show something even stronger than the above fact.

**Fact 2.** *Let  $\text{Disp} : \{0, 1\}^n \rightarrow \{0, 1\}$  be a disperser for a family of distributions  $\mathcal{X}$  over  $\{0, 1\}^n$ . Then  $\text{Disp}$  is also a disperser for any  $\mathbf{X}$  whose support contains the support of some  $\mathbf{X}' \in \mathcal{X}$ .*

Finally, we will make use of the following standard concentration bound.

**Lemma 2** (Chernoff bound, lower tail). *Let  $\mathbf{X}_1, \dots, \mathbf{X}_n$  be independent random variables over  $\{0, 1\}$ , and define  $\mathbf{Z} := \sum_{i \in [n]} \mathbf{X}_i$ . Then for every  $0 < \delta < 1$ , it holds that*

$$\Pr[\mathbf{Z} \leq (1 - \delta) \cdot \mathbb{E}[\mathbf{Z}]] \leq e^{-\mathbb{E}[\mathbf{Z}] \cdot \delta^2 / 2}.$$

### 3.3 Coding theory

We will now review some basics of coding theory, which will be used in both our entropy upper bounds and lower bounds. First, given a string  $v \in \{0, 1\}^n$ , we let  $\Delta(v) := \{i \in [n] : v_i = 1\}$  denote its *Hamming weight*, and for any strings  $u, v \in \{0, 1\}^n$ , we let  $\Delta(u, v) := \{i \in [n] : u_i \neq v_i\}$  denote their *Hamming distance*. Then, given any string  $v \in \{0, 1\}^n$  and integer  $r \in \{0, 1, \dots, n\}$ , we let

$$\mathcal{B}(v, r) := \{v' \in \{0, 1\}^n : \Delta(v, v') \leq r\}$$

denote the (closed) Hamming ball of radius  $r$  around (i.e., centered at)  $v$ . If we replace the inequality “ $\leq$ ” above with a strict inequality “ $<$ ”, we call this object the *open* Hamming ball of radius  $r$  around  $v$ , and

denote it by  $\mathcal{B}^-(v, r)$ . Notice that the closed Hamming ball has size  $\binom{n}{\leq r}$ , whereas the open Hamming ball has size  $\binom{n}{\leq r-1}$ .

An  $(n, k, d)$  code is a subset  $Q \subseteq \{0, 1\}^n$  of size  $2^k$  such that the pairwise Hamming distance between any distinct  $x, y \in Q$  is at least  $d$ . We call an  $(n, k, d)$  code  $Q \subseteq \{0, 1\}^n$  *linear* if it is an  $\mathbb{F}_2$ -linear subspace, and subsequently call it an  $[n, k, d]$  code.

A standard relaxation of  $(n, k, d)$  codes are *list-decodable codes*. We say that a subset  $Q \subseteq \{0, 1\}^n$  is a  $(\rho, L)$  list-decodable code if every Hamming ball of radius at most  $\rho n$  contains at most  $L$  codewords (i.e., elements of  $Q$ ). The following classical bound places a limit on the tradeoff between the size and list-decodability of arbitrary codes.

**Theorem 1** (Hamming bound for list-decodable codes). *For any  $(\rho, L)$ -list-decodable code  $Q \subseteq \{0, 1\}^n$ ,*

$$|Q| \leq \frac{2^n L}{\binom{n}{\leq \rho n}}.$$

*Proof.* Consider the quantity  $\sum_{q \in Q} |\mathcal{B}(q, \rho n)|$ . Notice that for any fixed  $v \in \{0, 1\}^n$ , there are at most  $L$  codewords  $q \in Q$  such that  $v \in \mathcal{B}(q, \rho n)$ , because otherwise  $|\mathcal{B}(v, \rho n) \cap Q| > L$ , contradicting the list-decodability of  $Q$ . Thus

$$|Q| \cdot \binom{n}{\leq \rho n} = \sum_{q \in Q} |\mathcal{B}(q, \rho n)| \leq \sum_{v \in \{0, 1\}^n} L \leq 2^n L,$$

and the inequality follows. □

Finally, a classic linear code that will be used in this paper is the *Reed-Muller code*, defined below.

**Definition 5.** *The Reed-Muller code  $\text{RM}(m, r)$  is the subset  $Q \subseteq \mathbb{F}_2^{2^m}$  defined as follows:*

$$Q := \{(p(\alpha))_{\alpha \in \mathbb{F}_2^m} : p \text{ is a multilinear polynomial of degree } \leq r.\}$$

*It is a  $[2^m, \binom{m}{\leq r}, 2^{m-r}]$  linear code.*

### 3.4 Boolean functions and $\mathbb{F}_2$ -polynomials

We now review some standard definitions and facts about boolean functions and  $\mathbb{F}_2$ -polynomials, which will be used throughout the paper. First, every function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  has a unique representation as a multilinear  $\mathbb{F}_2$ -polynomial. This means that there exist (unique) coefficients  $\{c_S\}_{S \subseteq [n]}$ , each from  $\mathbb{F}_2$ , so that

$$f(x) = \sum_{S \subseteq [n]} c_S x^S.$$

The *degree* of  $f$ , denoted  $\deg(f)$ , is the size of the largest  $S$  such that  $c_S = 1$ , and we say that  $\deg(f) = -\infty$  if all  $c_S = 0$ . A *random degree  $\leq r$  polynomial* (independently) sets each  $c_S$  to 1 with probability  $1/2$  if  $|S| \leq r$ , and otherwise sets  $c_S = 0$ . We often do not distinguish between a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  and its natural interpretation as a function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ , nor do we distinguish between a function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  and its unique representation as a multilinear  $\mathbb{F}_2$ -polynomial. This allows us to slightly abuse language, and gives meaning to phrases like “the degree of  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ .”

Next, we let  $\mathbb{F}_2[x_1, \dots, x_n]$  denote the set of (multilinear)  $\mathbb{F}_2$ -polynomials, and we let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  refer to a set (of unspecified size) of such polynomials. The *linear degree* of  $\{f_i\}$  is the sum of the degrees of the  $f_i$ 's which have degree 1, the *nonlinear degree* of  $\{f_i\}$  is the sum of the degrees of the  $f_i$ 's which have degree  $> 1$ , and the *degree* of  $\{f_i\}$  is the sum of the degrees of all the  $f_i$ 's. We say that  $x$  is a *common solution* to  $\{f_i\}$  if  $f_i(x) = 0$  for all  $i$ , and we say that  $x$  is *nontrivial* if  $x \neq 0$ .

The notion of *bias* and *correlation* of boolean functions will be important for our entropy upper bounds. Given arbitrary functions  $f, g : \{0, 1\}^n \rightarrow \{0, 1\}$ , we define their *correlation* as

$$\text{corr}(f, g) := |\mathbb{E}_{x \sim \{0, 1\}^n} [(-1)^{f(x)+g(x)}]| = |\Pr[f(x) = g(x)] - \Pr[f(x) \neq g(x)]|,$$

and we define the *bias* of  $f$  as

$$\text{bias}(f) := |\mathbb{E}_{x \sim \{0, 1\}^n} [(-1)^{f(x)}]| = |\Pr[f(x) = 0] - \Pr[f(x) = 1]|.$$

Observe that  $\text{bias}(f) = \text{corr}(f, 0)$ .

To conclude this section, we record some notation about function combination and composition. For any two functions  $a, b : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ , we let  $a + b : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  denote the function  $(a + b)(x) := a(x) + b(x)$ , and we let  $ab : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  denote the function  $ab(x) := a(x)b(x)$ . For any functions  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  and  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ , we let  $f(a_1, \dots, a_n) : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  denote the function  $f(a_1, \dots, a_n)(x) := f(a_1(x), \dots, a_n(x))$ . Finally, given functions  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  and  $S \subseteq [n]$ , we defined  $a^S : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  as  $a^S := \prod_{i \in S} a_i$ , and we let  $a^\emptyset := 1$ .

## 4 Entropy upper bounds

In this section, we obtain upper bounds on the entropy required to extract from  $d$ -local sources using degree  $\leq r$  polynomials, proving the following theorem.

**Theorem 2 (Theorem 1.1, restated).** *There are universal constants  $C, c > 0$  such that for all  $n, d, r \in \mathbb{N}$ , the following holds. With probability at least 0.99 over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , it holds that  $f$  is an  $\varepsilon$ -extractor for  $d$ -local sources with min-entropy  $\geq k$  and error  $\varepsilon = 2^{-\frac{ck}{r^3 2^{d^2}}}$ , as long as*

$$k \geq C 2^d d^2 r \cdot (2^d n \log n)^{1/r}.$$

In order to prove **Theorem 2**, we combine two key ingredients. Our first key ingredient reduces  $d$ -local sources to the more specialized family of  $d$ -local NOBF sources:

**Theorem 3 (Theorem 2, restated).** *There exists a universal constant  $c > 0$  such that for any  $n, k, d \in \mathbb{N}$ , the following holds. Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $\geq k$ . Then  $\mathbf{X}$  is  $\varepsilon$ -close to a convex combination of  $d$ -local NOBF sources with min-entropy  $\geq k'$ , where  $\varepsilon = 2^{-ck'}$  and*

$$k' = \frac{ck}{2^d d^2}.$$

Our second key ingredient gives upper bounds on the entropy required to extract from  $d$ -local NOBF sources using degree  $\leq r$  polynomials:

**Theorem 4.** *There are universal constants  $C, c > 0$  such that for all  $n, d, r \in \mathbb{N}$ , the following holds. With probability at least 0.99 over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , it holds that  $f$  is an  $\varepsilon$ -extractor for  $d$ -local NOBF sources of min-entropy  $\geq k$  with error  $\varepsilon = 2^{-ck/r^3}$ , as long as*

$$k \geq Cr \cdot (2^d \cdot n \log n)^{1/r}.$$

Recall that if an extractor works for a family  $\mathcal{X}$  of sources over  $\{0, 1\}^n$ , then it also works for any  $\mathbf{X} \sim \{0, 1\}^n$  which is a convex combination of sources from  $\mathcal{X}$  (**Fact 1**). As a result, by combining **Theorems 3** and **4**, we immediately get **Theorem 2**. Thus, in the remainder of this section, we just focus on proving **Theorems 3** and **4**. We prove **Theorem 3** in **Section 4.1**, and we prove **Theorem 4** in **Section 4.2**. We conclude the section in **Section 4.3**, where we show that **Theorem 2** can be optimized for the easier setting of *dispersers*, allowing us to obtain a formal version of **Remark 1**.

#### 4.1 A reduction from $d$ -local sources to $d$ -local NOBF sources

We start by proving our reduction, **Theorem 3**. In order to reduce  $d$ -local sources to  $d$ -local NOBF sources, we use an intermediate model called *biased  $d$ -local NOBF sources*.

**Definition 6.** A random variable  $\mathbf{X} \sim \{0, 1\}^n$  is a  $(\delta, k)$ -biased  $d$ -local NOBF source if there exists a set  $S \subseteq [n]$  of size  $k$  such that both of the following hold:

- The bits in  $\mathbf{X}_S$  are mutually independent (but need not be identically distributed), and each  $\mathbf{X}_i, i \in S$  has bias  $|\Pr[\mathbf{X}_i = 1] - \Pr[\mathbf{X}_i = 0]| \leq \delta$ .
- Every other bit  $\mathbf{X}_j, j \notin S$  is a deterministic function of at most  $d$  bits in  $\mathbf{X}_S$ .

Notice that this intermediate model generalizes  $d$ -local NOBF sources of min-entropy  $k$ , which are just  $(0, k)$ -biased  $d$ -local NOBF sources. Now, given this intermediate model, we prove **Theorem 3** by combining two lemmas.

The first lemma reduces  $d$ -local sources to biased  $d$ -local NOBF sources.

**Lemma 3** (Reduction, Part 1). Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $\geq k$ . Then  $\mathbf{X}$  is a convex combination of  $(\delta, k')$ -biased  $d$ -local NOBF sources, where  $\delta \leq 1 - 2^{-d}$  and  $k' \geq k/(2d^2)$ .

The second lemma reduces biased  $d$ -local NOBF sources to (unbiased)  $d$ -local NOBF sources.

**Lemma 4** (Reduction, Part 2). Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $(\delta, k)$ -biased  $d$ -local NOBF source. Then  $\mathbf{X}$  is  $\varepsilon$ -close to a convex combination of  $(0, k')$ -biased  $d$ -local NOBF sources, where  $k' \geq (1 - \delta)k/4$  and  $\varepsilon = 2^{-(1 - \delta)k/4}$ .

By combining these two lemmas, **Theorem 3** follows immediately. Thus, all that remains in the proof of our reduction (**Theorem 3**) is to prove **Lemmas 3** and **4**, which we do in **Sections 4.1.1** and **4.1.2**, respectively.

##### 4.1.1 A reduction from $d$ -local sources to biased $d$ -local NOBF sources

We now prove the first part of our reduction (**Lemma 3**), which shows that every  $d$ -local source is a convex combination of biased  $d$ -local NOBF sources.

*Proof of Lemma 3.* Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $\geq k$ . We wish to show that  $\mathbf{X}$  is a convex combination of  $(\delta, k')$ -biased  $d$ -local NOBF sources, where  $\delta \leq 1 - 2^{-d}$  and  $k' \geq k/(2d^2)$ .

The key observation that we will prove is that for any  $t$ , one of the following *must* hold: either

- $\mathbf{X}$  is a convex combination of  $(\delta, t)$ -biased  $d$ -local NOBF sources, for  $\delta \leq 1 - 2^{-d}$ ; or
- $\mathbf{X}$  is a convex combination of  $(d - 1)$ -local sources with min-entropy  $> k - td$ .

Before we prove this key observation, let us see how we can use it to prove the desired result. First, recall that convex combinations “stack” in the following sense: if a source  $\mathbf{X}$  is a convex combination of convex combinations of sources from a family  $\mathcal{X}$ , then  $\mathbf{X}$  is just a convex combination of sources from  $\mathcal{X}$ . Thus, by repeatedly applying the key observation until either the first item becomes true or we arrive at a 1-local source (the “base case”), we see that  $\mathbf{X}$  is a convex combination of sources  $\{\mathbf{Z}_i\}$ , where each  $\mathbf{Z}_i$  is either:

- A  $(\delta, t)$ -biased  $d$ -local NOBF source, for  $\delta \leq 1 - 2^{-d}$ ; or
- A 1-local source with min-entropy  $> k - t \cdot (d + (d - 1) + \dots + 2) = k - t \cdot (d^2 + d - 2)$ .

However, it is clear from the definitions that a 1-local source with min-entropy  $k'$  is a 1-local NOBF source with min-entropy  $k'$ . Furthermore, it is easy to see that a 1-local NOBF source with min-entropy  $\geq k'$  is a convex combination of 1-local NOBF sources with min-entropy exactly  $k'$ , by fixing any additional random “good” bits. Thus, for any  $t \leq k'$ , we know that a 1-local source with min-entropy  $\geq k'$  is a convex combination of  $(\delta, t)$ -biased  $d$ -local NOBF sources, for  $\delta \leq 1 - 2^{-d}$ .

By the above discussion, we see that for any  $t \leq k - t \cdot (d^2 + d - 2)$ ,  $\mathbf{X}$  is a convex combination of  $(\delta, t)$ -biased  $d$ -local NOBF sources, where  $\delta \leq 1 - 2^{-d}$ . Setting  $t = \frac{k}{2d^2}$  yields the result.

Thus, all that remains is to prove the key observation stated at the beginning of the proof. Towards this end, let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $\geq k$ . By definition of  $d$ -local source, there exists some  $\ell$  and  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}^n$  such that  $\mathbf{X} = f(\mathbf{Y})$  for uniform  $\mathbf{Y} \sim \mathbf{U}_\ell$ , such that each bit  $\mathbf{X}_i$  is a deterministic function of at most  $d$  bits in  $\mathbf{Y}$ . In other words, there exist sets  $S_1, \dots, S_n \subseteq [\ell]$  of size  $d$  and functions  $f_1, \dots, f_n : \{0, 1\}^d \rightarrow \{0, 1\}$  such that

$$\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_n) = (f_1(\mathbf{Y}_{S_1}), f_2(\mathbf{Y}_{S_2}), \dots, f_n(\mathbf{Y}_{S_n})).$$

Now, let  $T \subseteq [n]$  be any set of coordinates of *maximal size* such that:

- $H_\infty(\mathbf{X}_i) > 0$  for all  $i \in T$ ; and
- $S_i \cap S_j = \emptyset$  for any distinct  $i, j \in T$ .

Suppose  $T$  has size  $\tau$ . Without loss of generality, assume  $T = [\tau]$ . We conclude with two cases.

**Case (i):**  $\tau < t$ . In this case, we fix the random variable  $\mathbf{Y}_{S_1}, \dots, \mathbf{Y}_{S_\tau}$ . We know that with probability 1 over this fixing, all bits  $\mathbf{X}_i, i \in [n]$  become deterministic functions of at most  $d - 1$  unfixed variables in  $\mathbf{Y}$ , by the maximality of  $T$  and its intersection property. In other words,  $\mathbf{X}$  becomes a  $(d - 1)$ -local source. Furthermore, by [Lemma 1](#), we know that with probability 1 over this fixing,  $\mathbf{X}$  loses  $\sum_{i \in [\tau]} |S_i| = d\tau < dt$  bits of min-entropy. Thus in this case,  $\mathbf{X}$  is a convex combination of  $(d - 1)$ -local sources of min-entropy  $> k - dt$ .

**Case (ii):**  $\tau \geq t$ . In this case, define  $\bar{S} := [n] - (\bigcup_{i \in [\tau]} S_i)$  and notice that  $S_1, S_2, \dots, S_\tau, \bar{S}$  partition the coordinates of  $\mathbf{Y}$ . Next, define the random variables  $\mathbf{Z}_i := \mathbf{Y}_{S_i}$  for each  $i \in [\tau]$ , and define  $\bar{\mathbf{Z}} := \mathbf{Y}_{\bar{S}}$ . Notice that  $\mathbf{X}_i = f_i(\mathbf{Z}_i)$  for each  $i \in [\tau]$ . Furthermore, it is straightforward to verify that for all  $j > \tau$ , there exists a set  $Q_j \subseteq [\tau]$  of size at most  $d$  and a deterministic function  $f'_j$  such that  $\mathbf{X}_j = f'_j(\mathbf{Z}_{Q_j}, \bar{\mathbf{Z}})$ . In other words, we can rewrite  $\mathbf{X}$  as

$$\begin{aligned} \mathbf{X} &= (\mathbf{X}_1, \dots, \mathbf{X}_\tau, \mathbf{X}_{\tau+1}, \dots, \mathbf{X}_n) \\ &= (f_1(\mathbf{Z}_1), \dots, f_\tau(\mathbf{Z}_\tau), f'_{\tau+1}(\mathbf{Z}_{Q_{\tau+1}}, \bar{\mathbf{Z}}), \dots, f'_n(\mathbf{Z}_{Q_n}, \bar{\mathbf{Z}})). \end{aligned}$$

Now, for each  $i \in [\tau]$ , define  $\mathbf{A}_i := f_i(\mathbf{Z}_i)$ . Furthermore, it is straightforward to show that we can define a new random variable  $\mathbf{B}$  independent of  $\mathbf{Y}$ , and for each  $i \in [\tau]$  a deterministic function  $g_i$  such that

$g_i(\mathbf{A}_i, \mathbf{B}) = \mathbf{Z}_i$  for all  $i \in [\tau]$ . Thus, for any subset  $Q \subseteq [\tau]$  we have  $\mathbf{Z}_Q = g'_Q(\mathbf{A}_Q, \mathbf{B})$  for some deterministic function  $g'_Q$ . And finally, for each  $j > \tau$  there must be some deterministic function  $\psi_j$  such that

$$f'_j(\mathbf{Z}_{Q_j}, \bar{\mathbf{Z}}) = \psi_j(\mathbf{A}_{Q_j}, \mathbf{B}, \bar{\mathbf{Z}}).$$

Thus we can rewrite  $\mathbf{X}$  as:

$$\mathbf{X} = (\mathbf{A}_1, \dots, \mathbf{A}_\tau, \psi_{\tau+1}(\mathbf{A}_{Q_{\tau+1}}, \mathbf{B}, \bar{\mathbf{Z}}), \dots, \psi_n(\mathbf{A}_{Q_n}, \mathbf{B}, \bar{\mathbf{Z}})).$$

Notice that the collection  $\{\mathbf{A}_i\}_{i \in [\tau]}$  are mutually independent, and each has bias at most  $1 - 2^{-d}$  since it is a non-constant deterministic function of  $d$  uniform bits. Thus no matter how  $\mathbf{B}, \bar{\mathbf{Z}}$  are fixed,  $\mathbf{X}$  becomes a  $(\delta, t)$ -biased  $d$ -local NOBF source, for  $\delta \leq 1 - 2^{-d}$ .  $\square$

#### 4.1.2 A reduction from biased $d$ -local NOBF sources to (unbiased) $d$ -local NOBF sources

We now prove the second part of our reduction ([Lemma 4](#)), which shows that every biased  $d$ -local NOBF source is (close to) a convex combination of (unbiased)  $d$ -local NOBF sources.

*Proof of Lemma 4.* Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $(\delta, k)$ -biased  $d$ -local NOBF source. We wish to show that  $\mathbf{X}$  is  $\varepsilon$ -close to a convex combination of  $(0, k')$ -biased  $d$ -local NOBF sources, where  $k' \geq (1 - \delta)k/4$  and  $\varepsilon = 2^{-(1-\delta)k/4}$ .

Without loss of generality, assume that the first  $k$  bits in  $\mathbf{X}$  are the ‘‘good bits’’: that is, there exist  $d$ -local functions  $g_{k+1}, \dots, g_n : \{0, 1\}^k \rightarrow \{0, 1\}$  such that

$$\mathbf{X} = (\mathbf{X}_1, \dots, \mathbf{X}_k, g_{k+1}(\mathbf{X}_1, \dots, \mathbf{X}_k), \dots, g_n(\mathbf{X}_1, \dots, \mathbf{X}_k)),$$

where each  $\mathbf{X}_i$  is independent and has bias at most  $\delta$ . To remove the bias from this source, the key idea will be to simulate each  $\mathbf{X}_i$  by two independent coins: one which is biased, and one which is not.

In more detail, for every  $i \in [k]$  we construct a pair of independent random variables  $\mathbf{B}_i, \mathbf{A}_i \sim \{0, 1\}$  as follows. First, let  $\gamma_i \in \{0, 1\}$  be the value favored by  $\mathbf{X}_i$ , breaking ties arbitrarily. Then, define  $p_i := \Pr[\mathbf{X}_i = \gamma_i]$ , and notice that  $\frac{1}{2} \leq p_i \leq \frac{1+\delta}{2}$ , where the lower bound holds because  $\mathbf{X}_i$  favors  $\gamma_i$  over  $1 - \gamma_i$ , and the upper bound holds because the good bits have bias at most  $\delta$ . Next, define  $\mathbf{B}_i$  such that

$$\begin{aligned} \Pr[\mathbf{B}_i = 0] &= 2p_i - 1, \\ \Pr[\mathbf{B}_i = 1] &= 2 - 2p_i. \end{aligned}$$

Finally, let  $\mathbf{A}_i \sim \{0, 1\}$  simply be a uniform bit, and define the function  $h_i : \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$  as

$$h_i(b, a) := \begin{cases} \gamma_i & \text{if } b = 0, \\ a & \text{if } b = 1. \end{cases}$$

Given these definitions, it is straightforward to verify that  $\mathbf{X}_i$  has the same distribution as  $h_i(\mathbf{B}_i, \mathbf{A}_i)$ , and thus we may rewrite  $\mathbf{X}$  as

$$(h_1(\mathbf{B}_1, \mathbf{A}_1), \dots, h_k(\mathbf{B}_k, \mathbf{A}_k), g_{k+1}(h_1(\mathbf{B}_1, \mathbf{A}_1), \dots, h_k(\mathbf{B}_k, \mathbf{A}_k)), \dots, g_n(h_1(\mathbf{B}_1, \mathbf{A}_1), \dots, h_k(\mathbf{B}_k, \mathbf{A}_k))).$$

Now, define the random variable  $\mathbf{B} = (\mathbf{B}_1, \dots, \mathbf{B}_k)$ . Given the above description of  $\mathbf{X}$ , it is not too difficult to see that for any  $b \in \{0, 1\}^k$ , the conditional distribution  $(\mathbf{X} \mid \mathbf{B} = b)$  is a  $d$ -local (unbiased)

NOBF source, which has min-entropy equal to the Hamming weight of  $\mathbf{b}$ . Thus, we may write  $\mathbf{X}$  as the convex combination

$$\mathbf{X} = \sum_{\mathbf{b} \in \{0,1\}^k} \Pr[\mathbf{B} = \mathbf{b}] \cdot (\mathbf{X} \mid \mathbf{B} = \mathbf{b}).$$

This means that if  $\mathbf{B}$  has Hamming weight  $\geq k'$  with probability  $\geq 1 - \varepsilon$ , then  $\mathbf{X}$  is  $\varepsilon$ -close to a convex combination of  $d$ -local NOBF sources with min-entropy  $\geq k'$ . Such a claim will follow almost immediately from a Chernoff bound.

In more detail, define a random variable  $\mathbf{Z} := \sum_{i \in [k]} \mathbf{B}_i$  and notice that the value of  $\mathbf{Z}$  is exactly the Hamming weight of  $\mathbf{B}$ . Furthermore, recall that  $\mathbf{B}_i = 1$  with probability  $2 - 2p_i$  for some  $p_i \in [\frac{1}{2}, \frac{1+\delta}{2}]$ . Thus

$$\mu := \mathbb{E}[\mathbf{Z}] = \sum_{i \in [k]} \mathbb{E}[\mathbf{B}_i] \geq k \cdot (2 - 2 \cdot ((1 + \delta)/2)) = (1 - \delta)k.$$

Thus, by a standard Chernoff bound on the lower tail ([Lemma 2](#)), we get that

$$\Pr[\mathbf{Z} \leq \mu/4] \leq e^{-\mu \cdot (3/4)^2/2} \leq 2^{-\mu/4},$$

which means that  $\mathbf{B}$  has Hamming weight  $\geq \mu/4$  with probability  $\geq 1 - 2^{-\mu/4}$ . Thus,  $\mathbf{X}$  is  $2^{-\mu/4}$ -close to a convex combination of  $d$ -local NOBF sources with min-entropy  $\geq \mu/4$ , as desired.  $\square$

## 4.2 Low-degree polynomials extract from $d$ -local NOBF sources

Now that we have proven our reduction from  $d$ -local sources to  $d$ -local NOBF sources ([Theorem 3](#)), all that remains is to prove an upper bound on the entropy required to extract from  $d$ -local NOBF sources using degree  $\leq r$  polynomials ([Theorem 4](#)). In this section, we prove [Theorem 4](#).

In order to prove [Theorem 4](#), our main tool will be the following lemma, which shows that for *any* fixed NOBF source, a random low-degree polynomial can extract from it with very high probability.

**Lemma 5.** *There is a universal constant  $c > 0$  such that for any  $r \leq ck^{1/4}$ , the following holds. Let  $\mathbf{X} \sim \{0,1\}^n$  be an NOBF source with min-entropy  $k$ , and let  $f : \{0,1\}^n \rightarrow \{0,1\}$  be a random  $\mathbb{F}_2$ -polynomial of degree  $\leq r$ . Then*

$$\Pr_f[f \text{ is an extractor for } \mathbf{X} \text{ with error } \varepsilon = 2^{-ck/r^3}] \geq 1 - 2^{-c\binom{k}{\leq r}}$$

Before we prove this lemma, we show how it can be used to prove [Theorem 4](#). The proof is a straightforward application of the probabilistic method, which combines [Lemma 5](#) with a basic upper bound on the number of  $d$ -local NOBF sources over  $\{0,1\}^n$  with min-entropy  $k$ .

*Proof of [Theorem 4](#).* Let  $\mathcal{X}$  be the family of  $d$ -local NOBF sources over  $\{0,1\}^n$  with min-entropy  $k$ . Notice

$$|\mathcal{X}| \leq \binom{n}{k} \cdot \left( \binom{k}{d} \cdot 2^{2d} \right)^{n-k}.$$

By [Lemma 5](#), a random degree  $\leq r$  polynomial  $f : \{0,1\}^n \rightarrow \{0,1\}$  fails to extract from any fixed NOBF source of min-entropy  $k$  with error  $\varepsilon = 2^{-ck/r^3}$  with probability at most  $2^{-c\binom{k}{\leq r}}$ . Thus, a union bound

shows that a random degree  $\leq r$  polynomial  $f$  extracts from all sources in  $\mathcal{X}$  with error  $\varepsilon = 2^{-ck/r^3}$  with probability at least 0.99 (over the selection of  $f$ ) as long as

$$|\mathcal{X}| \cdot 2^{-c\binom{k}{\leq r}} \leq \binom{n}{k} \cdot \left( \binom{k}{d} \cdot 2^{2^d} \right)^{n-k} \cdot 2^{-c\binom{k}{\leq r}} \leq 0.01,$$

which is true if

$$k \geq Cr \cdot (2^d \cdot n \log n)^{1/r}$$

for a large enough constant  $C$ . □

Now, all that remains is to prove [Lemma 5](#), which says that for any fixed NOBF source, a random low-degree polynomial can extract from it. In order to prove this result, our main tool will be following, which shows that for any fixed function  $g$ , a random low-degree polynomial  $f$  has very low correlation with it.

**Lemma 6.** *There is a universal constant  $c > 0$  such that for any fixed  $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ , the following holds. For any  $1 \leq r \leq cn^{1/4}$ , let  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  be a random degree  $\leq r$  polynomial. Then*

$$\Pr[\text{corr}(f, g) > 2^{-cn/r^3}] \leq 2^{-c\binom{n}{\leq r}}.$$

Before we prove these correlation bounds ([Lemma 6](#)), we show how they can be used to show that for any fixed NOBF source, a random low-degree polynomial can extract from it ([Lemma 5](#)). Then, we conclude the section in [Section 4.2.1](#) by proving [Lemma 6](#).

*Proof of Lemma 5.* The proof is via the probabilistic method over the selection of  $f$ . In more detail, let  $\mathbf{X} \sim \{0, 1\}^n$  be an arbitrary NOBF source with min-entropy  $k$ , and let  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  be a random  $\mathbb{F}_2$ -polynomial of degree  $\leq r$ . Assume (without loss of generality) that  $\mathbf{X}_1, \dots, \mathbf{X}_k$  are the “good bits” in the NOBF source.

Now, let  $f'$  be the (sum of the) monomials in  $f$  that do not use any variables outside  $\mathbf{X}_1, \dots, \mathbf{X}_k$ , and let  $g$  be the (sum of the) monomials in  $f$  that use at least one variable outside  $\mathbf{X}_1, \dots, \mathbf{X}_k$ . This gives us  $f(\mathbf{X}) = f'(\mathbf{X}) + g(\mathbf{X})$ , where  $f'$  is a random degree  $\leq r$  polynomial over  $\mathbf{X}_1, \dots, \mathbf{X}_k$ , and  $g$  is an (independent) random polynomial over  $\mathbf{X}_1, \dots, \mathbf{X}_n$ . By definition of NOBF source, each of the bits  $\mathbf{X}_{k+1}, \dots, \mathbf{X}_n$  is a deterministic function of the good bits  $\mathbf{X}_1, \dots, \mathbf{X}_k$ , and thus we have

$$f(\mathbf{X}) = f'(\mathbf{X}_1, \dots, \mathbf{X}_k) + g'(\mathbf{X}_1, \dots, \mathbf{X}_k),$$

where  $f'$  is a random degree  $\leq r$  polynomial over  $\mathbf{X}_1, \dots, \mathbf{X}_k$  and  $g'$  is an independent (but not necessarily uniform) random polynomial over the same set of variables.

Since  $\mathbf{X}_1, \dots, \mathbf{X}_k$  are independent uniform bits, we get that  $f$  is an extractor with error

$$\varepsilon = \left| \Pr_{x \sim \mathbf{U}_k} [f(x) = 1] - \frac{1}{2} \right| = \left| \Pr_{x \sim \mathbf{U}_k} [f'(x) \neq g'(x)] - \frac{1}{2} \right| = \frac{1}{2} \text{corr}(f', g').$$

Thus

$$\Pr_f [f \text{ is not an extractor for } \mathbf{X} \text{ with error } \varepsilon] = \Pr_{f', g'} [\text{corr}(f', g') > 2\varepsilon] \leq \Pr_{f'} [\text{corr}(f', g^*) > 2\varepsilon],$$

where  $g^* = \operatorname{argmax}_{g'} \Pr_{f'}[\operatorname{corr}(f', g') > 2\varepsilon]$ . Thus  $g^* : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  is an arbitrary fixed function and  $f' : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  is a random degree  $\leq r$  polynomial. Thus, by combining the above inequality with [Lemma 6](#),

$$\begin{aligned} \Pr_f[f \text{ is not an extractor for } \mathbf{X} \text{ with error } 2^{-ck/r^3}] &\leq \Pr_{f'}[\operatorname{corr}(f', g^*) > 2 \cdot 2^{-ck/r^3}] \\ &\leq \Pr_{f'}[\operatorname{corr}(f', g^*) > 2^{-ck/r^3}] \\ &\leq 2^{-c\binom{k}{\leq r}}, \end{aligned}$$

which completes the proof.  $\square$

#### 4.2.1 Correlation bounds against a single arbitrary function

At last, all that remains in our proof of [Theorem 4](#) is a proof of [Lemma 6](#), which says that for any fixed function  $g$ , a random low-degree polynomial  $f$  has very low correlation with it. As it turns out, [Lemma 6](#) follows quite readily from the following bounds on the list-size of Reed-Muller codes.

**Theorem 5** ([\[KLP12\]](#)). *There is a universal constant  $C > 0$  such that for any  $n, r \in \mathbb{N}$  and  $\varepsilon > 0$ , the Reed-Muller code  $\operatorname{RM}(n, r)$  is  $(\frac{1-\varepsilon}{2}, L)$ -list-decodable, where*

$$\log L \leq C \cdot r \cdot (r + \log(1/\varepsilon)) \cdot \binom{n}{\leq r-1}.$$

Equipped with these bounds, we proceed to prove [Lemma 6](#).

*Proof of Lemma 6.* Let  $N := 2^n$ , and consider any arbitrary functions  $f, g : \{0, 1\}^n \rightarrow \{0, 1\}$ . If we let  $\hat{f}, \hat{g} \in \{0, 1\}^N$  denote the truth tables of  $f, g$ , notice that

$$N \cdot \operatorname{corr}(f, g) = |2\Delta(\hat{f}, \hat{g}) - N|,$$

which implies that  $\operatorname{corr}(f, g) \leq \varepsilon$  if and only if  $\Delta(\hat{f}, \hat{g}) \in [\frac{1-\varepsilon}{2} \cdot N, \frac{1+\varepsilon}{2} \cdot N]$ . Thus, if we let  $Q \subseteq \{0, 1\}^N$  denote the Reed-Muller code  $\operatorname{RM}(n, r)$ , the following holds: for any fixed function  $g$  and a random degree  $\leq r$  polynomial  $f$ ,

$$\begin{aligned} \Pr_f[\operatorname{corr}(f, g) > \varepsilon] &= \Pr_{q \sim Q} \left[ \Delta(q, \hat{g}) \notin \left[ \frac{1-\varepsilon}{2} N, \frac{1+\varepsilon}{2} N \right] \right] \\ &\leq \max_{v \in \{0, 1\}^N} \Pr_{q \sim Q} \left[ \Delta(q, v) \notin \left[ \frac{1-\varepsilon}{2} N, \frac{1+\varepsilon}{2} N \right] \right] \end{aligned}$$

Thus, we would like to upper bound the probability that a random Reed-Muller codeword  $q \in \{0, 1\}^N$  is *not* within relative Hamming distance  $[(1-\varepsilon)/2, (1+\varepsilon)/2]$  from an arbitrary point  $v \in \{0, 1\}^N$ . Towards this end, suppose that the Reed-Muller code  $Q$  is  $(\frac{1-\varepsilon}{2}, L)$ -list decodable. We claim that for any  $v \in \{0, 1\}^N$ ,

$$\Pr_{q \sim Q} \left[ \Delta(q, v) \notin \left[ \frac{1-\varepsilon}{2} N, \frac{1+\varepsilon}{2} N \right] \right] \leq \frac{2L}{|Q|}.$$

Indeed, this holds for *any*  $(\frac{1-\varepsilon}{2}, L)$ -list decodable code: to see why, simply note that  $\Delta(q, v) \notin [\frac{1-\varepsilon}{2} N, \frac{1+\varepsilon}{2} N]$  if and only if  $q$  is in one of the (open) balls  $\mathcal{B}(v, \frac{1-\varepsilon}{2} N)$  or  $\mathcal{B}(\bar{v}, \frac{1-\varepsilon}{2} N)$ , where  $\bar{v} \in \{0, 1\}^N$

denotes the vector  $v$  with all of its bits flipped. By definition of list-decodability, each of these balls contains  $\leq L$  codewords, and the claim follows.

To conclude, recall that the Reed-Muller code  $\text{RM}(n, r)$  has size  $|Q| = 2^{\binom{n}{\leq r}}$ , and **Theorem 5** tells us that, for any  $\varepsilon > 0$ ,  $Q$  is  $(\frac{1-\varepsilon}{2}, L)$ -list decodable, where  $\log L \leq C \cdot r \cdot (r + \log(1/\varepsilon)) \cdot \binom{n}{\leq r-1}$  and  $C$  is a universal constant. It is a straightforward calculation to verify that there is a universal constant  $c > 0$  such that for  $\varepsilon = 2^{-cn/r^3}$ , it holds that

$$\log L \leq C \cdot r \cdot (r + \log(1/\varepsilon)) \cdot \binom{n}{\leq r-1} \leq \binom{n}{\leq r} / 2,$$

as long as  $r \leq cn^{1/4}$ . Combining all of our inequalities, we get that as long as  $r \leq cn^{1/4}$ , it holds that for any fixed function  $g$  and a random degree  $\leq r$  polynomial  $f$ ,

$$\Pr_f[\text{corr}(f, g) > \varepsilon = 2^{-cn/r^3}] \leq \frac{2L}{|Q|} \leq \frac{2 \cdot 2^{\binom{n}{\leq r}/2}}{2^{\binom{n}{\leq r}}} = 2^{-(\binom{n}{\leq r})/2+1} \leq 2^{-(\binom{n}{\leq r})/4} \leq 2^{-c \binom{n}{\leq r}},$$

as desired. □

### 4.3 Optimized upper bounds for dispersers

In this subsection, we show that we can improve our entropy upper bounds if we only wish to *disperse* from  $d$ -local sources using degree  $\leq r$  polynomials (instead of *extract*). We prove the following theorem, which is an optimized version of **Theorem 2** for the setting of dispersers.

**Theorem 6** (Formal version of **Remark 1**). *There is a universal constant  $C > 0$  such that for all  $n, d, r \in \mathbb{N}$ , the following holds. With probability at least 0.99 over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , it holds that  $f$  is a disperser for  $d$ -local sources with min-entropy  $\geq k$ , as long as*

$$k \geq Cd^2r \cdot (dn \log n)^{1/r} + Cd^3 \cdot n^{1/r}.$$

As **Theorem 6** is an optimized version of **Theorem 2** for the setting of dispersers, we set out to prove **Theorem 6** by re-examining our proof of **Theorem 2**. Recall that **Theorem 2** shows that low-degree polynomials can extract from  $d$ -local sources, and in order to prove it, we combined two main ingredients:

1. A reduction from  $d$ -local sources to  $d$ -local NOBF sources (**Theorem 3**).
2. A result showing that low-degree polynomials can extract from  $d$ -local NOBF sources (**Theorem 4**).

In order to optimize **Theorem 2** for the setting of dispersers (and thereby prove **Theorem 6**), we show that both of these ingredients can be optimized for dispersers.

In more detail, in order to prove **Theorem 6**, we combine two key ingredients. Just like the first key ingredient in **Theorem 2** (**Theorem 3**), our first key ingredient for **Theorem 6** reduces  $d$ -local sources to the more specialized family of  $d$ -local NOBF sources. However, as we are dealing with the easier setting of *dispersing* (instead of *extracting*), the definition of *reduction* here is not as strict.

**Theorem 7** (Optimized version of **Theorem 3** for dispersers). *There exists a universal constant  $c > 0$  such that for any  $n, k, d \in \mathbb{N}$ , the following holds. Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $\geq k$ . Then there is a  $d$ -local NOBF source  $\mathbf{X}' \sim \{0, 1\}^n$  with min-entropy  $\geq k'$  such that  $\text{support}(\mathbf{X}') \subseteq \text{support}(\mathbf{X})$ , where*

$$k' = \frac{ck}{d^2}.$$

Next, while the second key ingredient in [Theorem 2](#) ([Theorem 4](#)) shows that a random low-degree polynomial *extracts* from  $d$ -local NOBF sources, the second key ingredient for [Theorem 6](#) just needs to show that a random low-degree polynomial *disperses* from  $d$ -local NOBF sources. Given this weaker requirement, we are able to improve the min-entropy requirement and prove the following, which is our second key ingredient.

**Theorem 8** (Optimized version of [Theorem 4](#) for dispersers). *There is a universal constants  $C > 0$  such that for all  $n, d, r \in \mathbb{N}$ , the following holds. With probability at least 0.99 over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , it holds that  $f$  is a disperser for  $d$ -local NOBF sources of min-entropy  $\geq k$ , as long as*

$$k \geq Cr \cdot (dn \log n)^{1/r} + Cd \cdot n^{1/r}$$

Now, recall that if a disperser works for a family  $\mathcal{X}$  of sources over  $\{0, 1\}^n$ , then it also works for any  $\mathbf{X} \sim \{0, 1\}^n$  whose support contains the support of some  $\mathbf{X}' \in \mathcal{X}$  ([Fact 2](#)). As a result, by combining [Theorems 7](#) and [8](#), we immediately get [Theorem 6](#). Thus, in the remainder of this section, we just focus on proving [Theorems 7](#) and [8](#). We prove [Theorem 7](#) in [Section 4.3.1](#), and we prove [Theorem 8](#) in [Section 4.3.2](#). This will conclude our discussion of entropy upper bounds (and [Section 4](#)).

#### 4.3.1 A reduction from $d$ -local sources to $d$ -local NOBF sources (optimized for dispersers)

We start by proving [Theorem 7](#), a reduction from  $d$ -local sources to  $d$ -local NOBF sources, which is optimized for dispersers. As it turns out, [Theorem 7](#) follows quite readily from our reduction from  $d$ -local sources to biased  $d$ -local NOBF sources ([Lemma 3](#)).

*Proof of [Theorem 7](#).* Let  $\mathbf{X} \sim \{0, 1\}^n$  be a  $d$ -local source with min-entropy  $k$ . By [Lemma 3](#),  $\mathbf{X}$  is a convex combination of  $(\delta, k')$ -biased  $d$ -local NOBF sources, where  $\delta < 1$  and  $k' \geq k/(2d^2)$ . Let  $\mathbf{Y} \sim \{0, 1\}^n$  be an element of this convex combination (that is assigned probability  $> 0$ ). Clearly  $\mathbf{Y}$  is a  $(\delta, k')$ -biased  $d$ -local NOBF source, and furthermore  $\text{support}(\mathbf{Y}) \subseteq \text{support}(\mathbf{X})$ .

Now, let  $\mathbf{X}' \sim \{0, 1\}^n$  be the “unbiased” version of  $\mathbf{Y}$ : that is, let  $\mathbf{X}'$  have the same set of  $k'$  “good” bits as  $\mathbf{Y}$ , and let the bad bits in  $\mathbf{X}'$  depend on the good bits via the same deterministic functions as in  $\mathbf{Y}$ . However, make the good bits in  $\mathbf{X}'$  have 0 bias. Then  $\mathbf{X}'$  is an (unbiased)  $d$ -local NOBF source with min-entropy  $k'$ , and  $\text{support}(\mathbf{X}') = \text{support}(\mathbf{Y}) \subseteq \text{support}(\mathbf{X})$ .  $\square$

#### 4.3.2 Low-degree polynomials disperse from $d$ -local NOBF sources (optimized for dispersers)

Now that we have proven our reduction from  $d$ -local sources to  $d$ -local NOBF sources ([Theorem 7](#)), all that remains is to prove an upper bound on the entropy required to disperse from  $d$ -local NOBF sources using degree  $\leq r$  polynomials ([Theorem 8](#)). In this section, we prove [Theorem 8](#).

In order to prove [Theorem 8](#), our key ingredient is a lemma about *function composition* and how it affects which degrees are “hit.” More formally, for any nonnegative integer  $r$ , we say that a function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  *hits degree  $r$*  if the unique multilinear  $\mathbb{F}_2$ -polynomial computing  $f$  includes a monomial of size  $r$ ,<sup>9</sup> and we say that  $f$  *hits degree  $\leq r$*  if there is some  $0 \leq r' \leq r$  such that  $f$  hits degree  $r'$ . Then, using standard notation for function composition, we prove the following.

**Lemma 7.** *Let  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  and  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  be functions such that  $f(a_1, \dots, a_n)$  hits degree  $r$ . Furthermore, let  $b_1, \dots, b_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  be functions that do not hit degree  $\leq r$ . Then the function  $f(a_1 + b_1, \dots, a_n + b_n) : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  hits degree  $r$ .*

<sup>9</sup>The monomial of size 0 is the constant 1.

Before we prove this lemma, we show how it can be used to show that degree  $\leq r$  polynomials disperse from  $d$ -local NOBF sources, proving [Theorem 8](#). Then, we conclude this section by proving [Lemma 7](#).

*Proof of Theorem 8.* We start with some basic definitions. First, recall that a  $d$ -local NOBF source of min-entropy  $k$  is a random variable  $\mathbf{X} \sim \{0, 1\}^n$  that is generated as follows: there exist  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  such that  $\mathbf{X} = (a_1(\mathbf{U}_k), \dots, a_n(\mathbf{U}_k))$ , where each  $\mathbf{U}_k$  is a copy of the same uniform random variable. Furthermore, the following must hold: there exists a “good” set  $S = \{\alpha_1, \dots, \alpha_k\} \subseteq [n]$  such that each  $a_{\alpha_i}$  simply outputs its  $i^{\text{th}}$  input, and for every other (bad) coordinate  $j \notin S$  we have that  $a_j$  depends on just  $d$  inputs. For convenience, we refer to the set of functions  $(a_1, \dots, a_n)$  as the *generating functions* of the  $d$ -local NOBF source. If each  $a_i$  is a degree  $\leq r$  polynomial, we say that  $\mathbf{X}$  is not just a  $d$ -local NOBF source, but a ( *$d$ -local, degree  $\leq r$* ) NOBF source.

Now, the goal is to use [Lemma 7](#) to show that, in order for a function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  to disperse from all  $d$ -local NOBF sources of min-entropy  $k$ , it suffices to show that  $f$  “hits” some degree in  $[1, r]$  on all ( *$d$ -local, degree  $\leq r$* ) NOBF sources of the same min-entropy. Then, a straightforward application of the probabilistic method over the latter (smaller) family will yield the result.

More formally, fix an arbitrary function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ . Suppose that for any ( *$d$ -local, degree  $\leq r$* ) NOBF source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy  $k$  and generating functions  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ , there is some  $r' \in [1, r]$  such that  $f(a_1, \dots, a_n)$  hits degree  $r'$ . Then, we **claim** that  $f$  is not only a disperser for all ( *$d$ -local, degree  $\leq r$* ) NOBF sources of min-entropy  $k$ , but it is also a disperser for all  $d$ -local NOBF sources of min-entropy  $k$ .

To see why, let  $\mathbf{X}' \sim \{0, 1\}^n$  be a  $d$ -local NOBF source with generating functions  $h_1, \dots, h_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ , and for each  $i \in [n]$  define the functions  $a'_i, b'_i : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  such that  $a'_i$  is the sum of all monomials in  $h_i$  of degree  $\leq r$ , and  $b'_i$  is the sum of all monomials in  $h_i$  of degree  $> r$ . Consider now the source

$$\mathbf{X} := (a'_1(\mathbf{U}_k), \dots, a'_n(\mathbf{U}_k)),$$

and notice that  $\mathbf{X}$  is a ( *$d$ -local, degree  $\leq r$* ) NOBF source with min-entropy  $k$  and generating functions  $a'_1, \dots, a'_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ . By the hypothesis,  $f(a'_1, \dots, a'_n)$  hits degree  $r'$ , where  $r' \in [1, r]$ . And since  $b'_1, \dots, b'_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  do *not* hit degree  $\leq r$ , we know by [Lemma 7](#) that  $f(a'_1 + b'_1, \dots, a'_n + b'_n) = f(h_1, \dots, h_n)$  hits degree  $r' \in [1, r]$ . This means that  $f(h_1, \dots, h_n)$  is not constant, and since  $f(\mathbf{X}') = f(h_1, \dots, h_n)(\mathbf{U}_k)$ , it holds that  $f(\mathbf{X}')$  is not constant: in other words,  $f$  is a disperser for  $\mathbf{X}'$ . Thus,  $f$  is a disperser for all  $d$ -local NOBF sources of min-entropy  $k$ .

Thus, all that remains is to show that with probability  $\geq 0.99$  over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , the following holds: for any ( *$d$ -local, degree  $\leq r$* ) NOBF source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy  $k$  and generating functions  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ , there is some  $r' \in [1, r]$  such that  $f(a_1, \dots, a_n)$  hits degree  $r'$ .

Towards this end, let  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  be a (uniformly) random degree  $\leq r$  polynomial, and let  $\mathbf{X} \sim \{0, 1\}^n$  be an arbitrary NOBF source with min-entropy  $k$  and generating functions  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ . Without loss of generality, assume that  $a_i(y) = y_i$  for all  $i \in [k]$ . Now, we want to upper bound the probability that for all  $r' \in [1, r]$ , it holds that  $f(a_1, \dots, a_n)$  does *not* hit degree  $r'$ . We **claim** that this probability is at most  $2^{-\binom{k}{\leq r} + 1}$ .

To see why, note that since  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  is a uniformly random degree  $\leq r$  polynomial, we have

$$f(x) := \sum_{S \subseteq [n]: |S| \leq r} c_S x^S,$$

where each  $c_S \sim \{0, 1\}$  is independent and uniform. Now, note that for  $y \in \mathbb{F}_2^k$ ,

$$\begin{aligned} f(a_1, \dots, a_n)(y) &= \sum_{S \subseteq [n]: |S| \leq r} c_S a^S(y) \\ &= \sum_{S \subseteq [k]: |S| \leq r} c_S a^S(y) + \sum_{S \subseteq [n]: |S| \leq r, S \not\subseteq [k]} c_S a^S(y) \\ &= \sum_{S \subseteq [k]: |S| \leq r} c_S y^S + \sum_{S \subseteq [n]: |S| \leq r, S \not\subseteq [k]} c_S a^S(y). \end{aligned}$$

Now, notice that for each fixing of  $\{c_S\}_{S \subseteq [n]: |S| \leq r, S \not\subseteq [k]}$ , we get that

$$f(a_1, \dots, a_n)(y) = f'(y) + g(y),$$

where  $f' : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  is a uniformly random polynomial of degree at most  $\leq r$ , and  $g : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  is a fixed polynomial. Now, for any  $S \subseteq [k]$  of size at most  $r$ , the probability that  $f' + g$  does not include the monomial  $y^S$  is the probability that  $f'$  copies the decision of  $g$  on whether or not to include  $y^S$ : this probability is  $1/2$ . More generally, the probability that  $f' + g$  does not hit degree  $r$  will be  $2^{-\binom{k}{r}}$ , and the probability that it does not hit any degree in  $[1, r]$  will be  $2^{-\binom{k}{\leq r} + 1}$ . Thus

$$\Pr_f[f(a_1, \dots, a_n)(x) \text{ does not hit any degree in } [1, r]] \leq 2^{-\binom{k}{\leq r} + 1}, \quad (1)$$

as claimed.

Now, we say that  $f$  fails if there exists a  $(d$ -local, degree  $\leq r$ ) NOBF source  $\mathbf{X} \sim \{0, 1\}^n$  of min-entropy  $k$  with generating functions  $a_1, \dots, a_n$  such that  $f(a_1, \dots, a_n)$  does not hit any degree in  $[1, r]$ . By combining Equation (1) with a simple union bound, we get that

$$\Pr_f[f \text{ fails}] \leq |\mathcal{X}| \cdot 2^{-\binom{k}{\leq r} + 1},$$

where  $\mathcal{X}$  is the family of  $(d$ -local, degree  $\leq r$ ) NOBF sources  $\mathbf{X} \sim \{0, 1\}^n$  of min-entropy  $k$ . To upper bound the size of  $\mathcal{X}$ , simply note that each  $\mathbf{X} \in \mathcal{X}$  can: (i) choose the locations of its  $k$  good bits; (ii) choose the  $d$  good bits that each bad bit depends on; and (iii) choose the degree  $\leq r$  polynomial that computes each bad bit. Thus

$$|\mathcal{X}| \leq \binom{n}{k} \cdot \left( \binom{k}{d} \cdot 2^{\binom{d}{\leq r}} \right)^{n-k}.$$

It is now a straightforward calculation to verify that there is a sufficiently large constant  $C > 0$  such that for all  $k \geq Cr(dn \log n)^{1/r} + Cdn^{1/r}$ , it holds that

$$\Pr_f[f \text{ fails}] \leq |\mathcal{X}| \cdot 2^{-\binom{k}{\leq r} + 1} \leq \binom{n}{k} \cdot \left( \binom{k}{d} \cdot 2^{\binom{d}{\leq r}} \right)^{n-k} \cdot 2^{-\binom{k}{\leq r} + 1} \leq 0.01.$$

To conclude, we get that with probability  $\geq 0.99$  over the choice of a random degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , it holds that  $f$  hits some degree in  $[1, r]$  on every ( $d$ -local, degree  $\leq r$ ) NOBF source with min-entropy  $k$ , provided that  $k \geq Cr \cdot (dn \log n)^{1/r}$ . By our claim from the beginning of the proof, it follows that  $f$  is also a disperser for all  $d$ -local NOBF sources of min-entropy  $k$ , as desired.  $\square$

At last, all that remains is to prove **Lemma 7**, which says that if  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  and  $a_1, \dots, a_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  are functions such that  $f(a_1, \dots, a_n)$  hits degree  $r$ , and  $b_1, \dots, b_n : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  are functions that do not hit degree  $\leq r$ , then  $f(a_1 + b_1, \dots, a_n + b_n)$  hits degree  $r$ .

*Proof of Lemma 7.* Since we can write any function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  as a unique multilinear  $\mathbb{F}_2$ -polynomial, we know that

$$f(x) = \sum_{S \subseteq [n]} c_S x^S$$

for some constants  $c_S \in \{0, 1\}$ ,  $S \subseteq [n]$ . Using this, we have

$$\begin{aligned} f(a_1 + b_1, \dots, a_n + b_n)(x) &= \sum_{S \subseteq [n]} c_S \prod_{i \in S} (a_i(x) + b_i(x)) \\ &= \sum_{S \subseteq [n]} c_S \sum_{T \subseteq S} a^T(x) b^{S-T}(x) \\ &= \sum_{S \subseteq [n]} c_S \left( a^S(x) + \sum_{T \subsetneq S} a^T(x) b^{S-T}(x) \right) \\ &= \sum_{S \subseteq [n]} c_S a^S(x) + \sum_{S \subseteq [n]} \sum_{T \subsetneq S} a^T(x) b^{S-T}(x) \\ &= f(a_1, \dots, a_n)(x) + \sum_{S \subseteq [n]} \sum_{T \subsetneq S} a^T(x) b^{S-T}(x) \\ &= f(a_1, \dots, a_n)(x) + \sum_{\substack{\emptyset \subsetneq S \subseteq [n] \\ T \subsetneq S}} a^T(x) b^{S-T}(x). \end{aligned}$$

Now, for each  $S \subseteq [n]$ ,  $T \subsetneq S$  such that  $S$  is nonempty, define the function  $g_{S,T}(x) := a^T(x) b^{S-T}(x)$ . Since  $f(a_1, \dots, a_n)$  hits degree  $r$ , notice that in order to complete the proof, it suffices to show that each  $g_{S,T}$  does *not* hit degree  $r$ . Towards this end, pick an arbitrary element  $\gamma \in S - T$ , and observe

$$\begin{aligned} g_{S,T}(x) &:= a^T(x) b^{S-T}(x) \\ &= \prod_{i \in T} a_i(x) \prod_{j \in S-T} b_j(x) \\ &= \left( \prod_{i \in T} a_i(x) \prod_{j \in (S-T) - \{\gamma\}} b_j(x) \right) b_\gamma(x). \end{aligned}$$

Next, it is straightforward to verify that for any functions  $p, q : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  such that  $q$  does not hit degree  $\leq r$ , it follows that the function  $pq : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  does not hit degree  $\leq r$ .<sup>10</sup> Thus, since  $b_\gamma$  does not hit degree  $\leq r$  by the hypothesis, it follows via the above observation and identity that  $g_{S,T}$  does not hit degree  $\leq r$ , which is even stronger than what we needed to complete the proof.  $\square$

<sup>10</sup>This is because any monomial that ‘‘pops out’’ of  $pq$  must be at least the size of the smallest monomial in  $q$ , which is  $> r$ .

## 5 Entropy lower bounds

In this section, we obtain lower bounds on the entropy required to extract from  $d$ -local sources using degree  $\leq r$  polynomials, proving the following theorem.

**Theorem 9** (Theorem 1.2, restated). *There is a constant  $c > 0$  such that for all  $n, d, r \in \mathbb{N}$  with  $2 \leq r \leq c \log(n)$  and  $d \leq n^{\frac{1}{r-1}-2^{-10r}} / \log(n)$ , the following holds. For any degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , there is a  $d$ -local source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy at least*

$$k \geq cr(dn \log n)^{1/r}$$

such that  $f(\mathbf{X})$  is constant.

In order to prove Theorem 9, we actually prove a stronger theorem, which can be viewed as a *local* version of a result by Cohen and Tal [CT15]. In particular, Cohen and Tal show that every  $n$ -variate polynomial of degree  $\leq r$  admits a subspace of dimension  $\Omega(rn^{\frac{1}{r-1}})$  on which it is constant, and that this is tight. We show that a similar result holds even for the special subclass of *local* subspaces.

**Theorem 10** (Theorem 3, restated). *There exist universal constants  $C, c > 0$  such that for every  $n, r, d \in \mathbb{N}$  such that  $2 \leq r \leq c \log(n)$  and  $d \leq n^{\frac{1}{r-1}-2^{-10r}} / \log(n)$ , the following holds. For any degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , there exists a  $d$ -local subspace  $X \subseteq \mathbb{F}_2^n$  of dimension*

$$k \geq cr(dn \log n)^{1/r}$$

on which  $f$  is constant.

*This is tight: there exists a degree  $\leq r$  polynomial  $g \in \mathbb{F}_2[x_1, \dots, x_n]$  which is an extractor for  $d$ -local affine sources of dimension  $k \geq Cr(dn \log n)^{1/r}$ , which has error  $\varepsilon = 2^{-ck/r}$ .*

Notice that Theorem 10 immediately implies Theorem 9, since (the uniform distribution over) a  $d$ -local subspace is not only an affine source, but it is also a  $d$ -local source. Thus, in the remainder of the section, we focus on proving Theorem 10. The key new ingredient we rely on is a so-called “low-weight Chevalley-Warning theorem,” which may be of independent interest. We prove this result in Section 5.1, and we show how it can be used to obtain Theorem 10 in Section 5.2. This will conclude our discussion of entropy lower bounds (and Section 5).

### 5.1 A low-weight Chevalley-Warning theorem

The *Chevalley-Warning theorem* is a classical result from number theory, which guarantees that a small set of low-degree polynomials admits a nontrivial common solution. More formally, it states the following.

**Theorem 11** (Chevalley-Warning theorem [War36]). *Let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  be a set of polynomials with degree at most  $D$  such that  $0$  is a common solution. Then there are at least  $2^{n-D}$  common solutions to  $\{f_i\}$ . In particular, if  $D < n$ , then there must be a nontrivial common solution.*

In this subsection, we prove a “low-weight” version of this theorem (which will be instrumental in our proof of Theorem 10). In more detail, we believe it is natural to ask not only if  $\{f_i\}$  contains a nontrivial common solution, but if  $\{f_i\}$  contains a nontrivial common solution of *low Hamming weight*.

In the case where all the  $f_i$  are linear, this is a question about the distance-dimension tradeoff of linear codes. Here, this question is answered by the *Hamming bound*, which says that there must be a nontrivial common solution of weight  $w \leq O(D/\log(n/D))$ .<sup>11</sup>

On the other hand, for general collections  $\{f_i\}$  that may have nonlinear polynomials, it is straightforward to use classical Chevalley-Waring ([Theorem 11](#)) to show that there is always a nontrivial common solution of weight  $w \leq D + 1$ ,<sup>12</sup> and one can show that this is tight in general.<sup>13</sup>

Thus, the upper bound on Hamming weight is much better when we know that all the polynomials in  $\{f_i\}$  are linear. This begs the question: if we know that *most* of the polynomials in  $\{f_i\}$  are linear, can we get an upper bound on Hamming weight that is almost as strong as in the purely linear case? And, more generally, can we get a granular bound that takes into account exactly how many  $f_i$  are linear and nonlinear?

Our *low-weight Chevalley-Waring theorem*, which we state next, provides a result of exactly this form.

**Theorem 12.** *Let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  be a set of polynomials with linear degree at most  $D$  and nonlinear degree at most  $\Delta$ , such that  $0$  is a common solution and  $D + \Delta < n$ . If all nontrivial common solutions to  $\{f_i\}$  have Hamming weight  $> w$ , then*

$$\binom{n}{\leq \lfloor w/2 \rfloor} \leq 2^{D+\Delta+1} \cdot \binom{n}{\leq \lfloor \Delta/2 \rfloor}.$$

As we will see, a relatively straightforward (but tedious) calculation yields the following corollary.

**Corollary 1** ([Theorem 4](#), restated). *Let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  be a set of polynomials with linear degree at most  $D$  and nonlinear degree at most  $\Delta$  such that  $0$  is a common solution and  $D + \Delta < n$ . Then there is a nontrivial common solution with Hamming weight*

$$w \leq 8\Delta + 8D/\log(n/D) + 8.$$
<sup>14</sup>

Notice that the weight upper bound in [Corollary 1](#) tightly interpolates (up to constant factors) between the linear and nonlinear cases discussed at the beginning of this section. We will also see that it is not difficult to extend [Corollary 1](#) to obtain the following, which is the result that we will actually end up using in our proof of [Theorem 10](#).

**Corollary 2.** *Let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  be a set of polynomials with linear degree at most  $D$  and nonlinear degree at most  $\Delta$  such that  $0$  is a common solution. Then for any  $S \subseteq [n]$  such that  $D + \Delta < |S|$ , there is a nontrivial common solution supported on  $S$  with Hamming weight*

$$w \leq 8\Delta + 8D/\log(|S|/D) + 8.$$

In the remainder of this section, we prove [Theorem 12](#) and [Corollaries 1](#) and [2](#). The proof of [Theorem 12](#) is most interesting, and can be found in [Section 5.1.1](#). The proofs of [Corollaries 1](#) and [2](#) are less interesting and somewhat tedious, and can be found in [Section 5.1.2](#).

<sup>11</sup>More formally, it says that if all nontrivial solutions have weight  $> w$ , then it must hold that  $\binom{n}{\leq \lfloor w/2 \rfloor} \leq 2^D$ .

<sup>12</sup>Given a collection  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  of degree  $D$ , apply [Theorem 11](#) to the collection  $\{f_i\} \cup \{x_1, x_2, \dots, x_{n-(D+1)}\}$ .

<sup>13</sup>Consider the singleton set  $\{f\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$ , where  $f(x) = \sum_{\emptyset \subseteq S \subseteq [n]: |S| \leq D} x^S$ .

<sup>14</sup>We define the expression  $8D/\log(n/D)$  to be 0 if  $D = 0$ .

### 5.1.1 A proof of our low-weight Chevalley-Warning theorem

We now prove our low-weight Chevalley-Warning theorem ([Theorem 12](#)). The key ingredient we need is the following lemma, which says that for any collection of polynomials  $\{f_i\}$  and any big enough set of common solutions  $A$ , it holds that  $A + A$  contains a nontrivial common solution.

**Lemma 8.** *Let  $\{f_i\} \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  be a set of polynomials with nonlinear degree at most  $\Delta$  such that  $0$  is a common solution. Then for any set  $A \subseteq \mathbb{F}_2^n$  of common solutions of size*

$$|A| > 2 \binom{n}{\leq \lfloor \Delta/2 \rfloor},$$

*it holds that  $A + A$  contains a nontrivial common solution.*

Before proving this result, we show how it can be combined with the Hamming bound and the classical Chevalley-Warning theorem to get [Theorem 12](#), our low-weight Chevalley-Warning theorem.

*Proof of Theorem 12.* Let  $Q \subseteq \mathbb{F}_2^n$  be the set of common solutions to  $\{f_i\}$ , and suppose that all  $v \in Q - \{0\}$  have Hamming weight  $> w$ . Then for any ball  $\mathcal{B}$  of radius  $\lfloor w/2 \rfloor$ , it must hold that

$$|Q \cap \mathcal{B}| \leq 2 \binom{n}{\leq \lfloor \Delta/2 \rfloor},$$

since otherwise [Lemma 8](#) (combined with the triangle inequality) implies that there is a nontrivial solution of weight at most  $2\lfloor w/2 \rfloor \leq w$ . Thus, we see that  $Q$  is a  $(\rho, L)$ -list-decodable code, where

$$\begin{aligned} \rho &= \lfloor w/2 \rfloor / n, \\ L &= 2 \binom{n}{\leq \lfloor \Delta/2 \rfloor}. \end{aligned}$$

Now, the Hamming bound ([Theorem 1](#)) implies that  $|Q| \leq 2^n L / \binom{n}{\leq \rho n}$ , whereas the Chevalley-Warning theorem ([Theorem 11](#)) implies that  $2^{n-(D+\Delta)} \leq |Q|$ . Combining these inequalities yields

$$2^{n-(D+\Delta)} \leq \frac{2^n L}{\binom{n}{\leq \rho n}} \leq \frac{2^n \cdot 2 \binom{n}{\leq \lfloor \Delta/2 \rfloor}}{\binom{n}{\leq \lfloor w/2 \rfloor}},$$

which immediately implies the result. □

All that remains is to prove our key ingredient, [Lemma 8](#). As it turns out, it follows quite readily from the following *CLP lemma*, which was instrumental in the recent resolution of the cap set conjecture.

**Lemma 9** ([\[CLP17\]](#)). *Let  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  be a polynomial of degree at most  $r$ , and let  $M$  denote the  $2^n \times 2^n$  matrix with entries  $M_{x,y} = f(x + y)$  for  $x, y \in \mathbb{F}_2^n$ . Then*

$$\text{rank}(M) \leq 2 \binom{n}{\leq \lfloor r/2 \rfloor}.$$

Given the CLP lemma, we are ready to prove [Lemma 8](#), which will conclude our proof of [Theorem 12](#).

*Proof of Lemma 8.* First, let  $\{g_i\} \subseteq \{f_i\}$  be the set of polynomials in  $\{f_i\}$  that have degree  $> 1$ . Notice that if  $A + A$  contains a nontrivial common solution to the system  $\{g_i\}$ , then it also contains a nontrivial common solution to  $\{f_i\}$ : this follows from the linearity of the polynomials of  $\{f_i\} - \{g_i\}$  and the fact that every  $a \in A$  is a common solution (by definition of  $A$ ). Thus, it suffices to show the result for the set  $\{g_i\}$ .

Next, consider the polynomial  $g \in \mathbb{F}_2[x_1, \dots, x_n]$  defined as

$$g(x) := \prod_i (1 + g_i(x)).$$

It is straightforward to verify that  $g$  has degree at most  $\Delta$ , and that  $g(x) = 1$  if and only if  $x$  is a common solution to  $\{g_i\}$ . Now, suppose for contradiction that  $A + A$  contains no nontrivial common solution to  $\{g_i\}$ : that is, for every distinct  $x, y \in A$  it holds that  $g(x + y) = 0$ . Then, consider the  $2^n \times 2^n$  matrix  $M$  with entries  $M_{x,y} = g(x + y)$  for every  $x, y \in \mathbb{F}_2^n$ . Define  $k := |A|$ , and let  $M[A, A]$  denote the  $k \times k$  submatrix of  $M$  obtained by taking the rows and columns of  $M$  indexed by  $A$ . Since 0 is a common solution to  $\{g_i\}$ , we get that  $M[A, A] = I_k$  and thus

$$\text{rank}(M) \geq \text{rank}(M[A, A]) = \text{rank}(I_k) = k > 2 \binom{n}{\lfloor \Delta/2 \rfloor},$$

which directly contradicts [Lemma 9](#). □

### 5.1.2 Proofs of its corollaries

Now that we have proven our general low-weight Chevalley-Warning theorem ([Theorem 12](#)), we are ready to prove its corollaries. These proofs are relatively straightforward, but somewhat tedious. We start with the proof of [Corollary 1](#), which says that we can always find a nontrivial common solution of Hamming weight  $w \leq 8\Delta + 8D/\log(n/D) + 8$ .

*Proof of Corollary 1.* First, note that the result is true if  $8\Delta + 8D/\log(n/D) + 8 \geq D + \Delta + 1$ , as the existence of a nontrivial common solution with Hamming weight  $\leq D + \Delta + 1$  is immediate from Chevalley-Warning (see the discussion following [Theorem 11](#)). Thus we henceforth assume, without loss of generality, that

$$8\Delta + 8D/\log(n/D) + 8 < D + \Delta + 1 \leq n, \tag{2}$$

where the last inequality comes from the given hypothesis  $D + \Delta < n$ . This string of inequalities will come in handy later.

Now, by [Theorem 12](#), we know that for any  $W$  satisfying both

$$\binom{n}{\leq \lfloor W/2 \rfloor} > 2^{(D+\Delta+1) \cdot 2}, \tag{3}$$

$$\binom{n}{\leq \lfloor W/2 \rfloor} > \left( \binom{n}{\leq \lfloor \Delta/2 \rfloor} \right)^2, \tag{4}$$

it holds that there is a nontrivial common solution of Hamming weight  $\leq W$ . We seek to find the smallest  $W$  satisfying both [Equations \(3\) and \(4\)](#).

We start with [Equation \(4\)](#). First, by relatively straightforward binomial inequalities, observe

$$\left( \binom{n}{\leq \lfloor \Delta/2 \rfloor} \right)^2 \leq \binom{2n}{\leq 2\lfloor \Delta/2 \rfloor} \leq \binom{n}{\leq 4\lfloor \Delta/2 \rfloor},$$

where the last inequality uses the fact that  $8\Delta < n$  (as implied by [Equation \(2\)](#)). Thus, any  $W$  satisfying

$$\binom{n}{\leq \lfloor W/2 \rfloor} > \binom{n}{\leq 4\lfloor \Delta/2 \rfloor}$$

also satisfies [Equation \(4\)](#). And the above inequality is satisfied by any  $W$  satisfying

$$\lfloor W/2 \rfloor > 4\lfloor \Delta/2 \rfloor,$$

where we have again used the assumption that  $8\Delta < n$  to ensure  $4\lfloor \Delta/2 \rfloor < n$ . Thus, any  $W$  satisfying

$$W > 4\Delta + 1.$$

also satisfies [Equation \(4\)](#).

We now consider [Equation \(3\)](#). By [Equation \(2\)](#), we may assume  $D > 7\Delta + 7$ , which means that  $\Delta < D/7 - 1$  and thus  $(D + \Delta + 1) \cdot 2 < 16D/7$ . As a result, any  $W$  satisfying

$$\binom{n}{\leq \lfloor W/2 \rfloor} > 2^{16D/7} \tag{5}$$

also satisfies [Equation \(3\)](#). We consider two cases.

*Case (i):*  $D \leq \log n$ : By [Equation \(2\)](#), we may assume  $n > 8$ . It is now easy to verify that for any  $W \geq 8$ ,

$$\binom{n}{\leq \lfloor W/2 \rfloor} \geq \binom{n}{\leq 4} > n^{16/7} \geq 2^{16D/7},$$

thereby satisfying [Equation \(5\)](#).

*Case (ii):*  $D > \log(n)$ : Let  $1 \leq k \leq n$  be a parameter we will pick later, and notice that for any  $W \geq 2k$  we have

$$\binom{n}{\leq \lfloor W/2 \rfloor} \geq \binom{n}{\leq \lfloor k \rfloor} \geq \binom{n}{\lfloor k \rfloor} \geq \left(\frac{n}{\lfloor k \rfloor}\right)^{\lfloor k \rfloor}.$$

Thus if  $1 \leq k \leq n$  is a parameter satisfying  $\lfloor k \rfloor \log(n/\lfloor k \rfloor) > 16D/7$  then any  $W \geq 2k$  satisfies [Equation \(5\)](#). Now, define  $k := 4D/\log(n/D)$ . By the case condition and [Equation \(2\)](#), we have  $4 \leq k < n$ , and thus

$$3D/\log(n/D) \leq \lfloor k \rfloor \leq 4D/\log(n/D).$$

By [Equation \(2\)](#), we may assume  $\log(n/D) \geq 8$ , and thus

$$\lfloor k \rfloor \log(n/\lfloor k \rfloor) \geq \frac{3D}{\log(n/D)} \log\left(\frac{n \log(n/D)}{4D}\right) \geq \frac{3D}{\log(n/D)} \log\left(\frac{2n}{D}\right) \geq 3D > 16D/7.$$

Thus, every  $W \geq 2k = 8D/\log(n/D)$  satisfies [Equation \(5\)](#).

To conclude, we get that every

$$W \geq \max\{4\Delta + 2, 8, 8D/\log(n/D)\}$$

satisfies both [Equations \(3\)](#) and [\(4\)](#), which completes the proof.  $\square$

We now turn towards proving [Corollary 2](#), which says that, not only is it possible to find a low weight common solution, but it is even possible to force this solution to be supported on a target set of coordinates  $S$ . The proof follows quite directly by combining [Corollary 1](#) with the idea of function restrictions.

*Proof of Corollary 2.* For any  $y \in \mathbb{F}_2^{|S|}$ , let  $y^+ \in \mathbb{F}_2^n$  denote the unique string where  $y_S^+ = y$  and  $y_S^+ = 0^{n-|S|}$ . Now, for each  $f_i$  let  $g_i \in \mathbb{F}_2[x_1, \dots, x_{|S|}]$  denote the polynomial  $g_i(x) := f_i(x^+)$ . Notice that each  $\deg(g_i) \leq \deg(f_i)$ . Now, for each  $i$  create a polynomial  $h_i \in \mathbb{F}_2[x_1, \dots, x_{|S|}]$  as follows. If  $\deg(f_i) > 1$  but  $\deg(g_i) = 1$ : assume without loss of generality that  $g_i(x) \neq x_1$ , and set  $h_i(x) := 1 + (1 + x_1)(1 + g_i(x))$ ; otherwise, just define  $h_i(x) := g_i(x)$ .

Consider the set of polynomials  $\{h_i\}$ . Notice that the nonlinear degree of  $\{h_i\}$  is at most  $\Delta$ , and the linear degree of  $\{h_i\}$  is at most  $D$ . Thus, by Corollary 1, there is a nontrivial common solution  $y$  to  $\{h_i\}$  with weight  $w \leq 8\Delta + 8D/\log(|S|/D) + 8$ . It is then straightforward to verify that  $y$  must be a common solution to  $\{g_i\}$ , and that  $y^+$  must be a common solution to  $\{f_i\}$ . Furthermore,  $y^+$  is clearly supported on  $S$  and has the same Hamming weight as  $y$ .  $\square$

## 5.2 A local version of Cohen-Tal

Equipped with our low-weight Chevalley-Warning theorem, we are now ready to prove our local version of Cohen-Tal (Theorem 10). Recall that this result says every degree  $\leq r$  polynomial admits a large local subspace on which it is constant, and that the lower bounds that we get on its size are tight. For convenience, we split this theorem into two lemmas: one which claims the lower bounds (Lemma 10), and one which claims their tightness (Lemma 12). We prove these lemmas in Sections 5.2.1 and 5.2.2, respectively. Theorem 10 will then follow immediately.

### 5.2.1 The lower bounds

We start with a proof of the lower bounds in Theorem 10, which is much more challenging to prove than the tightness result.

**Lemma 10** (Lower bound of Theorem 10). *There exists a universal constant  $c > 0$  such that for every  $n, r, d \in \mathbb{N}$  such that  $2 \leq r \leq c \log(n)$  and  $d \leq n^{\frac{1}{r-1}-2^{-10r}} / \log n$ , the following holds. For any degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$ , there exists a  $d$ -local affine subspace  $X \subseteq \mathbb{F}_2^n$  of dimension*

$$k \geq cr(dn \log n)^{1/r}$$

on which  $f$  is constant.

Our proof of Lemma 10 will combine our low-weight Chevalley-Warning theorem (Corollary 2) with a (known) ingredient from Cohen and Tal [CT15] that involves *directional derivatives*. Given a polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  and a set of vectors  $S \subseteq \mathbb{F}_2^n$ , we let  $f_S$  denote the *derivative of  $f$  in the directions of  $S$* , where

$$f_S(x) := \sum_{T \subseteq S} f \left( x + \sum_{v \in T} v \right).$$

One useful observation is that  $\deg(f_S) \leq \max\{0, \deg(f) - |S|\}$ . In addition to this, the key ingredient about directional derivatives that we import from Cohen and Tal is the following.

**Lemma 11** ([CT15]). *For any degree  $\leq r$  polynomial  $f \in \mathbb{F}_2[x_1, \dots, x_n]$  and  $B \subseteq \mathbb{F}_2^n$ ,*

$$f \left( x + \sum_{v \in S} v \right) = 0 \text{ for all } S \subseteq B \iff f_S(x) = 0 \text{ for all } S \subseteq B \text{ of size } |S| \leq r.$$

This shows that  $f$  is 0 on the entire affine space  $x + \text{span}(B)$  if and only if 0 is a common solution to all  $(\leq r)$ -wise directional derivatives of  $f$  across  $B$ . Now, given [Lemma 11](#) and our low-weight Chevalley-Waring theorem ([Corollary 2](#)), we are ready to prove our lower bound for extracting from  $d$ -local affine sources ([Lemma 10](#)).

*Proof of Lemma 10.* Assume without loss of generality that  $f(0) = 0$ , for otherwise we can work with the polynomial  $1 + f$ . We will iteratively build a basis  $B \subseteq \mathbb{F}_2^n$  of a  $d$ -local subspace  $X \subseteq \mathbb{F}_2^n$  on which  $f$  is constantly 0.

Towards this end, we start by initializing several sets:

- $B \leftarrow \emptyset$ .
- UNIQUE  $\leftarrow \emptyset$ .
- SATURATED  $\leftarrow \emptyset$ .
- $P \leftarrow \{f\}$ .

Now, **while** there exists a common nontrivial solution  $b \in \mathbb{F}_2^n$  to the set  $P \subseteq \mathbb{F}_2[x_1, \dots, x_n]$  such that  $b$  is supported on  $[n] \setminus (\text{UNIQUE} \cup \text{SATURATED})$ , **do** the following:

- Let  $b^*$  be the lowest (Hamming) weight vector of this type (breaking ties arbitrarily).
- Set  $B \leftarrow B \cup \{b^*\}$ .
- Define  $\alpha \in [n]$  as the smallest index such that  $b_\alpha^* = 1$ .
- Set UNIQUE  $\leftarrow \text{UNIQUE} \cup \{\alpha\}$ .
- Set SATURATED  $\leftarrow \{i \in [n] : \text{there are } d \text{ vectors } v \in B \text{ with } v_i = 1\}$ .
- For each  $S \subseteq B$  of size  $|S| \leq r$ , set  $P \leftarrow P \cup \{f_S\}$ .

This completes the construction of  $B$ .

We now proceed with the analysis. First, we argue that at the end of the above construction,  $B$  will hold a basis for a  $d$ -local subspace  $X := \text{span}(B)$ . To see why, first define  $T$  to be the number of times the above loop executes, and for each  $i \in [T]$  let  $b^i \in \mathbb{F}_2^n$  denote the vector added to  $B$  in iteration  $i$ . Then, let  $\alpha(i) \in [n]$  denote the smallest index such that  $b_{\alpha(i)}^i = 1$ , and observe that  $b_{\alpha(i)}^j = 0$  for all  $j > i$ , because of bullets 3-4 above (combined with the loop condition). Thus  $B = \{b^1, \dots, b^T\}$  is a collection of linearly independent vectors: in other words, a basis. Furthermore, bullet 5 above (combined with the loop condition) ensures that  $X := \text{span}(B)$  is  $d$ -local.

Thus we have argued that  $X$  is a  $d$ -local subspace of dimension  $T$ . Now, by combining bullet 6 above with the loop condition and [Lemma 11](#), we immediately get that  $f(x) = 0$  for all  $x \in X$ . Thus, all that remains is to get a lower bound on  $T$ , the number of times that the loop executes.

We call the first iteration of the loop *iteration 1*, and we call the pseudocode that precedes the while loop *iteration 0*. Now, for all  $t = 0, \dots, T$ , we define the following variables, for convenience:

- Let  $D_t$  denote the degree of the system  $P$  upon completing iteration  $t$ .
- Let  $\Delta_t$  denote the nonlinear degree of the system  $P$  upon completing iteration  $t$ .

- Let  $u_t$  denote the size of  $|\text{UNIQUE}|$  upon completing iteration  $t$ .
- Let  $s_t$  denote the size of  $|\text{SATURATED}|$  upon completing iteration  $t$ .
- Let  $w_t$  denote the Hamming weight of the vector  $b^*$  selected in iteration  $t$ .

Note that  $w_0$  is undefined above, and for convenience we define  $w_0 := 0$ . Furthermore, for any  $t > T$ , it will be convenient to define  $D_t := D_T$ ,  $\Delta_t := \Delta_T$ , and so on. Now, before we turn towards getting a lower bound on  $T$ , we *upper bound* the above quantities.

- $D_t \leq \sum_{i=0}^{r-1} \binom{t}{i} (r-i) \leq r \binom{t}{\leq r-1}$ . This is because, at the end of iteration  $t$  we have:  $|B| = t$ ; and  $P$  holds the set of polynomials  $f_S$  for all  $S \subseteq B$  of size  $|S| \leq r$ ; and  $\deg(f_S) \leq \max\{0, \deg(f) - |S|\}$ .
- $\Delta_t \leq \sum_{i=0}^{r-2} \binom{t}{i} (r-i) \leq r \binom{t}{\leq r-2}$ . This holds for the same reasons as above, except that we are now ignoring the polynomials  $f_S$  for all  $S \subseteq B$  of size  $|S| \geq r-1$  (since these have degree at most 1).
- $u_t = t$ , since we grow UNIQUE by a (unique) coordinate in every iteration.
- $s_t \leq \frac{1}{d} \sum_{i=1}^t w_i$ , since otherwise the sum of the Hamming weights of the vectors  $b^*$  selected in iterations  $1, \dots, t$  is at least  $ds_t > \sum_{i=1}^t w_i$ , a contradiction.
- $w_t \leq 8\Delta_{t-1} + 8D_{t-1} / \log\left(\frac{n-u_{t-1}-s_{t-1}}{D_{t-1}}\right) + 8$ , by **Corollary 2**.

We now turn towards getting a lower bound on  $T$ . Here, the key observation is that it *must* hold that

$$D_T \geq n - (u_T + s_T),$$

because otherwise the degree of the set of polynomials is strictly less than the size of the set on which it must be supported, so **Corollary 2** trivially implies that there is *some* nontrivial common solution supported on  $S$  (thereby forcing the next execution of the while condition to pass). A straightforward consequence of this is  $T \geq 1$  since  $D_0 = r < n = n - (u_0 + s_0)$ .

Instead of getting a lower bound on  $T$ , it will facilitate the analysis to instead lower bound some  $\tau \leq T$ . In particular, let  $\tau \in \{0, 1, \dots, T-1\}$  be the smallest integer such that

$$D_{\tau+1} + u_{\tau+1} + s_{\tau+1} \geq n/2. \quad (6)$$

Such a  $\tau$  must exist, since we saw above that  $D_T + u_T + s_T \geq n$ . We now seek to lower bound  $\tau$ , which will in turn lower bound  $T$ .

We start with a basic (but useful) lower bound on  $\tau$ . In particular, we claim that  $\tau \geq 2r$ . To see why, suppose for contradiction  $\tau < 2r$ . Then by definition of  $\tau$  it holds that  $D_{2r} + u_{2r} + s_{2r} \geq n/2$ . But by our upper bounds on these quantities (and the fact that  $r \geq 1$ ) we have

$$\begin{aligned} D_{2r} + u_{2r} + s_{2r} &\leq D_{2r} + u_{2r} + 8 \sum_{i=0}^{2r-1} (\Delta_i + D_i + 1) \\ &\leq D_{2r} + u_{2r} + 16r \cdot (\Delta_{2r} + D_{2r} + 1) \\ &\leq r \cdot \binom{2r}{\leq r-1} + 2r + 16r \cdot \left( r \cdot \binom{2r}{\leq r-2} + r \cdot \binom{2r}{\leq r-1} + r \right) \\ &\leq r \cdot 2^{2r} + 2r + 16r \cdot (r \cdot 2^{2r} + r \cdot 2^{2r} + r) \\ &\leq 2^{12r}. \end{aligned}$$

Thus we get that  $n/2 \leq D_{2r} + u_{2r} + s_{2r} \leq 2^{12r}$ , which implies that  $r \geq \log(n)/13$ . But the theorem hypothesis claims that  $r \leq c \log(n)$  for some universal constant  $c$ ; thus, we can just pick  $c$  later to ensure that  $c < \frac{1}{13}$ , which would yield a contradiction and conclude the proof of the claim that  $\tau \geq 2r$ . And since  $r \geq 1$  by the theorem hypothesis, we also know that  $\tau \geq 2$ .

Given the above, we now proceed to get a more general lower bound on  $\tau$ . We will do so by sandwiching the quantity  $D_{\tau+1} + u_{\tau+1} + s_{\tau+1}$  between two inequalities. Towards this end, the key observation is that for any  $i \in [\tau]$ , it holds that  $u_i + s_i \leq u_i + s_i + D_i < n/2$ .<sup>15</sup> Combining this with Equation (6) and our earlier upper bounds on  $s_t, w_t$ , we have

$$\begin{aligned}
n/2 &\leq D_{\tau+1} + u_{\tau+1} + s_{\tau+1} \leq D_{\tau+1} + u_{\tau+1} + \frac{1}{d} \sum_{i=1}^{\tau+1} w_i \\
&\leq D_{\tau+1} + u_{\tau+1} + \frac{8}{d} \sum_{i=0}^{\tau} \left( \Delta_i + \frac{D_i}{\log\left(\frac{n-u_i-s_i}{D_i}\right)} + 1 \right) \\
&\leq D_{\tau+1} + u_{\tau+1} + \frac{8}{d} \sum_{i=0}^{\tau} \left( \Delta_\tau + \frac{D_\tau}{\log\left(\frac{n-u_\tau-s_\tau}{D_\tau}\right)} + 1 \right) \\
&\leq D_{\tau+1} + (\tau + 1) + \frac{8}{d}(\tau + 1) \left( \Delta_\tau + \frac{D_\tau}{\log\left(\frac{n-u_\tau-s_\tau}{D_\tau}\right)} + 1 \right) \\
&\leq D_{\tau+1} + (\tau + 1) + \frac{8}{d}(\tau + 1) \left( \Delta_\tau + \frac{D_\tau}{\log\left(\frac{n}{2D_\tau}\right)} + 1 \right) \\
&\leq D_{\tau+1} + 2\tau + \frac{16\tau}{d} \left( \Delta_\tau + \frac{D_\tau}{\log\left(\frac{n}{2D_\tau}\right)} + 1 \right) \\
&\leq D_{\tau+1} + 18\tau + \frac{16\tau}{d} \left( \Delta_\tau + \frac{D_\tau}{\log\left(\frac{n}{2D_\tau}\right)} \right).
\end{aligned}$$

Thus we know that if we define

$$\begin{aligned}
K_1 &:= D_{\tau+1} + 18\tau + \frac{16\tau}{d} \Delta_\tau, \\
K_2 &:= \frac{16\tau D_\tau}{d \log\left(\frac{n}{2D_\tau}\right)},
\end{aligned}$$

it must hold that  $K_1 + K_2 \geq n/2$ , or rather we know that either  $K_1 \geq n/4$  or  $K_2 \geq n/4$  must hold. We analyze these cases separately, and get a lower bound on  $\tau$  in each case. But before we do so, it will be useful to recall that for any integers  $b > a \geq 0$  it holds that  $\binom{b}{a} \leq \binom{b}{a+1}$  if  $a + 1 \leq b/2$ . Since we saw earlier that  $\tau \geq 2r$ , we have  $\binom{2\tau}{\leq r-1} \leq r \cdot \binom{2\tau}{r-1}$  and  $\binom{\tau}{\leq r-2} \leq r \cdot \binom{\tau}{r-2}$  and  $\binom{\tau}{\leq r-1} \leq r \cdot \binom{\tau}{r-1}$ . We now proceed with the case analysis.

<sup>15</sup>This useful inequality is the reason we work with  $\tau$  instead of  $T$ , as this is not necessarily true for any  $i \in [T]$ .

*Case (1):*  $K_1 \geq n/4$ : By applying the upper bounds on  $D_t, \Delta_t$  obtained earlier in the proof, the standard binomial inequality  $\binom{n}{k} \leq (en/k)^k$ , and the fact that  $r \geq 2$ , we have:

$$\begin{aligned}
n/4 \leq K_1 = D_{\tau+1} + 18\tau + \frac{16\tau}{d}\Delta_\tau &\leq r \cdot \binom{\tau+1}{\leq r-1} + 18\tau + \frac{16\tau}{d}r \cdot \binom{\tau}{\leq r-2} \\
&\leq r \cdot \binom{2\tau}{\leq r-1} + 18\tau + \frac{16\tau}{d}r \cdot \binom{\tau}{\leq r-2} \\
&\leq r^2 \cdot \binom{2\tau}{r-1} + 18\tau + \frac{16\tau r^2}{d} \cdot \binom{\tau}{r-2} \\
&\leq r^2 \cdot (4e)^{r-1} \cdot \left(\frac{\tau}{r}\right)^{r-1} + 18r \left(\frac{\tau}{r}\right)^{r-1} + \frac{16}{d}r^3 \cdot (3e)^r \cdot \left(\frac{\tau}{r}\right)^{r-1} \\
&\leq 3 \cdot 18 \cdot (4e)^r \cdot r^3 \cdot \left(\frac{\tau}{r}\right)^{r-1} \\
&\leq 2^6 \cdot 2^{7r} \cdot \left(\frac{\tau}{r}\right)^{r-1},
\end{aligned}$$

which implies that

$$n \leq 2^8 \cdot 2^{7r} \cdot \left(\frac{\tau}{r}\right)^{r-1} \leq 2^{15r} \cdot \left(\frac{\tau}{r}\right)^{r-1},$$

which gives

$$\tau \geq r \cdot \left(n \cdot 2^{-15r}\right)^{\frac{1}{r-1}} \geq 2^{-30} \cdot rn^{\frac{1}{r-1}}.$$

*Case (2):*  $K_2 \geq n/4$ : In this case we have

$$n/4 \leq K_2 = \frac{16\tau D_\tau}{d \log\left(\frac{n}{2D_\tau}\right)},$$

which of course implies

$$64\tau D_\tau \geq dn \log\left(\frac{n}{2D_\tau}\right).$$

Now, notice that our earlier upper bounds on  $D_\tau$  yield

$$D_\tau \leq r \cdot \binom{\tau}{\leq r-1} \leq r^2 \cdot \binom{\tau}{r-1} \leq r^2 \cdot (2e)^{r-1} \cdot \left(\frac{\tau}{r}\right)^{r-1} \leq 2^{5r} \cdot \left(\frac{\tau}{r}\right)^{r-1},$$

and combining this with the previous inequality yields

$$64\tau \cdot 2^{5r} \cdot \left(\frac{\tau}{r}\right)^{r-1} \geq 64\tau D_\tau \geq dn \log\left(\frac{n}{2D_\tau}\right) \geq dn \log\left(\frac{n}{2^{5r+1} \cdot \left(\frac{\tau}{r}\right)^{r-1}}\right).$$

Then, applying straightforward bounds on both sides of the above chain of inequalities yields

$$2^{12r} \cdot \left(\frac{\tau}{r}\right)^r \geq dn \log\left(\frac{n}{2^{6r} \cdot \left(\frac{\tau}{r}\right)^{r-1}}\right). \quad (7)$$

We now seek to get a lower bound on all  $\tau$  that satisfy the above inequality. Towards this end, notice that for any  $\alpha > 0$  such that

$$2^{12r} \cdot \left(\frac{\alpha}{r}\right)^r < dn \log \left( \frac{n}{2^{6r} \cdot \left(\frac{\alpha}{r}\right)^{r-1}} \right), \quad (8)$$

it holds that all  $\tau$  that satisfy [Equation \(7\)](#) must also satisfy  $\tau \geq \alpha$ : this is because as  $\alpha$  decreases, the left hand side of the above inequality decreases, while its right hand side increases.

It is now straightforward to verify that

$$\alpha = 2^{-30} \cdot r \cdot (dn \log n)^{1/r}$$

satisfies [Equation \(8\)](#), as long as  $d \log n \leq n^{\frac{1}{r-1}-2^{-10r}}$ . Thus in this case we have

$$\tau \geq \alpha = 2^{-30} \cdot r \cdot (dn \log n)^{1/r},$$

provided  $d \log n \leq n^{\frac{1}{r-1}-2^{-10r}}$ .

To conclude, since one of the cases must hold, we get that

$$\tau \geq 2^{-30} \cdot \min\{rn^{\frac{1}{r-1}}, r(dn \log n)^{1/r}\}$$

if  $d \log n \leq n^{\frac{1}{r-1}-2^{-10r}}$ . But given this condition on  $d \log n$ , it always holds that  $r(dn \log n)^{1/r} \leq rn^{\frac{1}{r-1}}$ . Thus, as long as  $d \log n \leq n^{\frac{1}{r-1}-2^{-10r}}$ , we get that

$$T \geq \tau \geq 2^{-30} r (dn \log n)^{1/r},$$

as desired. □

## 5.2.2 On the tightness of our lower bounds

At last, all that remains is to show our lower bounds (in [Lemma 10](#)) are tight, in the following sense.

**Lemma 12** (Upper bound of [Theorem 10](#)). *There exist universal constants  $C, c > 0$  such that a random degree  $\leq r$  polynomial  $f \sim \mathbb{F}_2[x_1, \dots, x_n]$  is an extractor for  $d$ -local affine sources with min-entropy*

$$k \geq Cr \cdot (dn \log n)^{1/r}$$

*and error  $\varepsilon = 2^{-ck/r}$ , except with probability at most  $2^{-c\binom{k}{\leq r}}$  over the selection of  $f$ .*

Previously, we showed (in [Section 4](#)) that low-degree polynomials extract from  $d$ -local sources ([Theorem 2](#)), and our main ingredients were: (i) a reduction from  $d$ -local sources to  $d$ -local NOBF sources; and (ii) a result showing that low-degree polynomials extract from  $d$ -local NOBF sources (which relied heavily on a certain correlation bound we proved in [Section 4.2.1](#)).

To prove [Lemma 12](#), we wish to show that low-degree polynomials extract from  $d$ -local *affine* sources. These are much more structured than general  $d$ -local sources, and we are able to optimize the above framework to skip step (i) and rely on a stronger known correlation bound in step (ii). In particular, our key ingredient will be the following, which shows that a random low-degree polynomial has small bias (i.e., small correlation with the constant 1 function).

**Lemma 13** ([BHL12]). *For any fixed  $\varepsilon > 0$  there exist  $0 < c_1, c_2 < 1$  such that the following holds. Let  $f \sim \mathbb{F}_2[x_1, \dots, x_n]$  be a random polynomial of degree  $\leq r$  where  $r \leq (1 - \varepsilon)n$ . Then*

$$\Pr[\text{bias}(f) > 2^{-c_1 n/r}] \leq 2^{-c_2 \binom{n}{\leq r}}.$$

Given this result, we are now able to prove **Lemma 12** without too much trouble.

*Proof of Lemma 12.* Let  $\mathbf{X} \sim \mathbb{F}_2^n$  be a  $d$ -local affine source of dimension  $k$ . It is straightforward to show, via Gaussian elimination, that the following holds: there exists a subset  $S \subseteq [n]$  of size  $k$  such that  $\mathbf{X}_S$  is uniform over  $\mathbb{F}_2^k$ , and for every other  $j \in [n]$  there exists an affine function  $\ell_j : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$  such that  $\mathbf{X}_j = \ell_j(\mathbf{X}_S)$ . Without loss of generality, assume that  $S = [k]$ . Thus if we consider the function  $\ell : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n$  defined as

$$\ell(y_1, \dots, y_k) := (y_1, \dots, y_k, \ell_{k+1}(y_1, \dots, y_k), \dots, \ell_n(y_1, \dots, y_k))$$

we of course have  $\mathbf{X} = \ell(\mathbf{U}_k)$ , where  $\mathbf{U}_k \sim \mathbb{F}_2^k$  denotes the uniform random variable.

Now, let  $f \sim \mathbb{F}_2[x_1, \dots, x_n]$  be a random polynomial of degree  $\leq r$ . Notice that

$$|f(\mathbf{X}) - \mathbf{U}_1| = |f(\ell(\mathbf{U}_k)) - \mathbf{U}_1| = \text{bias}(f(\ell))/2$$

So we want to upper bound the probability that  $\text{bias}(f(\ell))$  is large, over our random selection of  $f$ . Well, consider fixing whether each monomial  $x^S$ ,  $S \not\subseteq [k]$  exists. Notice that under any such fixing,  $f(\ell)$  actually turns into a polynomial of the form  $f' + g$ , where  $f' \sim \mathbb{F}_2[x_1, \dots, x_n]$  is a uniformly random degree  $\leq r$  polynomial, and  $g$  is a sum of monomials, each of size at most  $r$ , where each term in each monomial is linear (i.e., degree 1). In other words,  $g$  is a fixed degree  $\leq r$  polynomial, and thus  $f' + g$  is a uniformly random degree  $\leq r$  polynomial over  $k$  variables.

Thus, by **Lemma 13**, we get that under *every* such fixing,  $\text{bias}(f(\ell)) \leq 2^{-c_1 k/r}$  except with probability  $\leq 2^{-c_2 \binom{k}{\leq r}}$ . Thus for a given  $d$ -local affine source  $\mathbf{X} \sim \mathbb{F}_2^n$  of min-entropy  $k$ , it holds that a random degree  $\leq r$  polynomial extracts from  $\mathbf{X}$  with error  $\leq 2^{-c_1 k/r}$ , except with probability  $\leq 2^{-c_2 \binom{k}{\leq r}}$ .

Now, it is not hard to show that there are at most  $\binom{k}{\leq d}^n \cdot 2^n$   $d$ -local affine sources of dimension  $k$ . Thus, by a union bound, we know that a random degree  $\leq r$  polynomial extracts from *all*  $d$ -local affine sources  $\mathbf{X} \sim \mathbb{F}_2^n$  of min-entropy  $k$ , except with probability at most

$$2^{-c_2 \binom{k}{\leq r}} \cdot \binom{k}{\leq d}^n \cdot 2^n.$$

Thus as long as  $\binom{k}{\leq d}^n \cdot 2^n \leq 2^{c_2 \binom{k}{\leq r}/2}$ , it holds that a random degree  $\leq r$  polynomial extracts from  $d$ -local affine sources with min-entropy  $k$  with error  $\leq 2^{-c_1 k/r}$ , with probability  $\geq 1 - 2^{-c_2 \binom{k}{\leq r}/2}$ . It is now easy to verify that the inequality  $\binom{k}{\leq d}^n \cdot 2^n \leq 2^{c_2 \binom{k}{\leq r}/2}$  holds for the stated lower bound on  $k$ .  $\square$

## 6 A barrier

In this final section, we prove a barrier result, which shows that previous techniques cannot be used to extract from local sources with min-entropy below  $\sqrt{n}$ .

In more detail, previous techniques [DW12, Vio14] show that local sources are close to a convex combination of affine sources (with almost the same min-entropy), which means that a black-box affine extractor can also extract from local sources. However, the arguments in [DW12, Vio14] only work if the local sources

start out with min-entropy  $\gg \sqrt{n}$ . On the other hand, it is not completely clear if this is an artifact of the exact arguments made in those works, or if local sources with min-entropy below  $\sqrt{n}$  simply cannot be shown to be close to a convex combination of affine sources, using *any* argument.

In our barrier result, stated below, we show that the latter is the case.

**Theorem 13** (Theorem 0, formal version). *There exists a 2-local source  $\mathbf{X} \sim \{0, 1\}^n$  with min-entropy  $k \geq \sqrt{n}$  that is  $(1/2)$ -far from a convex combination of affine sources with min-entropy 5.*

This barrier result confirms that it is impossible to use affine extractors in a standard black-box manner (i.e., using convex combinations) to extract from local sources with min-entropy below  $\sqrt{n}$ , for two reasons:

1. The statistical distance to a convex combination of affine sources is too large: since the statistical distance in Theorem 13 is  $\geq 1/2$ , a black-box application of an affine extractor result in error  $\geq 1/2$ , which is no better than the error of the trivial extractor (which just outputs a constant).
2. The entropy of the affine sources in the convex combination is too low: the entropy of the affine sources in Theorem 13 is 5, which is much less than the  $\Omega(\log n)$  entropy required for an affine extractor to even exist [ABGS21].

In order to prove Theorem 13, we use a 2-local source  $\mathbf{X} \sim \{0, 1\}^n$  called the *clique source*. We define the clique source over  $n = k + \binom{k}{2}$  bits to be the random variable  $\mathbf{X} \sim \{0, 1\}^n$  generated by sampling  $k$  independent and uniform bits  $\mathbf{Y}_1, \dots, \mathbf{Y}_k$  and outputting

$$\mathbf{X} = (\mathbf{Y}_1, \dots, \mathbf{Y}_k, (\mathbf{Y}_i \cdot \mathbf{Y}_j)_{1 \leq i < j \leq k}).$$

Then, we prove the following, from which Theorem 13 is immediate.

**Theorem 14.** *Let  $\mathbf{X} \sim \{0, 1\}^n$  be the clique source over  $n = \binom{k+1}{2}$  bits. Then for any  $t$ , it holds that  $\mathbf{X}$  is  $(1 - \varepsilon)$ -far from a convex combination of affine sources with min-entropy  $t$ , where*

$$\varepsilon = 2^{-(t-3)/2}.$$

The main lemma we use to prove Theorem 14 roughly shows that the collection of all cliques in the space of  $n$ -vertex graphs is a *subspace-evasive set* (a well-studied object in pseudorandomness: see, e.g., [DL12]). More formally, fix any  $n \in \mathbb{N}$  and let  $m := n + \binom{n}{2}$ . We identify  $\mathbb{F}_2^m$  with the set of all  $n$ -vertex (undirected) graphs as follows. First, fix an arbitrary identification of  $[m]$  with  $[n] \cup \binom{[n]}{2}$ , and let  $x \in \mathbb{F}_2^m$  represent the graph  $G_x = (V_x, E_x)$  where  $i \in V_x$  if and only if  $x_i = 1$  and  $e \in E_x$  if and only if  $x_e = 1$ . Then, we say that  $x \in \mathbb{F}_2^m$  is a clique if (and only if)  $E_x = \binom{V_x}{2}$ , and prove the following.

**Lemma 14.** *Let  $\mathcal{Q} \subseteq \mathbb{F}_2^m$  denote the collection of all cliques. Then for any affine subspace  $S \subseteq \mathbb{F}_2^m$  of dimension  $k$ ,*

$$\frac{|\mathcal{Q} \cap S|}{|S|} \leq 2^{-(k-3)/2}.$$

*That is, an exponentially small fraction of graphs in  $S$  are cliques.*

Before we prove Lemma 14 (in the following subsection), we show how it implies Theorem 14.

*Proof of Theorem 14.* Let  $\mathbf{Y} \sim \{0, 1\}^n$  be a convex combination of affine sources  $\{\mathbf{Y}^{(i)}\}_i$ , each with min-entropy  $t$ . Let  $S = \text{support}(\mathbf{X})$  and  $\bar{S} := \{0, 1\}^n - S$ . We have

$$\begin{aligned} |\mathbf{X} - \mathbf{Y}| &\geq \Pr[\mathbf{Y} \in \bar{S}] - \Pr[\mathbf{X} \in \bar{S}] = \Pr[\mathbf{Y} \in \bar{S}] \\ &\geq \min_i \Pr[\mathbf{Y}^{(i)} \in \bar{S}] = 1 - \max_i \Pr[\mathbf{Y}^{(i)} \in S] \\ &= 1 - \max_i \frac{|\text{support}(\mathbf{X}) \cap \text{support}(\mathbf{Y}^{(i)})|}{|\text{support}(\mathbf{Y}^{(i)})|}. \end{aligned}$$

It is easy to verify that each element  $x \in \text{support}(\mathbf{X})$  is a clique, and thus by Lemma 14 the above equality is at least  $1 - 2^{-(t-3)/2}$ , as desired.  $\square$

## 6.1 Cliques are subspace-evasive

Now, all that remains in the proof of our barrier result is to show that cliques are subspace-evasive (Lemma 14). We do so below.

*Proof of Lemma 14.* We start with the standard observation that it suffices to prove a slightly stronger version of the result just for vector subspaces, since every affine subspace  $T$  of dimension  $\kappa$  is contained in a vector subspace  $S$  of dimension  $k \leq \kappa + 1$  [PR04]. Thus

$$\frac{|\mathcal{Q} \cap T|}{|T|} > 2^{-(\kappa-3)/2} \implies \frac{|\mathcal{Q} \cap S|}{|S|} > 2^{-k/2+1}$$

so it suffices to show  $|\mathcal{Q} \cap S|/|S| \leq 2^{-k/2+1}$  for every vector subspace  $S$  of dimension  $k$ . Indeed, we proceed by proving this result.

Define  $\mathcal{Q}_S := \mathcal{Q} \cap S$ . Notice that for any  $x, y \in \mathcal{Q}_S$ , we know that  $x + y \in S$  as they each belong in  $S$ . By this observation, we see that  $\mathcal{Q}_S + \mathcal{Q}_S \subseteq S$ . Furthermore, we claim for any nonzero  $z \in \mathcal{Q}_S + \mathcal{Q}_S$ , there are at most 2 pairs  $(x, y) \in \mathcal{Q}_S \times \mathcal{Q}_S$  such that  $z = x + y$ . In other words,  $\mathcal{Q}_S$  is a Sidon set. Indeed, once we prove this, we find that  $|\mathcal{Q}_S|(|\mathcal{Q}_S| - 1)/2 \leq |\mathcal{Q}_S + \mathcal{Q}_S| - 1 \leq |S| - 1$ . Thus  $|\mathcal{Q}_S|^2/4 < |S|$ , and so  $|\mathcal{Q}_S|/|S| < 2/\sqrt{|S|} = 2^{-k/2+1}$ , which is what we wanted to show.

Consider the linear map  $\varphi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^{k \times k}$  where the matrix  $M = \varphi(Y)$  is defined by  $M_{ij} = M_{ji} = Y_{ij}$ . The key observation with this map is noticing that the set  $\varphi(Q)$  corresponds exactly to the rank-1 matrices in  $\text{im}(\varphi)$  as  $\varphi(Y) = xx^\top$  for any  $Y \in Q$ . Now, for any nonzero vector  $v \in \mathcal{Q}_S + \mathcal{Q}_S$ , let us count the number of  $y, y' \in \mathcal{Q}_S$  such that  $v = y + y'$ . By linearity and injectivity of  $\varphi$ , this is equivalent to counting the number of  $x, x' \in \mathbb{F}_2^l$  satisfying  $M_v = xx^\top + x'x'^\top$  where  $M_v = \varphi(v)$ .

Consider one such solution  $M_v = zz^\top + z'z'^\top$ . From the equation  $M_v = zz^\top + z'z'^\top$ , we see that the row space of  $M_v$ , which we denote by  $\mathcal{R}(M_v)$ , is contained in the span of  $z$  and  $z'$ . Furthermore, since  $M_v$  is nonzero, then  $z \neq z'$ . Thus at least two of the elements in  $\{z, z', z + z'\}$  must be rows in  $M_v$ . This implies that the span of  $z$  and  $z'$  is contained in  $\mathcal{R}(M_v)$ . Hence  $\mathcal{R}(M_v) = \{0, z, z', z + z'\}$ .

For any other such solution  $M_v = xx^\top + x'x'^\top$ , we also find by repeating the same steps that  $x \neq x'$  and  $\mathcal{R}(M_v) = \{0, x, x', x + x'\} = \{0, z, z', z + z'\}$ . Let us now consider 2 possible cases:

1. If either  $z$  or  $z'$  is zero, then without loss of generality, say  $z' = 0$ . Then either  $(x, x') = (z, 0)$  or  $(x, x') = (0, z)$ . Thus there are at most 2 possible pairs  $(x, x')$  for this case.
2. If both  $z$  and  $z'$  are nonzero, then both  $x$  and  $x'$  must be nonzero. Furthermore,  $x, x'$  must be one of the elements in  $\{z, z', z + z'\}$ . From all 6 possible pairs, only the pairs  $(z, z')$  and  $(z', z)$  satisfy the equation  $M_v = xx^\top + x'x'^\top$ . Thus there are at most 2 possible pairs  $(x, x')$  for this case.

Since these are the only two possible cases, this therefore shows that  $\mathcal{Q}_S$  is a Sidon set, which is what we wanted to show.  $\square$

## References

- [ABGS21] Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. Fine-grained hardness of CVP(P) - everything that we can prove (and nothing else). In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021*, pages 1816–1835. SIAM, 2021.
- [BG13] Andrej Bogdanov and Siyao Guo. Sparse extractor families for all the entropy. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS '13*, page 553–560, New York, NY, USA, 2013. Association for Computing Machinery.
- [BHL12] Ido Ben-Eliezer, Rani Hod, and Shachar Lovett. Random low-degree polynomials are hard to approximate. *Comput. Complex.*, 21(1):63–81, 2012.
- [CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.
- [CG21] Eshan Chattopadhyay and Jesse Goodman. Improved extractors for small-space sources. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 610–621, 2021.
- [CGGL20] Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, and Xin Li. Extractors for adversarial sources via extremal hypergraphs. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020*, page 1184–1197, 2020.
- [CL18] Kuan Cheng and Xin Li. Randomness extraction in  $AC^0$  and with small locality. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, volume 116 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 37:1–37:20, Dagstuhl, Germany, 2018.
- [CLP17] Ernie Croot, Vsevolod Lev, and Péter Pach. Progression-free sets in  $\mathbb{Z}_4^n$  are exponentially small. *Annals of Mathematics*, 185(1):331 – 337, 2017.
- [CT15] Gil Cohen and Avishay Tal. Two structural results for low degree polynomials and applications. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2015)*, volume 40 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 680–709, Dagstuhl, Germany, 2015.
- [DL12] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, STOC '12*, page 351–358, New York, NY, USA, 2012. Association for Computing Machinery.
- [DW12] Anindya De and Thomas Watson. Extractors and lower bounds for locally samplable sources. *ACM Trans. Comput. Theory*, 4(1), March 2012.

- [DY21] Yevgeniy Dodis and Kevin Yeo. Doubly-affine extractors, and their applications. In *2nd Conference on Information-Theoretic Cryptography (ITC 2021)*, pages 13:1–13:23, Dagstuhl, Germany, 2021.
- [GVW15] Oded Goldreich, Emanuele Viola, and Avi Wigderson. On randomness extraction in AC0. In *30th Conference on Computational Complexity (CCC 2015)*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 601–668, Dagstuhl, Germany, 2015.
- [HIV21] Xuangui Huang, Peter Ivanov, and Emanuele Viola. Affine extractors and AC0-parity. *Electron. Colloquium Comput. Complex.*, page 137, 2021.
- [KLP12] Tali Kaufman, Shachar Lovett, and Ely Porat. Weight distribution and list-decoding size of Reed–Muller codes. *IEEE Transactions on Information Theory*, 58(5):2689–2696, 2012.
- [KRVZ11] Jesse Kamp, Anup Rao, Salil P. Vadhan, and David Zuckerman. Deterministic extractors for small-space sources. *J. Comput. Syst. Sci.*, 77(1):191–220, 2011.
- [Li16] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 168–177, 2016.
- [Lu04] Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *J. Cryptol.*, 17(1):27–42, 2004.
- [LY21] Jiayu Li and Tianqi Yang.  $3.1n - o(n)$  circuit lower bounds for explicit functions. In *Electron. Colloquium Comput. Complex.*, volume 28, page 23, 2021.
- [PR04] Pavel Pudlák and Vojtěch Rödl. Pseudorandom sets and explicit constructions of Ramsey graphs. *Complexity of Computations and Proofs. Quad. Mat. 13 Dept. Math. Seconda Univ. Napoli Caserta*, pages 327–346, 2004.
- [TV00] Luca Trevisan and Salil Vadhan. Extracting randomness from samplable distributions. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 32–42, 2000.
- [Vad04] Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *J. Cryptol.*, 17(1):43–77, 2004.
- [Vio05] Emanuele Viola. The complexity of constructing pseudorandom generators from hard functions. *Comput. Complex.*, 13(3-4):147–188, 2005.
- [Vio14] Emanuele Viola. Extractors for circuit sources. *SIAM Journal on Computing*, 43(2):655–672, 2014.
- [Vio16] Emanuele Viola. Quadratic maps are hard to sample. *ACM Trans. Comput. Theory*, 8(4), jun 2016.
- [Vio20] Emanuele Viola. Sampling lower bounds: Boolean average-case and permutations. *SIAM Journal on Computing*, 49(1):119–137, 2020.
- [War36] Ewald Warning. Bemerkung zur vorstehenden arbeit von Herrn Chevalley. *Abh. Math. Sem. Univ. Hamburg*, 11:76–83, 1936.