Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 110 (2018)

Improved Extractors for Recognizable and Algebraic Sources

Fu Li*
Department of Computer Science,
University of Texas at Austin
fuli2015@cs.utexas.edu

David Zuckerman*
Department of Computer Science,
University of Texas at Austin
diz@cs.utexas.edu

September 5, 2018

Abstract

We study the task of seedless randomness extraction from recognizable sources, which are uniform distributions over sets of the form $\{x : f(x) = v\}$ for functions f in some specified class $\mathcal{C}$. We give two simple methods for constructing seedless extractors for $\mathcal{C}$-recognizable sources.

Our first method shows that if $\mathcal{C}$ admits XOR amplification, then we can construct a seedless extractor for $\mathcal{C}$-recognizable sources by using a mildly hard function for $\mathcal{C}$ as a black box. By exploiting this reduction, we give polynomial-time, seedless randomness extractors for three natural recognizable sources: (1) constant-degree algebraic sources over any prime field, where constant-degree algebraic sources are uniform distributions over the set of solutions to a system of constant degree polynomials; (2) sources recognizable by randomized multiparty communication protocols of cn bits, where $c > 0$ is a small enough constant; (3) halfspace sources, or sources recognizable by linear threshold functions. In particular, the new extractor for each of these three sources has linear output length and exponentially small error for min-entropy $k \geq (1 - \alpha)n$, where $\alpha > 0$ is a small enough constant.

Our second method shows that a seed-extending pseudorandom generator with exponentially small error for $\mathcal{C}$ yields an extractor with exponentially small error for $\mathcal{C}$-recognizable sources, improving a reduction by Kinne, Melkebeek, and Shaltiel [KvMS12]. Using the hardness of the parity function against AC^0 [Hås87], we significantly improve Shaltiel's extractor [Sha11] for AC^0-recognizable sources. Finally, assuming sufficiently strong one-way permutations, we construct seedless extractors for sources recognizable by BPP algorithms, and these extractors run in quasi-polynomial time.

*Supported by NSF Grant CCF-1526952, NSF Grant CCF-1705028, and a Simons Investigator Award (#409864, David Zuckerman).

ISSN 1433-8092

1 Introduction

Randomness is needed for many applications, such as statistics, algorithms and cryptography. However, most physical sources are not truly random, in the sense that they can have substantial biases and correlations. Weak random sources can also arise in cryptography when an adversary can learn partial information about a uniformly random string.

A natural approach to dealing with weak random sources is to apply a randomness extractor – a function that transforms a weak random source into an almost-perfect random source. However, it is impossible to give a single function that extracts even one bit of randomness from sufficiently general classes of sources [SV86]. There are two ways to combat this. One is to extract with the help of another short random string. An object constructed in this manner is called a seeded extractor [NZ96]. The focus of this paper is the second way: to extract from more structured sources (without using additional random bits). Such a function is called a seedless, or deterministic, extractor.

More formally, a random source X is modeled as a probability distribution over n bit strings with some entropy k. In the context of randomness extraction, the standard measure of entropy is the so called min-entropy – the min-entropy k of a source X is defined as $H_\infty(X) = \min_s(\log(1/\Pr[X = s]))$. Then, the definition of a seedless extractor can be presented as follows.

Definition 1.1 (Seedless extractors for structured sources)**.** *Let $\mathcal{D}$ be a class of distributions over $\{0,1\}^n$. We say a function $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ is a (k,ϵ)-extractor for $\mathcal{D}$ if for any distribution $D \in \mathcal{D}$ with min-entropy at least k, we have*

$$\mathrm{Ext}(D) \approx_\epsilon U_m,$$

where U_m denotes the uniform distribution over $\{0,1\}^m$ and $\approx_\epsilon$ stands for ϵ-close in statistical distance (Definition 4.1).

A large body of research has been devoted to constructing seedless extractors for various structured sources. There are mainly two natural perspectives to limit the structure of a distribution: an algebraic perspective and a computational perspective.

The algebraic perspective is to impose some algebraic structure on the distribution, such as an affine source [Bou07]. Later, affine sources were generalized to distributions defined using low-degree polynomials. On one hand, Dvir, Gabizon and Wigderson [DGW09] studied polynomial sources, which are the images of low-degree polynomial maps. On the other hand, viewing an affine source as the kernel, or set of zeros, of an affine mapping, Dvir [Dvi12] introduced the class of sources sampled uniformly from kernels or sets of common zeros of one or more polynomials, which he called algebraic sources[1].

The computational perspective is to assume a distribution has "low complexity". This started with Trevisan and Vadhan [TV00], who considered distributions that can be sampled by efficient algorithms. They showed that constructing a seedless extractor for this class is closely related to proving lower bound for circuits and gave a conditional construction of

[1]For clarification, in [Dvi12], Dvir mentioned sources which are distributed uniformly on varieties. A variety is also a set of common zeros of one or more polynomials, but it is often defined to require the ground field to be algebraically closed.

such an extractor based on lower bound assumptions. Later, in [KRVZ11], an unconditional extractor was constructed for sources generated by space-bounded algorithms. More recently, Viola [Vio14] constructed a seedless extractor for AC^0-samplable sources.

1.1 Recognizable sources

We focus on recognizable sources, first suggested by Shaltiel [Sha11]. Recognizable sources are uniform distributions over sets of the form $\{x : f(x) = v\}$ for functions f coming from some specified class. Formally, for any boolean function $f : \{0,1\}^n \to \{0,1\}$, define the source recognizable by f, denoted by U_f, as the uniform distribution over $f^{-1}(1)$. For short, we call this distribution the f-recognizable source. For any boolean function family $\mathcal{C}$, the set of $\mathcal{C}$-recognizable sources is the set of f-recognizable sources, for each $f \in \mathcal{C}$.

This notion naturally interacts with the algebraic and computational perspectives to limit the structure of a distribution, and also captures several distributions that were widely studied. For example, distributions with algebraic structures are those distributions recognizable by algebraic classes – affine sources are distributions recognizable by affine functions and algebraic sources are distributions recognizable by products of low-degree polynomials. Moreover, distributions that have "low complexity" could also be the distributions recognizable by low-complexity classes, such as small circuits.

Shaltiel [Sha11] initially proposed an extractor for recognizable sources. He showed that such extractors produced randomness that was in some sense not correlated with the input and hence could be used for derandomization. In particular, to derandomize any class of randomized algorithms, he needed to explicitly construct an extractor for distributions recognizable by the class. He showed that without further changes, some appropriate known extractors could work for distributions recognizable by decision trees, streaming algorithms, and AC^0. What's more, assuming average-case hardness against polynomial-size circuits, he showed that applying the hard function on disjoint blocks of the input was an extractor for distributions recognizable by general polynomial-time algorithms.

Later, Kinne, Melkebeek and Shaltiel [KvMS12] improved the derandomization results in [Sha11] by using seed-extending pseudorandom generators, which are pseudorandom generators that reveal their seed. They gave reductions between seed-extending PRGs and extractors for recognizable sources. However, both Shaltiel [Sha11] and this later paper [KvMS12] focused on derandomization rather than constructing new extractors.

1.2 XOR Amplification

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, let $f^{\oplus m}(x_1, \ldots, x_m) := \bigoplus_{i \in [m]} f(x_i)$ denote the XOR of m independent copies of f. The XOR Amplification Lemma[2] states that if a function f is hard on average for some computational class $\mathcal{C}$, (i.e., f cannot be computed correctly by any function in $\mathcal{C}$ on at most a $(1/2 + p)$-fraction of of the inputs), then $f^{\oplus m}$ cannot be computed correctly on at most a $(1/2 + p^{\Omega(m)})$-fraction of of the inputs. Loosely speaking, the hardness of f is amplified when the outputs of independent copies of f are XOR together. Indeed, this idea is analogously to the information theoretic setting. If f is

[2]This is usually called simply the XOR lemma, but we want to distinguish it from a different XOR lemma.

a biased coin with $\Pr[f = 1] = 1/2 + p$, then the XOR of m independent biased coins, $f^{\oplus m}$, induces a coin with $\Pr[f^{\oplus m} = 1] = 1/2 - (-2p)^m/2$. However, showing that such an idea holds in the computational ideas is significantly more involved.

There are several works dedicated to proving XOR amplification for computational models. Yao [Yao82] first suggested XOR amplification, and proved that XOR (hardness) amplification held for polynomial-size circuits. Unfortunately, the amplification stops when XORing more than logarithmically many copies, which makes it not so useful for us. Later, Viola and Wigderson [VW08] showed XOR amplification for multi-party communication complexity and polynomials over GF(2). Subsequently, their proof was extended by Bogdanov, Kawachi and Tanaka [BKT13], to prove XOR amplification for polynomials over any prime field.

In this paper, we give a new application of XOR amplification – constructing seedless extractors for recognizable sources.

2 Overview of our results

2.1 From XOR amplification to Extractors for recognizable sources

As others have independently observed, it is not hard to use correlation bounds to extract a single bit. In this paper, we use XOR amplification to extend the output length from one bit to linear in the input length.

Intuitively, XOR amplification states that if a function f is hard on average for some computational class $\mathcal{C}$, then $f^{\oplus m}(x_1, \ldots, x_m) = f(x_1) \oplus \cdots \oplus f(x_m)$ is exponentially harder on average. In particular, consider a computational class $\mathcal{C}$ as a family of boolean functions.

Let $\mathcal{C} \subseteq \{\{0,1\}^* \to \{0,1\}\}$ be a class of boolean functions. For a positive constant α, we say $\mathcal{C}$ has α-XOR amplification if there exists a function $h : \{0,1\}^t \to \{0,1\}$ such that for any positive integer k, $Cor(h^{\oplus k}, g) \leq 2^{-\alpha k}$, for any $g \in \mathcal{C}$.

We show that if $\mathcal{C}$ is closed under restrictions and $\mathcal{C}$ has α-XOR amplification, then there is an efficient extractor for $\mathcal{C}_n$-recognizable sources, where $\mathcal{C}_n$ denotes the set of all n-variate functions in $\mathcal{C}$.

Theorem 2.1. *Let $\mathcal{C} \subseteq \{\{0,1\}^* \to \{0,1\}\}$ be any boolean function class closed under restrictions and α be any positive constant. If $\mathcal{C}$ has α-XOR amplification, then for any positive integer n, there is an explicit seedless $((1-\beta)n, 2^{-\Omega(\alpha n)})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ for $\mathcal{C}_n$-recognizable sources, where $\beta > 0$, $m = \Omega(\alpha n)$, and $\mathcal{C}_n$ denotes the set of all n-variate functions in $\mathcal{C}$.*

Our construction uses $h : \{0,1\}^t \to \{0,1\}$ and the generator matrix M of a good $[l, m, r]$-code, where $l = n/t$. We think of the input length t as a large constant, and the distance r as being linear in l. Then $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ is simply

$$\mathrm{Ext}(x) = h^{(l)}(x)M, \text{ where } h^{(l)}(x = (x_1, \ldots, x_l)) = (h(x_1), \ldots, h(x_l)).$$

Li [Li16] uses a similar construction to extend the output length of two-source extractors from one bit to more.

2.1.1 Algebraic sources over GF(2)

An algebraic set is a set of common zeros of one or more multivariate polynomials defined over a finite field $\mathbb{F}$. An *algebraic source* is a random variable distributed uniformly over an algebraic set, which was originally introduced by Dvir [Dvi12]. Algebraic sources are a natural generalization of affine sources that have been widely studied. Furthermore, we say that an algebraic source has degree d if the algebraic source can be defined by polynomials of degree at most d. Dvir obtained explicit extractors for degree-d algebraic sources with entropy rate greater than $1/2$ over moderately sized fields, where $|\mathbb{F}| = \mathrm{poly}(d)$, and with small entropy rate over large fields, where $|\mathbb{F}| = d^{\Omega(n^2)}$.

Golovnev and Kulikov [GK16] related the study of Boolean dispersers for quadratic algebraic sets to improving circuit lower bounds. A disperser is a relaxation of an extractor, which is only required to output a non-constant bit from a weak random source. They posed the open question of constructing a disperser for any algebraic set of size $2^{0.03n}$ and defined by using at most $1.78n$ quadratic polynomials. Such a disperser yields a new circuit lower bound.

To the best of our knowledge, the best known extractor for algebraic sources over GF(2) was due to Remscrim [Rem16], outputting one bit with error $O(1/\sqrt{n})$ for min-entropy $n-n^c$ for any $c < 1/2$. However it can handle larger degree $n^{1/2-\alpha}$, where $\alpha > 0$ is a constant. Our construction significantly improves the extractor for constant-degree algebraic sources, outputting more bits and handling lower min-entropy.

We construct a seedless extractor for algebraic sources of constant degree for some linear min-entropy. In particular, the new extractor has linear output length and exponentially small error for min-entropy $k \geq (1-\alpha)n$, where $\alpha > 0$ is a small enough constant.

Definition 2.2 (Algebraic extractor)**.** *We say that* $\mathrm{Ext} : \mathbb{F}^n \to \mathbb{F}^m$ *is a* (k, d, ϵ)*-algebraic extractor over* $\mathbb{F}$ *if for any degree-*d *algebraic source* U_V *with* $|V| \geq |\mathbb{F}|^k$, $\mathrm{Ext}(U_V) \approx_\epsilon U_m$.

Applying Theorem 2.1 to this setting, we prove the following theorem.

Theorem 2.3. *For any positive integer* d*, there is an efficient* $\left((1-1/c_d)n, d, 2^{-\Omega(n/c_d)}\right)$*-algebraic extractor* $\mathrm{Ext} : \mathbb{F}_2^n \to \mathbb{F}_2^m$*, where* $c_d = \Theta(d^2 4^d)$*,* $m = \Omega(n/c_d)$.

2.1.2 Algebraic sources over prime fields

We can extend our algebraic extractor to any prime field $\mathbb{F}_q$.

Theorem 2.4. *For any positive integer* d *and any prime field* $\mathbb{F}_q$*, there is an efficient* $\left((1-1/c_{d,q})n, d, q^{-\Omega(n/c_{d,q})}\right)$*-algebraic extractor* $\mathrm{Ext} : \mathbb{F}_q^n \to \mathbb{F}_q^m$*, where* $c_{d,q} = \Theta(d^2 2^{2d} q^3 \log q)$*,* $m = \Omega(n/c_{d,q})$.

2.1.3 Sources recognizable by communication protocols

We consider a boolean function class that has low communication complexity. Communication complexity was defined by Yao [Yao79], who introduced a standard 2-party communication model. Later, Chandra, Furst, and Lipton [CFL83] generalized this to the multiparty model. In a t-party communication NOF (number-on-forehead) model, each party holds a

separate input and each party knows all but its own input. These parties attempt to compute (or approximate) a given function of these t inputs by exchanging few bits of communication. The complexity of a communication protocol is the number of bits exchanged on the worst input. Both deterministic and randomized communication protocols are considered. A randomized protocol can be viewed as a distribution on deterministic protocols.

For deterministic 2-party protocols, Shaltiel [Sha11] already constructed an efficient extractor that has linear output for linear min-entropy and exponentially small error. To do this, he proved that 2-source extractors are also extractors for sources recognizable by deterministic 2-party protocols, and hence some known constructions of 2-source extractors could be used. However, this approach is tailored to the 2-party case and does not generalize to the t-party case for some $t > 2$.

We construct an extractor for sources recognizable by randomized t-party protocols. Formally, we prove the following theorem.

Theorem 2.5. *There exists an explicit seedless $((1 - 1/c_t)n,\ 2^{-c_1 n/c_t})$ extractor* $\mathrm{Ext} : \left(\{0,1\}^{n/t}\right)^t \to \{0,1\}^{c_2 n/c_t}$ *for sources recognizable by randomized t-party communication protocols of at most $c_3 n/4^t$ bits, where $c_t = \Theta(t4^t)$ and c_1, c_2, c_3 are some positive constants.*

This extractor has linear output for linear min-entropy and exponentially small error, and is simply $\mathrm{Ext}(x) = \left(\wedge_t^{(l)}(x)\right) M$, where $l = n/t$, $\wedge_t$ is the AND function over t variables and M is the $l \times (c_2 n/c_t)$ generator matrix of a good linear code.

2.1.4 Halfspace sources

Halfspace sources are sources recognizable by linear threshold functions. A linear threshold function (abbreviated LTF) is a boolean function $f : \{0,1\}^n \to \{0,1\}$ that can be represented as $f(x) = 1_{\sum_{i \in n} a_i x_i > a_0}$ for some constants $a_0, a_1, \ldots, a_n \in \mathbb{R}$. From a geometric perspective, a boolean LTF is a halfspace-indicator to the discrete cube $\{0,1\}^n$.

We construct an efficient extractor that has linear output for linear min-entropy and exponentially small error for halfspace sources.

Theorem 2.6. *There exists an explicit seedless $((1 - c_1)n,\ 2^{-c_2 n})$ extractor* $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{c_3 n}$ *for halfspace sources, where c_1, c_2, c_3 are some positive small enough constants.*

The construction of this extractor is simply $\mathrm{Ext}(x) = \left(\wedge_2^{(l)}(x)\right) M$, where $l = n/2$, M is the $l \times c_3 n$ generator matrix of a good linear code.

2.2 From Seed-extending PRGs to Extractors for recognizable sources

The Kinne et al. reductions between seed-extending pseudorandom generators and extractors for recognizable distributions were asymmetric. They showed that an extractor with exponentially small error yielded a seed-extending pseudorandom generator with exponentially small error. However, they proved a weak converse.

In this paper, we prove that a seed-extending pseudorandom generator with exponentially small error yields an extractor with exponentially small error. This applies to flip-invariant families of boolean functions, which are invariant under flipping input bits (see Definition 4.11).

Lemma 2.7. *Let $\mathcal{C}$ be a flip-invariant family of boolean functions over n bits. If G is a seed-extending (d, ϵ)-pseudorandom generator $G : \{0,1\}^d \to \{0,1\}^n$ for $\mathcal{C}$, then for any $\Delta = \Delta(n) > 0$ we can construct an $(n - \Delta, 2^{\Delta}\epsilon)$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-d}$ for $\mathcal{C}$-recognizable sources. Specifically, if $G(x) = (x, E(x))$ fools any function in $\mathcal{C}$, then $\mathrm{Ext}(x \circ y) = y \oplus E(x)$ is an $(n - \Delta, 2^{\Delta}\epsilon)$-extractor for $\mathcal{C}$-recognizable sources, where $x \in \{0,1\}^d, y \in \{0,1\}^m$, where $m = n - d$.*

In particular, the reduction in [KvMS12] requires a tiny $\epsilon \leq 2^{-(m+2\Delta)}$ for the seed-extending PRG to get an $(n - \Delta, 2^{-\Delta})$-extractor. Moreover, the reduction in [KvMS12] breaks down for a seed-extending PRG, $G(x) = (x, E(x))$, where $E(x)$ is longer than x. We improve the reduction from seed-extending PRGs to extractors to require only $\epsilon \leq 2^{-2\Delta}$, without depending on the output length m. Furthermore, the new reduction can still work even for a seed-extending PRG, $G(x) = (x, E(x))$, where $E(x)$ is longer than x.

Based on this new reduction, we significantly improve extractors for two important types of recognizable sources as follows.

2.2.1 Circuit-recognizable sources

Kinne et al. proved that the well-known Nisan-Wigderson pseudorandom generator construction [NW88] can be made seed-extending. Therefore, assuming hardness against small circuits, we can construct an extractor for sources recognizable by small circuits.

Proposition 2.8. *For any $\Delta = \Delta(n) > 0$ and positive integers $l < n$, if there is a function H that is ϵ-hard at input length $\sqrt{l}/2$ for circuits of size $s + (n-l)2^{O(\log(n-l)/\log l)}$ and depth $d+1$, then we can get an $(n - \Delta, (n-l)2^{\Delta}\epsilon)$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-l}$ for any sources recognizable by circuits of size s and depth d.*

Using the hardness of the parity function against AC^0 [Hås87], we significantly improve Shaltiel's extractor [Sha11] for AC^0-recognizable sources.

Theorem 2.9. *For any $\Delta = \Delta(n) > 0$, there exists a polynomial time computable $(n - \Delta, (n-l)2^{\Delta - \Omega(l^{1/(2d+2)})})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-l}$ for any sources recognizable by circuits of size $2^{n^{1/d}}$ and depth d.*

In particular, for min-entropy $n - n^{1/(\alpha d)}$, our extractor outputs $n - n^{2/\alpha + O(1/d)}$ bits, whereas Shaltiel's extractor outputs only $n^{1/(\alpha d)}$ bits. When $\alpha > 2d/(d-1)$ is a large enough constant, our extractor outputs $n - o(n)$ bits whereas Shaltiel's extractor outputs only $n^{1/(\alpha d)}$ bits. For min-entropy $n - \mathrm{polylog}(n)$ bits, our extractor outputs $n - \mathrm{polylog}(n)$, whereas Shaltiel's extractor outputs only $\mathrm{polylog}(n)$ bits.

Our methods also apply to formulas. Komargodski, Raz and Tal [KRT17] constructed an explicit function $h : \{0,1\}^n \to \{0,1\}$ that is $2^{-\Omega(r)}$-hard for any deMorgan formula of size $n^{3-o(1)}/r^2$. Based on this hardness result, we can construct an efficient extractor for sources recognizable by deMorgan formulas of size close to $n^{3/2}$.

Theorem 2.10. *For any $\Delta, r, \alpha > 0$ and $m \leq (1-\alpha)n$, there exists a polynomial time computable $(n-\Delta, m2^{\Delta-\Omega(r)})$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ for any sources recognizable by deMorgan formulas of size $n^{3/2-o(1)}/r^2$.*

2.2.2 Sources recognizable by efficient randomized algorithms

Note that there are no efficient seed-extending cryptographic PRGs. Otherwise, with revealed seeds, it is easy to efficiently distinguish the output of an efficient seed-extending PRG, $G(x) = (x, E(x))$, from a random string (x, y), by checking whether y equals $E(x)$.

We show that there is an inefficient seed-extending cryptographic PRG implied by the existence of one-way permutations. By our reduction, we show that a one-way permutation with exponentially small error yields an $(n-n^{\Omega(1)}, 2^{-n^{\Omega(1)}})$ extractor extracting $n-n^{O(1)}$ bits from sources recognizable by BPP algorithms. Formally, this follows by taking $\epsilon = 2^{-cn^{\alpha}}$ and $q(n) = n^{w(1)}$ in the following theorem.

Theorem 2.11. *For any polynomial-time computable functions $t(\cdot)$ and $\epsilon(\cdot)$, assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way permutation with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded inverters. Then for any $\Delta = \Delta(n) > 0$ and a positive constant $\delta < 1$, we can construct an $\left(n-\Delta, O\left(2^{\Delta}\epsilon(n^{\delta})^{c_\delta}\right)\right)$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-n^{\delta}}$ for sources recognizable by randomized algorithms running in time $\left(t(n^{\delta})\right)^{c_\delta}$, where c_δ is a constant depending on δ. The running time of the extractor is a polynomial times the time to compute the inverse function f^{-1} of the one-way permutation f with input length n^{δ}.*

Furthermore, the running time of such an extractors will be quasi-polynomial if there exists a sufficiently strong one-way permutations. In particular, by scaling down, we have the following corollary.

Corollary 2.12. *For any constants $a, b, c, \delta > 0$, assume that there exists a one-way permutation invertible in time $O\left(2^{n^a}\right)$ with error 2^{-n^c} against $2^{\delta n^b}$-bounded inverters, Then, for any positive constants α and $\beta < 1$, we can get an $\left(n - c_\beta \log^{c\alpha}(n), O\left(2^{-c_\beta \log^{c\alpha}(n)}\right)\right)$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-n^{\beta}}$ for sources recognizable by randomized algorithms running in time $2^{c_\beta \delta \log^{b\alpha}(n)}$, where c_β is a constant depending on β.The running time of the extractor is $O\left(2^{\log^{a\alpha}(n^{\beta})}\right)$.*

3 Overview of our main constructions and proofs

3.1 From XOR amplification to Extractors

In this subsection, we describe how to construct a seedless extractor for $\mathcal{C}$-recognizable sources if there exists a function $h : \{0,1\}^t \to \{0,1\}$ such that for any $g \in \mathcal{C}$ and $k \leq n/t$, $Cor(h^{\oplus k}, g) \leq 2^{-\Omega(k)}$. Think of $t = O(1)$.

We start with the statistical XOR lemma[3], usually attributed to Vazirani. We say a random variable Z over $\{0,1\}$ is ϵ-biased if $bias(Z) = Cor(Z, 0) = |\Pr[Z = 0] - \Pr[Z = 1]| \leq \epsilon$.

[3]The statistical XOR lemma is unrelated to the XOR amplification used in our proof.

Lemma 3.1 (Statistical XOR Lemma)**.** *Let $X_1, \ldots, X_m$ be* 0-1 *random variables such that for any nonempty $S \subseteq \{1, \ldots, m\}$, the random variable $\bigoplus_{i \in S} X_i$ is ϵ-biased. Then, the distribution of $(X_1, \ldots, X_m)$ is $\epsilon 2^{m/2}$-close to uniform.*

Let $g_i(x)$ be the i-th bit of $\mathrm{Ext}(x)$ for each $i \in [m]$. Thus, to show that the output of Ext is close to uniform, it suffices to show that for any non-empty set $S \subseteq [m]$, $g_S = \sum_{i \in S} g_i$ is low-biased conditioned on $f(x) = 1$ for each $f \in \mathcal{C}$. By XOR amplification, it is enough to guarantee that each g_S is the sum of $\Omega(n)$ independent copies of h, and hence g_S has $2^{-\Omega(n)}$ correlation with any function in $\mathcal{C}$.

A linear code is a natural candidate to guarantee that each g_S is the sum of $\Omega(n)$ independent copies. Let $h^{(l)} : \{0,1\}^{tl} \to \{0,1\}$ denote the concatenation of l copies of h and M be the generating matrix of an asymptotically good $[l, m, r]_2$ code. Our construction is simply

$$\mathrm{Ext}(x) = (g_1(x), \ldots, g_m(x)) = h^{(l)}(x)M.$$

Finally, we observe that the bias of g_S conditioned on $f(x) = 1$ can be bounded by the correlation between g_S and f plus the bias of g_S.

Lemma 3.2. $|\Pr[g_S(X) = 1 | f(X) = 1] - \Pr[g_S(X) = 0 | f(X) = 1]| \leq \frac{Cor(g_S, f) + bias(g_S)}{2 \Pr[f(X)=1]}$.

That is, if we choose a good linear code, then $\mathrm{Ext}(x) = h^{(l)}(x)M$ is an extractor for $\mathcal{C}$-recognizable sources with exponentially small error.

For details, see Section 5.

3.2 Algebraic extractors over GF(2)

In this subsection, we describe our algebraic extractor construction.

Notice that to construct a degree-d algebraic extractor that outputs only one bit, it is enough to let the extractor have small correlation bounds with degree-d polynomials. This fact is implicitly proved by Dvir [Dvi12] and observed by others, e.g., Eshan Chattopadhyay and Avishay Tal (personal communication). Based on this fact, we combine XOR amplification and linear codes to extend the output length form one bit to more.

First we observe that an algebraic source over n bits defined by n-variate polynomials $p_1, \ldots, p_k$ is also a source recognizable by the product $\prod_{i \in [k]}(p_i + 1)$. Let $\mathcal{V}_d$ denote the set of all products of polynomials of degree at most d. Thus, for any positive integer n, to get an extractor for n-bit algebraic sources of degree d, it suffices to construct an extractor for $\mathcal{V}_d$-recognizable sources over n bits. In particular, by the previous discussion, it suffices to show that XOR amplification holds for $\mathcal{V}_d$.

Second we observe that to show that a function f has low correlations with $\mathcal{V}_d$, it suffices to show that f has low correlation with any d-degree polynomials. This is because the L1 norm of the Fourier transform of the AND function is at most 2.

Viola and Wigderson [VW08] proved XOR amplification for low-degree polynomials over GF(2). Specifically, if a Boolean function h over $\{0,1\}^{O(d)}$ has correlation at most $1 - 1/2^d$ with degree-d polynomials, then the correlation between $h^{\oplus l}$ (see Section 1.2) and degree-d polynomials drops exponentially with l. Such h are known.

For details, see Section 5.1.

3.3 From seed-extending PRGs to Extractors

We start with a new reduction from pseudorandom generators to seedless extractors. Observe that a seedless extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ partitions $\{0,1\}^m$ as $\bigcup_{z\in\{0,1\}^m} \mathrm{Ext}^{-1}(z)$. If Ext is a (k,ϵ)-extractor for $\mathcal{C}$-recognizable sources, then for every $f \in \mathcal{C}$ with $|f^{-1}(1)| \geq 2^k$, most intersections $\mathrm{Ext}^{-1}(z) \cap f^{-1}(1)$ should have almost the same size. That is, for most m-bit strings z, the preimage $\mathrm{Ext}^{-1}(z)$ is an ϵ-pseudorandom set against any $f \in \mathcal{C}$ with $|f^{-1}(1)| \geq 2^k$.

Now, given PRGs, how do we construct extractors? From the above observation, converting an ϵ-pseudorandom set into a partition of ϵ-pseudorandom sets is a possible way. If each preimage $\mathrm{Ext}^{-1}(z)$ of Ext is an ϵ-pseudorandom set for $\mathcal{C}$, Ext should be an extractor for $\mathcal{C}$-recognizable sources with a bit worse parameters.

To make $\mathrm{Ext}^{-1}(z)$ an ϵ-pseudorandom set for each z, we need a seed-extending PRG $G(x)$, i.e., $G(x) = x \circ E(x)$ for some function $E : \{0,1\}^d \to \{0,1\}^{n-d}$. By linearly shifting the set $\{(x, E(x))\}$, we can partition $\{0,1\}^n$ as $\bigcup_{z\in\{0,1\}^{n-d}} \{(x, (E(x) \oplus z)) : x \in \{0,1\}^d\}$. We therefore define $\mathrm{Ext}(x, z) = E(x) \oplus z$. Since $\mathcal{C}$ is a flip-invariant function family, we have that the set $\mathrm{Ext}^{-1}(z) = \{(x, (E(x) \oplus z)) : x \in \{0,1\}^d\}$ fools any function f in $\mathcal{C}$.

For details, see Section 6.

3.4 Algebraic extractors over prime fields

We remark that the main results used in building our algebraic extractor over GF(2) – the XOR amplification, the statistical XOR lemma and the asymptotically linear code – all have been extended to prime fields. Thus, to generalize our algebraic extractor, the remaining difficulties are not hard.

Bogdanov, Kawachi and Tanaka [BKT13] proved XOR amplification for low-degree polynomials over prime fields, i.e., the sum of k independent copies of h was $q^{-\Omega(k)}$-hard for P_d if h was mildly hard. However, besides the sum of copies, we require the same hardness result for linear combinations of k copies of h. We prove this hardness result by using the original proof of Bogdanov, Kawachi and Tanaka with some slight modifications. The main revision of our proof uses the fact that the Gowers norm is multiplicative for functions over disjoint sets of input variables.

Furthermore, over a prime field $\mathbb{F}_q$, an algebraic source over n bits defined by n-variate polynomials $p_1, \ldots, p_k$ is a source recognizable by the product $\prod_{i\in[k]}(1 - p_i^{q-1})$. We need to analyze the product of the special form $\prod_{i\in[k]}(1 - x_i^{q-1})$, as an analog of the AND function over GF(2).

The reason we assume prime fields in our results is that XOR amplification for polynomials is known only over prime fields.

For details, see Section 7.

4 Preliminaries

In the following, for any two binary strings x, y, let $x \circ y$ denote their concatenation, and let $x \oplus y$ denote their bitwise XOR when x and y have the same length.

Definition 4.1 (Statistical distance)**.** *Let D_1 and D_2 be two distributions over a set S. Define the* statistical distance *between D_1 and D_2 as $|D_1 - D_2| = \frac{1}{2}\sum_{s\in S} |\Pr[D_1 = s] - \Pr[D_2 = s]|$. We say D_1 is ϵ-close to D_2, denoted by $D_1 \approx_\epsilon D_2$, if $|D_1 - D_2| \leq \epsilon$.*

Definition 4.2 (Recognizable source)**.** *For any boolean function $f : \{0,1\}^n \to \{0,1\}$, define the source recognizable by f, denoted by U_f, as the uniform distribution over $f^{-1}(1)$. For short, we call this distribution the f-recognizable source.*

For any boolean function family $\mathcal{C}$, the set of $\mathcal{C}$-recognizable sources is the set of f-recognizable sources for $f \in \mathcal{C}$.

For $l \in \mathbb{N}$, let U_l denote the uniform distribution on l bits.

Definition 4.3 (Extractor for recognizable sources [Sha11])**.** *Let $\mathcal{C}$ be a class of functions $C : \{0,1\}^n \to \{0,1\}$. We say that* Ext $: \{0,1\}^n \to \{0,1\}^m$ *is a (k,ϵ)-extractor for $\mathcal{C}$-recognizable sources if for every $f \in \mathcal{C}$ such that $|f^{-1}(1)| \geq 2^k$, $\mathrm{Ext}(U_f) \approx_\epsilon U_m$.*

Note that when the output length $m = 1$, the extractor is simply a boolean function which has low correlation with any function in $\mathcal{C}$.

4.1 Algebraic sources

An algebraic set is a set of common zeros of one or more multivariate polynomials defined over a finite field $\mathbb{F}$.

Definition 4.4 (Algebraic set)**.** *For any s polynomials $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$, the set $V(f_1, \ldots, f_s) = \{x \in \mathbb{F}^n | f_i(x) = 0, \forall i \in [s]\}$ is an algebraic set. We say V is an algebraic set of degree d, if each polynomial f_i has degree at most d.*

An *algebraic source* is a random variable distributed uniformly over an algebraic set as initially defined by Dvir [Dvi12].

Definition 4.5 (Algebraic source)**.** *An algebraic source is the uniform distribution U_V over an algebraic set V. If V is a degree-d algebraic set, then we say U_V is an algebraic source of degree d.*

Definition 4.6 (Algebraic extractor)**.** *We say that* Ext $: \mathbb{F}^n \to \mathbb{F}^m$ *is a (k,d,ϵ)-algebraic extractor if for any degree-d algebraic source U_V with $|V| \geq |\mathbb{F}|^k$, $\mathrm{Ext}(U_V) \approx_\epsilon U_m$.*

Definition 4.7 (Linear codes over prime fields)**.** *For a prime q, a linear code of length n and dimension k is a k-dimensional linear subspace C of the vector space $\mathbb{F}_q^n$. If the distance of the code C is d we say that C is an $[n,k,d]_q$ code. A family of codes $\{C_n\}$ is asymptotically good if there exist constants $0 < \delta_1, \delta_2 < 1$ s.t. $k \geq \delta_1 n$ and $d \geq \delta_2 n$.*

Note that every linear code has an associated generating matrix $M \in \mathbb{F}_q^{kn}$, and every codeword can be expressed as vM, for some vector $v \in \mathbb{F}_q^k$. There are explicit constructions of asymptotically good linear codes, such as the Justensen codes over GF(2) constructed in [Jus72] and the expander codes over GF(q) in [ABN+92] for any prime q.

Definition 4.8 (Correlation over prime fields)**.** *Let $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$ be two functions over n inputs. The correlation between f and g with respect to the uniform distribution is defined as*

$$Cor(f, g) := |Ee_q[f(x) + g(x)]| \in [0, 1],$$

where $e_q[x] := w^x$ for $x \in \{0, 1, \ldots, q-1\}$, where w denotes the q-th root of unity.

For a class $\mathcal{C}$ of functions, we denote by $Cor(f, \mathcal{C})$ the maximum of $Cor(f, C)$ over all $C \in \mathcal{C}$ whose domain is the same as f.

Furthermore, when $q = 2$, $e_2[x] = (-1)^x$ and $Cor(f, g) = |\Pr[f(x) = g(x)] - \Pr[f(x) \neq g(x)]|$. We often write $e_2[x]$ as $e[x]$ for convenience.

Definition 4.9 ($f^{(m)}, f^v$)**.** *For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$, let $f^{(m)}$ denote the concatenation of m copies of f, i.e., $f^{(m)}(x_1, x_2, \ldots, x_m) := (f(x_1), \ldots, f(x_m))$, where $x_1, \ldots, x_m \in \mathbb{F}_q^n$. For each $v = (v_1, \ldots, v_m) \in \mathbb{F}_q^m$, let f^v denote the linear combination of m copies of f according to v, i.e., $f^v(x_1, x_2, \ldots, x_m) := \sum_{i \in [m]} v_i f(x_i)$.*

Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ denotes the set of non-zero elements in $\mathbb{F}_q$. We remark that the statistical XOR lemma has been generalized to prime fields by e.g., Goldreich [Gol95].

Lemma 4.10 (Statistical XOR Lemma over $\mathbb{F}_q$)**.** *Let $X = (X_1, \ldots, X_m)$ be random vector over $\mathbb{F}_q^m$ such that for any nonzero vector $v = (v_1, \ldots, v_m) \in \mathbb{F}_q^m \setminus \{0^m\}$, the random variable $v \cdot X = \sum_{i \in [m]} v_i X_i$ is ϵ-biased. Then, the distribution of $(X_1, \ldots, X_m)$ is $\epsilon q^{m/2}$-close to the uniform distribution over $\mathbb{F}_q^m$.*

For example, when $m = 1$, for a random variable X over F_q, to show that $X \approx_\epsilon U_{\mathbb{F}_q}$, we need to show that $bias(\alpha X) \leq \epsilon/\sqrt{q}$ for each $\alpha \in \mathbb{F}_q^*$.

4.2 Seed-extending PRGs

Definition 4.11 (Flip-invariant family)**.** *We say a boolean function family $\mathcal{C}$ over n bits is* flip-invariant *if for any string $s \in \{0,1\}^n$, $f \in \mathcal{C}$ implies $f(x \oplus s) \in \mathcal{C}$.*

Definition 4.12 (Seed-extending pseudorandom generator)**.** *A seed-extending pseudorandom generator is a generator G that outputs the seed as part of the pseudorandom string.*

Formally, a seed-extending (d, ϵ)-pseudorandom generator $G : \{0,1\}^d \to \{0,1\}^n$ for a class of functions f over n bits, is a seed-extending function, i.e., $G(s) = (s, E(s))$ for some function E, such that

$$|\Pr[f(G(U_d)) = 1] - \Pr[f(U_n) = 1]| \leq \epsilon.$$

5 From XOR Amplification to Extractors for Recognizable Sources

First we define XOR amplification for a boolean function class that contains functions with various input lengths. Recall that $f^{\oplus m}(x_1, \ldots, x_m) = \bigoplus_{i \in [m]} f(x_i)$.

Definition 5.1 (α-XOR amplification for a boolean function class)**.** *Let $\mathcal{C} \subseteq \{\{0,1\}^* \to \{0,1\}\}$ be a class of boolean functions. For a positive constant α, we say $\mathcal{C}$ has α-XOR amplification if there exists a function $h : \{0,1\}^t \to \{0,1\}$ such that for any positive integer k, $Cor(h^{\oplus k}, g) \leq 2^{-\alpha k}$, for any $g \in \mathcal{C}$.*

However, for constructing extractors for n-bit recognizable sources, we need to focus on the specific subset $\mathcal{C}_n \subseteq \mathcal{C}$ that contains all n-variate functions in $\mathcal{C}$. We define XOR amplification for $\mathcal{C}_n$ to also allow fixing some input bits.

Definition 5.2 ((α, w)-XOR amplification for functions with a fixed input length)**.** *For a set $\mathcal{C}_n$ of n-variate functions $C : \{0,1\}^n \to \{0,1\}$ and a positive constant α, we say $\mathcal{C}_n$ has (α, w)-XOR amplification for a function $h : \{0,1\}^t \to \{0,1\}$ if for any vector $v \in \{0,1\}^{\lfloor n/t \rfloor}$ with at least w ones, $Cor(h^v, \mathcal{C}_n) \leq 2^{-\alpha w}$, where we add dummy variables to the input of h^v if h^v has less than n input variables.*

Moreover, we say C_n has α-XOR amplification for h, if C_n has (α, w)-XOR amplification for h for each positive integer $w \leq \lfloor n/t \rfloor$.

Note that if $\mathcal{C}$ is closed under restrictions, the fact that $\mathcal{C}$ has α-XOR amplification implies that $\mathcal{C}_n$ has also α-XOR amplification for every positive integer n. Formally,

Lemma 5.3. *Let $\mathcal{C} \subseteq \{\{0,1\}^* \to \{0,1\}\}$ be a class of boolean functions closed under restrictions. Let $\mathcal{C}_n \subseteq \mathcal{C}$ denote the set of all n-variate functions in $\mathcal{C}$. If $\mathcal{C}$ has α-XOR amplification for a function $h : \{0,1\}^t \to \{0,1\}$, then $\mathcal{C}_n$ has also α-XOR amplification for h for every positive integer n.*

Proof. Assume that $\mathcal{C}$ has α-XOR amplification for a function $h : \{0,1\}^t \to \{0,1\}$, i.e., $Cor(h^{\oplus k}, \mathcal{C}) \leq 2^{-\alpha k}$ for each positive integer k. Then, we need to prove that for every positive integer n, $\mathcal{C}_n$ has also α-XOR amplification for h. In particular, fix n and let $l = \lfloor n/t \rfloor$. It suffices to prove that for any vector $v \in \{0,1\}^l$ with k ones, $Cor(h^v, \mathcal{C}_n) \leq Cor(h^{\oplus k}, \mathcal{C})$, as $Cor(h^{\oplus k}, \mathcal{C}) \leq 2^{-\alpha k}$.

To prove this, without loss of generality, assume that the first k coordinates of v are all 1's, and the remaining coordinates are all 0's. Thus, h^v depends only on the first kt variables. For any n-variate function $C(x_1, \ldots, x_n) \in \mathcal{C}_n$,

$$\begin{aligned}
Cor(h^v, C) &= E_{X \sim U_{kt}, Y \sim U_{n-kt}} e[h^v(X,Y) + C(X,Y)] \\
&= E_{Y \sim U_{n-kt}} \left[E_{X \sim U_{kt}} e[h^v(X,Y) + C(X,Y)] \right] \\
&\leq \frac{1}{2^{n-kt}} \sum_{Y_0 \in \{0,1\}^{n-kt}} Cor\left(h^{\oplus k}(X), C(X, Y_0)\right) \\
&\leq \frac{1}{2^{n-kt}} \sum_{Y_0 \in \{0,1\}^{n-kt}} Cor(h^{\oplus k}, \mathcal{C}) \\
&= Cor(h^{\oplus k}, \mathcal{C}).
\end{aligned}$$

The last inequality follows since $\mathcal{C}$ is closed under restrictions, i.e., $C(X, Y_0) \in \mathcal{C}$ for any $Y_0 \in \{0,1\}^{n-kt}$. □

Theorem 5.4. *Let $\mathcal{C}_n$ be a family of boolean functions over n bits containing the constant function $f(x) = 0$. Let M be the $l \times m$ generating matrix of an asymptotically good $[l, m, r_0]_2$ code, where $l = n/t$. Assume that $\mathcal{C}_n$ has (α, r)-XOR amplification for $h : \{0,1\}^t \to \{0,1\}$, where $r \leq r_0$. Then, the function* $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$,

$$\mathrm{Ext}(x) = h^{(l)}(x)M,$$

is an $(n - \Delta, 2^{m/2+\Delta-\alpha r})$ extractor for $\mathcal{C}_n$-recognizable sources.

Proof. For convenience, let $(g_1(x), \ldots, g_m(x)) = h^{(l)}(x)M$. To show that the output of Ext is $2^{m/2+\Delta-\alpha r}$-closed to the uniform, by the statistical XOR Lemma, it suffices to show that for any non-empty set $S \subseteq [m]$, $g_S = \sum_{i \in S} g_i$ is $2^{\Delta-\alpha r}$-biased conditioned on $f(x) = 1$ for any $f \in \mathcal{C}_n$ with $|f^{-1}(1)| \geq 2^{n-\Delta}$.

First we observe that the bias of g_S conditioned on $f(x) = 1$ can be bounded by the correlation between g_S and f plus the bias of g_S.

Lemma 5.5 (Lemma 3.2, restated)**.**

$$|\Pr[g_S(X) = 1 | f(X) = 1] - \Pr[g_S(X) = 0 | f(X) = 1]| \leq \frac{Cor(g_S, f) + bias(g_S)}{2 \Pr[f(X) = 1]}.$$

Proof. By multiplying $2 \Pr[f(X) = 1]$ on both sides, it is equivalent to prove that

$$2 \left|\Pr[g_S(X) = 1 \wedge f(X) = 1] - \Pr[g_S(X) = 0 \wedge f(X) = 1]\right| \leq Cor(g_S, f) + bias(g_S).$$

Notice that

$$\begin{aligned} Cor(g_S, f) &= |\Pr[g_S(X) = f(X)] - \Pr[g_S(X) \neq f(X)]| \\ &= |\Pr[g_S(X) = 1 \wedge f(X) = 1] + \Pr[g_S(X) = 0 \wedge f(X) = 0] \\ &\quad - \Pr[g_S(X) = 0 \wedge f(X) = 1] - \Pr[g_S(X) = 1 \wedge f(X) = 0]|, \end{aligned}$$

and

$$\begin{aligned} bias(g_S) &= |\Pr[g_S(X) = 1] - \Pr[g_S(X) = 0]| \\ &= |\Pr[g_S(X) = 1 \wedge f(X) = 1] + \Pr[g_S(X) = 1 \wedge f(X) = 0] \\ &\quad - \Pr[g_S(X) = 0 \wedge f(X) = 1] - \Pr[g_S(X) = 0 \wedge f(X) = 0]|. \end{aligned}$$

Thus, by the triangle inequality,

$$\begin{aligned} bias(g_S) + Cor(g_S, f) &\geq |2 \Pr[g_S(X) = 1 \wedge f(X) = 1] - 2 \Pr[g_S(X) = 0 \wedge f(X) = 1]| \\ &= 2 \left|\Pr[g_S(X) = 1 \wedge f(X) = 1] - \Pr[g_S(X) = 0 \wedge f(X) = 1]\right|. \end{aligned}$$

□

Then, observe that not only is each g_i a sum of at least r independent copies, but also so is any non-empty sum of the g_i, and hence has exponentially small correlation with degree-d polynomials.

Lemma 5.6. *For any nonempty set $S \subseteq [m]$, $Cor(g_S, \mathcal{C}_n) \leq 2^{-\alpha r}$.*

Proof. Note that

$$g_S(x) = \sum_{i \in S} M_i \cdot h^{(l)}(x) = \left(\sum_{i \in S} M_i \right) h^{(l)}(x),$$

where M_i denotes the i-th row of the matrix M. As M is the generating matrix of an $[l, m, r]_2$ code and S is non-empty, $\sum_{i \in S} M_i$ is a codeword and hence has at least r 1's. Thus, g_S is the XOR of at least r_0 independent copies of h. By the assumed (α, r)-XOR amplification, we know $Cor(g_S, \mathcal{C}_n) \leq 2^{-\alpha r}$. □

Since the constant function $0 \in \mathcal{C}_n$, we also have that $bias(g_S) = Cor(g_S, 0) \leq 2^{-\alpha r}$. Thus, by Lemma 5.5, the bias of g_S conditioned on $f(x) = 1$ is at most $2^{-\alpha r}/p$, where $p = \Pr[f(X) = 1]$.

At last, we have $p = \frac{|f^{-1}(1)|}{2^n} \geq 2^{-\Delta}$ by the min-entropy requirement that $|f^{-1}(1)| \geq 2^{n-\Delta}$. Therefore, $g_S(x)$ is $2^{\Delta - \alpha r}$-biased conditioned on $f(x) = 1$.

□

Combining with an explicit asymptotically good $[l, m, r]_2$ code, we prove the following theorem.

Theorem 5.7. *Let $\mathcal{C} \subseteq \{\{0,1\}^* \to \{0,1\}\}$ be any boolean function class closed under restrictions and α be any positive constant. Let $\mathcal{C}_n$ denote the set of all n-variate functions in $\mathcal{C}$. If $\mathcal{C}_n$ has $(\alpha, \delta n)$-XOR amplification for $h : \{0,1\}^t \to \{0,1\}$, where $\delta < 1/t$ is a positive constant, then there is an explicit $(n - c_1 \alpha l,\ 2^{-c_2 \alpha l})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{c_3 \alpha l}$ for $\mathcal{C}_n$-recognizable sources, where $l = n/t$ and c_1, c_2, c_3 are some positive constants.*

Moreover, if $\mathcal{C}$ has α-XOR amplification for a function $h : \{0,1\}^t \to \{0,1\}$, then for any positive integer n, there is an explicit seedless $(n - c_1 \alpha l,\ 2^{-c_2 \alpha l})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{c_3 \alpha l}$ for $\mathcal{C}_n$-recognizable sources, where $l = n/t$ and c_1, c_2, c_3 are some positive constants.

Proof. Note that if $\mathcal{C}$ has α-XOR amplification for a function h, then by Lemma 5.3, $\mathcal{C}_n$ also has α-XOR amplification for h for every positive integer n, i.e., $\mathcal{C}_n$ also has $(\alpha, \delta l)$-XOR amplification for h by definition. Now, we start with the assumption that $\mathcal{C}_n$ has $(\alpha, \delta l)$-XOR amplification for h. We use an explicit $[l, \delta_1 l, \delta_2 l]_2$ linear code for some constants $\delta_1 > 0$ and $\delta_2 > \delta$ by Justesen [Jus72]. Therefore, Theorem 5.4 yields an $(n - \Delta,\ 2^{m/2 + \Delta - \alpha \delta_2 l})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ for $\mathcal{C}_n$-recognizable sources. That is, by setting $\Delta = c_1 \alpha l$ and $m = c_3 \alpha l$ for some small positive constants c_1, c_3, we get the desired $(n - c_1 \alpha l,\ 2^{-c_2 \alpha l})$ extractor, where $c_2 = -(c_3/2 + c_1 - \delta_2) > 0$ is also a positive constant. □

5.1 Algebraic extractors over GF(2)

In this subsection, we will show that for any algebraic sources of constant degree over GF(2), there exists an efficient extractor that has linear output for linear min-entropy and exponentially small error. Formally, we will prove the following theorem:

Theorem 5.8. *For any positive integer d, there is an efficient $\left((1 - 1/c_d)n, d, 2^{-\Omega(n/c_d)}\right)$-algebraic extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$, where $c_d = \Theta(d^2 4^d)$, $m = \Omega(n/c_d)$.*

Let P_d denote the set of all polynomials of degree at most d over GF(2). Let $\mathcal{V}_d$ denote the set of all products of polynomials in P_d and $\mathcal{V}_{d,n}$ denote the set of all products of n-variate polynomials in P_d.

Notice that an algebraic source of degree d over n bits is also a $\mathcal{V}_{d,n}$-recognizable source.

Lemma 5.9. *An n-bit algebraic source of degree d iff it is a $\mathcal{V}_{d,n}$-recognizable source.*

Proof. Let U_V denote an arbitrary algebraic source, where $V = \{x \in \{0,1\}^n | p_i(x) = 0, p_i \in P_d, \forall i \in [k]\}$ is an algebraic set of degree d over n bits. Notice that V can be viewed as the set of 1-inputs of function $\prod_{i\in[k]}(p_i(x)+1)$. That is, the uniform distribution over V is also the source recognizable by $\prod_{i\in[k]}(p_i(x)+1) \in \mathcal{V}_{d,n}$. In other words, an algebraic source of degree d is a $\mathcal{V}_{d,n}$-recognizable source.

For the other direction, let U_f denote an arbitrary $\mathcal{V}_{d,n}$-recognizable source, where $f = \prod_{i\in[k]} p_i \in \mathcal{V}_{d,n}$ with $\deg(p_i) \le d$ for each $i \in [k]$. Note that $f^{-1}(1) = \{x \in \{0,1\}^n | p_i(x) = 1, \forall i \in [k]\} = \{x \in \{0,1\}^n | p_i(x) + 1 = 0, \forall i \in [k]\}$. Hence, $f^{-1}(1)$ is the algebraic set of $p_1(x)+1, \ldots, p_k(x)+1$. Since $\deg(p_i(x)+1) = \deg(p_i) \le d$ for each $i \in [k]$, $f^{-1}(1)$ is an algebraic set of degree d over n bits. Therefore, U_f is an n-bit algebraic source of degree d. □

Then, observe that $\mathcal{V}_d$ is closed under restrictions. Thus, by Theorem 5.4, to get an extractor for $\mathcal{V}_{d,n}$-recognizable sources, it is enough to show that $\mathcal{V}_d$ has α-XOR amplification for some positive constant α.

Note that to show that a function f has low correlations with $\mathcal{V}_d$, it suffices to show that f has low correlation with any polynomial of degree at most d. Recall that the correlation between a function f and a class $\mathcal{C}$ of functions is defined as the maximum of $Cor(f, C)$ over all $C \in \mathcal{C}$ whose input length is the same as f. In particular, to show that a function $f : \{0,1\}^t \to \{0,1\}$ has low correlations with $\mathcal{V}_d$, it suffices to show that f has low correlation with any t-variate polynomial of degree at most d.

Lemma 5.10. *If a function $f : \{0,1\}^t \to \{0,1\}$ is ϵ-correlated with any polynomial of degree at most d in t variables, then f is at most 2ϵ-correlated with any product of polynomials of degree at most d in t variables.*

The lemma follows because the L1 norm of the Fourier transform of the AND function is at most 2.

Proof. We need to show that if for any t-variate $p \in P_d$ $Cor(f,p) = |Ee[f+p]| \le \epsilon$, then for any product $\prod_{i\in[k]}(p_i+1) \in \mathcal{V}_{d,t}$ where $p_1+1, \ldots, p_k+1 \in P_{d,t}$, we have

$$Cor\left(f, \prod_{i\in[k]}(p_i(X)+1)\right) = \left|Ee\left[f + \prod_{i\in[k]}(p_i(X)+1)\right]\right| \le 2\epsilon.$$

Consider the Fourier expansion of the function

$$e\left[\prod_{i\in[k]}(y_i+1)\right] = -\sum_{S\neq\emptyset} \frac{e\left[\sum_{i\in S} y_i\right]}{2^{k-1}} + (1 - 1/2^{k-1}).$$

Now, substituting each y_i by p_i, we have $e\left[\prod_{i\in[k]}(p_i+1)\right] = -\sum_{S\neq\emptyset}\frac{e\left[\sum_{i\in S}p_i\right]}{2^{k-1}}+(1-1/2^{k-1})$.

That is,

$$\left|Ee\left[f+\prod_{i\in[k]}(p_i(X)+1)\right]\right| \leq \sum_{S\neq\emptyset}\frac{\left|Ee\left[f+\sum_{i\in S}p_i(X)\right]\right|}{2^{k-1}}.$$

Notice that for each $S\neq\emptyset$, the sum $\sum_{j\in S}p_i$ is also a polynomial of degree at most d. For the polynomial of degree at most d, $\sum_{j\in S}p_i$, we have that $\left|Ee\left[f+\sum_{j\in S}p_i(X)\right]\right| \leq \epsilon$. In other words, $\left|Ee\left[f+\prod_{i\in[k]}(p_i(X)+1)\right]\right| \leq 2^k\frac{2\epsilon}{2^{k-1}} = 2\epsilon$.

□

Moreover, Viola and Wigderson [VW08] proved XOR amplification for GF(2) polynomials, which implies XOR amplification for $\mathcal{V}_d$ by Lemma 5.10.

Theorem 5.11. *[VW08, Theorem 1.1] Let $h:\{0,1\}^n\to\{0,1\}$ be a function such that $Cor(h,P_{d,n})\leq 1-1/2^d$. Then $Cor(h^{\oplus m},P_d)\leq 2^{-\Omega(m/(4^d\cdot d))}$.*

Finally, by brute force search, it is easy to find a function h over $O(d)$ bits such that $Cor(h,P_d)\leq 1-1/2^d$ as d is a constant. That is, P_d has $\Omega(\frac{1}{4^d\cdot d})$-XOR amplification for the function $h:\{0,1\}^{O(d)}\to\{0,1\}$. This implies that V_d has $\Omega(\frac{1}{4^d\cdot d})$ -XOR amplification for the function $h:\{0,1\}^{O(d)}\to\{0,1\}$ by Lemma 5.10. Therefore, Theorem 5.7 yields our main theorem of this subsection, i.e., constructing an efficient $\left((1-1/c_d)n,d,2^{-\Omega(n/c_d)}\right)$-algebraic extractor $\mathrm{Ext}:\{0,1\}^n\to\{0,1\}^m$, where $c_d=\Theta(d^2 4^d)$, $m=\Omega(n/c_d)$.

We remark that an explicit example of h is the mod_3 function, which outputs 1 if and only if the number of input bits that are 1 is congruent to 1 modulo 3. Smolensky [Smo87] proved that the mod_3 function over $O(d^2)$ bits is 2/3-hard for P_d (see Viola [Vio09] for a proof), that is, P_d has $\Omega(\frac{1}{4^d\cdot d})$-XOR amplification for the function $\mathrm{mod}_3:\{0,1\}^{O(d^2)}\to\{0,1\}$. Using the mod_3 function, Theorem 5.7 yields an efficient $\left((1-1/c'_d)n,d,2^{-\Omega(n/c'_d)}\right)$-algebraic extractor $\mathrm{Ext}:\{0,1\}^n\to\{0,1\}^m$, where $c'_d=\Theta(d^3 4^d)$, $m=\Omega(n/c'_d)$.

5.2 Sources recognizable by communication protocols

In this subsection, we construct an extractor for sources recognizable by randomized t-party protocols. Formally, we prove the following theorem.

Theorem 5.12. *There exists an explicit seedless $((1-1/c_t)n,\ 2^{-c_1 n/c_t})$ extractor $\mathrm{Ext}:\left(\{0,1\}^{n/t}\right)^t\to\{0,1\}^{c_2 n/c_t}$ for sources recognizable by randomized t-party communication protocols of at most $c_3 n/c_t$ bits, where $c_t=\Theta(t4^t)$ and c_1,c_2,c_3 are some positive constants.*

Let $\mathcal{RCC}_{n,t,w}$ denote the class of n-variate randomized t-party protocols using at most w communication bits. Now, to construct extractors for $\mathcal{RCC}_{n,t,w}$-recognizable sources with exponentially small error, by Theorem 5.4, it suffices to show $\mathcal{RCC}_{n,t,w}$ has $(\alpha,r)-$XOR amplification for some function h, where $r=\Omega(n)$ is the distance of some good linear code.

Notice that, Babai, Nisan, and Szegedy [BNS92] proved a lower bound for randomized t-party protocols for the Generalized Inner Product (GIP) function, which is the XOR of

AND functions. Formally, let $\wedge_t : \{0,1\}^t \to \{0,1\}$ denote the AND function on t variables. Then, the GIP function $\mathrm{GIP}_{kt} : (\{0,1\}^t)^k \to \{0,1\}$ is defined as the function$\wedge_t^{\oplus k}$, i.e., $GIP_{kt}(x_1, \ldots, x_k) := \bigoplus_{i=1}^k \wedge_t(x_i)$. Moreover, let $R_{t,\epsilon}(f)$ denote the complexity of the best randomized t-party protocol correlating f with at least ϵ.

Theorem 5.13 ([BNS92, Theorem 2])**.**

$$R_{t,\epsilon}(GIP_n) = \Omega\left(\frac{n}{4^t} - \log(1/\epsilon)\right).$$

Now, for any constant $0 < \delta < 1/t$ and some constant $c_t = \Theta(t4^t)$, we prove that $\mathcal{RCC}_{n,t,O(n/4^t)}$ has $(\Omega(1/c_t), \delta n)-$XOR amplification for $\wedge_t$, which directly yields Theorem 5.12 by Theorem 5.7.

Proposition 5.14. *For any constant $0 < \delta < 1/t$, $\mathcal{RCC}_{n,t,c'n/4^t}$ has $(c/c_t, \delta n)-$XOR amplification for $\wedge_t$, where $c_t = \Theta(t4^t), c, c' > 0$ are constants.*

Proof. Assume by contradiction that $\mathcal{RCC}_{n,t,c'n/4^t}$ does not have $(c/c_t, \delta n)-$XOR amplification for $\wedge_t$, where c, c' are some constants to be decided later. That is, there exists some vector $v \in \{0,1\}^{n/t}$ with at least δn ones, $Cor(h^v, \mathcal{RCC}_{n,t,c'n/4^t}) \le 2^{-\frac{c}{c_t}\delta n}$, That is, there exists a $(c'n/4^t)$-bit randomized protocol that approximates h^v within $2^{-\frac{c}{c_t}\delta n}$ error. Furthermore, observe that h^v is the XOR of at least δn copies of $\wedge_t$, i.e, h^v depends on $\ge \delta nt$ variables. Therefore, by Theorem 5.13, we have

$$R_{t,2^{-\frac{c}{c_t}\delta n}}(h^v) \ge R_{t,2^{-\frac{c}{c_t}\delta n}}(GIP_{\delta n}) = \Omega\left(\delta n/4^t - \frac{c}{c_t}\delta nt\right).$$

That is, letting the constant c be small enough, we know there exists a positive constant c'' such that

$$R_{t,2^{-\alpha\delta n}}(h^v) \ge c''n/4^t.$$

Now letting $c' < c''$ yields a contraction. Therefore, $\mathcal{RCC}_{n,t,c'n/4^t}$ has $(c/c_t, \delta n)-$XOR amplification for $\wedge_t$. □

5.3 Halfspace sources

In this subsection, for halfspace sources, we construct an efficient extractor that has linear output for linear min-entropy and exponentially small error. Formally, we will prove the following theorem.

Theorem 5.15. *There exists an explicit seedless $((1-c_1)n, 2^{-c_2 n})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{c_3 n}$ for halfspace sources, where c_1, c_2, c_3 are some positive small enough constants.*

Note that Nisan already proved an exponentially small correlation bound for Inner Product function against LTFs. Formally, let $IP_n : (\{0,1\}^2)^{n/2} \to \{0,1\}$ denote the inner product function over n variables, i.e., $IP_n(x_1, \ldots, x_{n/2}) = \bigoplus_{i \in [n/2]} \wedge_2(x_i)$. Then, we have the following lemma.

Lemma 5.16. *For any LTF f on n variables, we have*

$$Cor(IP_n, f) \leq 2^{-\Omega(n)}.$$

Proof of sketch. Nisan proved that a LTF on n variables can be approximated within ϵ error by a randomized 2-party protocol of complexity $O(\log(n/\epsilon))$ by [Nis93, Theorem 1]. Moreover, by Chor and Goldreich [CG88], we know at least $n/2-\log(1/\epsilon)$ complexity needed for randomized 2-party protocol computing the function IP_n.

Therefore, for any LTF f over n variables, there is a protocol $\mathcal{P}$ of complexity cn bits approximating f within $2^{-\Omega(n)}$ error and $Cor(IP_n, \mathcal{P}) \leq 2^{-\Omega(n)}$. That is, replacing f by IP_n in $Cor(IP_n, f)$, we can bound $Cor(IP_n, f) \leq 2^{-\Omega(n)} + Cor(IP_n, \mathcal{P}) = 2^{-\Omega(n)}$. □

Let $\mathcal{LTF}_n$ denote the class of LTFs over n variables. Then, the above lemma directly yields that $\mathcal{LTF}_n$ has $(\alpha, \delta n)$-XOR amplification for $\wedge_2$ for any positive constant $\delta < 1/2$, where α is some positive constant. Hence Theorem 5.15 directly follows by Theorem 5.7.

6 From Seed-Extending PRGs to Extractors for Recognizable Sources

Note that Kinne et al. [KvMS12] already showed reductions between extractors for recognizable sources and seed-extending PRGs.

Lemma 6.1 ([KvMS12, Theorem 7])**.** *Let $C : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ be a function. Let $\Delta = m + \log(1/\epsilon)$ and let $E : \{0,1\}^n \to \{0,1\}^m$ be an $(n - \Delta, 2^{-\Delta})$-extractor for $\mathcal{C}$-recognizable distributions, where each function in $\mathcal{C}$ is of the form $f_r(x) = C(x, r)$ where $r \in \{0,1\}^m$ is an arbitrary string. Then, $G(x) = (x, E(x))$ is ϵ-pseudorandom for $\mathcal{C}$.*

Lemma 6.2 ([KvMS12, Theorem 8])**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a function and let $E : \{0,1\}^n \to \{0,1\}^m$ be a function such that $G(x) = (x, E(x))$ is ϵ-pseudorandom for tests $T(x, r)$ of the form $T_z(x, r) = f(x) \wedge (r = z)$ where $z \in \{0,1\}^m$ is an arbitrary string. For any $\Delta > 0$, if $\epsilon \leq 2^{-(m+2\Delta)}$ then E is an $(n-\Delta, 2^{-\Delta})$-extractor for the distribution recognized by f.*

The Lemma 3.2 requires a tiny $\epsilon \leq 2^{-(m+2\Delta)}$ for the seed-extending PRG to get an $(n - \Delta, 2^{-\Delta})$-extractor. In the following, we improve the reduction from seed-extending PRGs to extractors to require only $\epsilon \leq 2^{-2\Delta}$. Moreover, our extractor is even stronger – the output of our extractor is close to uniform with relative error, which will be defined as follows.

Definition 6.3 (Statistical distance with relative error)**.** *We say that a distribution Z on $\{0,1\}^m$ is ϵ-close to uniform with relative error if for every event $A \subseteq \{0,1\}^m$,*

$$|\Pr[Z \in A] - \mu(A)| \leq \epsilon \cdot \mu(A), \text{ where } \mu(A) = |A|/2^m.$$

Note that if Z is ϵ-close to uniform with relative error, then it is also ϵ-close to uniform. Next we define extractors with relative error analogously.

Definition 6.4 (Seedless extractor with relative error, [AASY16, Definition 1.19])**.** *Let $\mathcal{C}$ be a class of distributions over $\{0,1\}^n$. A function $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ is a (k,ϵ)-relative-error extractor for $\mathcal{C}$ if for every distribution X in the class $\mathcal{C}$ such that $H_\infty(X) \geq k$, $\mathrm{Ext}(X)$ is ϵ-close to uniform with relative error.*

We remark that the notions of statistical distance and extractors with relative error were introduced by Applebaum, Artemenko, Shaltiel, and Yang [AASY16]. They translate relative-error extractors for distributions recognizable by small circuits into incompressible functions. However, parameters of our relative-error extractors are not strong enough to get incompressible functions.

Now we prove the reduction lemma from seed-extending PRGs to seedless extractors with relative error, which directly implies the reduction from seed-extending PRGs to seedless extractors.

Lemma 6.5. *Let $\mathcal{C}$ be a flip-invariant family of boolean functions over n bits. If G is a seed-extending (d,ϵ)-pseudorandom generator $G : \{0,1\}^d \to \{0,1\}^n$, then we can construct an $(n-\Delta, 2^\Delta\epsilon)$-relative-error extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-d}$ as follows. If $G(x) = (x, E(x))$ fools any function in $\mathcal{C}$, then $\mathrm{Ext}(x \circ y) = y \oplus E(x)$ is an extractor for $\mathcal{C}$-recognizable sources, where $x \in \{0,1\}^d, y \in \{0,1\}^{n-d}$.*

For intuition, observe that a seedless extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ partitions $\{0,1\}^m$ as $\bigcup_{z\in\{0,1\}^m} \mathrm{Ext}^{-1}(z)$. If Ext is a (k,ϵ)-relative-error extractor for $\mathcal{C}$-recognizable sources, then for every $f \in \mathcal{C}$ with $|f^{-1}(1)| \geq 2^k$, all intersections $\mathrm{Ext}^{-1}(z) \cap f^{-1}(1)$ should have almost the same size. That is, for most m-bit strings z, the preimage $\mathrm{Ext}^{-1}(z)$ is an ϵ-pseudorandom set against any $f \in \mathcal{C}$ with $|f^{-1}(1)| \geq 2^k$.

Now, given PRGs, how to construct extractors? From the above observation, converting an ϵ-pseudorandom set into a partition of ϵ-pseudorandom sets is a possible way. If each preimage $\mathrm{Ext}^{-1}(z)$ of Ext is an ϵ-pseudorandom set for $\mathcal{C}$, Ext should be a relative-error extractor for $\mathcal{C}$-recognizable sources with a bit worse parameters, which will be precisely calculated in the following formal proof.

To make $\mathrm{Ext}^{-1}(z)$ an ϵ-pseudorandom set for each z, we need a PRG of the specific form: $G(x) = B(x) \circ E(x)$, for some bijection $B : \{0,1\}^d \to \{0,1\}^d$ and some function $E : \{0,1\}^d \to \{0,1\}^{n-d}$. By linearly shifting the set $\{(B(x), E(x))\}$, we can partition $\{0,1\}^n$ as $\bigcup_{z\in\{0,1\}^{n-d}} \{(B(x), (E(x) \oplus z)) : x \in \{0,1\}^d\}$. Since $\mathcal{C}$ is a flip-invariant function family, we have that the set $\mathrm{Ext}^{-1}(z) = \{(B(x), (E(x) \oplus z)) : x \in \{0,1\}^d\}$ fools any function f in $\mathcal{C}$.

Note that to convert the PRG of the form $(B(x), E(x))$ into an extractor, the above intuition gives $\mathrm{Ext}(x) = E(B^{-1}(x))$. Thus, to get an efficient extractor, we have to assume that $E(B^{-1}(x))$ can be efficiently computed. That is, the PRG of the form $(B(x), E(x))$ also gives an efficient seed-extending PRG $(x, E(B^{-1}(x)))$. Therefore, for constructing extractors from the above intuition, we only need to focus on the seed-extending PRGs.

Proof. For convenience, let $m = n - d$ denote the output length of Ext.

First, we observe that, for any fixed z, $G_z(x) = (x, (E(x) \oplus z))$ fools any function $f(x, y)$ in $\mathcal{C}$. Notice that to prove $G_z(x)$ fools $f(x, y)$, it is equivalent to prove $(x, E(x))$ fools $f(x, y \oplus z)$. Because of the flip-invariant property of $\mathcal{C}$, we know if $f(x, y) \in C$, then $f(x, y \oplus z) \in \mathcal{C}$. So $G(x) = x \circ E(x)$ fools $f(x, y \oplus z)$. That is, $G_z(x)$ fools the function $f(x, y)$.

Note that $\mathrm{Ext}^{-1}(z)$ is the range of G_z. Then, we can get

$$\begin{aligned}
\Pr[\mathrm{Ext}(X \circ Y) = z | f(X \circ Y) = 1] &= \frac{\Pr[\mathrm{Ext}(X \circ Y) = z \wedge f(X \circ Y) = 1]}{\Pr[f(X \circ Y) = 1]} \\
&= \frac{\Pr[\mathrm{Ext}(X \circ Y) = z]}{\Pr[f(X \circ Y) = 1]} \Pr[f(X \circ Y) = 1 | \, \mathrm{Ext}(X \circ Y) = z] \\
&= \frac{\Pr[\mathrm{Ext}(X \circ Y) = z]}{\Pr[f(X \circ Y) = 1]} \Pr[f(G_z(X)) = 1] \\
&= \frac{\Pr[\mathrm{Ext}(X \circ Y) = z]}{\Pr[f(X \circ Y) = 1]} (\Pr[f(X \circ Y) = 1] \pm \epsilon) \\
&= \frac{p \pm \epsilon}{p} \Pr[\mathrm{Ext}(X \circ Y) = z], \text{ where } p = \Pr[f(X \circ Y) = 1], \\
&= \frac{p \pm \epsilon}{p} \frac{1}{2^m}.
\end{aligned}$$

For any nonempty subset $S \subseteq \{0,1\}^m$, summing over all $z \in S$, we deduce that the output of Ext is $\frac{\epsilon}{p}\mu(S)$-close to the uniform distribution over S. Furthermore, we have $\frac{\epsilon}{p} \leq 2^{\Delta}\epsilon$, since $p = \frac{|f^{-1}(1)|}{2^n} \geq 2^{-\Delta}$ by the min-entropy requirement that $|f^{-1}(1)| \geq 2^{n-\Delta}$. Therefore, $\mathrm{Ext}(x \circ y) = y \oplus E(x)$ is an $(n - \Delta, 2^{\Delta}\epsilon)$-relative-error extractor for $\mathcal{C}$-recognizable sources. □

6.1 Applications

In this section, we construct extractors for sources recognized by several widely used function families. These constructions are all based on Lemma 6.5 proved in the previous section, which means we can convert seed-extending PRGs into extractors. In the following subsections, the main points are to construct seed-extending PRGs for some specific common function families.

6.1.1 Circuit-recognizable sources

Recall that we say a function $h : \{0,1\}^t \to \{0,1\}$ is ϵ-hard for $\mathcal{C}$ if $Cor(h, \mathcal{C}) \leq \epsilon$.

For any circuit family, Nisan and Wigderson [NW88] already constructed a hardness-based PRG. Reviewing the NW generator, Kinne et al. [KvMS12] proved that it could be made seed-extending, and hence they gave a seed-extending PRG for circuits. In particular, they proved the following lemma.

Lemma 6.6. *[KvMS12, Lemma 2.9] Let l and m be positive integers and $H : \{0,1\}^{\sqrt{l}/2} \to \{0,1\}$ a function. If H is $\frac{\epsilon}{m}$-hard at input length $\sqrt{l}/2$ for circuits of size $s + m \cdot 2^{O(\log m / \log l)}$ and depth $d + 1$, then there is a seed-extending (l, ϵ)-PRG $NW_{H;l,m} : \{0,1\}^l \to \{0,1\}^{l+m}$ for tests $T : \{0,1\}^{l+m} \to \{0,1\}$ computable by circuits of size s and depth d.*

Notice that the set of bounded-size circuits is flip-invariant since flipping the inputs of a circuit does not change its size. Thus, applying Lemma 6.5, we get an extractor.

Proposition 6.7. *For any positive integer $l < n$, if there is a function H that is ϵ-hard at input length $\sqrt{l}/2$ for circuits of size $s + (n-l) \cdot 2^{O(\log(n-l)/\log l)}$ and depth $d+1$, then for any $\Delta = \Delta(n) > 0$ we can get an $(n - \Delta, (n-l)2^{\Delta}\epsilon)$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-l}$ for any sources recognizable by circuits of size s and depth d.*

We remark that, in the best case, the above lemma yields an $(n - \tilde{O}(\sqrt{l}), 2^{-\tilde{\Omega}(\sqrt{l})})$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-l}$, if we can get a function at input length $\sqrt{l}/2$ which is $2^{-\tilde{\Omega}(\sqrt{l})}$-hard for circuits of polynomial size.

6.1.2 AC^0-recognizable sources

Hastad [Hås87] proved that the parity function is $2^{-n^{1/(d+1)}}$-hard against any AC^0 circuit of size $2^{n^{1/(d+1)}}$ and depth d. Based on this hardness, Shaltiel [Sha11] constructed extractors for AC^0-recognizable sources.

Theorem 6.8 (Corollary 4.25, [Sha11])**.** *For any $\Delta = \Delta(n) > 0$, there is a constant $\alpha > 0$ such that for every sufficiently large n, $m \leq n^{1/(\alpha d)}$, and sources recognizable by circuits of size $2^{n^{1/(\alpha d)}}$ and depth d, we can construct an $(n - n^{1/(\alpha d)}, 2^{-100m})$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$.*

Theorem 6.9 (Theorem 4.21, [Sha11])**.** *For any constants $c, d, e > 1$ there is a constant $d > 1$ and a uniform family $E = \{E_n\}$ of circuits of polynomial-size and depth d such that $E_n : \{0,1\}^n \to \{0,1\}^m$ for $m(n) = (\log n)^e$ and E_n is a $(n - 100m(n), 2^{-100m(n)})$-extractor for sources recognizable by circuits of size n^c and depth d.*

However, directly using the Lemma 6.7 with the hardness of parity function, we can get the following lemma.

Theorem 6.10. *For any $\Delta = \Delta(n) > 0$, there exists a polynomial time computable $(n - \Delta, (n-l)2^{\Delta - \Omega\left(l^{1/(2d+2)}\right)})$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-l}$ for any sources recognizable by circuits of size $2^{n^{1/d}}$ and depth d.*

Proposition 6.11. *For any constants $c, d, e > 1$ there is a constant $e' < e$ and a polynomial-time computable uniform family $E = \{E_n\}$ such that $E_n : \{0,1\}^n \to \{0,1\}^m$ for $m(n) = n - (\log n)^e$ and E_n is a $(n - 100(\log n)^{e'}, 2^{-100(\log n)^{e'}})$-extractor for sources recognizable by circuits of size n^c and depth d.*

In particular, for min-entropy $n - n^{1/(\alpha d)}$, our extractor outputs $n - n^{2/\alpha + O(1/d)}$ bits, whereas Shaltiel's extractor outputs only $n^{1/(\alpha d)}$ bits. When $\alpha > 2d/(d-1)$ is a large enough constant, our extractor outputs $n - o(n)$ bits whereas Shaltiel's extractor outputs only $n^{1/(\alpha d)}$ bits. For min-entropy $n - \mathrm{polylog}(n)$ bits, our extractor outputs $n - \mathrm{polylog}(n)$, whereas Shaltiel's extractor outputs only $\mathrm{polylog}(n)$ bits

For circuit sources, Viola [Vio14] also constructed extractors for AC^0-samplable sources, extracting $k(k/n^{1+\gamma})^{O(1)}$ bits with super-polynomially small error from n-bit sources of min-entropy k, for any $\gamma > 0$. Nevertheless, AC^0-samplable sources are different from AC^0-recognizable sources.

6.1.3 Sources recognizable by deMorgan formulas of size $n^{3/2-o(1)}$

A deMorgan formula F is a Boolean formula with AND, OR and NOT gates with fan in at most 2. Notice that a deMorgan formula is also a circuit where each gate has fan-out at most 1. Therefore, to construct extractors for formula-recognizable sources, we can follow the same route as constructing extractors for AC^0-recognizable sources.

Now, our starting point becomes a hardness result for bounded-size formulas, proved by Komargodski, Raz and Tal [KRT17]. In particular, they constructed an explicit function $h : \{0,1\}^n \to \{0,1\}$ that is $2^{-\Omega(r)}$-hard for any deMorgan formula of size $n^{3-o(1)}/r^2$.

Next, we consider the following hardness-based seed-extending PRG for formulas.

Lemma 6.12. *Let l and m be positive integers and $H : \{0,1\}^{\sqrt{l}/2} \to \{0,1\}$ a function. If H is $\frac{\epsilon}{m}$-hard at input length $\sqrt{l}/2$ for formulas of size $s + m \cdot 2^{O(\log m/\log l)}$, then there is a seed-extending (l,ϵ)-PRG $NW_{H;l,m} : \{0,1\}^l \to \{0,1\}^{l+m}$ for tests $T : \{0,1\}^{l+m} \to \{0,1\}$ computable by formulas of size s.*

Proof (Sketch). The proof of this lemma is almost the same as the proof of Lemma 2.9 by Kinne, Melkebeek, and Shaltiel [KvMS12]. Their proof goes by contradiction: assume a distinguisher T computable by a circuit of size s that distinguishes the output of $NW_{H;l,m}$ with at least ϵ probability. There are two main steps in their proof. First, they use a standard reduction from the distinguisher T to a next-bit predictor $\tilde{T}$ as in [NW88]. Second, based on the predictor $\tilde{T}$, they construct a circuit C of size not much larger than T but computing the given hard function H well on average. The construction of C concludes a contradiction with the assumed hardness of H. In the following, we briefly describe these two steps and explain why similar operations also hold if we take formulas instead.

For transforming from the distinguisher T to a next-bit predictor $\tilde{T}$, they mainly use a hybrid argument together with an average argument on the $(n+m)$-bit output of $NW_{H;l,m}$. As a result, they show that there must exist a position $i > n$ and a fixing of last $n+m-i+1$ bits such that after this fixing either T or $\neg T$ predicts the i-th bit well, when given the first $i-1$ bits. They let $\tilde{T}$ be this circuit, or the next-bit predictor. We remark that this transformation holds for formulas: if the distinguisher T is assumed as a formula instead, then all these arguments still hold and the predictor $\tilde{T}$ will become a formula.

For building a circuit C computing H from $\tilde{T}$, they start with fixing all variables in $\tilde{T}$ that are independent of the i-th output bit of $NW_{H;l,m}$. By an average argument, this can be done with the prediction probability of $\tilde{T}$ preserved. Furthermore, the construction of $NW_{H;l,m}$ guarantees that the function computing the i-th output bit is precisely H, and for each $j \in [i-1]$ the function computing j-th bit depends on only few unfixed variables, which hence can be computed by a very small CNF or DNF. Therefore, after plugging either a CNF or DNF into $\tilde{T}$ for each of the first $i-1$ bits, they can get a circuit C computing the i-th output bit, i.e., H. Moreover, the increased size of C from $\tilde{T}$ is only due to these at most m very small CNFs or DNFs, and hence cannot be large. Notice that if $\tilde{T}$ is a formula, then C will become a formula after plugging CNFs or DNFs, and the increased size will be the same as for circuits. Therefore, this step also holds if we take formulas instead. □

Then, as the set of bounded-size deMorgan formulas is flip-invariant, we can get an extractor by applying Lemma 6.5.

Proposition 6.13. *For any positive integer $l < n$, if there is a function H that is ϵ-hard at input length $\sqrt{l}/2$ for formulas of size $s+(n-l)\cdot 2^{O(\log(n-l)/\log l)}$, then for any $\Delta = \Delta(n) > 0$ we can construct an $(n-\Delta, (n-l)2^{\Delta}\epsilon)$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-l}$ for any sources recognizable by formulas of size s.*

Finally, combining with the $2^{-\Omega(r)}$-hardness result [KRT17] against deMorgan formulas of size $n^{3-o(1)}/r^2$, Proposition 6.13 yields the following theorem by setting $l = \Omega(n)$.

Theorem 6.14. *For any $\Delta, r, \alpha > 0$ and $m \leq (1-\alpha)n$, there exists a polynomial time computable $(n-\Delta, m2^{\Delta-\Omega(r)})$-extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ for any sources recognizable by deMorgan formulas of size $n^{3/2-o(1)}/r^2$.*

6.1.4 Sources recognizable by efficient randomized algorithms

In this subsection we mainly talk about sources recognizable by probabilistic polynomial time algorithms, or BPP algorithms. First we define extractors for recognizable sources in the asymptotic setting.

Definition 6.15 (Extractors for sources recognizable by randomized algorithms)**.** *For a function t, let $\mathcal{C} \subseteq \mathrm{BPTIME}(t)$. We say that a deterministic algorithm $\mathrm{Ext} = \{\mathrm{Ext}_n : \{0,1\}^n \to \{0,1\}^{m(n)}\}_{n\geq 0}$ is a $(k(\cdot), \epsilon(\cdot))$-extractor for distributions recognizable by $\mathcal{C}$ if for every language $L \in \mathcal{C}$ such that $S_n = \{x \in L : |x| = n\}$ is of size at least $2^{k(n)}$ for all large enough n, then $\mathrm{Ext}(U_{S_m})$ is $\epsilon(m)$-close to the uniform distribution for all large enough m.*

To construct an extractor for sources recognizable by efficient randomized algorithms, think of t as a polynomial. Note that when the output length $m = 1$, an extractor for sources recognizable by BPP algorithms is simply a function that cannot be computed by any BPP algorithm on at most $(1/2+\epsilon)$ fraction of inputs. Therefore, such an extractor is not polynomial-time-computable.

To construct the above extractor, we use a widely-used cryptographic primitive – a family of one-way permutations.

Definition 6.16 (One-way permutation)**.** *For any functions $t(\cdot)$ and $\epsilon(\cdot)$, a one-way permutation with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded inverters is a polynomial-time-computable permutation $f : \{0,1\}^* \to \{0,1\}^*$ such that for any randomized algorithm A with running time bounded by $t(n)$ and all large enough n,*

$$\Pr_{x \leftarrow U_n}[A(f(x)) = x] \leq \epsilon(n).$$

The running time of our extractor is polynomially related to the time for inverting the one-way permutations. Therefore, our ideal one-way permutation is invertible in the worst case in time just slightly larger than $t(n)$. For example, think of $t(n) = n^{\sqrt{\log n}}$, $\epsilon = n^{-\sqrt{\log n}}$, and f invertible in the worst case in time $n^{O(\log n)}$. One can also scale down harder functions.

Lemma 6.17. *For any functions $T(\cdot)$, $\epsilon(\cdot)$ and $t(\cdot)$, assume that there exists a one-way permutation invertible in time $T(n)$ with error $\epsilon(n)$ against $t(n)$-bounded inverters. Then for any $m = m(n)$, we can construct a one-way permutation invertible in time $T(m) + O(n)$ with error $\epsilon(m)$ against $t(m)$-bounded inverters.*

Proof. Let $f : \{0,1\}^* \to \{0,1\}^*$ be the assumed permutation invertible in time $T(n)$, and for any algorithm A with running time bounded by $t(n)$ and all large enough n,

$$\Pr_{x \leftarrow U_n}[A(f(x)) = x] \leq \epsilon(n).$$

Let $m = m(n)$ be given. Then consider the permutation $p : \{0,1\}^* \to \{0,1\}^*$ defined by

$$p(x, y) = f(x) \circ y, \text{ where } x \in \{0,1\}^m, \text{ and } y \in \{0,1\}^{n-m}.$$

Clearly, since f is efficiently computable and invertible in time $T(n)$, p is also efficiently computable and invertible in time $T(m) + O(n)$.

Finally, we prove that p has error $\epsilon(m)$ against $t(m)$-bounded inverters, i.e., for any algorithm A that runs in time $t(m)$,

$$\Pr_{z \leftarrow U_n}[A(p(z)) = z] \leq \epsilon(m).$$

Otherwise, assume that there exists an algorithm A^* running in time $t(m)$ inverting $p(z)$ with probability more than $\epsilon(m)$. Then A^* yields an algorithm B running in $t(n)$ inverting $f(x)$ with probability more than $\epsilon(n)$, which contradicts the hardness assumption of f.

In particular, given $f(\cdot)$ and an m-bit input x, B runs A^* to invert $p(x \circ y) = f(x) \circ y$ for uniform random $y \in \{0,1\}^{n-m}$, and outputs the first m bits of the output of A^*. Note that if A^* inverts $f(x) \circ y$ correctly, then B inverts $f(x)$ correctly. Due to the assumption that A^* inverts $f(x) \circ y$ with probability more than $\epsilon(m)$, B also inverts $f(x)$ with probability more than $\epsilon(m)$.

□

In the following corollary, think of $a = \delta = 1$, $b = c = 1/2$, and $\alpha = 3$.

Corollary 6.18. *For any constants $a, b, c, \delta > 0$, assume that there exists a one-way permutation invertible in time $O\left(2^{n^a}\right)$ with error 2^{-n^c} against $2^{\delta n^b}$-bounded inverters. Then for any constant $\alpha \geq 1/a$, we can construct a one-way permutation invertible in time $O\left(2^{\log^{a\alpha}(n)}\right)$ with error $2^{-\log^{c\alpha}(n)}$ against $2^{\delta \log^{b\alpha}(n)}$-bounded inverters.*

Proof. Apply Lemma 6.17 with $m = \log^{\alpha}(n)$. □

Next, we define PRGs in the asymptotic setting, which are usually called cryptographic PRGs.

Definition 6.19 (Cryptographic Pseudorandom Generator)**.** *A family of pseudorandom generators with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded distinguishers is an efficiently evaluable family of functions $G : \{0,1\}^l \to \{0,1\}^{p(l)}$ such that for any algorithm A with running time bounded by $t(l)$ and for all large enough l,*

$$|\Pr[A(G(U_l)) = 1] - \Pr[A(U_{p(l)}) = 1]| \leq \epsilon(l).$$

Notice that there are no efficient seed-extending cryptographic PRGs. Otherwise, with revealed seeds, it is easy to efficiently distinguish the output of an efficient seed-extending PRG, $G(x) = (x, E(x))$, from a random string (x, y), by checking whether y equals $E(x)$.

However, assuming one-way permutations, the key observation is that there are constructions of inefficient seed-extending cryptographic PRGs. Formally, we define inefficient seed-extending cryptographic PRGs as cryptographically secure functions.

Definition 6.20 (Cryptographically secure functions)**.** *A cryptographically secure function $f : \{0,1\}^l \to \{0,1\}^{p(l)}$ with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded distinguishers is a function such that for any algorithm A with running time bounded by $t(l)$,*

$$|\Pr[A(f(U_l)) = 1] - \Pr[A(U_{p(l)}) = 1]| \leq \epsilon(l).$$

Let $\langle \cdot, \cdot \rangle$ denote the inner product over GF(2). First, in the following lemma, we construct cryptographic PRGs from one-way permutations.

Lemma 6.21 ([GL89])**.** *For any functions $t(\cdot)$ and $\epsilon(\cdot)$, assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way permutation with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded inverters. Then for any polynomial $p(n)$, there exists a constant $c > 0$ such that the function $G : \{0,1\}^{2n} \to \{0,1\}^{2n+p(n)}$,*

$$G(x,r) = \left(f^{p(n)}(x), r, \langle x, r\rangle, \langle f(x), r\rangle, \ldots, \langle f^{p(n)-1}(x), r\rangle\right),$$

is a pseudorandom generator with error $\epsilon(\cdot)^c$ against $t(\cdot)^c$-bounded distinguishers.

Then, to convert $G(x)$ into the seed-extending form, let $h(\cdot) = f^{-1}(\cdot)$ compute the inverse of f. Notice that the image of $G(x,r)$ is the same as the image of

$$G'(x,r) = x, r, \langle h(x), r\rangle, \langle h^2(x), r\rangle, \ldots, \langle h^{p(n)}(x), r\rangle, \text{ which is a seed-extending function.}$$

That is, $G'(x,r)$ is a seed-extending cryptographically secure functions with error $\epsilon(\cdot)^c$ against $t(\cdot)^c$-bounded distinguishers. Formally, we have the following corollary.

Corollary 6.22. *For any functions $t(\cdot)$ and $\epsilon(\cdot)$, assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way permutation with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded inverters. Then for any polynomial $p(n)$, there exists a constant $c > 0$ such that the function $G : \{0,1\}^{2n} \to \{0,1\}^{2n+p(n)}$,*

$$G(x,r) = x, r, \langle h(x), r\rangle, \langle h^2(x), r\rangle, \ldots, \langle h^{p(n)}(x), r\rangle, \text{ where } h(\cdot) = f^{-1}(\cdot).$$

is a seed-extending cryptographically secure function with error $\epsilon(\cdot)^c$ against $t(\cdot)^c$-bounded distinguishers.

Therefore, combining with Lemma 6.5, we have the following:

Theorem 6.23. *For any functions $t(\cdot)$ and $\epsilon(\cdot)$, assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way permutation with error $\epsilon(\cdot)$ against $t(\cdot)$-bounded inverters. Then for any $\Delta = \Delta(n) > 0$ and a positive constant $t < 1$, we can get an $\left(n - \Delta, O\left(2^{\Delta}\epsilon(n^t)^{c_t}\right)\right)$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-n^t}$ for sources recognizable by randomized algorithms running in time $(t(n^t))^{c_t}$, where c_t is a constant depending on t. The running time of our extractor is a polynomial times the time to compute the inverse function f^{-1} of the one-way permutation f with input length n^t.*

In the case that $\epsilon = \frac{1}{n^{w(1)}}$ and $q(n) = n^{w(1)}$, for any positive constant t, setting $\Delta = \frac{c_t}{2}\log 1/\epsilon(n^t)$ we get an $(n - O\left(\log(1/\epsilon(n^t))\right), \epsilon(n^t)^{c_t/2} = 1/n^{w(1)})$ extractor outputting $n - n^t$ bits from sources recognizable by BPP algorithms. By Lemma 6.17, one can scale down harder functions to get an extractor running in quasi-polynomial time.

Corollary 6.24. *For any constants $a, b, c, \delta > 0$, assume that there exists a one-way permutation invertible in time $O\left(2^{n^a}\right)$ with error 2^{-n^c} against $2^{\delta n^b}$-bounded inverters. Then, for any positive constants α and $\beta < 1$, we can get an $\left(n - c_\beta \log^{c\alpha}(n), O\left(2^{-c_\beta \log^{c\alpha}(n)}\right)\right)$ extractor $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^{n-n^\beta}$ for sources recognizable by randomized algorithms running in time $2^{c_\beta \delta \log^{b\alpha}(n)}$, where c_β is a constant depending on β. The running time of the extractor is $O\left(2^{\log^{a\alpha}(n^\beta)}\right)$.*

7 Algebraic Extractors over Prime Fields

In this section we explain how our algebraic extractor extends to any prime field $\mathbb{F}_q$. Recall that for two n-variate functions $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$, $Cor(f,g) = |Ee_q[f(x) + g(x)]|$, where $e_q[x] := w^x$ and w denotes the q-th root of unity. Moreover, over $\mathbb{F}_q$, we say a random variable Z is ϵ-biased if $bias(Z) = |\sum_{i \in \mathbb{F}_q} w^i \Pr[Z = i]| \leq \epsilon$.

Formally, we will prove the following:

Theorem 7.1. *For any positive integer d and an prime field $\mathbb{F}_q$, there is an efficient $\left((1 - 1/c_{d,q})n, d, 2^{-\Omega(n/c_{d,q})}\right)$-algebraic extractor* $\mathrm{Ext} : \mathbb{F}_q^n \to \mathbb{F}_q^m$*, where $c_{d,q} = \Theta(d^2 2^{2d} q^3 \log q)$ and $m = \Omega(n/c_{d,q})$.*

We follow the same proof outline as over GF(2). For simplicity, we focus on the set of fixed-length functions over $\mathbb{F}_q$, i.e., $\mathcal{C}_n \subseteq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ for any positive integer n. We first show that a naturally generalized XOR amplification for $\mathcal{C}_n$ over $\mathbb{F}_q$ yields a seedless extractor for $\mathcal{C}_n$-recognizable sources. Then, we prove that the generalized XOR amplification holds for n-bit algebraic sources over $\mathbb{F}_q$.

We first generalize the definition of α-XOR amplification for functions with a fixed input length to $\mathbb{F}_q$.

Definition 7.2 (α-XOR amplification over $\mathbb{F}_q$)**.** *For a class $\mathcal{C}_n$ of functions $C : \mathbb{F}_q^n \to \mathbb{F}_q$ and a positive constant α, we say $\mathcal{C}_n$ has α-XOR amplification for a function $h : \mathbb{F}_q^t \to \mathbb{F}_q$ such that for any vector $v \in \mathbb{F}_q^{\lfloor n/t \rfloor}$ with k non-zero coordinates, $Cor(h^v, \mathcal{C}_n) \leq q^{-\alpha k}$, where we add dummy variables to the input of h^v if h^v has less than n input variables.*

Theorem 7.3. *Let $\mathcal{C}_n$ be a class of n-variate functions $C : \mathbb{F}_q^n \to \mathbb{F}_q$, such that $C \in \mathcal{C}_n$ implies $\gamma C \in \mathcal{C}_n$ for any $\gamma \in \mathbb{F}_q$. Assume that $\mathcal{C}_n$ has α-XOR amplification for a function $h : \mathbb{F}_q^t \to \mathbb{F}_q$. Let M be the generating matrix of a linear $[l, m, r]_q$ code, where $l = n/t$. Then, the function* $\mathrm{Ext} : \mathbb{F}_q^n \to \mathbb{F}_q^m$*,*

$$\mathrm{Ext}(x) = h^{(l)}(x)M,$$

is an $\left(n - \Delta, q^{m/2+\Delta+1.5-\alpha r}\right)$ extractor for $\mathcal{C}$-recognizable sources.

Proof. For convenience, let $g = (g_1(x), \ldots, g_m(x)) = h^{(l)}(x)M$. To show that the output of Ext is $q^{m/2+\Delta+1.5-\alpha r}$-closed to uniform, by the statistical XOR lemma over $\mathbb{F}_q$, it suffices to show that for any vector $v \in \mathbb{F}_q^l \setminus \{0^l\}$, $g^v = \sum_{i \in [l]} v_i g_i$ is $q^{\Delta+1.5-\alpha r}$-biased conditioned on $C(x) = 1$ with $|C^{-1}(1)| \geq q^{n-\Delta}$.

Notice that for any $\gamma \in \mathbb{F}_q^*$,

$$\gamma g^v(x) = \gamma \left[v \cdot \left(M h^{(l)}(x)\right)\right] = \left(\sum_{i \in [l]} \gamma v_i M_i\right) h^{(l)}(x),$$

where M_i denotes the i-th row of the matrix M. As M is the generating matrix of an $[l, m, r]_q$ code and v is a non-zero vector, $\sum_{i \in [l]} \gamma v_i M_i$ is a non-zero codeword that has at least r non-zero coordinates. Thus, by the assumed XOR amplification, we have $Cor(\gamma g^v, \mathcal{C}_n) \leq q^{-\alpha r}$.

Furthermore, by the property of $\mathcal{C}_n$, we know that for any $\beta \in \mathbb{F}_q$, $\beta C \in \mathcal{C}_n$. Therefore, for any $C \in \mathcal{C}_n$, any $\gamma \in \mathbb{F}_q^*$, and any $\beta \in \mathbb{F}_q$, we have

$$Cor(\gamma g^v, \beta C) \leq Cor(\gamma g^v, \mathcal{C}_n) \leq q^{-\alpha r}.$$

Notice that this implies that for each $\beta \in \mathbb{F}_q$ and each $\gamma \in \mathbb{F}_q^*$, $\gamma(g^v + \beta C)$ is $q^{-\alpha r}$-biased. Then, by the statistical XOR lemma over $\mathbb{F}_q$, $g^v + \beta C$ is $q^{0.5-\alpha r}$-close to the uniform.

Now, we need the following two lemmas on connections between correlations and statistical distances over $\mathbb{F}_q$. The proofs of these two lemmas are given in the appendix.

Lemma 7.4. *For any prime q, let $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$ be two functions. If for any $\beta, \gamma \in \mathbb{F}_q$ $\Pr_{X \sim U_{\mathbb{F}_q^n}}[f(X) + \beta g(X) = \gamma] \leq \frac{1}{q} + \epsilon$, then for any $u, v \in \mathbb{F}_q$, we have*

$$\Pr_{X \sim U_{\mathbb{F}_q^n}}[f(X) = u | g(X) = v] \leq \frac{1}{q} + \frac{\epsilon}{\Pr[g(X) = v]}.$$

We remark that Dodis, Li, Wooley and Zuckerman [DLWZ14] proved the above lemma by Fourier analysis, which they called the non-uniform XOR lemma. For completeness, we include a proof in the appendix.

Lemma 7.5. *For a random variable Z over $\mathbb{F}_q$ and each $j \in \mathbb{F}_q$, if $\Pr[Z = j] \leq 1/q + \delta$, then Z is $q\delta$-biased.*

Combining with the fact that $g^v + \beta C$ is $q^{0.5-\alpha r}$-close to the uniform, i.e., $\Pr[g^v + \beta C = \lambda] \leq q^{0.5-\alpha r}$ for any $\lambda \in \mathbb{F}_q$, these two lemmas directly imply that the bias of g^v is at most $q^{1.5-\alpha r}/\Pr[C(X) = 1]$ conditioned on $C(x) = 1$. As $|C^{-1}| \geq q^{n-\Delta}$, $\Pr[C(x) = 1] \geq 2^{-\Delta}$, and hence the bias of g^v is at most $q^{\Delta+1.5-\alpha r}$ conditioned on $C(x) = 1$, which concludes the proof.

□

The next, we prove that XOR amplification over $\mathbb{F}_q$ holds for n-bit algebraic sources.

Now, let P_d denote the set all polynomials of degree at most d over $\mathbb{F}_q$, and $\mathcal{V}_{d,n}$ denote the set of the specific products $\Pi_{i \in [k]} (1 - p_i(x)^{q-1})$ for any positive integer k and any n-variate polynomials $p_1(x), \ldots, p_k(x) \in P_d$. Note that the product $\Pi \left(1 - x_i^{q-1}\right)$ is the analog of the AND function over GF(2). Using the same idea as in the case GF(2), we can prove the following two lemmas. See the appendix for their proofs.

Lemma 7.6. *An n-bit algebraic source of degree d over $\mathbb{F}_q$ iff it is a $\mathcal{V}_{d,n}$-recognizable source.*

Lemma 7.7. *If $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is a function such that $Cor(f, P_d) \leq \epsilon$, then $Cor(f, \mathcal{V}_{d,n}) \leq 2\epsilon$.*

Lemma 7.7 follows because the L1 norm of Fourier transform of any one-point indicator functions $\Pi(1 - x_i^{q-1})$ over $\mathbb{F}_q$ is at most 2.

Therefore, to prove XOR amplification for algebraic sources, it suffices to prove XOR amplification for P_d.

Bogdanov, Kawachi and Tanaka [BKT13] proved XOR amplification for low-degree polynomials over prime fields. They proved that the sum of k independent copies of h was $q^{-\Omega(k)}$-hard for P_d if h was mildly hard. However, besides the sum of copies, we require the same hardness result for linear combinations of k copies of h.

Formally, for a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$, let $\delta_d(f) := \min_{p \in P_d} \Pr_{X \sim U_{\mathbb{F}_q^n}}[f(x) \neq p(x)]$ denote the distance of f to P_d. We prove the following lemma.

Lemma 7.8. *Let q be a prime number, t a positive integer, and $h : \mathbb{F}_q^n \to \mathbb{F}_q$ a function. If $\delta_d(h) \geq q/(d+1)2^{d+1}$, then for any $v \in \mathbb{F}_q^{n/t}$ with t non-zero coordinates,*

$$\delta_d(h^v) \geq \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{3t}{q^2(d+1)2^{2d+3}}\right).$$

We remark that the lemma is implicitly implied by the proof of Bogdanov, Kawachi and Tanaka. The main revision of our proof is using the fact that the Gowers norm is multiplicative for functions over disjoint sets of input variables. Please see the appendix for the proof.

Finally, to get the desired XOR amplification for P_d, we need to prove the following lemma.

Lemma 7.9. *If $\delta_d(h^v) \geq \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{3t}{q^2(d+1)2^{2d+3}}\right)$, then $Cor(h^v, P_d) \leq q^{-t/c_{d,q}}$, where $c_{d,q} = \Theta(d2^{2d}q^2 \log q)$.*

Proof. To show that $Cor(h^v, P_d) \leq q^{-t/c_{d,q}}$, it is equivalent to show that for any n-variate polynomial $p \in P_d$, $h^v + p$ is $q^{-t/c_{d,q}}$-biased as $Cor(h^v, p) = bias(h^v + p)$. By Lemma 7.5, it suffices to show that for any $\alpha \in \mathbb{F}_q$, $\Pr[h^v + p = \alpha] \leq 1/q + q^{-t/c_{d,q}}$, or

$$\Pr[h^v \neq \alpha - p] \geq (q-1)/q - q^{-t/c_{d,q}}.$$

This follows if $\delta_d(h^v) \geq \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{3t}{q^2(d+1)2^{2d+3}}\right)$. □

In conclusion, we give the proof of our main theorem in this section, i.e., constructing an algebraic extractor over $\mathbb{F}_q$.

Proof. We use an explicit $[l, \delta_1 l, \delta_2 l]_q$ linear code over $\mathbb{F}_q$ for some constant δ_1, δ_2 by Alon et al. [ABN+92]. By brute force search, it is easy to find a function h over $O(dq)$ bits such that $\delta_d(h) \geq q/(d+1)2^{d+1}$ as d, q are constants. Let $c_{d,q} = \Theta(d2^{2d}q^2 \log q)$. By Lemma 7.8 and Lemma 7.9, $Cor(h^v, P_d) \leq q^{-\Omega(t/c_{d,q})}$ for any $v \in \mathbb{F}_q^l$ with t non-zero coordinates. That is,

$$Cor(h^v, \mathcal{V}_{d,n}) \leq q^{-\Omega(t/c_{d,q})}, \text{ by Lemma 7.4.}$$

Thus, Theorem 7.3 yields a $\left(n - O(l/c_{d,q}), q^{-\Omega(l/c_{d,q})}\right)$ extractor for $\mathcal{V}_{d,n}$-recognizable sources, i.e., a $\left((1 - 1/c'_{d,q})n, d, q^{-\Omega(n/c'_{d,q})}\right)$-algebraic extractor $\mathrm{Ext} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, where $c'_{d,q} = \Theta(d^2 2^{2d} q^3 \log q)$ and $m = \Omega(n/c'_{d,q})$. □

Acknowledgements

We wish to thank Salil Vadhan, Ronen Shaltiel, Avishay Tal, and William Hoza for helpful discussions and comments.

References

[AASY16] Benny Applebaum, Sergei Artemenko, Ronen Shaltiel, and Guang Yang. Incompressible functions, relative-error extractors, and the power of nondeterministic reductions. *computational complexity*, 25(2):349–418, 2016.

[ABN+92] Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ron M Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on information theory*, 38(2):509–516, 1992.

[BKT13] Andrej Bogdanov, Akinori Kawachi, and Hidetoki Tanaka. Hard functions for low-degree polynomials over prime fields. *ACM Transactions on Computation Theory (TOCT)*, 5(2):5, 2013.

[BNS92] László Babai, Noam Nisant, and Márió Szegedy. Multiparty protocols, pseudo-random generators for logspace, and time-space trade-offs. *Journal of Computer and System Sciences*, 45(2):204–232, 1992.

[Bou07] Jean Bourgain. On the construction of affine extractors. *GAFA Geometric And Functional Analysis*, 17(1):33–57, 2007.

[CFL83] Ashok K Chandra, Merrick L Furst, and Richard J Lipton. Multi-party protocols. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 94–99. ACM, 1983.

[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.

[DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009.

[DLWZ14] Yevgeniy Dodis, Xin Li, Trevor D Wooley, and David Zuckerman. Privacy amplification and nonmalleable extractors via character sums. *SIAM Journal on Computing*, 43(2):800–830, 2014.

[Dvi12] Zeev Dvir. Extractors for varieties. *Computational complexity*, 21(4):515–572, 2012.

[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*, pages 405–411. ACM, 2016.

[GL89] Oded Goldreich and Leonid A Levin. A hard-core predicate for all one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 25–32. ACM, 1989.

[Gol95] O Goldreich. Three xor-lemmas – an exposition, 1995.

[Hås87] Johan Håstad. Computational limitations of small-depth circuits. 1987.

[Jus72] Jørn Justesen. Class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18(5):652–656, 1972.

[KRT17] Ilan Komargodski, Ran Raz, and Avishay Tal. Improved average-case lower bounds for de morgan formula size: Matching worst-case lower bound. *SIAM Journal on Computing*, 46(1):37–57, 2017.

[KRVZ11] Jesse Kamp, Anup Rao, Salil Vadhan, and David Zuckerman. Deterministic extractors for small-space sources. *Journal of Computer and System Sciences*, 77(1):191–220, 2011.

[KvMS12] Jeff Kinne, Dieter van Melkebeek, and Ronen Shaltiel. Pseudorandom generators, typically-correct derandomization, and circuit lower bounds. *computational complexity*, 21(1):3–61, 2012.

[Li16] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. In *Foundations of Computer Science (FOCS), 2016 IEEE 57th Annual Symposium on*, pages 168–177. IEEE, 2016.

[Nis93] Noam Nisan. The communication complexity of threshold gates. *Combinatorics, Paul Erdos is Eighty*, 1:301–315, 1993.

[NW88] Noam Nisan and Avi Wigderson. Hardness vs. randomness. In *Foundations of Computer Science, 1988., 29th Annual Symposium on*, pages 2–11. IEEE, 1988.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[Rem16] Zachary Remscrim. The Hilbert function, algebraic extractors, and recursive fourier sampling. In *Foundations of Computer Science (FOCS), 2016 IEEE 57th Annual Symposium on*, pages 197–208. IEEE, 2016.

[Sha11] Ronen Shaltiel. Weak derandomization of weak algorithms: explicit versions of Yao's lemma. *computational complexity*, 20(1):87, 2011.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82. ACM, 1987.

[SV86] Miklos Santha and Umesh V Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1):75–87, 1986.

[TV00] Luca Trevisan and Salil Vadhan. Extracting randomness from samplable distributions. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 32–42. IEEE, 2000.

[Vio09] Emanuele Viola. Guest column: correlation bounds for polynomials over {0 1}. *ACM SIGACT News*, 40(1):27–44, 2009.

[Vio14] Emanuele Viola. Extractors for circuit sources. *SIAM Journal on Computing*, 43(2):655–672, 2014.

[VW08] Emanuele Viola and Avi Wigderson. Norms, xor lemmas, and lower bounds for polynomials and protocols. *Theory of Computing*, 4(1):137–168, 2008.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, pages 209–213. ACM, 1979.

[Yao82] Andrew C Yao. Theory and application of trapdoor functions. In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*, pages 80–91. IEEE, 1982.

A Appendix

In the appendix, we give all missing proofs. Before each proof, we restate the statement which it proves.

Lemma A.1 (Lemma 7.4, restated)**.** *For a prime q, let $f, g : \mathbb{F}_q^n \to \mathbb{F}_q$ be two functions. If for any $\beta, \lambda \in \mathbb{F}_q$ $\Pr_{X\sim U_{\mathbb{F}_q^n}}[f(X) + \beta g(X) = \lambda] \le \frac{1}{q} + \epsilon$, then for any $u, v \in \mathbb{F}_q$, we have*

$$\Pr_{X\sim U_{\mathbb{F}_q^n}}[f(X) = u | g(X) = v] \le \frac{1}{q} + \frac{\epsilon}{\Pr[g(X) = v]}.$$

Proof. Let $a_{i,j} = \Pr[f(X) = i \wedge g(X) = j]$ for any $i, j \in \mathbb{F}_q$, and $S_{\beta,\lambda} = \sum_{t\in\mathbb{F}_q} a_{\lambda-\beta t,t}$ for any $\beta, \lambda \in \mathbb{F}_q$. Then, we have

$$S_{\beta,\lambda} = \sum_{t\in\mathbb{F}_q} a_{\lambda-\beta t,t} = \sum_{t\in\mathbb{F}_q} \Pr[f(X) = \lambda - \beta t \wedge g(X) = t] = \Pr[f(X) + \beta g(X) = \lambda] \le \frac{1}{q} + \epsilon.$$

Furthermore, we know

$$\sum_{i,j\in\mathbb{F}_q} a_{i,j} = \sum_{i,j\in\mathbb{F}_q} \Pr[f(X) = i \wedge g(X) = j] = 1.$$

Note that for any $u, v \in \mathbb{F}_q$, to bound $\Pr_{X\sim U_{\mathbb{F}_q^n}}[f(X) = u | g(X) = v]$, it suffices to bound $a_{u,v}$. Summing over all $S_{\beta,\lambda}$ containing $a_{u,v}$ in the sum, we have

$$\sum_{\beta,\lambda\in\mathbb{F}_q:\exists t,\lambda-\beta t=u\wedge t=v} S_{\beta,\lambda} = \sum_{\beta\in\mathbb{F}_q} S_{\beta,u+\beta v} = \sum_{\beta\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q} a_{u+\beta(v-t),t} = \sum_{t\in\mathbb{F}_q}\left(\sum_{\beta\in\mathbb{F}_q} a_{u+\beta(v-t),t}\right).$$

Notice that, when $t \neq v$, $\sum_{\beta\in\mathbb{F}_q} a_{u+\beta(v-t),t} = \sum_{i\in\mathbb{F}_q} a_{i,t}$ as q is a prime. Thus,

$$\sum_{t\in\mathbb{F}_q}\left(\sum_{\beta\in\mathbb{F}_q} a_{u+\beta(v-t),t}\right) = \sum_{t\neq v}\left(\sum_{i\in\mathbb{F}_q} a_{i,t}\right) + \sum_{\beta\in\mathbb{F}_q} a_{u,v} = 1 - \left(\sum_{i\in\mathbb{F}_q} a_{i,v}\right) + qa_{u,v}.$$

To sum up, we prove that

$$1 - \left(\sum_{i\in\mathbb{F}_q} a_{i,v}\right) + qa_{u,v} = \sum_{\beta\in\mathbb{F}_q} S_{\beta,u+\beta v}.$$

Combining with the fact that $S_{\beta,u+\beta v} \leq 1/q + \epsilon$, we have

$$a_{u,v} \leq \frac{1}{q}\left(\sum_{i\in\mathbb{F}_q} a_{i,v}\right) + \epsilon = \frac{1}{q}\Pr[g(X) = v] + \epsilon.$$

Therefore, $\Pr[f(X) = u | g(X) = v] = \frac{a_{u,v}}{\Pr[g(X)=v]} \leq \frac{1}{q} + \frac{\epsilon}{\Pr[g(X)=v]}$. □

Lemma A.2 (Lemma 7.5, restated)**.** *For a random variable Z over $\mathbb{F}_q$ and each $j \in \mathbb{F}_q$, if $\Pr[Z = j] \leq 1/q + \delta$, then Z is $q\delta$-biased.*

Proof. Let

$$\Pr[Z = j] = 1/q + \delta - \alpha_j,$$

where $\alpha_j \geq 0$. Notice that

$$1 = \sum_{j\in\mathbb{F}_q} \Pr[Z = j] = \sum_{j\in\mathbb{F}_q}(1/q + \delta - \alpha_j) = 1 + q\delta - \sum_{j\in\mathbb{F}_q} \alpha_j.$$

That is, $\sum_{j\in\mathbb{F}_q} \alpha_j = q\delta$. Therefore, the bias of Z can be bounded as follows.

$$\begin{aligned} bias(Z) = \left|\sum_{j\in\mathbb{F}_q} w^j\,(1/q + \delta - \alpha_j)\right| &\leq \left|\sum_{j\in\mathbb{F}_q} w^j\,(1/q + \delta)\right| + \left|\sum_{j\in\mathbb{F}_q} w^j\alpha_j\right| \\ &\leq 0 + \sum_{j\in\mathbb{F}_q} |\alpha_j| = \sum_{j\in\mathbb{F}_q} \alpha_j = q\delta. \end{aligned}$$

□

Recall that P_d denotes the set of all polynomials of degree at most d over $\mathbb{F}_q$, and $\mathcal{V}_{d,n}$ denotes the set of the specific products $\Pi_{i\in[k]}\,(1 - p_i(X)^{q-1})$ for any positive integer k and any n-variate polynomials $p_1(x), \ldots, p_k(x) \in P_d$.

Lemma A.3 (Lemma 7.6, restated)**.** *An n-bit algebraic source of degree d over $\mathbb{F}_q$ iff it is a $\mathcal{V}_{d,n}$-recognizable source.*

Proof. Let U_V denote an arbitrary algebraic source over $\mathbb{F}_q$, where V is an algebraic set of degree d defined by n-variate polynomials $p_1, \ldots, p_k \in P_d$. By Fermat's Little Theorem, for each p_i, we know $1 - p_i(x)^{q-1} = 1$ iff $p_i(x) = 0$ over $\mathbb{F}_q$. Namely, V can be viewed as the set of 1-inputs of the function $\prod_{i\in[k]}(1 - p_i(x)^{q-1})$. That is, the uniform distribution over V is also the source recognizable by $\prod_{i\in[k]}(1 - p_i(x)^{q-1}) \in \mathcal{V}_{d,n}$. In other words, an algebraic source of degree d over $\mathbb{F}_q$ is a $\mathcal{V}_{d,n}$-recognizable source.

For the other direction, let U_f denote an arbitrary $\mathcal{V}_{d,n}$-recognizable source, where $f = \prod_{i\in[k]}(1-p_i(x)^{q-1}) \in \mathcal{V}_{d,n}$ with $\deg(p_i) \le d$ for each $i \in [k]$. By the fact that $1-p_i(x)^{q-1} = 1$ iff $p_i(x) = 0$, we have $f^{-1}(1) = \{x \in \mathbb{F}_q^n | p_i(x) = 0, \forall i \in [k]\}$. Hence, $f^{-1}(1)$ is the algebraic set defined by $p_1(x), \ldots, p_k(x) \in P_d$, i.e., $f^{-1}(1)$ is an algebraic set of degree d over n bits. Therefore, U_f is an n-bit algebraic source of degree d. □

Lemma A.4 (Lemma 7.7, restated)**.** *If $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is a function such that $Cor(f, P_d) \le \epsilon$, then $Cor(f, \mathcal{V}_{d,n}) \le 2\epsilon$.*

The lemma follows because the L1 norm of the Fourier transform of any one-point indicator function $\Pi\left(1 - x_i^{q-1}\right)$ over $\mathbb{F}_q$ is at most 2.

Proof. We need to show that if for any $p \in P_d$ $Cor(f, p) = |Ee_q[f + p]| \le \epsilon$, then for any product $\Pi_{i\in[k]}(1 - p_i(X)^{q-1})$ where $p_1, \ldots, p_k \in P_d$, we have

$$Cor\left(f, \Pi_{i\in[k]}\left(1 - p_i(X)^{q-1}\right)\right) = \left|Ee_q\left[f + \Pi_{i\in[k]}\left(1 - p_i(X)^{q-1}\right)\right]\right| \le 2\epsilon.$$

Consider the Fourier expansion of the function

$$e_q\left[\prod_{i\in[k]}(1 - y_i^{q-1})\right] = \sum_{\beta\neq 0^k} \hat{f}_\beta e_q\left[\sum_{i\in[k]} \beta_i y_i\right] + (1 - 1/q^k) + w/q^k,$$

where $\hat{f}_\beta = Ee_q[\prod_{i\in[k]}(1 - y_i^{q-1}) + \sum_{i\in[k]} \beta_i y_i]$.

Notice that $Ee_q[\sum_{i\in[k]} \beta_i y_i] = 0$ if $\beta \neq 0^k$. Thus,

$$|\hat{f}_\beta| = \left|\frac{e_q[1] + \sum_{y\neq 0^k} e_q[\sum_{i\in[k]} \beta_i y_i]}{q^k}\right| = \left|\frac{e_q[1] + \sum_{y\in\mathbb{F}_q^k} e_q[\sum_{i\in[k]} \beta_i y_i] - e_q[0]}{q^k}\right| \le \frac{2}{q^k}.$$

Now, substituting each y_i by p_i and multiplying $e_q[f]$ on both sides, we have

$$\left|Ee_q\left[f(X) + \Pi_{i\in[k]}\left(1 - p_i(X)^{q-1}\right)\right]\right| \le \sum_{\beta\neq 0^k} |\hat{f}_\beta| \left|Ee_q\left[f(X) + \sum_{i\in[k]} \beta_i p_i(X)\right]\right|.$$

Note that $\left|Ee_q\left[f + \sum_{i\in[k]} \beta_i p_i(X)\right]\right| \le \epsilon$ as $\sum_{i\in[k]} \beta_i p_i(X) \in P_d$. In other words,

$$\left|Ee_q\left[f + \prod_{i\in[k]}(1 - p_i^k(X))\right]\right| \le \left(\sum_{\beta\neq 0^k} |\hat{f}_\beta|\right)\epsilon \le 2\epsilon.$$

□

Lemma A.5 (Lemma 7.8, restated)**.** *Let q be any prime number, $t > 0$ be any integer, and $h : \mathbb{F}_q^n \to \mathbb{F}_q$ be any function. If $\delta_d(h) \geq q/(d+1)2^{d+1}$, then for any $v \in \mathbb{F}_q^{n/t}$ with t non-zero coordinates,*

$$\delta_d(h^v) \geq \frac{q-1}{q} - \frac{q-1}{q}\frac{3t}{q^2(d+1)2^{2d+3}}.$$

Recall that $\delta_d(f) = \min_{p \in P_d} \Pr_{X \sim U_{\mathbb{F}_q^n}}[f(x) \neq p(x)]$. Furthermore, let $f^{+t} : (\mathbb{F}_q^n)^t \to \mathbb{F}_q$ denote the sum over $\mathbb{F}_q$ of t independent copies of f, namely, $f^{+t}(x_1, \ldots, x_n) = \sum_{i \in [t]} f(x_i)$, and for any vector $v \in \mathbb{F}_q^m$, f^v denote the linear combination of m copies of f according to v, i.e., $f^v(x_1, x_2, \ldots, x_m) := \sum_{i \in [m]} v_i f(x_i)$, where $x_1, \ldots, x_m \in \mathbb{F}_q^n$.

Note that Bogdanov, Kawachi and Tanaka proved the following XOR lemma for polynomials over prime fields.

Lemma A.6. *[BKT13, Theorem 1.1] Let q be any prime number, $t > 0$ be any integer, and $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be any function. If $\delta_d(f) \geq q/(d+1)2^{d+1}$, then*

$$\delta_d(f^{+t}) > \frac{q-1}{q}\left(1 - \exp\left(-\frac{3t}{q^2(d+1)2^{2d+3}}\right)\right).$$

We note that with some modifications, their proof proves Lemma 7.8. Thus, we first briefly describe their proof, and then give our proof.

In their proof, for a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and any integer d, they prove two lemmas on relations between the distance from degree-d polynomials, $\delta_d(f)$, and the Gowers uniformity $U_{d+1}(f)$ and between the Gowers uniformity and the rejection probability, $\rho_d(f)$, of a specific low-degree test for polynomial. They proved that $\rho_d(f) \geq \min\{\delta_d(f)/q, 1/(d+1)2^{d+1}\}$, stated as Theorem 3.2, and $\rho_d(f) = \rho_d(\alpha f)$ for any $\alpha \in \mathbb{F}_q^*$.

More precisely, for a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and a vector $y \in \mathbb{F}_q^n$, we take $\Delta_y(f)$ to be the directional derivative of f in direction y by setting $\Delta_y f(x) = f(x+y) - f(x)$. On vectors $y_1, \ldots, y_k$, the derivative of f is recursively defined as $\Delta_{y_1,\ldots,y_k}(f) := \Delta_{y_1,\ldots,y_{k-1}}(\Delta_{y_k} f)$. Then, for every integer $k \geq 0$, the degree-k Gowers uniformity $U_k(f)$ is defined as

$$U_k(f) := E_{x,y_1,\ldots,y_k \in \mathbb{F}_q^n}\left[w^{\Delta_{y_1,\ldots,y_k} f(x)}\right].$$

Formally, we state the two lemmas as follows.

Lemma A.7. *[BKT13, Lemma 4.2][DISTANCE TO UNIFORMITY] For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and any integer $d \geq 0$,*

$$\delta_d(f) \geq \frac{q-1}{q}\left(1 - E_{a \in \mathbb{F}_q^*}\left[(U_{d+1}(af))^{1/2^{d+2}}\right]\right).$$

Lemma A.8. *[BKT13, Lemma 4.3][UNIFORMITY TO TEST] For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and any integer $d \geq 0$,*

$$U_{d+1}(f) < 1 - \frac{3}{q^2}\rho_d(f).$$

Now, we give the proof of Lemma 7.8, based on the above two lemmas and the properties of $\rho_d(f)$.

Proof. By Lemma A.7 and the averaging principle, there is an $\alpha \in \mathbb{F}_q^*$ such that,

$$\delta_d(h^v) \geq \frac{q-1}{q}\left(1 - U_{d+1}(\alpha h^v)^{1/2^{d+2}}\right).$$

By the definition of the U_{d+1}, we know the the Gowers uniformity is multiplicative for functions over disjoint sets of input variables. That is,

$$U_{d+1}(\alpha h^v) = U_{d+1}\left(\sum_{i\in[m]} \alpha v_i h\right) = \prod_{i\in[m]} U_{d+1}(\alpha v_i h).$$

Note that if $v_i = 0$, then $U_{d+1}(\alpha v_i h) = U_{d+1}(0) = 1$. Thus, it suffices to consider those t non-zero v_i's. By Lemma A.8, $U_{d+1}(\alpha v_i h) \leq 1 - \frac{3}{q^2}\rho_d(\alpha v_i h) = 1 - \frac{3}{q^2}\rho_d(h)$ for $\alpha v_i \neq 0$. That is,

$$U_{d+1}(\alpha h^v) \leq \left(1 - \frac{3}{q^2}\rho_d(h)\right)^t.$$

Note that $\rho_d(h) \geq \min\{\delta_d(h)/q, 1/(d+1)2^{d+1}\} = 1/(d+1)2^{d+1}$. Thus, it is not hard to calculate that $\delta_d(h^v) \geq \frac{q-1}{q}\left(1 - U_{d+1}(\alpha h^v)^{1/2^{d+2}}\right) \geq \frac{q-1}{q} - \frac{q-1}{q}\exp(-\frac{3t}{q^2(d+1)2^{2d+3}})$. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il