Electronic Colloquium on Computational Complexity, Report No. 140 (2023)

Extractors for Polynomial Sources over $\mathbb{F}_2$

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

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

Mohit Gurumukhani*
Cornell University
mgurumuk@cs.cornell.edu

Abstract

We explicitly construct the first nontrivial extractors for degree $d \geq 2$ polynomial sources over $\mathbb{F}_2^n$. Our extractor requires min-entropy $k \geq n - \frac{\sqrt{\log n}}{(d \log \log n)^{d/2}}$. Previously, no constructions were known, even for min-entropy $k \geq n-1$. A key ingredient in our construction is an *input reduction lemma*, which allows us to assume that any polynomial source with min-entropy k can be generated by $O(k)$ uniformly random bits.

We also provide strong formal evidence that polynomial sources are unusually challenging to extract from, by showing that even our most powerful general purpose extractors cannot handle polynomial sources with min-entropy below $k \geq n - o(n)$. In more detail, we show that *sumset extractors* cannot even *disperse* from degree 2 polynomial sources with min-entropy $k \geq n - O(n/\log \log n)$. In fact, this impossibility result even holds for a more specialized family of sources that we introduce, called *polynomial non-oblivious bit-fixing (NOBF) sources*. Polynomial NOBF sources are a natural new family of algebraic sources that lie at the intersection of polynomial and variety sources, and thus our impossibility result applies to both of these classical settings. This is especially surprising, since we *do* have variety extractors that slightly beat this barrier - implying that sumset extractors are not a panacea in the world of seedless extraction.

1 Introduction

Randomness is a very important resource in computation. It is widely used in theoretical and practical implementations of algorithms, distributed computing protocols, cryptographic protocols, machine learning algorithms, and much more [MR95]. Unfortunately, the randomness produced in practice is not of the highest quality, and the corresponding distribution over bits is often biased and has various correlations [HG17]. To overcome this, an extractor is used to convert this biased distribution to a uniform distribution. The extractors used in practice are based on unproven theoretical assumptions and so the theoretical study of constructing efficient extractors is important. Extractors usually come in two flavors: seeded and seedless extractors. We focus here on constructing seedless extractors and whenever we mention 'extractor' we refer to seedless extractor.

Let's formally define extractor for a class of distributions:

*Supported by a Sloan Research Fellowship and NSF CAREER Award 2045576.

ISSN 1433-8092

Definition 1 (Extractor)**.** *A function* $\mathsf{Ext} : \{0,1\}^n \to \{0,1\}^m$ *is called an* ε*-extractor for a class* $\mathcal{C}$ *of distributions over* $\{0,1\}^n$ *if for all* $\mathbf{X} \in \mathcal{C}$*,*

$$|\mathsf{Ext}(\mathbf{X}) - \mathbf{U}_m| \leq \varepsilon,$$

where $|\cdot|$ *denotes statistical distance and* $\mathbf{U}_m$ *is the uniform random variable.*

In this paper and throughout, we use min-entropy as our measure for randomness: For a source $\mathbf{X}$ with support Ω, we define it's min-entropy $H_\infty(\mathbf{X}) = -\log(\max_{x\in\Omega} \Pr(\mathbf{X} = x))$. Note that for $\mathbf{X} \sim \{0,1\}^n$, $0 \leq H_\infty(\mathbf{X}) \leq n$.

It is well known that there do not exist extractors for arbitrary distributions even when they have a lot of randomness (min-entropy = $n-1$). To overcome this, a long body of work has been dedicated to extracting randomness from distributions that have some min-entropy, and further are samplable, i.e., generated by low complexity classes such as AC^0 circuits, decision trees, local sources, branching programs, etc, [TV00; KRVZ11; DW12; Vio14; CG21; ACGLR22]. This study has provided insights into the structure of such complexity classes. Moreover, there is an argument to be made that in practice, the distributions encountered by extractors seem to be generated by such low complexity classes. We here study *algebraic sources*, i.e., sampled by low degree multivariate polynomials over $\mathbb{F}_2$, which is another such natural computational model.

Primarily, two kinds of algebraic sources have been studied: variety sources and polynomial sources. The task of constructing extractors for these sources, apart from being a fundamentally important task to help us gain structural insights into polynomials, also has other nice motivations.

Extractors for polynomial sources (over $\mathbb{F}_2$) with $\mathrm{poly}(\log n)$ degree would immediately yield extractors for sources sampled by $\mathsf{AC}^0[\oplus]$ circuits based on well-known approximations of such circuits by polynomials [Raz87; Smo93].[1] To the best of our knowledge, there are no nontrivial efficient extractors for sources sampled by such circuits.

The task of constructing variety extractors has a very nice circuit lower bound motivation: It is known that if one can construct explicit extractors or even dispersers (see Definition 3.9) against degree 2 varieties over $\mathbb{F}_2^n$ with min-entropy $0.01n$ or against degree $n^{0.01}$ varieties over $\mathbb{F}_2^n$ with min-entropy $0.99n$, then one immediately gets new state-of-the-art circuit lower bounds [GK16; GKW21].

Let's finally define these sources. Both variety sources and polynomial sources are parameterized by min-entropy k, degree d and finite field $\mathbb{F}_q^n$:

Remark 1. *In the algebraic setting, it is typical to associate* $\{0,1\}^n$ *equivalently with* $\mathbb{F}_2^n$*. More generally, one can also define extractors over other domains and co-domains such as* $\mathbb{F}_q^n$ *for arbitrary prime power* q*.*

Definition 2 (Polynomial sources)**.** *Here, each source* $\mathbf{X} \sim \mathbb{F}_q^n$ *is associated with a degree* d *polynomial map* $P = (p_1, \ldots, p_n)$ *where for* $1 \leq i \leq n, p_i : \mathbb{F}_q^m \to \mathbb{F}_q$*. Then,* $\mathbf{X} = P(U_m)$ *where* U_m *is the uniform distribution over* $\mathbb{F}_q^m$*.*

Definition 3 (Variety sources)**.** *Here, each source* $\mathbf{X} \sim \mathbb{F}_q^n$ *has associated polynomials* $p_1, \ldots, p_m : \mathbb{F}_q^n \to \mathbb{F}_q$*.* $\mathbf{X}$ *is uniform over the variety generated by these degree* d *polynomials, i.e., it is uniform over the set* $V = \{x \in \mathbb{F}_q^n : \forall i \in [m] : p_i(x) = 0\}$*.*

In this paper, we introduce and study a natural class of sources that is a subclass of polynomial sources and the widely studied NOBF sources. Surprisingly, it is also a subclass of variety sources (see Claim 1).

[1] $\mathsf{AC}^0[\oplus]$ circuits are constant depth, polynomial sized circuits with unbounded fan-in AND, OR, NOT, PARITY gates.

Definition 4 (Polynomial NOBF sources)**.** *Here, each source $\mathbf{X} \sim \mathbb{F}_q^n$ with $H_\infty(\mathbf{X}) = k$ must have k as an integer. Moreover, it is associated with $n-k$ degree d polynomials $p_1, \ldots, p_{n-k}$ where for each $1 \leq i \leq n-k, p_i : \mathbb{F}_q^k \to \mathbb{F}_q$. Then, $\mathbf{X}$ is uniform over the set*

$$S = \{\forall x_1, \ldots, x_k \in \mathbb{F}_q^k : (x_1, \ldots, x_k, p_1(x_1, \ldots, x_k), \ldots, p_{n-k}(x_1, \ldots, x_k))\}$$

Typically, NOBF sources have k independent uniform bits which we call 'good' bits and $n-k$ 'bad' bits which are arbitrary functions of the good bits. Polynomial NOBF sources are a subset of such sources where the $n-k$ bad bits are degree d polynomial functions of the good bits. We make a basic observation regarding polynomial NOBF sources (this observation seems to apply to most classes of samplable, NOBF, and recognizable sources):

Claim 1. *If $\mathbf{X} \sim \mathbb{F}_q^n$ is a degree d polynomial NOBF source then it is also a degree d polynomial source and a degree d variety source.*

Proof. Let $H_\infty(\mathbf{X}) = k$ and the bad bits be specified by polynomials $p_1, \ldots, p_{n-k}$. As the k good bits are degree 1 polynomials over $x_1, \ldots, x_k$ and the $n-k$ bad bits are degree d polynomials over $x_1, \ldots, x_k$, $\mathbf{X}$ is indeed a polynomial source. Without loss of generality assume that first k bits of $\mathbf{X}$ are the good bits and last $n-k$ are the bad bits. Consider the following set of polynomial equations over variables $y_1, \ldots, y_n$:

$$\begin{aligned} y_{k+1} + p_1(y_1, \ldots, y_k) &= 0 \\ &\vdots \\ y_n + p_{n-k}(y_1, \ldots, y_k) &= 0 \end{aligned}$$

We observe that $\mathbf{X}$ is uniform over the variety defined by these equations and hence is also a variety source. □

1.1 Related work

Degree 1 polynomial / variety sources, i.e., affine sources have been widely studied both over $\mathbb{F}_2^n$ as well as other $\mathbb{F}_q^n$ [Bou07; GR08; Rao09; BKSSW10; DG10; Li11; Sha11; Yeh11; BK12; BDL16; Li16; CGL21; GVJZ23]. Recently, [Li23] constructed affine extractors over $\mathbb{F}_2^n$ with asymptotically optimal dependence on min-entropy.

[DGW09] initiated the study of extractors for polynomial sources. Their extractors worked when either when $q \geq \mathrm{poly}(n,d)^{\Omega(k)}$ or when field has characteristic $\geq \mathrm{poly}(n,k,d)$. [BG13] used sum product estimates and constructed extractors for degree 2 polynomial sources when $q \geq \Omega(1)$ and min-entropy is $\geq \Omega(n)$. They also constructed dispersers for arbitrary multilinear polynomials over $\mathbb{F}_4^n$ with min-entropy $\geq n/2 + \Omega(1)$. Extractors for variety sources were first constructed by [Dvi12]. They constructed extractors for when either $q \geq \exp(n)$ or $q \geq \mathrm{poly}(d)$ and min-entropy $\geq \Omega(n)$. Recently, [GVJZ23] constructed extractors for images of varieties over $\mathbb{F}_q^n$ when $q \geq \mathrm{poly}(n,d)$ with no min-entropy restrictions. Over $\mathbb{F}_2^n$, [Rem16] constructed extractors for degree n^{δ_1} varieties with min-entropy $\geq n - n^{\delta_2}$ for arbitrary $\delta_1 + \delta_2 < \frac{1}{2}$. Using correlation bounds against low degree polynomials, [CT19; LZ19] constructed extractors for constant degree d variety sources over $\mathbb{F}_2^n$ with min-entropy $\geq (1 - c_d)n$ where c_d is a tiny constant that depends on d.

We reiterate that before our work, no extractors were constructed for polynomial sources over $\mathbb{F}_2^n$ even for min-entropy $k \geq n - 1$!

1.2 Our results

We construct extractors for polynomial sources over $\mathbb{F}_2^n$:

Theorem 1 (Explicit extractor for polynomial sources, informal version of Theorem 5.3)**.** *Let $\varepsilon > 0$ be arbitrary constant. For all $d \in \mathbb{N}$, there exists an explicit ε-extractor for degree d polynomial sources over $\mathbb{F}_2^n$ with min-entropy $k \geq n - \frac{\sqrt{\log n}}{(d \log\log n)^{d/2}}$.*

We emphasize that these are the first ever extractors constructed for any degree $d > 1$ polynomial sources over $\mathbb{F}_2^n$. Algebraic extractors have been studied several times before for either degree 1 sources over $\mathbb{F}_2^n$ or for base field $\mathbb{F}_q$ when $q > 2$. (This was discussed above in Section 1.1.)

As polynomial sources can have arbitrarily large input length, it's not clear what is the size of the class of degree d polynomial sources. Hence, it's unclear whether an extractor should even exist for this class. To get around this problem, we come up with an input reduction technique that allows us to bound the number of inputs to the polynomial source by the min-entropy of the source. We view this as our main technical contribution and this proved to be the key ingredient for our extractor construction:

Lemma 1 (Input reduction, informal version of Corollary 4.2)**.** *Let $\mathsf{Ext} : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be an extractor for the class of degree d polynomial sources with min-entropy k and $O(k)$ inputs. Then, Ext is also an extractor for the class of degree d polynomial sources with min-entropy $\Omega(k)$ and arbitrary inputs.*

We also show negative results for polynomial NOBF sources against sumset extractors. Sumset extractors are extremely powerful and can be used to extract not only from sumset sources but also, using reductions to sumset sources, from many well studied models of weak sources such as degree 1 polynomial / variety sources (affine sources), class of two independent sources, sources generated by branching programs, sources generated by AC^0 circuits and many more [CL22]. Let's first define sumset sources:

Definition 5. *A source $\mathbf{X}$ is a (k, k) sumset source if it is of the form $\mathbf{A} + \mathbf{B}$, where $\mathbf{A}, \mathbf{B}$ are independent distributions on $\{0,1\}^n$ with $H_\infty(\mathbf{A}) \geq k, H_\infty(\mathbf{B}) \geq k$, and $+$ denotes bitwise xor.*

Note that $k \leq H_\infty(\mathbf{X}) \leq 2k$ and so, $H_\infty(\mathbf{X}) = \Theta(k)$. When we write $H_\infty(\mathbf{X})$ is a sumset source of min-entropy k, we actually mean $\mathbf{X} = \mathbf{A} + \mathbf{B}$ where $H_\infty(\mathbf{A}) \geq k, H_\infty(\mathbf{B}) \geq k$. Recently, sumset extractors with the smallest possible dependence on min-entropy ($O(\log n)$) were constructed [Li23]. A natural question is whether various algebraic sources can be reduced to sumset sources. We show here that sumset extractors cannot even disperse (see Definition 3.9) let alone extract below certain min-entropy against quadratic NOBF sources.

Theorem 2 (Sumset extractor lower bound, informal version of Theorem 6.7)**.** *Sumset extractors cannot be used to disperse from degree 2 polynomial NOBF sources with min-entropy $n - O\left(\frac{n}{\log\log n}\right)$.*

As polynomial NOBF sources are both variety *and* polynomial sources, this also implies that sumset extractors cannot be used to extract from degree 2 variety sources or degree 2 polynomial sources over $\mathbb{F}_2^n$ with min-entropy below $n - O\left(\frac{n}{\log\log n}\right)$. For degree 2 variety sources over $\mathbb{F}_2^n$, one can use a sumset extractor to extract above min-entropy $n - O\left(\frac{n}{\log n}\right)$ [CT15]. Moreover, using correlation bounds, one can construct explicit extractors against degree 2 varieties with min-entropy $(1-c)n$ for very small constant c [LZ19]. Hence, the above result shows that sumset extractors cannot be used to get better extractors than what we get using correlation bounds against low degree polynomials. We find this surprising as it implies the generalized inner product function is a better extractor for degree 2 variety sources than any optimal sumset extractor.

Organization The rest of the paper is organized as follows: In Section 2, we give an overview of our proofs. In Section 3, we provide basic definitions and useful properties that we use later. In Section 4, we prove Lemma 1, our input reduction argument. In Section 5, we prove Theorem 1, the construction of polynomial source extractor. In Section 6, we prove Theorem 2, limitations of the sumset extractor against quadratic NOBF sources. In Section 7, we conclude with various open problems.

2 Proof overview

2.1 Probabilistic construction

To warm up, it is not clear whether a random function is a good extractor for degree d polynomial sources. Usually such proofs proceed by arguing that for a fixed source of min-entropy k, a random function is an ε-extractor with probability at least $1-2^{-2^k\varepsilon^2}$. Then, one can do a union bound over total number of sources in the class to obtain that a random function is a good extractor. The main issue that arises for polynomial sources is that the number of input variables to the polynomials can be arbitrary and hence, it's not clear what is the size of this class. To overcome this difficulty, we use our input reduction argument:

Lemma 2.1 (Informal version of Corollary 4.7)**.** *For any degree d polynomial source $\mathbf{X} \sim \mathbb{F}_2^n$ with arbitrary input length, there exists a degree d polynomial source $\mathbf{X}' \sim \mathbb{F}_2^n$ with input length $\ell = O(n)$ such that $|\mathbf{X}' - \mathbf{X}| \leq 2^{-n}$.*

This is an incomparable version of our input reduction statement Lemma 1. This version of input reduction result reduces input length to $O(n)$ but is more general: we show that for any source $\mathbf{X}$ and $\varepsilon > 0$, there exists a single degree d polynomial source X' with input length at most $\ell = n + 3\log(1/\varepsilon)$ such that $|X - X'| \leq \varepsilon$. We refer the reader to Lemma 4.6 for more details.

Using this it suffices to consider degree d polynomial sources with $O(n)$ inputs. This class of polynomial sources has size $2^{O(n)^d \cdot n}$. Thus, the the earlier union bound based argument now works out:

Lemma 2.2 (Informal version of Lemma 5.1)**.** *A random function with $O(k)$ output bits is a $2^{-\Omega(k)}$ extractor for degree d polynomial sources over $\mathbb{F}_2^n$ with min-entropy $k \geq d \log n$.*

2.2 Input reduction

The input reduction argument was useful for showing existential results. It turns out to be useful for explicit constructions as well. We first sketch a proof of Lemma 2.1, that we noted is an incomparable version of our general input reduction result (Lemma 1). We then present a proof sketch of Lemma 1.

Proof sketch of Lemma 2.1. We get input reduction by showing that for a fixed degree d polynomial source $\mathbf{X}$ with m input bits, there exists another degree d polynomial source $\mathbf{X}'$ with $O(n)$ input bits such that $|\mathbf{X} - \mathbf{X}'| \leq \varepsilon$. It suffices to prove the following:

Lemma 2.3 (Informal version of Lemma 4.4)**.** *For any function $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$, there exists a degree 1 polynomial map $G : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ with $\ell = O(n)$ such that*

$$|f(\mathbf{U}_m) - f(G(\mathbf{U}_\ell))| \leq 2^{-n}$$

If f is a degree d polynomial map, then $f(G(\cdot))$ is also a degree d polynomial map and hence, we set $\mathbf{X}' = f(G(U_\ell))$ to get the desired input reduction. □

Proof sketch of Lemma 2.3. We use a strong linear seeded extractor (Definition 3.10) $\mathsf{sExt} : \{0,1\}^m \times \{0,1\}^s \to \{0,1\}^{m-O(n)}$. The existence of such a linear seeded extractor is guaranteed by Theorem 3.13.[2] Using the min-entropy chain rule (see Lemma 3.6) and properties of the extractor, we show that:

Proposition 2.4 (Informal version of Proposition 3.12)**.** *For any function $f : \{0,1\}^m \to \{0,1\}^n$ and independent uniform $\mathbf{A} \sim \{0,1\}^m, \mathbf{S} \sim \{0,1\}^s$,*

$$|\mathsf{sExt}(\mathbf{A},\mathbf{S}) \circ \mathbf{S} \circ f(\mathbf{A}) - \mathbf{U}_{m-O(n)} \circ \mathbf{S} \circ f(\mathbf{A})| \leq 2^{-n}$$

where $\mathbf{U}_{m-O(n)} \sim \{0,1\}^{m-O(n)}$ is the uniform distribution.

This implies there must exist a fixing $b \in \{0,1\}^{m-O(n)}$ such that

$$|(f(\mathbf{A})|\mathsf{sExt}(\mathbf{A},\mathbf{S}) = b) - f(\mathbf{A})| \leq 2^{-n}.$$

However, fixing $\mathsf{sExt}(\mathbf{A},\mathbf{S}) = b$ induces $m - O(n)$ linear constraints on the input bits. Equivalently, there exists an affine subspace of dimension $O(n)$ over which the resulting polynomial source is close to the original polynomial source. For more details, see Lemma 4.4. □

For our actual construction, the use of better input reduction from Lemma 1 does matter and gives us better parameters than what the weaker version would give. Here is a proof sketch for this, see Corollary 4.2 for more details:

Proof sketch of Lemma 1. Fix a polynomial source $\mathbf{X} \sim \mathbb{F}_2^n$ with m inputs and min-entropy slightly more than k. Let $g : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be an extractor for polynomial sources with $O(k)$ inputs and min-entropy k (so $t \leq k$). Let $\mathsf{sExt} : \mathbb{F}_2^n \times \mathbb{F}_2^s \to \mathbb{F}_2^k$ be a linear seeded extractor. Let $y \in \mathbb{F}_2^s$ be a good seed of the extractor for sExt when applied to $\mathbf{X}$. Now, define $h : \mathbb{F}_2^m \to \mathbb{F}_2^{k+t}$ as

$$h(x) = \mathsf{sExt}(f(x), y) \circ g(f(x))$$

Now, apply Lemma 2.3 to h to infer that there exists an affine function $A : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ with $\ell = O(k+t) = O(k)$ such that $h(\mathbf{U}_m) \approx_{2^{-\Omega(k)}} h(A(\mathbf{U}_\ell))$. Notice that $H_\infty(h(\mathbf{U}_m)) \geq k$ and so $h(A(\mathbf{U}_\ell))$ has smooth min-entropy (Definition 3.7) at least k. Let $\mathbf{Z} = f(A(\mathbf{U}_\ell))$. Then, $\mathbf{Z}$ is a degree d polynomial source from $O(k)$ bits to n bits. We also see that

$$h(A(\mathbf{U}_\ell)) = \mathsf{sExt}(f(A(\mathbf{U}_\ell), y)) \circ g(f(A(\mathbf{U}_\ell))) = \mathsf{sExt}(\mathbf{Z}, y) \circ g(\mathbf{Z})$$

As $h(A(\mathbf{U}_\ell))$ has smooth min-entropy at least k, it must be that $\mathbf{Z}$ has smooth min-entropy at least k (see Lemma 3.8 for a proof). We set the distance parameter in smooth min-entropy small enough so that if $\mathbf{Z}$ has smooth min-entropy k, then it has min-entropy $\Omega(k)$. Furthermore, it must be that $g(f(\mathbf{U}_m)) \approx_{2^{-\Omega(k)}} g(\mathbf{Z}) = g(f(A(\mathbf{U}_\ell)))$. Thus, as g extracts from $\mathbf{Z}$, it also extracts from $g(f(\mathbf{U}_m))$ as desired. □

We also note that all these input reduction arguments work in general for arbitrary samplable sources as long as they are closed under affine restrictions.

[2] Interestingly, for our argument, we do not need this extractor to be explicit.

2.3 Explicit construction

We here sketch the proof for a slightly weaker result that illustrates our main idea:

Theorem 2.5 (Weaker version of Theorem 1)**.** *There exists explicit extractor* $\mathsf{Ext} : \mathbb{F}_2^n \to \mathbb{F}_2$ *for all constant degree* $d \in \mathbb{N}$ *polynomial sources with min-entropy* $k \geq n - O(\log\log n)$.

Proof sketch. Fix degree d polynomial source $\mathbf{X}$ with m inputs and n outputs with min-entropy $n - g$ where $g = O(\log\log n)$. Consider a small length $t = 2g$ prefix of the output bits and let this source be $\mathbf{X}_{pre}$. We observe that $\mathbf{X}_{pre}$ has min-entropy at least $t - g = t/2$ (see Claim 5.4). We now use our input reduction argument: Lemma 2.1 over $\mathbf{X}_{pre}$ to infer there exists a source $\mathbf{X}'_{pre}$ with $O(t)$ inputs such that $|\mathbf{X}'_{pre} - \mathbf{X}_{pre}| \leq 2^{-t}$. Hence, it suffices to construct an extractor for min-entropy $t/2$ degree d polynomial sources with $O(t)$ inputs and t outputs.

By Lemma 2.2, we know a random function over t bits will be an extractor for such sources. We exhaustively try all the 2^{2^t} functions from t bits to 1 bits as our candidate extractor. We brute force search over all $2^{O(t)^d \cdot t}$ degree d polynomial sources with $O(t)$ inputs and t outputs and for each of them, check if it has enough min-entropy. If it does, we input the source into our candidate extractor and check if the output is close to uniform. We will eventually find a candidate extractor that will work for all such sources, and we output that function as our extractor.

The time required by the above procedure is $2^{2^t + O(t)}$. As $t = O(\log\log n)$, the above procedure indeed runs in $\mathrm{poly}(n)$ time. □

In our actual construction, we achieve better parameters by brute forcing over all r-wise independent functions (for very large r) as our candidate extractor instead of all functions. We also use our more powerful input reduction lemma (Lemma 1) to reduce number of input variables to $O(k)$ so that the class of polynomial sources that we have to brute force over becomes smaller. Together, these optimizations allow us to handle smaller min-entropy. See Theorem 5.3 for details.

2.4 Impossibility results

All our impossibility results are against polynomial NOBF sources and hence apply to both polynomial sources and variety sources. We show that sumset extractors, arguably the most powerful general purpose extractors, cannot be used to even disperse from degree 2 polynomial NOBF sources below min-entropy $n - O\left(\frac{n}{\log\log n}\right)$ (Theorem 2). We will use the following useful theorem to show this:

Theorem 2.6 (Informal version of Theorem 6.6)**.** *There exists a degree* 2 *polynomial NOBF source* $\mathbf{X} \sim \mathbb{F}_2^n$ *with* $H_\infty(\mathbf{X}) = n - O\left(\frac{n}{\log\log n}\right)$ *such that for all* $\mathbf{A}, \mathbf{B} \sim \mathbb{F}_2^n, H_\infty(\mathbf{A}) \geq \Omega(\log\log n), H_\infty(\mathbf{B}) \geq \Omega(\log\log n)$*, it holds that* $\mathit{support}(\mathbf{A}) + \mathit{support}(\mathbf{B}) \not\subset \mathit{support}(\mathbf{X})$.

Proof sketch. We take the $n - k$ bad bits in $\mathbf{X}$ to be random degree 2 polynomials. Say such $\mathbf{A}, \mathbf{B}$ exist and let C, D be projections of support$(\mathbf{A})$, support$(\mathbf{B})$ respectively onto the good bits of $\mathbf{X}$. Let $P : \mathbb{F}_2^k \to \mathbb{F}_2^{n-k}$ be the polynomial map of the bad bits. Then, it holds that $P(C)+P(D) = P(C+D)+y$ for some $y \in \mathbb{F}_2^{n-k}$. To simplify presentation, assume for this proof sketch that $y = 0^{n-k}$. We first observe the following:

Claim 2.7 (Informal version of Claim 6.9)**.** *There exist affine subspaces* U, V *such that* $P(U) + P(V) = P(U + V)$ *and* $|U| \geq |C|, |V| \geq |D|$.

Hence, without loss of generality we can assume that C and D are affine subspaces. We now use a probabilistic argument to show such large affine subspaces C and D cannot exist with high probability for a random quadratic map:

Claim 2.8 (Informal version of Claim 6.8)**.** *There exists degree 2 polynomial map $P : \mathbb{F}_2^k \to \mathbb{F}_2^{k-n}$ such that for every pair of affine subspaces U, V, both of dimension $\geq \Omega(\log \log n)$, there exist $u \in U, v \in V$ such that $P(u) + P(v) \neq P(u + v)$.*

Hence, the sumset property is violated and we get a contradiction. □

Using these, we finally present the proof of our lower bound result:

Proof sketch of Theorem 2. Let $\mathbf{X}$ be the degree 2 polynomial NOBF source with min-entropy $n - O\left(\frac{n}{\log \log n}\right)$ that doesn't contain any sumset of min-entropy $O(\log \log n)$. We apply a bipartite Ramsey bound (Corollary 3.17), to show that if a quadratic NOBF source doesn't contain sumsets where each of the two sets has size s, then it has small intersection with sumsets where each of the two sets has size $O(2^s)$ (see Lemma 6.11 for details). This implies $\mathbf{X}$ has very small intersection with sumset sources of min-entropy $\Omega(\log n)$. From this, we infer $\mathbf{X}$ is far away from any convex combination (see Definition 3.14) of sumset sources with min-entropy $\Omega(\log n)$. As sumset extractors below min-entropy $O(\log n)$ cannot exist (every function is constant on $\Omega(\log n)$ dimensional affine subspace), this shows we cannot use sumset extractors to even disperse against quadratic NOBF sources. See Theorem 6.7 for further details. □

3 Preliminaries

To simplify notation, we use $\circ$ to mean concatenation throughout this paper. Also, all $\log$ in this paper has base 2.

3.1 Basic probability lemmas

Given two random variables $\mathbf{X}, \mathbf{Y}$, we let $|\mathbf{X} - \mathbf{Y}|$ denote their statistical distance, defined as

$$|\mathbf{X} - \mathbf{Y}| := \max_S [\Pr[\mathbf{X} \in S] - \Pr[\mathbf{Y} \in S]] = \frac{1}{2} \sum_z |\Pr[\mathbf{X} = z] - \Pr[\mathbf{Y} = z]| .$$

We write $\mathbf{X} \approx_\varepsilon \mathbf{Y}$ and say that $\mathbf{X}, \mathbf{Y}$ are *ε-close* if $|\mathbf{X} - \mathbf{Y}| \leq \varepsilon$, and we write $\mathbf{X} \equiv \mathbf{Y}$ if $|\mathbf{X} - \mathbf{Y}| = 0$.

Fact 3.1 (data-processing inequality)**.** *For any random variables $\mathbf{X}, \mathbf{X}' \sim X$ and function $f : X \to Y$,*

$$|\mathbf{X} - \mathbf{X}'| \geq |f(\mathbf{X}) - f(\mathbf{X}')|.$$

Corollary 3.2. *For any random variables $\mathbf{X}, \mathbf{X}' \sim X$ and (constant) string $y \in Y$,*

$$|\mathbf{X} \circ y - \mathbf{X}' \circ y| = |\mathbf{X} - \mathbf{X}'|.$$

Lemma 3.3. *For any random variables $\mathbf{X}, \mathbf{X}' : \Omega \to X$ and $\mathbf{Y}, \mathbf{Y}' : \Omega \to Y$ such that $\mathbf{Y} \equiv \mathbf{Y}'$,*

$$|\mathbf{X} \circ \mathbf{Y} - \mathbf{X}' \circ \mathbf{Y}'| = \mathbb{E}_{y \sim \mathbf{Y}} [|(\mathbf{X} \mid \mathbf{Y} = y) - (\mathbf{X}' \mid \mathbf{Y}' = y)|]$$

Corollary 3.4. *There exists some $y \in \text{support}(\mathbf{Y}) = \text{support}(\mathbf{Y}')$ such that*

$$|\mathbf{X} \circ \mathbf{Y} - \mathbf{X}' \circ \mathbf{Y}'| \geq |(\mathbf{X} \mid \mathbf{Y} = y) - (\mathbf{X}' \mid \mathbf{Y}' = y)|$$

Combining Lemma 3.3 with Fact 3.1 yields the following stronger "randomized" version of the data-processing inequality.

Fact 3.5 (Randomized data-processing inequality)**.** *For any random variables $\mathbf{X}, \mathbf{X}' \sim X$, any independent random variable $\mathbf{Z} \sim Z$, and any function $f : X \times Z \to Y$, it holds that*

$$|\mathbf{X} - \mathbf{X}'| \geq |f(\mathbf{X}, \mathbf{Z}) - f(\mathbf{X}', \mathbf{Z})|.$$

Proof. By applying Lemma 3.3 and Corollary 3.2, we have

$$|\mathbf{X} \circ \mathbf{Z} - \mathbf{X}' \circ \mathbf{Z}| = \mathbb{E}_{z \sim \mathbf{Z}}[|\mathbf{X} \circ z - \mathbf{X}' \circ z|] = \mathbb{E}_{z \sim \mathbf{Z}}[|\mathbf{X} - \mathbf{X}'|] = |\mathbf{X} - \mathbf{X}'|.$$

By rewriting this backwards and applying the data-processing inequality (Fact 3.1), we have

$$|\mathbf{X} - \mathbf{X}'| = |\mathbf{X} \circ \mathbf{Z} - \mathbf{X}' \circ \mathbf{Z}| \geq |f(\mathbf{X} \circ \mathbf{Z}) - f(\mathbf{X}' \circ \mathbf{Z})|,$$

as desired. □

Lemma 3.6 (Min-entropy chain rule)**.** *For any random variables $\mathbf{X} \sim X$ and $\mathbf{Y} \sim Y$ and $\varepsilon > 0$,*

$$\Pr_{y \sim \mathbf{Y}}[H_\infty(\mathbf{X} \mid \mathbf{Y} = y) \geq H_\infty(\mathbf{X}) - \log |\text{support}(\mathbf{Y})| - \log(1/\varepsilon)] \geq 1 - \varepsilon.$$

3.2 Smooth min-entropy

Let's first define the notion of smooth min-entropy:

Definition 3.7 (Smooth min-entropy)**.** *The ε-smooth min-entropy of a source $\mathbf{X}$ over Ω is defined as*

$$H_\infty^\varepsilon(\mathbf{X}) := \sup_{\mathbf{Y} \sim \Omega, |\mathbf{X} - \mathbf{Y}| \leq \varepsilon} H_\infty(\mathbf{Y})$$

We will use a useful lemma which shows that for a random variable, smooth min-entropy can never increase after applying a function:

Lemma 3.8. *For any random variable $\mathbf{X} \sim X$ and function $f : X \to Y$, and any $\varepsilon > 0$,*

$$H_\infty^\varepsilon(\mathbf{X}) \geq H_\infty^\varepsilon(f(\mathbf{X}))$$

Proof. Let $\mathbf{Y}' \sim Y$ be an arbitrary source that is ε-close to $f(\mathbf{X})$. It suffices to show there exists some $\mathbf{X}'$ that is ε-close to $\mathbf{X}$ with $H_\infty(\mathbf{X}') \geq H_\infty(\mathbf{Y}')$. Towards this end, note that it is straightforward to define an independent random variable $\mathbf{Z}$ over a new space Z and a function $g : Y \times Z \to X$ such that for all $y \in Y$,

$$\Pr[g(y, \mathbf{Z}) = x] := \Pr[\mathbf{X} = x \mid f(\mathbf{X}) = y].$$

In other words, one can design g and $\mathbf{Z}$ so that the random variable $g(y, \mathbf{Z})$ samples from $(\mathbf{X} \mid f(\mathbf{X}) = y)$. We now argue that $\mathbf{X}' := g(\mathbf{Y}', \mathbf{Z})$ is ε-close to $\mathbf{X}$, and furthermore that $H_\infty(\mathbf{X}') \geq H_\infty(\mathbf{Y}')$, as desired. To see why the former is true, simply note that the randomized data-processing inequality (Fact 3.5) implies

$$\varepsilon \geq |\mathbf{Y}' - f(\mathbf{X})| \geq |g(\mathbf{Y}', \mathbf{Z}) - g(f(\mathbf{X}), \mathbf{Z})| = |\mathbf{X}' - \mathbf{X}|.$$

To show that $H_\infty(\mathbf{X}') \geq H_\infty(\mathbf{Y}')$, it suffices to show that $\Pr[\mathbf{X}' = x] \leq \max_y \Pr[\mathbf{Y}' = y]$ for all x. Towards this end, note that for an arbitrary x we have

$$\begin{aligned}\Pr[\mathbf{X}' = x] = \Pr[g(\mathbf{Y}', \mathbf{Z}) = x] &= \sum_y \Pr[\mathbf{Y}' = y] \cdot \Pr[g(y, \mathbf{Z}) = x] \\ &\leq \max_y \Pr[\mathbf{Y}' = y] \sum_y \Pr[\mathbf{X} = x \mid f(\mathbf{X}) = y].\end{aligned}$$

But note that there is only one nonzero term in the sum: namely, the term corresponding to the y such that $f(x) = y$. Thus the entire sum is bounded above by 1, which completes the proof. □

3.3 Extractors

We first define an object weaker than extractors, namely disperser:

Definition 3.9 (Disperser)**.** *A function* $\mathsf{Disp} : \{0,1\}^n \to \{0,1\}$ *is a disperser for a class of distributions* $\mathcal{C}$ *if for all* $\mathbf{X} \in \mathcal{C}$*, the set* $\{\mathsf{Disp}(\mathbf{X})\} = \{0,1\}$.

Dispersers are weaker objects than extractors as dispersers are required only to be non-constant over the distribution.

Definition 3.10. *We say that a deterministic function* $\mathsf{sExt} : \{0,1\}^m \times \{0,1\}^s \to \{0,1\}^r$ *is a* (k, ε)-strong seeded extractor *if for any* $\mathbf{X} \sim \{0,1\}^m$ *with min-entropy at least* k*,*

$$\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \approx_\varepsilon \mathbf{U}_r \circ \mathbf{Y},$$

where $\mathbf{Y} \sim \{0,1\}^s$ *and* $\mathbf{U}_r \sim \{0,1\}^r$ *are independent uniform random variables.*

Remark 3.11. *We say* sExt *is* linear *if the function* $\mathsf{sExt}(\cdot, y) : \{0,1\}^m \to \{0,1\}^r$ *is a degree* 1 *function, for all* $y \in \{0,1\}^s$.

Proposition 3.12. *Let* $\mathsf{sExt} : \{0,1\}^m \times \{0,1\}^s \to \{0,1\}^r$ *be a* $(k - \log(1/\varepsilon), \varepsilon)$*-strong seeded extractor. Then for any function* $f : \{0,1\}^m \to \{0,1\}^{n-k}$ *and independent uniform* $\mathbf{X} \sim \{0,1\}^m, \mathbf{Y} \sim \{0,1\}^s$*,*

$$\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \circ f(\mathbf{X}) \approx_{2\varepsilon} \mathbf{U}_r \circ \mathbf{Y} \circ f(\mathbf{X}),$$

where $\mathbf{U}_r \sim \{0,1\}^r$ *is uniform and independent of* $\mathbf{X}, \mathbf{Y}$.

Proof. By Lemma 3.3 and the definition of expectation, we have

$$\begin{aligned}|\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \circ f(\mathbf{X}) - \mathbf{U}_r \circ \mathbf{Y} \circ f(\mathbf{X})| &= \mathbb{E}_{z \sim f(\mathbf{X})}[(\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \mid f(\mathbf{X}) = z) - \mathbf{U}_r \circ \mathbf{Y}] \\ &\leq \Pr_{z \sim f(\mathbf{X})}[H_\infty(\mathbf{X} \mid f(\mathbf{X}) = z) < k - \log(1/\varepsilon)] \\ &\quad + |(\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \mid f(\mathbf{X}) = z^*) - \mathbf{U}_r \circ \mathbf{Y}|,\end{aligned}$$

where $z^* = \operatorname{argmax}_{z : H_\infty(\mathbf{X} | f(\mathbf{X}) = z) \geq k - \log(1/\varepsilon)} |(\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \mid f(\mathbf{X}) = z) - \mathbf{U}_r \circ \mathbf{Y}|$. Now, since $\mathbf{X}$ is uniform over m bits and f has output length $m - k$, the entropy chain rule (Lemma 3.6) allows us to upper bound the above probability by ε. And the definition of strong seeded extractor (Definition 3.10) allows us to upper bound the statistical distance in the last expression by ε. Thus we have

$$\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \circ f(\mathbf{X}) - \mathbf{U}_r \circ \mathbf{Y} \circ f(\mathbf{X})| \leq 2\varepsilon,$$

as desired. □

Theorem 3.13 (Leftover hash lemma [HILL99]). *For any $m, k \in \mathbb{N}$ and $\varepsilon > 0$, there exists a (k, ε)-strong linear seeded extractor* $\mathsf{sExt} : \{0,1\}^m \times \{0,1\}^s \to \{0,1\}^r$, *where $r = k - 2\log(1/\varepsilon)$.*

Typically, one wants sExt to be *explicit* and the *seed length* s to be small. For our purposes, however, these features do not matter - and, thus, we leave them out of the statement of Theorem 3.13.

We here define reductions for extractors:

Definition 3.14 (Convex combination). *We say $\mathbf{X}$ is a convex combination of distributions $\{\mathbf{Y}_i\}$ if there exist probabilities $\{p_i\}$ summing up to 1 such that $\mathbf{X} = \sum_i p_i \mathbf{Y}_i$.*

Fact 3.15. *Let* $\mathsf{Ext} : \{0,1\}^n \to \{0,1\}$ *be an ε extractor for class $\mathcal{C}$. Let $\mathbf{X} \sim \{0,1\}^n$ be a distribution that can be written as convex combination of distributions in $\mathcal{C}$. Then,* Ext *is also an ε extractor for $\mathbf{X}$.*

3.4 Bipartite Ramsey bound

We will use the following bipartite Ramsey bound to prove lower bounds against sumset extractors in Lemma 6.11.

Lemma 3.16 ([Zná63]). *The maximum number of edges in a bipartite graph over $[n] \times [n]$ without inducing a complete bipartite $t \times t$ subgraph is at most $(t-1)^{1/t} \cdot n^{2-1/t} + \frac{1}{2} \cdot (t-1) \cdot n$.*

We will use a corollary of this statement:

Corollary 3.17. *Fix $0 < \delta \leq 1$. Let G be a bipartite graph over $[n] \times [n]$ with at $\delta \cdot n^2$ edges. Then, G induces a complete bipartite subgraph H over $[\varepsilon \cdot \log n] \times [\varepsilon \cdot \log n]$ where $0 < \varepsilon \leq 1$ is a constant depending only on δ.*

3.5 Polynomials

We present useful definitions and properties that we will use in Section 6.

Definition 3.18 (Directional derivative). *For a polynomial $p : \mathbb{F}_2^n \to \mathbb{F}_2$ and $a \in \mathbb{F}_2^n$, we define its directional derivative in direction a, i.e., $D_a(p)(\cdot) : \mathbb{F}_2^n \to \mathbb{F}_2$ as*

$$D_a(p)(x) = p(x) + p(x+a)$$

Clearly $D_a(p)(\cdot)$ is a polynomial. It's well known that $\deg(D_a(p)(\cdot)) \leq \deg(p) - 1$. We also extend the definition of directional derivatives to apply to a polynomial map $P : \mathbb{F}_2^n \to \mathbb{F}_2^t$. For a fixed direction $a \in \mathbb{F}_2^n$, we define $D_a(P)(\cdot) : \mathbb{F}_2^n \to \mathbb{F}_2^m$ as $D_a(P)(x) = (D_a(p_1)(x), \ldots, D_a(p_m)(x))$.

Definition 3.19. *For a finite field $\mathbb{F}_{2^t}$, we define the function $v : \mathbb{F}_{2^t} \to \mathbb{F}_2^t$ that sends the field element to its vector representation.*

Fact 3.20. *For all $x, y \in \mathbb{F}_{2^t}$, it holds that $v(x+y) = v(x) + v(y)$. Moreover, v is a bijection.*

Lemma 3.21 ([Kop10, Lemma 2.3.1]). *Let $p : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ be a degree d polynomial where hamming weight of d when expressed in binary is w. Then, there exists a degree w multilinear polynomial $q : \mathbb{F}_2^t \to \mathbb{F}_2^t$ such that for all $x \in F_{2^t}$, it holds that $v(p(x)) = q(v(x))$.*

Lemma 3.22 ([BHL12, Lemma 2]). *Fix $\varepsilon > 0$. Let f be a random degree d polynomial for $d \leq (1-\varepsilon)n$. Then,*

$$\Pr[|\operatorname{bias}(f)| > 2^{-c_1 n/d}] \leq 2^{-c_2 \binom{n}{\leq d}}$$

where $0 < c_1, c_2 < 1$ are constants depending only on ε.

3.6 k-wise independence

We will use k-wise independent hash functions to help construct extractors for polynomial sources in *Section 5*.

Lets first define them:

Definition 3.23 (Definition 3.3.1 in [Vad12]). *For $n, m, k \in \mathbb{N}$ such that $k \leq 2^n$, a family of functions $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ is k-wise independent, if for all distinct $x_1, \ldots, x_k \in \{0,1\}^n$, the random variables $h(x_1), \ldots, h(x_k)$ are independently and uniformly distributed in $\{0,1\}^m$ when h is a randomly chosen function from $\mathcal{H}$.*

We will use the following lemma to construct k-wise independent hash function family:

Lemma 3.24 (follows from Corollary 3.3.4 in [Vad12]). *For every $n, m, k \in \mathbb{N}$, there exists a family of k-wise independent functions $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ such that we can enumerate the family in time $2^{k \cdot \max(n,m)} \cdot \mathrm{poly}(n, m, k)$ time and evaluate each function in $\mathrm{poly}(n, m, k)$ time.*

We will rely on the following property of k-wise independent hash functions in our construction:

Lemma 3.25 (Implicit in [TV00, Proposition A.1]). *Let $\mathcal{C}$ be arbitrary class of min-entropy at least k distributions over n bits. Let $\mathcal{H}$ be class of t-wise independent hash functions from n bits to r bits where $t = 2\log(k + |\mathcal{C}|), r = k - 2\log(1/\varepsilon) - \log(t) - 2$. Then, there exists $h \in \mathcal{H}$ such that h is a (k, ε) extractor against all sources in class $\mathcal{C}$.*

3.7 Sidon sets

We here define Sidon sets. In Section 6, we will show that degree 2 polynomial NOBF sources can sample largest possible Sidon sets.

Definition 3.26 (Sidon sets). *We say $S \subset \mathbb{F}_2^n$ is a Sidon set if for all $a, b, c, d \in S$ such that $a + b = c + d$, it holds that $\{a, b\} = \{c, d\}$.*

4 Reducing the input length

We show that it suffices to construct extractors for polynomial sources with input length linear in k:

Theorem 4.1. *Let k, ε_2 be such that $2^{-k} < \varepsilon_2 < 1$. Let $\mathsf{Ext} : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be ε_1-extractor for class of degree d polynomial sources with min-entropy $\min(k - \log(1/\varepsilon_2), \log(1/\varepsilon_2)) - O(1)$ and $\ell = k + t + 3\log(1/\varepsilon_2)$ inputs. Then, Ext is also a $2\varepsilon_2 + \varepsilon_1$-extractor for class of degree d polynomial sources with min-entropy k and arbitrary inputs.*

We will end up using the following corollary of this theorem (follows by setting $\varepsilon_2 = 2^{-k/100}$ say) in our constructions:

Corollary 4.2. *Let $\mathsf{Ext} : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be ε-extractor for class of degree d polynomial sources with min-entropy k and $\ell = O(k)$ inputs. Then, Ext is also a $\varepsilon + 2^{-\Omega(k)}$-extractor for class of degree d polynomial sources with min-entropy $\Omega(k)$ and arbitrary inputs.*

This theorem follows from the following lemma which shows that for any function g applied on a source of the type $f(\mathbf{U}_m)$, we can find an affine subspace S of dimension $O(H_\infty(f(\mathbf{U}_m)))$ such that $g(f(\mathbf{U}_m))$ has the same distribution as $g(f(\cdot))$ evaluated over random inputs from S.

Lemma 4.3. *Let $\mathbf{U}_m \sim \mathbb{F}_2^m$ be the uniform distribution over m bits. Let $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be an arbitrary function. Let $\mathbf{X} = f(\mathbf{U}_m)$ be such that $H_\infty(\mathbf{X}) \geq k + 2\log(1/\varepsilon)$. Then, for any $g : \mathbb{F}_2^n \to \mathbb{F}_2^t$, there exists affine function $A : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ with $\ell = k+t+3\log(1/\varepsilon)$ such that $g(f(A(\mathbf{U}_\ell))) \approx_{2\varepsilon} g(f(\mathbf{U}_m))$. Moreover, $H_\infty^{3\varepsilon}(f(A(\mathbf{U}_\ell))) \geq k$.*

Before proving this lemma, we show how it can be used to assume extractors for polynomial sources without loss of generality have about k inputs.

Proof of Theorem 4.1. We apply Lemma 4.3 with $g = \mathsf{Ext}$. The proof immediately follows by observing that if $H_\infty^{3\varepsilon_2}(\mathbf{X}) \geq k - 2\log(1/\varepsilon_2)$, then $H_\infty(\mathbf{X}) \geq \min(k - \log(1/\varepsilon), \log(1/\varepsilon)) - O(1)$. □

We first prove a useful lemma which shows that any boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ admits a small affine subspace that approximates the output distribution of f.

Lemma 4.4 (Existence of affine white-box PRGs)**.** *For any function $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ and $\varepsilon > 0$, there exists an affine function $G : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ with $\ell = n + 3\log(1/\varepsilon)$ such that*

$$f(\mathbf{U}_m) \approx_{2\varepsilon} f(G(\mathbf{U}_\ell)).$$

Proof. Assume that $n + 3\log(1/\varepsilon) < m$, because otherwise the statement is immediate, by setting G to output the first m bits of its input. Now, define $t := m-n$ and let $\mathsf{sExt} : \mathbb{F}_2^m \times \mathbb{F}_2^s \to \mathbb{F}_2^r$ be a $(t-\log(1/\varepsilon), \varepsilon)$-strong linear seeded extractor with output length $r = t - 3\log(1/\varepsilon)$, whose existence is guaranteed by Theorem 3.13 (note that it may not be explicit, but this is okay for our application). By Proposition 3.12, we know that for independent uniform random variables $\mathbf{X} \sim \mathbb{F}_2^m$ and $\mathbf{Y} \sim \mathbb{F}_2^s$ and $\mathbf{U}_r \sim \mathbb{F}_2^r$,

$$\mathsf{sExt}(\mathbf{X}, \mathbf{Y}) \circ \mathbf{Y} \circ f(\mathbf{X}) \approx_{2\varepsilon} \mathbf{U}_r \circ \mathbf{Y} \circ f(\mathbf{X})$$

Next, by applying Corollary 3.4 to the above (combined with a basic application of the data-processing inequality, Corollary 3.2), we know that there exists some $y \in \mathbb{F}_2^s$ such that

$$\mathsf{sExt}(\mathbf{X}, y) \circ f(\mathbf{X}) \approx_{2\varepsilon} \mathbf{U}_r \circ f(\mathbf{X}).$$

Next, we let $g : \mathbb{F}_2^m \to \mathbb{F}_2^r$ denote the function $g(x) := \mathsf{sExt}(x, y)$, and can rewrite the above as

$$g(\mathbf{X}) \circ f(\mathbf{X}) \approx_{2\varepsilon} \mathbf{U}_r \circ f(\mathbf{X}),$$

where $\mathbf{X} \sim \mathbb{F}_2^m$ and $\mathbf{U}_r \sim \mathbb{F}_2^r$ are independent uniform random variables and $g : \mathbb{F}_2^m \to \mathbb{F}_2^r$ is linear (since sExt was a *linear* strong seeded extractor). By applying Corollary 3.4 once more to the above (combined with the same basic application of the data-processing inequality, Corollary 3.2), we know that there is some $b \in \mathbb{F}_2^r$ such that

$$(f(\mathbf{X}) \mid g(\mathbf{X}) = b) \approx_{2\varepsilon} f(\mathbf{X}). \tag{1}$$

But notice that, since g is linear (and full rank, without loss of generality), the random variable $(\mathbf{X} \mid g(\mathbf{X}) = b)$ is uniform over an affine space $S \subseteq \mathbb{F}_2^m$ of dimension $m - r = m - t + 3\log(1/\varepsilon) = n + 3\log(1/\varepsilon) = \ell$. Thus, there exists an affine function $G : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ such that $G(\mathbf{U}_\ell) \equiv (\mathbf{X} \mid g(\mathbf{X}) = b)$ and thus $f(G(\mathbf{U}_\ell)) \equiv (f(\mathbf{X}) \mid g(\mathbf{X}) = b)$. Combining this with Equation (1) completes the proof. □

Using this lemma, we show that any polynomial source can be approximated by another one with short input length.

Remark 4.5. *Let $\mathbf{X}$ be the original polynomial source with $H_\infty(\mathbf{X}) = k$. This lemma is very nice as it helps us find a single polynomial source $\mathbf{X}'$ with n inputs such that $\mathbf{X} \approx \mathbf{X}'$. Contrast this to our main lemma where for a fixed function $g : \mathbb{F}_2^n \to \mathbb{F}_2^t$, we can find a source $\mathbf{X}'$ with k inputs such that $H_\infty(\mathbf{X}')$ is about k and $g(\mathbf{X}) \approx g(\mathbf{X}')$.*

Lemma 4.6. *For any polynomial source $\mathbf{X} \sim \mathbb{F}_2^n$ of degree at most d, and any $\varepsilon > 0$, there exists a polynomial source $\mathbf{X}' \sim \mathbb{F}_2^n$ of degree at most d and input length $\ell = n + 3\log(1/\varepsilon)$ such that $\mathbf{X}' \approx_{2\varepsilon} \mathbf{X}$ and $\mathsf{Supp}(\mathbf{X}') \subset \mathsf{Supp}(\mathbf{X})$.*

Proof. By definition of polynomial source, there exists some $m \in \mathbb{N}$ and degree $\leq d$ polynomial $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ such that $\mathbf{X} \equiv f(\mathbf{U}_m)$. By Lemma 4.4, there exists some degree 1 polynomial $G : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ with $\ell = n + 3\log(1/\varepsilon)$ such that $f(\mathbf{U}_m) \approx_{2\varepsilon} f(G(\mathbf{U}_\ell))$. If we define $\mathbf{X}' := f(G(\mathbf{U}_\ell))$, then $\mathbf{X}'$ is a polynomial source of degree at most d (and input length ℓ), since the composition $f(G) : \mathbb{F}_2^\ell \to \mathbb{F}_2^n$ has degree at most $d \cdot 1 = d$. Since $\mathbf{X}' = f(G(\mathbf{U}_\ell)) \approx_{2\varepsilon} f(\mathbf{U}_m) \equiv \mathbf{X}$, this completes the proof. □

In our various probabilistic proofs, we will use the following corollary of this lemma:

Corollary 4.7. *For any polynomial source $\mathbf{X} \sim \mathbb{F}_2^n$ of degree at most d, there exists a polynomial source $\mathbf{X}' \sim \mathbb{F}_2^n$ of degree at most d and input length $\ell = O(n)$ such that $\mathbf{X}' \approx_{2^{-n}} \mathbf{X}$.*

With this approximation lemma, we finally have all the ingredients to prove our main lemma:

Proof of Lemma 4.3. Let $\mathsf{sExt} : \mathbb{F}_2^n \times \mathbb{F}_2^s \to \mathbb{F}_2^k$ be the seeded extractor guaranteed by Theorem 3.13. Let $\mathbf{Y} = \mathbf{U}_s$. Then, as sExt is a strong seeded extractor Definition 3.10:

$$\mathsf{sExt}(f(\mathbf{U}_m), \mathbf{Y}) \circ \mathbf{Y} \approx_\varepsilon \mathbf{U}_k \circ \mathbf{Y}$$

Using Corollary 3.2, we infer that there exists $y \in \mathbb{F}_2^s$ such that

$$\mathsf{sExt}(f(\mathbf{U}_m), y) \approx_\varepsilon \mathbf{U}_k$$

Let $\mathsf{Ext} : \mathbb{F}_2^n \to \mathbb{F}_2^k$ be defined as $\mathsf{Ext}(x) = \mathsf{sExt}(x, y)$. Then, it must be that

$$\mathsf{Ext}(f(\mathbf{U}_m)) \approx_\varepsilon \mathbf{U}_k$$

We define $h : \mathbb{F}_2^m \to \mathbb{F}_2^{k+t}$ as

$$h(x) = \mathsf{Ext}(f(x)) \circ g(f(x))$$

We now apply Lemma 4.4 to infer that there exists an affine function $A : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ with $\ell = k + t + 3\log(1/\varepsilon)$ such that $h(\mathbf{U}_m) \approx_{2\varepsilon} h(A(\mathbf{U}_\ell))$. As $\mathsf{Ext}(f(\mathbf{U}_m)) \approx_\varepsilon \mathbf{U}_k$, it must be that $H_\infty^\varepsilon(h(\mathbf{U}_m)) \geq k$ and so, $H_\infty^{3\varepsilon}(h(A(\mathbf{U}_\ell))) \geq k$. Let $\mathbf{Z} = f(A(\mathbf{U}_\ell))$. We will now show that $H_\infty^{3\varepsilon}(\mathbf{Z}) \geq k$:

$$h(A(\mathbf{U}_\ell)) = \mathsf{Ext}(f(A(\mathbf{U}_\ell))) \circ g(f(A(\mathbf{U}_\ell))) = \mathsf{Ext}(\mathbf{Z}) \circ g(\mathbf{Z})$$

Hence, $H_\infty^{3\varepsilon}(\mathsf{Ext}(\mathbf{Z}) \circ g(\mathbf{Z})) \geq k$. Applying Lemma 3.8, we infer that $H_\infty^{3\varepsilon}(\mathbf{Z}) \geq k$. We also see that

$$\mathsf{Ext}(f(\mathbf{U}_m)) \circ g(f(\mathbf{U}_m)) = h(\mathbf{U}_m) \approx_{2\varepsilon} h(A(\mathbf{U}_\ell)) = \mathsf{Ext}(\mathbf{Z}) \circ g(\mathbf{Z})$$

Hence, $g(f(\mathbf{U}_m)) \approx_{2\varepsilon} g(\mathbf{Z}) = g(f(A(\mathbf{U}_\ell)))$, as desired. □

5 Constructing extractors

5.1 Existential results

We first show that with high probability, a random function is a good extractor. We will then improve upon it to show that for large enough t, a function sampled using t-wise distribution is a good enough extractor.

Lemma 5.1. *Let n, d, k, ε be such that $d < n/2, k \geq \Omega(d \log n), 2^{-\Omega(k)} \leq \varepsilon \leq 1/2, m = k - 2\log(1/\varepsilon) - O(1)$. For any polynomial source $\mathbf{X} \sim \mathbb{F}_2^n$ of degree at most d, $H_\infty(\mathbf{X}) \geq k$, a random function $r : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a ε-extractor with high probability.*

Proof. By Corollary 4.7, there exists a degree d polynomial source $\mathbf{X}' \sim \mathbb{F}_2^n$ such that $\mathbf{X}' \approx_{2^{-n}} \mathbf{X}$ and input length of $\mathbf{X}'$ is $O(n)$. Using Fact 3.1, we infer that an extractor with error ε for $\mathbf{X}'$ is also an extractor for $\mathbf{X}$ with error $\varepsilon + 2^{-n}$.

For a fixed source $\mathbf{Y}$ with $H_\infty(\mathbf{Y}) = k$, a random function $r : \mathbb{F}_2^n \to \mathbb{F}_2^m$ satisfies $r(\mathbf{Y}) \approx_\varepsilon \mathbf{U}_m$ with probability $1 - 2^{-\Omega(2^k)\varepsilon^2}$ where $m = k - 2\log(1/\varepsilon) - O(1)$ (Proposition 6.12 in [Vad12]). We now do a union bound over all the $2^{\binom{\ell}{\leq d} \cdot n}$ degree d sources with ℓ inputs and n outputs. As $\varepsilon \geq 2^{-\Omega(k)}, k \geq \Omega(d \log n), \ell = O(n)$. the union bound indeed succeeds and we infer the claim. □

Lemma 5.2. *Let n, d, k, t, ε be such that $d < O(n/\log n), k \geq \Omega(d \log n), t = 2\log\left(k + 2^{\binom{O(n)}{d} \cdot n}\right), 2^{-\Omega(k)} \leq \varepsilon \leq 1/2, m = k - 2\log(1/\varepsilon) - O(1)$. For any polynomial source $\mathbf{X} \sim \mathbb{F}_2^n$ of degree at most d, $H_\infty(\mathbf{X}) \geq k$, a random function $r : \mathbb{F}_2^n \to \mathbb{F}_2^m$ from a family of t-wise independent functions is a ε-extractor with high probability.*

Proof. By Corollary 4.7, there exists a degree d polynomial source $\mathbf{X}' \sim \mathbb{F}_2^n$ such that $\mathbf{X}' \approx_{2^{-n}} \mathbf{X}$ and input length of $\mathbf{X}'$ is $O(n)$. Using Fact 3.1, an extractor with error ε for $\mathbf{X}'$ is also an extractor for $\mathbf{X}$ with error $\varepsilon + 2^{-n}$. We now apply Lemma 3.25 and infer the claim. □

5.2 Algorithmic construction

We use the input reduction trick and the existential results to construct non-trivial extractors for polynomial sources.

Theorem 5.3. *Let d, n, k be such that $d < \log\log n$ and $k \geq n - O\left(\frac{\sqrt{\log n}}{(d \log\log n)^{d/2}}\right)$. Let $\mathcal{C}$ be class of degree d polynomial sources that output n bits and have min-entropy at least k. Then we can construct an extractor for $\mathcal{C}$ in time $\mathrm{poly}(n)$ that extracts $\Omega(\log\log n)$ bits and has error $2^{-\Omega(\log\log n)}$.*

We note that our explicit construction can handle degree up to $O(\log\log n)$. Towards proving the theorem, we first need the following simple observation:

Claim 5.4. *Let $\mathbf{X} \sim \mathbb{F}_2^n$ be an arbitrary source such that $H_\infty(\mathbf{X}) = k$. Let $\mathbf{X}_0$ be projection of $\mathbf{X}$ onto arbitrary n_0 bits. Then, $H_\infty(X_0) \geq n_0 - (n - k)$.*

Proof. Let $x_0 \in \mathbb{F}_2^{n_0}$ be arbitrary. Let $\Pr(\mathbf{X}_0 = x_0) = p_0$. Then, there exists $x \in \mathbb{F}_2^n$ such that the project of x onto coordinates corresponding to $\mathbf{X}_0$ equals x_0 and $\Pr(\mathbf{X} = x) = p \geq p_0 \cdot 2^{-(n-n_0)}$. Hence, if $p_0 > 2^{-(n_0-(n-k))}$, then $p > 2^{-k}$, a contradiction. □

Here is the construction algorithm that we will utilise to construct extractors in Lemma 5.5.

Algorithm 1: Extractor from t-wise independent family

input : degree d, input source length ℓ, output source length n_0, min-entropy $k_0 = n_0 - g$, extractor output length r, target error ε, the parameter t for t-wise independence

output: An extractor f from n_0 bits to r bits with error ε for degree d polynomial sources from ℓ bits to n_0 bits if it exists from some t-wise independent family

```
Let F be some fixed family of t-wise independent functions from n_0 bits to r bits.
for every function f ∈ F do
    flag ← True.
    for every degree d polynomial map P from ℓ bits to n_0 bits do
        Brute force over all 2^ℓ assignments to compute min-entropy of P(U_ℓ) and let it be k_p.
        if k_p ≥ k_0 then
            Brute force over all 2^ℓ assignments to compute ε_{f,P} = |U_m − f(P(U_ℓ))|.
            if ε_{f,P} > ε then
                flag ← False.
            end
        end
    end
    if flag = True then
        return f
    end
end
return Fail
```

Lemma 5.5. *Let d, g, n, k, r be such that $0 \le g \le n, k \ge n - g, d \le O\left(\frac{g}{\log g}\right), O(d \log g) \le r \le O(g)$. Let $\mathcal{C}$ be class of degree d polynomial sources that output n bits and have min-entropy at least k. Then we can construct an extractor for $\mathcal{C}$ in time $2^{O\left(\binom{r}{\le d} \cdot g^2\right)}$ that extracts r bits and has error $2^{-\Omega(r)}$.*

Proof. Let $\mathbf{X} \in \mathcal{C}$ be arbitrary. Consider the first $n_0 = 1.01g$ bits of $\mathbf{X}$ and let this source be $\mathbf{X}_0$. Then, by Claim 5.4, it holds that $H_\infty(\mathbf{X}_0) \ge n_0 - g \ge \Omega(n_0)$. As we want to output r bits and we can get input reduction up to the min-entropy bound, we use Corollary 4.2 with min-entropy $k = \Omega(r)$ to infer that it suffices to construct extractors polynomial sources with input length $\ell = O(k)$. By Lemma 5.2, there exists a function $f : \mathbb{F}_2^{n_0} \to \mathbb{F}_2^r$ such that for all polynomial sources $\mathbf{Y}$, $|f(\mathbf{Y}) - \mathbf{U}_r| \le 2^{-\Theta(k)}$. Moreover, such f will be one of the functions in family of t-wise independent functions where $t = 2\log(\Theta(k) + |\mathcal{C}|)$. By setting relevant input parameters to Algorithm 1, it will indeed find such f.

Let's analyze runtime of Algorithm 1. The number of degree d sources with input length ℓ and output length n_0 is $2^{\binom{\ell}{\le d} \cdot n_0}$. The time to enumerate the t-wise independent family is $2^{tg}\,\mathrm{poly}(t, g) \le 2^{2\binom{\ell}{\le d} \cdot n_0^2}\,\mathrm{poly}(\ell, d, n_0)$ (Lemma 3.24). Computing entropy and checking if the function is an extractor takes $O(2^{O(\ell+n_0)} \cdot \mathrm{poly}(n_0))$. As $\ell = \Theta(r)$ and $d \le O(n_0/\log n_0)$, the overall runtime of this algorithm is $2^{O\left(\binom{r}{\le d} \cdot n_0^2\right)}$. As $n_0 = 1.01g$, the runtime is as desired. □

We specialize above lemma to obtain Theorem 5.3.

Proof of Theorem 5.3. Set $g = n - O\left(\frac{\sqrt{\log n}}{(d \log\log n)^{d/2}}\right)$ and $r = O(d \log g)$ in Lemma 5.5. □

6 Impossibility results

In this section, we show various impossibility results for polynomial NOBF sources and hence, these results apply to both polynomial sources and variety sources. We first show a sampling result that demonstrates power of the quadratic NOBF sources: they can sample optimal sized Sidon sets. We then show affine dispersers cannot be used to disperse from degree d polynomial NOBF sources below certain min-entropy (this is tight). We finally will prove Theorem 2, that sumset extractors cannot be used to even disperse against quadratic NOBF sources below certain min-entropy.

6.1 Sampling Sidon Set

We show that quadratic NOBF sources can uniformly sample largest Sidon sets possible over $\mathbb{F}_2^n$ and hence, we cannot use sumset extractors below min-entropy $n/2$ to extract from polynomial NOBF sources. We will obtain a much stronger version of the latter claim later.

Claim 6.1. *There exists a degree 2 polynomial NOBF source $\mathbf{Y}$ with $H_\infty(\mathbf{Y}) = n/2$ such that $\mathbf{Y}$ uniformly samples a Sidon set.*

Proof. Consider the set $S = \{(x, x^3) : x \in \mathbb{F}_{2^{n/2}}\}$. It's well known that this set is a Sidon set [RRW22]. Using Lemma 3.21, we infer that there exists a degree 2 polynomial map $q : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ such that for all $x \in \mathbb{F}_2^{n/2}$, $v(x^3) = q(v(x))$. Applying Fact 3.20 we infer that $T = \{(y, q(y)) : y \in \mathbb{F}_2^{n/2}\}$ is also a Sidon set. Hence, we define $\mathbf{Y} : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^n$ to be the degree 2 polynomial NOBF source that is uniform over the set T. We see that $\mathbf{Y}$ uniformly samples a Sidon set and $H_\infty(\mathbf{Y}) = n/2$ as desired. □

Corollary 6.2. *There exists a degree 2 polynomial NOBF source $\mathbf{Y}$ with $H_\infty(\mathbf{Y}) = n/2$ such that for all $A, B \subset \mathbb{F}_2^n, |A| \geq 5, |B| \geq 5 : A + B \not\subset$ support$(\mathbf{Y})$.*

Proof. Say such A, B existed. Then, there exist $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that all 4 of them are distinct and $a_1 + a_2 \neq b_1 + b_2$. Let $C = \{a_1 + b_1, a_1 + b_2, a_2 + b_1, a_2 + b_2\}$. Then, $|C| = 4$ and $C \subset$ support$(\mathbf{Y})$. However, $(a_1 + b_1) + (a_1 + b_2) = (a_2 + b_1) + (a_2 + b_2)$ which contradicts the fact that support$(\mathbf{Y})$ is a Sidon set. □

Hence, we cannot use a sumset extractor in a blackbox way to extract from polynomial NOBF sources of min-entropy $n/2$.

6.2 Polynomial NOBF source lower bound against affine extractors

We show that we cannot use affine dispersers to disperse from degree d polynomial NOBF sources below min-entropy $n - n/(\log n)^{d-1}$. As polynomial NOBF sources are also variety sources, using [CT15], this result is tight.

Theorem 6.3. *Let $c_1 > 0$ be an arbitrary constant. Then, there exists another constant $c_2 > 0$ such that the following holds: For $2 \leq d \leq \frac{\log n}{2 \cdot \log\log n}$, There exists a degree d polynomial NOBF source $\mathbf{X}$ with $H_\infty(\mathbf{X}) = n - c_2 \frac{n}{(\log n)^{d-1}}$ such that support$(\mathbf{X})$ does not contain any affine subspace of dimension $c_1 \log n$.*

As affine dispersers with min-entropy requirement $0.5 \log n$ can't exist, it indeed follows that we can't use affine dispersers to disperse from polynomial NOBF sources the stated min-entropy bound.

We first show that a random degree d polynomial map will not become a linear map over any small affine subspace.

Claim 6.4. *There exists a universal constant c such that the following holds. Let d, n, t be such that $2 \leq d < n/2$ and $t < n$. Then, there exist degree d polynomials $p_1, \ldots, p_t$ such that on every affine subspace U of dimension $k \geq cd \cdot (n/t)^{1/(d-1)}$, there exists at least one i such that p_i has degree ≥ 2.*

Proof. Let $p_1, \ldots, p_t : \mathbb{F}_2^n \to \mathbb{F}_2$ be random polynomials of degree d. Let U be arbitrary but fixed affine subspace of dimension k. Then, $p_1|_U, \ldots, p_t|_U$ are also uniform polynomials over k variables of degree d. Hence, it must be that:

$$\Pr_{p_1,\ldots,p_t}\left[\bigwedge_{1\leq i\leq t} \deg(f|_U) \leq 1\right] \leq 2^{-\left(\binom{k}{\leq d}-\binom{k}{\leq 1}\right)t}$$

We union bound over all $\leq 2^n\binom{2^n}{k}$ affine subspaces of dimension k and see that the probability that there exists some affine subspace of dimension k over which all these polynomials have degree at most 1 is at most

$$2^{-\left(\binom{k}{\leq d}-\binom{k}{\leq 1}\right)t} \cdot 2^n \cdot \binom{2^n}{k}$$

We set c to a large constant so that the above probability less than 1. □

We now show random polynomial NOBF source does not contain any small affine subspace.

Claim 6.5. *There exists a universal constant c such that the following holds: Let d, k be such that $2 \leq d < k/2$. For any $0 < t < k$, there exists a degree d polynomial NOBF source $\mathbf{X}$ over $k + t$ bits with $H_\infty(\mathbf{X}) = k$ such that support$(\mathbf{X})$ does not contain any affine subspace of dimension $cd \cdot (k/t)^{1/(d-1)}$.*

Proof. Let $s = cd \cdot (k/t)^{1/(d-1)}$. Let $(p_1, \ldots, p_t) : \mathbb{F}_2^k \to \mathbb{F}_2^t$ be the t polynomials from *Claim* 6.4. Let X be the polynomial NOBF source over $k + t$ bits where first k bits are $x_1, \ldots, x_k$ and last t bits are $p_1(x_1, \ldots, x_k), \ldots, p_t(x_1, \ldots, x_k)$.

Assume that there exists an affine subspace $U \subset \text{support}(\mathbf{X})$ such that $\dim(U) = s$. Observe that once the first k bits of $\mathbf{X}$ are fixed, the last t bits are also fixed. As $U \subset \text{support}(\mathbf{X})$, U must also have this property. Let $P \subset \mathbb{F}_2^k$ be the projection of U over the first k bits. Then, $\dim(P) = \dim(U) = s$. Moreover, as U is an affine subspace, the last t bits of U are linear functions of the first k bits. However, this implies that for each $1 \leq i \leq t$, $\deg(p_i|_P) \leq 1$, which is a contradiction. □

Proof of Theorem 6.3. Use Claim 6.5 and set $t = O(k/\log n)$. □

6.3 Polynomial NOBF source lower bound against sumset extractors

We show that we cannot use sumset dispersers to disperse from quadratic NOBF sources below min-entropy $n - n/\log n$. We also show that we cannot use sumset extractors to disperse from quadratic NOBF sources below min-entropy $n - n/\log\log n$.

Theorem 6.6. *Let $c_1 > 0$ be an arbitrary constant. Then, there exists another constant $c_2 > 0$ such that the following holds: There exists a degree 2 polynomial NOBF source $\mathbf{X}$ with $H_\infty(\mathbf{X}) = n - c_2\frac{n}{\log n}$ such that support$(\mathbf{X})$ does not contain any sumset $A + B$ where $|A| \geq n^{c_1}, |B| \geq n^{c_1}$.*

Theorem 6.7. *Let $0 < \varepsilon < 1, 0 < c_1$ be arbitrary constants. Then, there exists another constant $c_2 > 0$ such that the following holds: There exists a degree 2 polynomial NOBF source $\mathbf{X}$ with $H_\infty(\mathbf{X}) = n - c_2\frac{n}{\log\log n}$ such that $\mathbf{X}$ is $(1 - \varepsilon)$-far from a convex combination of sumset sources of min-entropy $c_1 \log n$.*

Note that if a distribution is 0.5 distance away from any convex combination of sumset sources then a sumset extractor cannot be used in a blackbox way as a disperser. Also, as no sumset extractor can exist for min-entropy below $0.5 \log n$, these results show we can't use sumset extractors/dispersers in a blackbox way to disperse from degree 2 polynomial NOBF sources.

We first show that random quadratic maps P have the property that $P(U) + P(V) \neq P(U + V)$ where U and V are small affine subspaces.

Claim 6.8. *There exists a universal constant c such that the following holds. Let $t, n \in \mathbb{N}$ be such that $t < n$. There exist degree 2 polynomials $p_1, \ldots, p_t : \mathbb{F}_2^n \to \mathbb{F}_2$ such that for every pair of affine subspaces U, V of dimensions $r \geq c(n/t)$ each, and for all $y \in \mathbb{F}_2^n$, there exists at least at least one i and at least one $u \in U, v \in V$ such that $p_i(u + v) \neq p_i(u) + p_i(v) + y_i$.*

Proof. Fix $y \in \mathbb{F}_2^t$. At the end, we will union bound over these 2^t distinct y. Let $P = (p_1, \ldots, p_t) : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be a random degree 2 polynomial map. Without loss of generality assume that $y = 0^t$. Indeed, we can define $P'(x) = P(x) + y$ so that $P'(A) + P'(B) = P'(A + B)$ and from $P'(U) + P'(V) = P'(U + V)$, we will again recover $P(U) + P(V) = P(U + V) + y$ as desired. Moreover, P' will still be a random degree 2 polynomial map. Let $u_0 + U, v_0 + V$ be arbitrary but fixed affine subspaces of dimension r each. We consider two cases:

Case 1. $\dim(U \cap V) \geq r/2$.
Let $W = (U \cap V)$. Assume that for all $u \in (u_0 + U), v \in (v_0 + V)$, it holds that $P(u) + P(v) = P(u+v)$. We claim that $P|_{(u_0+W)}$ is a degree 1 polynomial map. Indeed, above condition guarantees that $\forall w_1, w_2 \in W : P(u_0 + w_1) + P(v_0 + w_2) = P(u_0 + v_0 + w_1 + w_2)$. This also implies that $\forall w \in W : P(u_0 + w) + P(v_0 + w) = P(u_0 + v_0)$. Repeatedly applying these, we infer that:

$$\begin{aligned} P(u_0 + (w_1 + w_2)) &= P(u_0 + v_0) + P(v_0 + (w_1 + w_2)) \\ &= P(u_0 + v_0) + (P(u_0 + w_1) + P(u_0 + v_0 + w_2)) \\ &= P(u_0 + w_1) + (P(u_0 + v_0)) + (P(v_0 + (u_0 + w_2))) \\ &= P(u_0 + w_1) + (P(u_0) + P(v_0)) + (P(v_0) + P(u_0 + w_2))) \\ &= P(u_0 + w_1) + P(u_0 + w_2) + P(u_0) \end{aligned}$$

Hence, P restricted to $u_0 + W$ is indeed an affine map. We observe that $p_1|_{u_0+W}, \ldots, p_t|_{u_0+W}$ are distributed as uniform degree at most 2 polynomials over $r/2$ variables. The probability that each of these polynomials has degree at most 1 is at most $2^{-\binom{r/2}{2}t}$.

Case 2. $\dim(U \cap V) < r/2$.
Let $u_0 + S$ be the largest affine subspace inside $u_0 + U$ such that $S \cap (U \cap V) = \emptyset$. Similarly, let $v_0 + T$ be the largest affine subspace inside V such that $T \cap (U \cap V) = \emptyset$. It must be that $\dim(S), \dim(T) \geq r/2$ and $S \cap T = \emptyset$. By considering appropriate subsets of S and T, we without loss of generality assume $\dim(S) = \dim(T) = r/3, (u_0 + S) \cap (T \cup (v_0 + T)) = (v_0 + T) \cap (S \cup (u_0 + S)) = \emptyset$. Let basis vectors of S and T be $(s_1, \ldots, s_{r/3})$, and $(t_1, \ldots, t_{r/3})$ respectively. Without loss of generality, let it be that $u_0 + s_1, \ldots, u_0 + s_{r/3}$ are linearly independent and $v_0 + t_1, \ldots, v_0 + t_{r/3}$ are also linearly independent. Then, by using the various empty intersection conditions above, the vectors $u_0 + s_1, \ldots, u_0 + s_{r/3}, v_0 + t_1, \ldots, v_0 + r_{r/3}$ are also linearly independent. Let $b_1, \ldots, b_{n-r/3}$ be linearly independent vectors so that $u_0 + s_1, \ldots, u_0 + s_{r/3}, v_0 + t_1, \ldots, v_0 + r_{r/3}, b_1, \ldots, b_{n-r/3}$ are all linearly independent. Let's rename these vectors to be $c_1, \ldots, c_n$.

Now, we choose the random quadratic polynomials $p_1, \ldots, p_t$ by randomly sampling monomials of degree at most 2 over these c_i. As the c_i are linearly independent, P will still be a uniformly random quadratic map. Say there exists i such that p_i contains the monomial $c_j c_k$ where $c_j \in \{u_0 + s_1, \ldots, u_0 + s_{r/3}\}$ and $c_k \in \{v_0 + t_1, \ldots, v_0 + t_{r/3}\}$. Without loss of generality we assume that the singleton monomials c_j and c_k are not present in p_i and degree 0 monomial is also absent. Consider the following two assignments:

(a) Assignment α_1 where $c_j = 1$, and remaining variables are set to 0.

(b) Assignment α_2 where $c_k = 1$, and remaining variables set to 0.

Then, $p_i(\alpha_1) = p_i(\alpha_2) = 0$. However, we observe that $p_i(\alpha_1 + \alpha_2) = 1$. As $\alpha_1 \in (u_0 + U)$ and $\alpha_2 \in (v_0 + V)$, this would be a contradiction to our assumption. For this not to happen, all such 'cross' monomials must not occur in any p_i. This happens with probability at most $2^{-(r/3)^2 t}$.

We union bound over all pairs of affine subspaces of dimension r and consider whether these pairs fall into the first case or the second case. If they fall into the first case, then we only union bound over $\leq 2^n \cdot \binom{2^n}{r/2}$ affine subspaces of dimension $r/2$ and consider the probability that P becomes linear over that affine subspace. If they fall into the second case, then we union bound over all $\leq \left(2^n \cdot \binom{2^n}{r/3}\right)^2$ disjoint pairs of affine subspaces of dimension $r/3$ use the probability bound above. We finally add both these probabilities to get our final bound. For the first case, the expression will be

$$2^{-\binom{r/2}{2}t} \cdot 2^n \cdot \binom{2^n}{r/2}$$

For the second case, the expression will be:

$$2^{-(r/3)^2 t} \cdot \left(2^n \cdot \binom{2^n}{r/3}\right)^2$$

We can choose c large enough so that the sum of the above probabilities is less than 2^{-t}. Then, we union bound over all 2^t of the $y \in \mathbb{F}_2^t$ to get the desired claim. □

We now show that for a quadratic map P, if there exist sets A, B such that $P(A) + P(B) = P(A + B)$, then we can also find affine subspaces U, V with the same property and of same sizes.

Claim 6.9. *Let $P = (p_1, \ldots, p_t) : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be a degree 2 polynomial map. Let $y \in \mathbb{F}_2^t$ be arbitrary. Let $A, B \subset \mathbb{F}_2^n$ be such that $P(A) + P(B) = P(A + B) + y$. Then, there exist affine subspaces $U, V \subset \mathbb{F}_2^n$ such that $P(U) + P(V) = P(U + V) + y$ and $|U| \geq |A|, |V| \geq |B|$.*

Proof. Without loss of generality assume that $y = 0^t$. Indeed, let $P'(x) = P(x) + y$ so that $P'(A) + P'(B) = P'(A + B)$. From $P'(U) + P'(V) = P'(U + V)$, we will again recover $P(U) + P(V) = P(U + V) + y$ as desired. Let C, D be such that $A \subset C$, $B \subset D$, $P(C) + P(D) = P(C + D)$, and C and D are the largest such sets. To prove the claim, it suffices to show that C and D are affine subspaces.

For $a \in F_2^n$, define $D_a(P)(x) = (D_a(p_1)(x), \ldots, D_a(p_t)(x)) = P(x) + P(x + a)$, the map of directional derivatives in direction a. Let $S_a = \{z \in \mathbb{F}_2^n : D_a(P)(z) = P(a)\}$. We claim that $y \in S_a \iff P(y) + P(a) = P(a + y)$. Indeed,

$$D_a(P)(y) = P(a) \iff P(y) + P(y + a) = P(a)$$

Let $S_C = \bigcap_{c \in C} S_c$. Then, it must be that $B \subset S_C$. Moreover, as $P(C) + P(S_C) = P(C + S_C)$ and D is maximal, $D = S_C$. By a symmetric argument, $C = S_D$. Observe that for arbitrary $a \in \mathbb{F}_2^n$, S_a is an affine subspace. As intersection of affine subspaces is an affine subspace, $S_C = D$ as well as $S_D = C$ are affine subspaces. □

We now prove a general trade-off for random quadratic NOBF sources containing a sumset:

Claim 6.10. *There exists a universal constant c such that the following holds. For any $0 < t < k$, there exists a degree d polynomial NOBF source $\mathbf{X}$ over $n = k + t$ bits with $H_\infty(\mathbf{X}) = k$ such that support$(\mathbf{X})$ does not contain any sumset $A + B$ where $|A| \geq 2^{cn/t}, |B| \geq 2^{cn/t}$.*

Proof. Let $\mathbf{X}$ be the polynomial NOBF source where first k bits are uniform variables and last t bits are output of polynomial map P from Claim 6.8 (hence set c to the universal constant from there). We now proceed by contradiction and assume there exist $A, B \subset \mathbb{F}_2^n$ such that $|A| \geq 2^{cn/t}, |B| \geq 2^{cn/t}$, and $A+B \subset$ support$(\mathbf{X})$. Let $a_0 \in A, b_0 \in B$ be arbitrary. Let $A' = a_0 + A, B' = b_0 + B, \mathbf{X}' = \mathbf{X} + (a_0 + b_0)$. Then, $A' + B' \subset$ support$(\mathbf{X}')$. Observe that $0^n \in A'$ and $0^n \in B'$. So, $A' \subset$ support$(\mathbf{X}')$, and $B' \subset$ support$(\mathbf{X}')$. Moreover, $\mathbf{X}'$ is a degree 2 polynomial NOBF source with $H_\infty(\mathbf{X}') = H_\infty(\mathbf{X})$.

Let the last $n - k$ bits of $\mathbf{X}'$ be the output of the degree 2 polynomial map P'. Let $A'_0, B'_0 \subset \mathbb{F}_2^k$ be the projections of A', B' respectively onto the first k bits. As $A' \subset$ support$(\mathbf{X}'), B' \subset$ support$(\mathbf{X}')$, and the last $n-k$ bits are deterministic functions of the first k bits, it must be that $|A'_0| = |A'|$ and $|B'_0| = |B'|$. Similarly, as $A'+B' \subset$ support$(\mathbf{X}')$, it must be that $P'(A'_0)+P'(B'_0) = P'(A'_0+B'_0)$. By Claim 6.9, there exist affine subspaces $U', V' \subset \mathbb{F}_2^k$ such that $P'(U') + P'(V') = P'(U' + V')$, $|U'| \geq |A'_0| = |A'|, |V'| \geq |B'_0| = |B'|$.

Observe that $P'(x) = P(g + x) + h$ where $g \in \mathbb{F}_2^k, h \in \mathbb{F}_2^t$ are some fixed strings. Then, $P(g + U') + P(g + V') = P(g + U' + V') + h$. Let $U, V \subset \mathbb{F}_2^k$ be such that $U = g + U', V = g + V'$. Then, U, V are affine subspaces, $P(U) + P(V) = P(U + V) + h$, and $|U| = |U'| \geq |A'| = |A|, |V| = |V'| \geq |B'| = |B|$. However, this is a contradiction to the choice of P. □

Proof of Theorem 6.6. The theorem immediately follows by setting $t = O(n/\log n)$ in Claim 6.10. □

We now prove a worst case to average case type reduction for sumsets using a bipartite Ramsey bound. Using this we show that sumset extractors cannot even disperse from degree 2 polynomial NOBF sources below certain min-entropy.

Lemma 6.11. *Let $0 < \delta < 1$ be a fixed constant. Let $\mathbf{X} \sim \mathbb{F}_2^n$ be such that for all flat sources $\mathbf{A}, \mathbf{B} \sim \mathbb{F}_2^n$ with $H_\infty(\mathbf{A}) = H_\infty(\mathbf{B}) = t$, it holds that $(\mathbf{A} + \mathbf{B}) \not\subset$ support$(\mathbf{X})$. Then, for all flat sources $\mathbf{R}, \mathbf{S} \sim \mathbb{F}_2^n$ such that $H_\infty(\mathbf{R}) = H_\infty(\mathbf{S}) = c \cdot 2^t$, it holds that $\Pr_{r \sim \mathbf{R}, s \sim \mathbf{S}}[r + s \in$ support$(\mathbf{X})] \leq \delta$. Here, $c > 0$ is a constant depending only on δ.*

Proof. Assume this is not the case and there exist such $\mathbf{R}$ and $\mathbf{S}$. Let $H_\infty(\mathbf{R}) = H_\infty(\mathbf{S}) = k$. Consider a bipartite graph G over support$(\mathbf{R}) \times$ support$(\mathbf{S})$ with an edge between $r \in$ support$(\mathbf{R})$ and $s \in$ support$(\mathbf{S})$ if $r + s \in$ support$(\mathbf{X})$. By assumption, G has at least $\delta \cdot 2^{2k}$ edges. Using *Corollary* 3.17, we infer that G induces a complete bipartite subgraph where where each part has size $\varepsilon \cdot k$ (ε depends only on δ). Equivalently, there exist sets $C \subset$ support$(\mathbf{R}), D \subset$ support$(\mathbf{S})$ such that $|C| = |D| = \varepsilon \cdot k$ and $(C + D) \subset$ support$(\mathbf{X})$. Let $\mathbf{A}$ be the uniform distribution over C and $\mathbf{B}$ be the uniform distribution over D. Then, $H_\infty(\mathbf{A}) = H_\infty(\mathbf{B}) = \log(\varepsilon \cdot k)$. Setting $c = 1/\varepsilon$, we get a contradiction. □

Using this reduction and previous results, we finally present the proof showing limitations of the sumset extractor against quadratic NOBF sources:

Proof of Theorem 6.7. Let $\mathbf{X}$ be source guaranteed by Claim 6.10 with $H_\infty(\mathbf{X}) = n - c_2 \frac{n}{\log\log n}$ such that for all $A, B \subset \mathbb{F}_2^n$ with $|A| = |B| = c \log n$, it holds that $(A + B) \not\subset \text{support}(\mathbf{X})$. Using Lemma 6.11, we infer that for all flat sources $\mathbf{R}, \mathbf{S} \sim \mathbb{F}_2^n$ with $H_\infty(\mathbf{R}) = H_\infty(\mathbf{S}) = c_1 \log n$, it holds that $\Pr(\mathbf{R} + \mathbf{S}) \in \text{support}(\mathbf{X}) \leq \delta$.

Let $\mathbf{Y} \sim \mathbb{F}_2^n$ be arbitrary convex combination of sumset sources $\{(\mathbf{R}^{(i)} + \mathbf{S}^{(i)})\}_i$, each with min-entropy $c_1 \log n$. Let $T = \text{support}(\mathbf{X})$. Then,

$$\begin{aligned}
|\mathbf{X} - \mathbf{Y}| &\geq \Pr[\mathbf{Y} \in \overline{T}] - \Pr[\mathbf{X} \in \overline{T}] \\
&= \Pr[\mathbf{Y} \in \overline{T}] \\
&\geq \min_i \Pr[\mathbf{Y}^{(i)} \in \overline{T}] \\
&= 1 - \max_i \Pr[\mathbf{Y}^{(i)} \in T] \\
&= 1 - \max_i \Pr[\mathbf{Y}^{(i)} \in T] \\
&\geq 1 - \delta.
\end{aligned}$$

□

7 Open problems

The problem of constructing extractors for sources sampled by $\mathbb{F}_2$-polynomials is a natural one, and we view our results as initial progress on this question. We leave open a number of interesting open directions:

1. Construct extractors or dispersers for polynomial sources with better min-entropy dependence than what we constructed here. For instance, some interesting potential candidates to explore are the MAJORITY function, or the generalized inner product function.

2. It will be interesting to make progress on the easier question of extracting from constant degree polynomial NOBF sources below min-entropy $0.999n$. Extracting from constant degree variety sources below min-entropy $0.999n$ is an important open problem and here, we introduced an interesting subclass of variety sources - polynomial NOBF sources - for which we don't have any better extractors either.

   An even simpler question is to construct *dispersers* for constant degree polynomial NOBF sources below min-entropy $n/2$. Note that for any NOBF source with $> n/2$ good bits, the MAJORITY function is a disperser.

3. Construct extractors or dispersers for polynomial sources with degree $\text{poly}(\log n)$. Such an extractor will also extract from sources sampled by $\mathsf{AC}^0[\oplus]$ circuits, a model for which no non-trivial extractors are known. Our constructions here work for degree up to $O(\log\log n)$, and fall short of achieving this.

8 Acknowledgements

We want to thank Michael Jaber for helpful discussions.

References

[Zná63] S Znám. "On a combinatorical problem of K. Zarankiewicz". In: *Colloquium Mathematicum*. Vol. 11. Instytut Matematyczny Polskiej Akademii Nauk. 1963, pp. 81–84 (cit. on p. 11).

[Raz87] Razbarov. "Lower bounds on the size of bounded depth circuits over a complete basis with logical addition". In: *Mathematical Notes of the Academy of Sciences of the USSR* 41.4 (1987), pp. 333–338 (cit. on p. 2).

[Smo93] R. Smolensky. "On representations by low-degree polynomials". In: *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. 1993, pp. 130–138. DOI: 10.1109/SFCS.1993.366874 (cit. on p. 2).

[MR95] Rajeev Motwani and Prabhakar Raghavan. *Randomized algorithms*. Cambridge University Press, 1995 (cit. on p. 1).

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. "A pseudorandom generator from any one-way function". In: *SIAM Journal on Computing* 28.4 (1999). Preliminary version in STOC 1989, pp. 1364–1396 (cit. on p. 11).

[TV00] Luca Trevisan and Salil P. Vadhan. "Extracting Randomness from Samplable Distributions". In: *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*. IEEE Computer Society, 2000, pp. 32–42. DOI: 10.1109/SFCS.2000.892063 (cit. on pp. 2, 12).

[Bou07] Jean Bourgain. "On the construction of affine extractors". In: *GAFA Geometric And Functional Analysis* 17.1 (2007), pp. 33–57 (cit. on p. 3).

[GR08] Ariel Gabizon and Ran Raz. "Deterministic extractors for affine sources over large fields". In: *Comb.* 28.4 (2008), pp. 415–440. DOI: 10.1007/s00493-008-2259-3 (cit. on p. 3).

[DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. "Extractors And Rank Extractors For Polynomial Sources". In: *Comput. Complex.* 18.1 (2009), pp. 1–58. DOI: 10.1007/s00037-009-0258-4 (cit. on p. 3).

[Rao09] Anup Rao. "Extractors for Low-Weight Affine Sources". In: *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*. IEEE Computer Society, 2009, pp. 95–101. DOI: 10.1109/CCC.2009.36 (cit. on p. 3).

[BKSSW10] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson. "Simulating independence: New constructions of condensers, ramsey graphs, dispersers, and extractors". In: *J. ACM* 57.4 (2010), 20:1–20:52. DOI: 10.1145/1734213.1734214 (cit. on p. 3).

[DG10] Matt DeVos and Ariel Gabizon. "Simple Affine Extractors Using Dimension Expansion". In: *Proceedings of the 25th Annual IEEE Conference on Computational Complexity, CCC 2010, Cambridge, Massachusetts, USA, June 9-12, 2010*. IEEE Computer Society, 2010, pp. 50–57. DOI: 10.1109/CCC.2010.14 (cit. on p. 3).

[Kop10] Swastik Kopparty. "Algebraic methods in randomness and pseudorandomness". PhD thesis. Massachusetts Institute of Technology, Cambridge, MA, USA, 2010 (cit. on p. 11).

[KRVZ11] Jesse Kamp, Anup Rao, Salil Vadhan, and David Zuckerman. "Deterministic extractors for small-space sources". In: *Journal of Computer and System Sciences* 77.1 (2011). Preliminary version in STOC 2006, pp. 191–220 (cit. on p. 2).

[Li11] Xin Li. "A New Approach to Affine Extractors and Dispersers". In: *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, USA, June 8-10, 2011*. IEEE Computer Society, 2011, pp. 137–147. DOI: 10.1109/CCC.2011.27 (cit. on p. 3).

[Sha11] Ronen Shaltiel. "Dispersers for Affine Sources with Sub-polynomial Entropy". In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*. Ed. by Rafail Ostrovsky. IEEE Computer Society, 2011, pp. 247–256. DOI: 10.1109/FOCS.2011.37 (cit. on p. 3).

[Yeh11] Amir Yehudayoff. "Affine extractors over prime fields". In: *Comb.* 31.2 (2011), pp. 245–256. DOI: 10.1007/s00493-011-2604-9 (cit. on p. 3).

[BHL12] Ido Ben-Eliezer, Rani Hod, and Shachar Lovett. "Random low-degree polynomials are hard to approximate". In: *Comput. Complex.* 21.1 (2012), pp. 63–81. DOI: 10.1007/s00037-011-0020-6 (cit. on p. 11).

[BK12] Eli Ben-Sasson and Swastik Kopparty. "Affine Dispersers from Subspace Polynomials". In: *SIAM J. Comput.* 41.4 (2012), pp. 880–914. DOI: 10.1137/110826254 (cit. on p. 3).

[DW12] Anindya De and Thomas Watson. "Extractors and Lower Bounds for Locally Samplable Sources". In: *ACM Trans. Comput. Theory* 4.1 (2012), 3:1–3:21. DOI: 10.1145/2141938.2141941 (cit. on p. 2).

[Dvi12] Zeev Dvir. "Extractors for varieties". In: *Comput. Complex.* 21.4 (2012), pp. 515–572. DOI: 10.1007/s00037-011-0023-3 (cit. on p. 3).

[Vad12] Salil P. Vadhan. "Pseudorandomness". In: *Found. Trends Theor. Comput. Sci.* 7.1-3 (2012), pp. 1–336. DOI: 10.1561/0400000010 (cit. on pp. 12, 15).

[BG13] Eli Ben-Sasson and Ariel Gabizon. "Extractors for Polynomial Sources over Fields of Constant Order and Small Characteristic". In: *Theory Comput.* 9 (2013), pp. 665–683. DOI: 10.4086/toc.2013.v009a021 (cit. on p. 3).

[Vio14] Emanuele Viola. "Extractors for Circuit Sources". In: *SIAM J. Comput.* 43.2 (2014), pp. 655–672. DOI: 10.1137/11085983X (cit. on p. 2).

[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, August 24-26, 2015, Princeton, NJ, USA*. Vol. 40. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015, pp. 680–709. DOI: 10.4230/LIPIcs.APPROX-RANDOM.2015.680 (cit. on pp. 4, 17).

[BDL16] Jean Bourgain, Zeev Dvir, and Ethan Leeman. "Affine extractors over large fields with exponential error". In: *Comput. Complex.* 25.4 (2016), pp. 921–931. DOI: 10.1007/s00037-015-0108-5 (cit. on p. 3).

[GK16] Alexander Golovnev and Alexander S. Kulikov. "Weighted Gate Elimination: Boolean Dispersers for Quadratic Varieties Imply Improved Circuit Lower Bounds". In: *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, January 14-16, 2016*. Ed. by Madhu Sudan. ACM, 2016, pp. 405–411. DOI: 10.1145/2840728.2840755 (cit. on p. 2).

[Li16] Xin Li. "Improved Two-Source Extractors, and Affine Extractors for Polylogarithmic Entropy". In: *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*. Ed. by Irit Dinur. IEEE Computer Society, 2016, pp. 168–177. DOI: 10.1109/FOCS.2016.26 (cit. on p. 3).

[Rem16] Zachary Remscrim. "The Hilbert Function, Algebraic Extractors, and Recursive Fourier Sampling". In: *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*. Ed. by Irit Dinur. IEEE Computer Society, 2016, pp. 197–208. DOI: 10.1109/FOCS.2016.29 (cit. on p. 3).

[HG17] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. "Quantum random number generators". In: *Reviews of Modern Physics* 89.1 (2017), p. 015004 (cit. on p. 1).

[CT19] Eshan Chattopadhyay and Avishay Tal. *Personal Communication to Li and Zuckerman*. 2019 (cit. on p. 3).

[LZ19] Fu Li and David Zuckerman. "Improved extractors for recognizable and algebraic sources". In: *23rd International Conference on Randomization and Computation (RANDOM)*. 2019 (cit. on pp. 3, 4).

[CG21] Eshan Chattopadhyay and Jesse Goodman. "Improved Extractors for Small-Space Sources". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 610–621. DOI: 10.1109/FOCS52979.2021.00066 (cit. on p. 2).

[CGL21] Eshan Chattopadhyay, Jesse Goodman, and Jyun-Jie Liao. "Affine Extractors for Almost Logarithmic Entropy". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 622–633. DOI: 10.1109/FOCS52979.2021.00067 (cit. on p. 3).

[GKW21] Alexander Golovnev, Alexander S. Kulikov, and R. Ryan Williams. "Circuit Depth Reductions". In: *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*. Ed. by James R. Lee. Vol. 185. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 24:1–24:20. DOI: 10.4230/LIPIcs.ITCS.2021.24 (cit. on p. 2).

[ACGLR22] Omar Alrabiah, Eshan Chattopadhyay, Jesse Goodman, Xin Li, and João Ribeiro. "Low-Degree Polynomials Extract From Local Sources". In: *arXiv preprint arXiv:2205.13725* (2022) (cit. on p. 2).

[CL22] Eshan Chattopadhyay and Jyun-Jie Liao. "Extractors for sum of two sources". In: *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*. Ed. by Stefano Leonardi and Anupam Gupta. ACM, 2022, pp. 1584–1597. DOI: 10.1145/3519935.3519963 (cit. on p. 4).

[RRW22] Maximus Redman, Lauren Rose, and Raphael Walker. "A Small Maximal Sidon Set in $\mathbb{Z}_2^n$". In: *SIAM J. Discret. Math.* 36.3 (2022), pp. 1861–1867. DOI: 10.1137/21m1454663 (cit. on p. 17).

[GVJZ23] Zeyu Guo, Ben Lee Volk, Akhil Jalan, and David Zuckerman. "Extractors for Images of Varieties". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. Ed. by Barna Saha and Rocco A. Servedio. ACM, 2023, pp. 46–59. DOI: 10.1145/3564246.3585109 (cit. on p. 3).

[Li23] Xin Li. "Two Source Extractors for Asymptotically Optimal Entropy, and (Many) More". In: *Electron. Colloquium Comput. Complex.* TR23-023 (2023). ECCC: TR23-023 (cit. on pp. 3, 4).

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il