Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 119 (2015)

Explicit Two-Source Extractors and Resilient Functions

Eshan Chattopadhyay*
Department of Computer Science,
University of Texas at Austin
eshanc@cs.utexas.edu

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

March 19, 2016

Abstract

We explicitly construct an extractor for two independent sources on n bits, each with min-entropy at least $\log^C n$ for a large enough constant C. Our extractor outputs one bit and has error $n^{-\Omega(1)}$. The best previous extractor, by Bourgain [Bou05], required each source to have min-entropy $.499n$.

A key ingredient in our construction is an explicit construction of a monotone, almost-balanced boolean function on n bits that is resilient to coalitions of size $n^{1-\delta}$, for any $\delta > 0$. In fact, our construction is stronger in that it gives an explicit extractor for a generalization of non-oblivious bit-fixing sources on n bits, where some unknown $n - q$ bits are chosen almost polylog(n)-wise independently, and the remaining $q = n^{1-\delta}$ bits are chosen by an adversary as an arbitrary function of the $n - q$ bits. The best previous construction, by Viola [Vio14], achieved $q = n^{1/2-\delta}$.

Our explicit two-source extractor directly implies an explicit construction of a $2^{(\log \log N)^{O(1)}}$-Ramsey graph over N vertices, improving bounds obtained by Barak et al. [BRSW12] and matching independent work by Cohen [Coh16].

*Partially supported by NSF Grant CCF-1218723.
†Partially supported by NSF Grant CCF-1218723.

ISSN 1433-8092

1 Introduction

The area of randomness extraction deals with the problem of obtaining nearly uniform bits from sources that are only weakly random. This is motivated by the ubiquitous use of randomness in various branches of computer science like algorithms, cryptography, and more. Further, most applications require truly random, uncorrelated bits, but most easily-obtainable sources of randomness do not satisfy these conditions. In particular, pseudorandom generators in practice try to accumulate entropy by using thermal noise or clock drift, but then this needs to be purified before using it to seed a pseudorandom generator; see e.g., [JK99, BH05].

As is standard, we model a weak source on n bits using min-entropy. A source $\mathbf{X}$ on n bits is said to have min-entropy at least k if for any x, $\mathbf{Pr}[\mathbf{X} = x] \leq 2^{-k}$.

Definition 1.1. *The min-entropy of a source* $\mathbf{X}$ *is defined to be:* $H_\infty(\mathbf{X}) = \min_x(-\log(\Pr[\mathbf{X} = x]))$. *The min-entropy rate of a source* $\mathbf{X}$ *on* $\{0,1\}^n$ *is defined to be* $H_\infty(\mathbf{X})/n$. *Any source* $\mathbf{X}$ *on* $\{0,1\}^n$ *with min-entropy at least* k *is called an* (n,k)*-source.*

An extractor $\text{Ext} : \{0,1\}^n \to \{0,1\}^m$ is a deterministic function that takes input from a weak source with sufficient min-entropy and produces nearly uniform bits. Unfortunately, a simple argument shows that it is impossible to design an extractor to extract even 1 bit for sources with min-entropy $n-1$. To circumvent this difficulty, Santha and Vazirani [SV86], and Chor and Goldreich [CG88] suggested the problem of designing extractors for two or more independent sources, each with sufficient min-entropy. When the extractor has access to just two sources, it is called a two-source extractor. An efficient two-source extractor could be quite useful in practice, if just two independent sources of entropy can be found.

We use the notion statistical distance to measure the error of the extractor. The statistical distance between two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over some universal set Ω is defined as $|\mathcal{D}_1 - \mathcal{D}_2| = \frac{1}{2}\sum_{d\in\Omega}|\mathbf{Pr}[\mathcal{D}_1 = d] - \mathbf{Pr}[\mathcal{D}_2 = d]|$. We say $\mathcal{D}_1$ is ϵ-close to $\mathcal{D}_2$ if $|\mathcal{D}_1 - \mathcal{D}_2| \leq \epsilon$ and denote it by $\mathcal{D}_1 \approx_\epsilon \mathcal{D}_2$.

Definition 1.2 (Two-source extractor)**.** *A function* $\text{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ *is called a two-source extractor for min-entropy* k *and error* ϵ *if for any independent* (n,k)*-sources* $\mathbf{X}$ *and* $\mathbf{Y}$

$$|\text{Ext}(\mathbf{X},\mathbf{Y}) - \mathbf{U}_m| \leq \epsilon,$$

where $\mathbf{U}_m$ *is the uniform distribution on* m *bits. Further,* Ext *is said to be strong in* $\mathbf{Y}$ *if it also satisfies* $|(\text{Ext}(\mathbf{X},\mathbf{Y}),\mathbf{Y}) - (\mathbf{U}_m,\mathbf{Y})| \leq \epsilon$*, where* $\mathbf{U}_m$ *is independent from* $\mathbf{Y}$*.*

Note that for $m = 1$, this corresponds to an $N \times N$ matrix with entries in $\{0,1\}$ such that every $K \times K$ submatrix has $1/2 \pm \varepsilon$ fraction of 1's, where $N = 2^n$ and $K = 2^k$.

A simple probabilistic argument shows the existence of 2-source extractors for min-entropy $k \geq \log n + 2\log(1/\epsilon) + 1$. However, in computer science, it is important to construct such functions explicitly, and this has drawn a lot of attention in the last three decades. Chor and Goldreich [CG88] used Lindsey's Lemma to show that the inner-product function is a 2-source extractor for min-entropy more than $n/2$. However, no further progress was made for around 20 years, when Bourgain [Bou05] broke the "half-barrier" for min-entropy, and constructed a 2-source extractor for min-entropy $0.499n$. This remains the best known result prior to this work. Bourgain's extractor was based on breakthroughs made in the area of additive combinatorics.

Raz [Raz05] obtained an improvement in terms of total min-entropy, and constructed 2-source extractors requiring one source with min-entropy more than $n/2$ and the other source with min-entropy $O(\log n)$. A different line of work investigated a weaker problem of designing dispersers for two independent sources due to its connection with Ramsey graphs. We discuss this in Section 1.1.

The lack of progress on constructing two-source extractors motivated researchers to use more than two sources. Several researchers managed to construct excellent extractors using a constant number of sources [BIW06, Rao09a, RZ08, Li11, Li13a, Li13b] culminating in Li's construction of a 3-source extractor for polylogarithmic min-entropy [Li15c]. Recently Cohen [Coh15] also constructed a 3-source extractor with one source having min-entropy δn, the second source having min-entropy $O(\log n)$ and the third source having min-entropy $O(\log \log n)$.

Another direction has been the construction of seeded extractors [NZ96]. A seeded extractor uses one (n, k)-source and one short seed to extract randomness. There was a lot of inspiring work over two decades culminating in almost optimal seeded extractors [LRVW03, GUV09, DKSS09]. Such seeded extractors have found numerous applications; see e.g., Shaltiel's survey [Sha02].

However despite much attention and progress over the last 30 years, it remained open to explicitly construct two-source extractors for min-entropy rate significantly smaller than $1/2$.

Our main result is an explicit two-source extractor for polylogarithmic min-entropy.

Theorem 1 (Main theorem)**.** *There exists a constant $C > 0$ such that for all $n \in \mathbb{N}$, there exists a polynomial time computable construction of a 2-source extractor $2\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ for min-entropy at least $\log^C(n)$ and error $n^{-\Omega(1)}$.*

The min-entropy requirement in the above theorem can be taken to be $C_1(\log n)^{74}$, where C_1 is a large enough constant.

By an argument of Barak [Rao09b], every 2-source extractor is also a strong 2-source extractor with similar parameters. Thus the extractor 2Ext in Theorem 1 is also a strong 2-source extractor.

Note that an improvement of the output length of the above extractor to $c \log n$ bits, for a large enough constant c, will immediately allow one to extract $\Omega(k)$ bits using a standard trick of composing with a strong-seeded extractor.

Furthermore, improving the error to negligible while outputting many bits would have applications in cryptography and distributed computing. For example, several researchers have studied whether cryptographic or distributed computing protocols can be implemented if the players' randomness is defective [DO03, GSV05, KLRZ08, KLR09]. Kalai et al. [KLRZ08] used C-source extractors to build network extractor protocols, which allow players to extract private randomness in a network with Byzantine faults. A better 2-source extractor with negligible error would improve some of those constructions. Kalai, Li, and Rao [KLR09] showed how to construct a 2-source extractor under computational assumptions, and used it to improve earlier network extractors in the computational setting; however, their protocols rely on computational assumptions beyond the 2-source extractor, so it would not be clear how to match their results without assumptions.

If we allow the 2-source extractor to run in time $\mathrm{poly}(n, 1/\epsilon)$, then our technique in fact generalizes to obtain arbitrary error ϵ. In particular, we have the following theorem.

Theorem 2. *There exists a constant $C > 0$ such that for all $n \in \mathbb{N}$ and any $\epsilon > 0$, there exists a 2-source extractor $2\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ computable in time $\mathrm{poly}(n, 1/\epsilon)$ for min-entropy at least $\log^C(n/\epsilon)$ and error ϵ.*

Subsequent Work: Recently, Li [Li15b] extended our construction to achieve an explicit strong 2-extractor with output length k^α bits, for some small constant α. By our observation above, this immediately implies a 2-source extractor for min-entropy $k \geq \log^{C'} n$, for some large enough constant C', with output length $\Omega(k)$; in fact, the output can be k bits.

Meka built on our ideas to construct a resilient function matching Altai-Linial [Mek15]. This improves the min-entropy requirement from $C_1(\log n)^{74}$ to $C_2(\log n)^{18}$ for polynomially small error and $C_3(\log n)^{10}$ for constant error.

Li also used our construction to build an affine extractor for polylogarithmic min-entropy [Li15a]. In another work, Chattopadhyay and Li [CL16] used components from our construction to construct extractors for sumset sources, which allowed them to give improved extractors for sources that are generated by algorithms with access to limited memory.

1.1 Ramsey Graphs

Definition 1.3 (Ramsey graphs)**.** *A graph on N vertices is called a K-Ramsey graph if does not contain any independent set or clique of size K.*

It was shown by Erdös in one of the first applications of the probabilistic method that there exists K-Ramsey graphs for $K = 2\log N$. By explicit, we mean a polynomial-time algorithm that determines whether there is an edge between two nodes, i.e., the running time should be polylogarithmic in the number of nodes.

Frankl and Wilson [FW81] used intersection theorems to construct K-Ramsey graphs on N vertices, with $K = 2^{O(\sqrt{\log N \log\log N})}$. This remained the best known construction for a long time, with many other constructions [Alo98, Gro00, Bar06] achieving the same bound. Gopalan [Gop14] explained why approaches were stuck at this bound, showing that apart from [Bar06], all other constructions can be seen as derived from low-degree symmetric representations of the OR function. Finally, subsequent works by Barak et al. [BKS+10, BRSW12] obtained a significant improvement and gave explicit constructions of K-Ramsey graphs, with $K = 2^{2^{\log^{1-\alpha}(\log N)}}$, for some absolute constant α.

We also define a harder variant of Ramsey graphs.

Definition 1.4 (Bipartite Ramsey graph)**.** *A bipartite graph with N left vertices and N right vertices is called a bipartite K-Ramsey graph if it does not contain any complete $K \times K$-bipartite sub-graph or empty $K \times K$ sub-graph.*

Explicit bipartite K-Ramsey graphs were known for $K = \sqrt{N}$ based on the Hadamard matrix. This was slightly improved to $o(\sqrt{N})$ by Pudlak and Rődl [PR04], and the results of [BKS+10, BRSW12] in fact constructed bipartite K-Ramsey graphs, and hence achieved the bounds as mentioned above.

The following lemma is easy to obtain (see e.g.,[BRSW12]).

Lemma 1.5. *Suppose that for all $n \in \mathbb{N}$ there exists a polynomial time computable 2-source extractor $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ for min-entropy k and error $\epsilon < 1/2$. Let $N = 2^n$ and $K = 2^k$. Then there exists an explicit construction of a bipartite K-Ramsey on N vertices.*

Thus, Theorem 1 implies the following.

Theorem 3. *There exists a constant $C > 0$ such that for all large enough $n \in \mathbb{N}$, there exists an explicit construction of a bipartite K-Ramsey graph on $2N$ vertices, where $N = 2^n$ and $K = 2^{(\log\log N)^C}$.*

The parameter K in the above theorem can be taken to be $2^{C_1(\log\log N)^{74}}$, where C_1 is a large enough constant.

Given any bipartite K-Ramsey graph, a simple reduction gives a $K/2$-Ramsey graph on N vertices [BKS+10]. As an immediate corollary, we have explicit constructions of Ramsey graphs with the same bound.

Corollary 1.6. *There exists a constant $C > 0$ such that for all large enough $n \in \mathbb{N}$, there exists an explicit construction of a K-Ramsey graph on N vertices, where $N = 2^n$ and $K = 2^{(\log\log N)^C}$.*

Independent work: In independent work[1], Cohen [Coh16] used the challenge-response mechanism introduced in [BKS+10] with new advances in constructions of extractors to obtain a two-source disperser for polylogarithmic min-entropy. Using this, he obtained explicit constructions of bipartite-Ramsey graphs with $K = 2^{(\log\log N)^{O(1)}}$, which matches our result and thus provides an alternate construction.

1.2 Construction Overview

In this section, we describe our 2-source extractor construction. Since our construction is involved and uses a lot of components from prior work, we sometimes give informal definitions of these components for easier presentation. Further, some of the new components that we develop for our construction are important in their own right, and have applications in other areas. We discuss these applications in later sections.

An important component in our construction are explicit constructions of seeded extractors.

Definition 1.7 ([NZ96]). *A function $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a seeded extractor for min-entropy k and error ϵ if for any source $\mathbf{X}$ of min-entropy k, $|\mathrm{Ext}(\mathbf{X}, \mathbf{U}_d) - \mathbf{U}_m| \le \epsilon$. Ext is strong if, informally, the output of Ext is close to uniform even conditioned on the seed (with high probability), i.e., $|(\mathrm{Ext}(\mathbf{X}, \mathbf{U}_d), \mathbf{U}_d) - (\mathbf{U}_m, \mathbf{U}_d)| \le \epsilon$, where $\mathbf{U}_m$ and $\mathbf{U}_d$ are independent.*

We use explicit constructions of seeded extractors with almost optimal parameters i.e., $d = O(\log(n/\epsilon))$ and $m = \Omega(k)$ [LRVW03, GUV09, DKSS09].

To motivate our construction, first, let's try to build a 1-source extractor (even though we know it is impossible). Let $\mathbf{X}$ be an (n, k)-source, where $k = \mathrm{polylog}(n)$. Let Ext be a strong seeded extractor designed to extract 1 bit from min-entropy k with error ϵ. Since, for $(1-\epsilon)$-fraction of the seeds, the extractor output is close to uniform, a natural idea is to do the following: cycle over all the seeds of Ext and concatenate the outputs to obtain a D-bit string $\mathbf{Z}$ where most individual bits are close to uniform. Note that since the seed length of Ext is $O(\log n)$, $D = \mathrm{poly}(n)$. At this point, we might hope to take majority of these D bits of $\mathbf{Z}$ to obtain a bit is close to uniform. However, the output of Ext with different seeds may be correlated in arbitrary ways (even if individually the bits are close to uniform), so this approach doesn't work.

Our next idea is to try to fix this approach by introducing some independence among the uniform bits.

Definition 1.8. *A distribution $\mathcal{D}$ on n bits is t-wise independent if the restriction of $\mathcal{D}$ to any t bits is uniform. Further $\mathcal{D}$ is (t, ϵ)-wise independent if the distribution obtained by restricting $\mathcal{D}$ to any t coordinates is ϵ-close to uniform.*

For example, if we obtain a source $\mathbf{Z}$ such that $D - D^{0.49}$ bits are uniform, and further these bits are (almost) constant-wise independent, then it is known that the majority function can extract

[1] Cohen's work appeared before ours. When his paper appeared, we had an outline of the proof but had not filled in the details.

an almost-uniform bit [Vio14]. In an attempt to obtain such a source, we use a strong generalization of strong-seeded extractors, called as non-malleable extractors. Dodis and Wichs [DW09] introduced non-malleable extractors in the context of privacy amplification, and some connections to constructing extractors for independent sources was shown by Li [Li12a, Li12b]. Informally, the output of a non-malleable extractor looks uniform even given the seed and the output of the non-malleable extractor on a correlated seed. We require a slightly more general object.

Definition 1.9. *A function* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a* (t, k, ϵ)*-non-malleable extractor if it satisfies the following property: If* $\mathbf{X}$ *is a* (n, k)*-source and* $\mathbf{Y}$ *is uniform on* $\{0,1\}^d$*, and* f_1*,* $\ldots, f_t$ *are arbitrary functions from* d *bits to* d *bits with no fixed points*[2]*, then*

$$\begin{aligned}(\mathrm{nmExt}(\mathbf{X},\mathbf{Y}), \mathrm{nmExt}(\mathbf{X}, f_1(\mathbf{Y})), \ldots, \mathrm{nmExt}(\mathbf{X}, f_t(\mathbf{Y})), \mathbf{Y})\\ \approx_\epsilon (\mathbf{U}_m, \mathrm{nmExt}(\mathbf{X}, f_1(\mathbf{Y})), \ldots, \mathrm{nmExt}(\mathbf{X}, f_t(\mathbf{Y})), \mathbf{Y}).\end{aligned}$$

Let nmExt be a (t, k, ϵ)-non-malleable extractor that outputs 1 bit with seed-legth d, and let $D = 2^d$. We show in Lemma 3.4, that there exists large subset of seeds $S \subset \{0,1\}^d$, $|S| \geq (1 - O(\sqrt{\epsilon}))D$, such that for any t distinct seeds $s_1, \ldots, s_t$ in S, $|\mathrm{nmExt}(\mathbf{X}, s_1), \ldots, \mathrm{nmExt}(\mathbf{X}, s_t) - U_t| \leq O(t\sqrt{\epsilon})$. Thus, we could use our earlier idea of cycling through all seeds, but now using an explicit non-malleable extractor instead of a strong-seeded extactor. For this, we use recent constructions of such non-malleable extractors from the work of Chattopadhyay, Goyal and Li [CGL16] (see Theorem 3.2). Their construction requires min-entropy $k = O(t \log^2(n/\epsilon))$ and seed-length $d = O(t^2 \log^2(n/\epsilon))$. Thus, we could cycle over all the seeds of nmExt, and produce a string $\mathbf{Z}$ of length $D = 2^{O(t^2 \log^2(n/\epsilon))}$, such that the i'th bit of $\mathbf{Z}$, $\mathbf{Z}_i = \mathrm{nmExt}(\mathbf{X}, i)$. Further, except for at most $O(\sqrt{\epsilon}D)$ bits in $\mathbf{Z}$, the remaining bits in $\mathbf{Z}$ follow a $(t, O(t\sqrt{\epsilon}))$-wise independent distribution. We could now try to set parameters such that the majority function extracts a bit from $\mathbf{Z}$. However, it is easy to check that $\sqrt{\epsilon}D > D^{1-\delta}$, for any constant $\delta > 0$. Since the majority function can handle at most $\sqrt{D}$ bad bits, this idea fails.

Our next idea is to look for functions that can handle larger number of "bad bits" to extract from $\mathbf{Z}$. To formalize our ideas, we introduce the notion of resilient functions and non-oblivious bit-fixng sources.

Ben-Or and Linial [BL85] first studied resilient functions when they introduced the perfect information model. In the simplest version of this model, there are n computationally unbounded players that can each broadcast a bit once. At the end, some function is applied to the broadcast bits. In the collective coin-flipping problem, the output of this function should be a nearly-random bit. The catch is that some malicious coalition of players may wait to see what the honest players broadcast before broadcasting their own bits. Thus, a resilient function is one where the bit is unbiased even if the malicious coalition is relatively large (but not too large). We now introduce this notion more formally.

Definition 1.10 (Influence of a set)**.** *Let* $f : \{0,1\}^D \to \{0,1\}$ *be any Boolean function on variables* $x_1, \ldots, x_D$*. The influence of a set* $Q \subseteq \{x_1, \ldots, x_D\}$ *on* f*, denoted by* $\mathbf{I}_Q(f)$*, is defined to be the probability that* f *is undetermined after fixing the variables outside* Q *uniformly at random.*

Further, for any integer q define $\mathbf{I}_q(f) = \max_{Q \subseteq \{x_1,\ldots,x_D\}, |Q|=q} \mathbf{I}_Q(f)$. More generally, let $\mathbf{I}_{Q,\mathcal{D}}(f)$ denote the probability that f is undetermined when the variables outside Q are fixed by sampling from the distribution $\mathcal{D}$. We define $\mathbf{I}_{Q,t}(f) = \max_{\mathcal{D} \in \mathcal{D}_t} \mathbf{I}_{Q,\mathcal{D}}(f)$, where $\mathcal{D}_t$ is the set of all t-wise independent distributions. Similarly, $\mathbf{I}_{Q,t,\gamma}(f) = \max_{\mathcal{D} \in \mathcal{D}_{t,\gamma}} \mathbf{I}_{Q,\mathcal{D}}(f)$ where $\mathcal{D}_{t,\gamma}$ is the set of all (t, γ)-wise

[2] We say that x is a fixed point of a function f if $f(x) = x$.

independent distributions. Finally, for any integer q define $\mathbf{I}_{q,t}(f) = \max_{Q \subseteq \{x_1,\ldots,x_D\}, |Q|=q} \mathbf{I}_{Q,t}(f)$ and $\mathbf{I}_{q,t,\gamma}(f) = \max_{Q \subseteq \{x_1,\ldots,x_D\}, |Q|=q} \mathbf{I}_{Q,t,\gamma}(f)$.

Definition 1.11 (Resilient Function). *Let $f : \{0,1\}^D \to \{0,1\}$ be any Boolean function on variables $x_1, \ldots, x_D$ and q any integer. We say f is (q,ϵ)-resilient if $\mathbf{I}_q(f) \le \epsilon$. More generally, we say f is t-independent (q,ϵ)-resilient if $\mathbf{I}_{q,t}(f) \le \epsilon$ and f is (t,γ)-independent (q,ϵ)-resilient if $\mathbf{I}_{q,t,\gamma}(f) \le \epsilon$.*

We now continue with our attempt to extract a bit from the source $\mathbf{Z}$. To formalize our intuition of constructing an extractor for $\mathbf{Z}$ via resilient functions, we define a class of sources that captures $\mathbf{Z}$, and record a simple lemma which shows that resilient functions are indeed extractors for this class of sources.

Definition 1.12 (Non-Oblivious Bit-Fixing Sources). *A source $\mathbf{Z}$ on $\{0,1\}^D$ is called a (q,t,γ)-non-oblivious bit-fixing source (NOBF source for short) if there exists a subset of coordinates $Q \subseteq [D]$ of size at most q such that the joint distribution of the bits indexed by $\overline{Q} = [D] \setminus Q$ is (t,γ)-wise independent. The bits in the coordinates indexed by Q are allowed to depend arbitrarily on the bits in the coordinates indexed by $\overline{Q}$.*

Lemma 1.13. *Let $f : \{0,1\}^D \to \{0,1\}$ be a Boolean function such that for any t-wise independent distribution $\mathcal{D}$, $|\mathbf{E}_{\mathbf{x}\sim\mathcal{D}}[f(x)] - \frac{1}{2}| \le \epsilon_1$. Suppose for some $q > 0$, $\mathbf{I}_{q,t}(f) \le \epsilon_2$. Then, f is an extractor for (q,t,γ)-NOBF sources on D bits with error $\epsilon_1 + \epsilon_2 + \gamma D^t$.*

Thus, it is sufficient for us to construct an explicit resilient functions, since this can be used to extract from $\mathbf{Z}$. We note that for transforming the source $\mathbf{X}$ in to a (q,t,γ)-NOBF source $\mathbf{Z}$ (on D bits) via the non-malleable extractor, the min-entropy required in $\mathbf{X}$ is roughly $O(t^2 \log n)$. Unfortunately, for $t < \sqrt{n}$, the only known function that is t-independent (q,ϵ_1)-resilient function is the majority function [Vio14] for $t = O(1)$ and $q < D^{\frac{1}{2}-\tau}$, $\tau > 0$.

However, for larger t, there are better known resilient functions. In particular, the iterated majority function of Ben-Or and Linial handles a larger $q = O(D^{0.63})$ for $t = D$, but it is not clear if it remains resilient for smaller t. Further, Ajtai and Linial showed the existence of functions that are resilient for $q = O(D/\log^2 D)$ and $t = D$. However, their functions are not explicit and require time $D^{O(D^2)}$ to deterministically construct. We note here that by a result in [KKL88], the largest q one can hope to handle is $O(D/\log D)$.

Our main contribution here is to give explicit constructions of $(\log(D))^{O(1)}$-independent $(D^{1-\delta}, D^{-\Omega(1)})$-resilient functions. In particular, we prove the following theorem.

Theorem 4. *There exists a constant c such that for any $\delta > 0$ and every large enough integer $D \in \mathbb{N}$, there exists an efficiently computable monotone Boolean function $f : \{0,1\}^D \to \{0,1\}$ satisfying: For any $q > 0, t \ge c(\log D)^{18}$,*

- *f is a depth 4 circuit of size $D^{O(1)}$.*
- *For any (t,γ)-wise independent distribution $\mathcal{D}$, $|\mathbf{E}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})] - \frac{1}{2}| \le \frac{1}{D^{\Omega(1)}}$.*
- *$\mathbf{I}_{q,t}(f) \le q/D^{1-\delta}$.*

Our proof of Theorem 4 is based on derandomizing the probabilistic construction of Ajtai-Linial mentioned above. Further, we also have to argue that $\mathbf{I}_{q,t}(f)$ is bounded (instead of just $\mathbf{I}_q(f)$ as in Ajtai-Linial construction), which requires us to use a breakthrough result of Braverman [Bra10] that t-wise independence fools low-depth circuits. However, before outlining these ideas, we first assume Theorem 4 and try to complete our 2-source extractor construction.

Recall that $\mathbf{Z} = \text{nmExt}(\mathbf{X}, 1) \circ \ldots \circ \text{nmExt}(\mathbf{X}, D)$ is a (q, t, γ)-NOBF source on D bits, where $q = \sqrt{\epsilon} D, \gamma = O(\sqrt{\epsilon} t)$ and $D = 2^{O(t^2 \log^2(n/\epsilon))}$. We set $t = \log^{O(1)}(D)$, and thus we require $H_\infty(\mathbf{X}) = \log^{(O(1))}(n/\epsilon)$. As we observed before, $q > D^{1-\delta}$ for any $\delta > 0$. Thus, we cannot directly apply the function f from Theorem 4 on $\mathbf{Z}$ to extract an almost bit. (A more important issue in directly applying f to $\mathbf{Z}$ is that while using Lemma 4.1, we have to bound the term γD^t in the error, which is clearly greater than 1 for the current parameters.) We note that it is not suprising that f cannot extract from $\mathbf{Z}$ since we just used 1 source up to this point.

We now use the second independent source $\mathbf{Y}$ to sample a pseudorandom subset T of coordinates from $[D]$, $|T| = D' = n^{O(1)}$, such that the fraction of bad bits $\mathbf{Z}_T$ (the projection of $\mathbf{Z}$ to the coordiantes in T) remains almost the same as that of $\mathbf{Z}$ (with high probability). A well known way of using a weak source to sample a pseudorandom subset was discovered by Zuckerman [Zuc97], and uses a seeded extractor, with the size of the sample being the total number of seeds and fraction of bad bits increases at most by the error of the extractor (with high probability). Thus using known optimal constructions of seeded extractors with seed-length $d' = O(\log(n/\epsilon'))$, we have $D' = (n/\epsilon')^{O(1)}$. Thus $\mathbf{Z}_t$ is (q, t, γ)-NOBF source on D' bits, where $q = (\sqrt{\epsilon} + \epsilon')D', \gamma = O(\sqrt{\epsilon} t)$. Further, the incurred error on applying f (from Theorem 4) on $\mathbf{Z}_t$ is $(D')^{-\Omega(1)} + \gamma(D')^t$ (using Lemma 4.1). By choosing δ to be a small enough constant, the term $\epsilon' D'$ can be made smaller than $(D')^{1-\delta}/2$. Further, by choosing ϵ small enough $(n^{-(\log n)^{O(1)}})$, we can ensure that $\sqrt{\epsilon} D' < (D')^{1-\delta}/2$ and $\gamma D' = (D')^{-\Omega(1)}$. This completes the description of our 2-source extractor.

We now outline the main ideas in the proof of Theorem 4. We first show that if the function f is monotone, in AC^0 and almost unbiased, then it is enough to bound $\mathbf{I}_q(f)$ to show that f satisfies the conclusions of Theorem 4. The key observation is the following simple fact: for any set of variables Q, it is possible to check using another small AC^0 circuit $\mathcal{E}$ if the function f is undetermined for some setting of the variables outside Q. This crucially relies on the fact that f is monotone. Next, using the result of Braverman [Bra10] that bounded independence fools small AC^0 circuits, we conclude that the bias of the circuit $\mathcal{E}$ is roughly the same when the variables outside Q are drawn from a bounded-independence distribution, and when they are drawn from the uniform distribution. The conclusion now follows using the bound on $\mathbf{I}_Q(f)$.

Thus all that remains is to construct a small monotone AC^0 circuit f, that is almost balanced under the uniform distribution, and $\mathbf{I}_q(f) = o(1)$ for $q < D^{1-\delta}$. The high level idea for this construction is to derandomize the probabilistic construction of Ajtai-Linial [AL93] using extractors. The tribes function introduced by Ben-Or and Linial [BL85] is a disjunction taken over AND's of equi-sized blocks of variables. The Ajtai-Linial function is essentially a conjunction of non-monotone tribes functions, with each tribes function using a different partition and the variables in each tribes function being randomly negated with probability 1/2, and the partitions are chosen according to the probabilistic method. We sketch informally our ideas to derandomize this construction. For each $i \in [R]$, let P^i be a equi-partition of $[n]$, $n = MB$, into blocks of size B. Let P^i_j denote the j'th block in P^i. Define,

$$f(x) = \bigwedge_{1 \le i \le R} \bigvee_{1 \le j \le M} \bigwedge_{\ell \in P^i_j} x_\ell.$$

First, we abstract out properties that these partitions need to satisfy for f to be almost unbiased and also $(n^{1-\delta}, \epsilon)$-resilient. Informally, we show that

1. If for all i_1, i_2, j_1, j_2 with $(i_1, j_1) \neq (i_2, j_2)$, $|P^{i_1}_{j_1} \cap P^{i_2}_{j_2}| \le 0.9B$, then f is almost unbiased,

2. If for any set Q of size $q < n^{1-\delta}$, the number of partitions P^i containing a block P^i_j such that $|P^i_j \cap Q| > \delta B/2$ is $o(R)$, then f is $(n^{1-\delta}, \epsilon)$-resilient.

An ingredient in the proof of (1) is Janson's inequality (see Theorem 5.21).

It is important that unlike in Ajtai-Linial and earlier modifications [RZ01], we don't need to negate variables, and thus f is monotone.

The second property seems related to the property of extractors captured in Theorem 2.4. However, it is not obvious how to use such extractors to construct these partitions. We construct a family of equi-partitions from a seeded extractor $\mathrm{Ext} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ as follows. Each P^w corresponds to some $w \in \{0,1\}^r$. One block of P^w is $P^w_{\vec{0}} = \{(y, \mathrm{Ext}(x,y)) : y \in \{0,1\}^b\}$. The other block are shifts of this, i.e., for any $s \in \{0,1\}^m$, define $P^w_s = \{(y, \mathrm{Ext}(x,y) \oplus s) : y \in \{0,1\}^b\}$. This gives $R = 2^r$ partitions of $[n]$ with $n = 2^{m+b}$.

For any good enough extractor, we show that (2) is satisfied using a basic property of extractors and an averaging argument. To show that the partitions satisfy (1), we need an additional property of the extractor, which informally requires us to prove that the intersection of any two arbitrary shifts of neighbors of any two distinct nodes $w_1, w_2 \in \{0,1\}^r$ in G_{Ext} is bounded. This essentially is a strong variant of a design extractor of Li [Li12a]. We show that Trevisan's extractor has this property. This completes the informal sketch of our resilient function construction. We note that our actual construction is slightly more complicated and is a depth 4 circuit. The extra layer enables us to simulate each of the bits $x_1, \ldots, x_n$ having $\Pr[x_1 = 1]$ close to 1, which we need to make f almost unbiased.

1.3 Comparison with Previous Techniques

As mentioned earlier, Bourgain's 2-source extractor for min-entropy $0.499n$ relied on new advances in additive combinatorics. Following this, Rao [Rao09a] introduced a novel elementary approach for extracting from multiple independent sources that relied on only explicit seeded extractors. His approach was to first convert the independent sources into matrices with many uniformly random rows, called somewhere-random sources, and then iteratively reduce the number of rows in one of the somewhere-random sources (while still maintaining a good fraction of uniform rows) using the other somewhere-random sources. This allowed him to construct an explicit extractor for a constant number of sources with min-entropy n^γ for any constant $\gamma > 0$.

In a series of works [Li13b, Li13a, Li15c], Li introduced a new way of iteratively reducing the number of rows in the somewhere-random sources. His idea was to use a few independent sources to construct a more structured somewhere-random source with the additional guarantee that the uniform rows are t-wise independent and then iteratively reduce the number of rows using leader election protocols from the work of Feige [Fei99]. Using this approach and clever compositions of extractors, Li [Li15c] constructed an explicit extractor for 3 independent sources with polylogarithmic min-entropy.

In particular, Li had already shown how to use two sources to obtain a source with almost polylog-wise independent bits, except for 1/3 of the rows. Using a better seeded extractor in his construction could make the bad rows at most an $n^{-\Omega(1)}$ fraction. Thus, we could have used Li's construction to replace our Theorem 3.1. However, the rest of our construction is significantly different. Instead of iteratively reducing the number of bits in the non-oblivious source, we directly construct an explicit function that is an extractor for such sources.

1.4 Applications to Collective Coin-Flipping

Ben-Or and Linial [BL85] first studied resilient functions when they introduced the perfect information model. In the simplest version of this model, there are n computationally unbounded players that can each broadcast a bit once. At the end, some function is applied to the broadcast bits. In the collective coin-flipping problem, the output of this function should be a nearly-random bit. The catch is that some malicious coalition of players may wait to see what the honest players broadcast before broadcasting their own bits. Thus, a resilient function is one where the bit is unbiased even if the malicious coalition is relatively large (but not too large).

This model can be generalized to allow many rounds, and has been well studied [BL85, KKL88, Sak89, AL93, AN93, BN96, RZ01, Fei99, RSZ02]; also see the survey by Dodis [Dod06]. Resilient functions correspond to 1-round protocols. Thus, our construction of resilient functions directly implies an efficient 1-round coin-flipping protocol resilient to coalitions of size $n^{1-\delta}$, for any $\delta > 0$. The previous best published result for 1-round collective coin flipping was by Ben-Or and Linial [BL85], who could handle coalitions of size $O(n^{0.63})$. A non-explicit 1-round collective coin flipping protocol was given by Ajtai and Linial [AL93], where the size of the coalition could be as large as $O(n/\log^2 n)$. However, to deterministically simulate this protocol requires time at least $n^{O(n^2)}$. In unpublished work, Meka had achieved similar bounds to us. However, our results extend in ways that Meka's doesn't.

The following theorem is direct from Theorem 4, even ignoring the t-wise independent part; see e.g., Lemma 2 in [Dod06].

Theorem 5. *For any constant $\delta > 0$, for all $n > 0$ there exists an efficient one-round collective coin-flipping protocol in the perfect information model with n players that is $(n^{1-\delta}, n^{-\Omega(1)})$-resilient.*

1.5 Bit-Fixing Sources

As we discussed before, resilient functions can be used to build extractors for bit-fixing sources. We first formally define the notion of a deterministic extractor for a class of sources.

Definition 1.14. *An efficiently computable function $f : \{0,1\}^n \to \{0,1\}^m$ is a (deterministic) extractor for a class of sources $\mathcal{X}$ with error ϵ if, for any source $\mathbf{X} \in \mathcal{X}$, $|f(\mathbf{X}) - \mathbf{U}_m| \leq \epsilon$.*

Roughly, a bit-fixing source is a source where some subset of the bits are fixed and the remaining ones chosen in some random way. Usually these remaining bits are chosen uniformly at random, but in our case they are chosen t-wise independently. Extraction is easier if the fixed bits cannot depend on the random bits. Such sources are called oblivious bit-fixing sources, and have been investigated in a line of work [CGH+85, KZ07, GRS06, Rao09b]. The best known explicit extractors for oblivious sources work for min-entropy at least $\log^C(n)$ with exponentially small error [Rao09b], and from arbitrary min-entropy with polynomially small error [KZ07]. They have applications to cryptography [CGH+85, KZ07].

Resilient functions immediately give an extractor for the more difficult family of non-oblivious bit-fixing sources, where the fixed bits may depend on the random bits. While such an extractor outputs 1 bit, Kamp and Zuckerman [KZ07] observed that dividing the source into blocks and applying the function to each block can extract more bits. Using the iterated-majority function of Ben-Or and Linial [BL85] they obtained an extractor for min-entropy at least $n - O(n^{\log_3 2})$. They didn't use Ajtai-Linial because it is not explicit.

Our main result on extracting from bit-fixing sources is the following.

Theorem 6. *There exists a constant c such that for any constant $\delta > 0$, and for all $n \in \mathbb{N}$, there exists an explicit extractor* $\text{bitExt} : \{0,1\}^n \to \{0,1\}$ *for the class of (q,t,γ)-non-oblivious bit-fixing sources with error $n^{-\Omega(1)}$, where $q \le n^{1-\delta}, t \ge c\log^{18}(n)$ and $\gamma \le 1/n^{t+1}$.*

We note that the work of Kahn, Kalai and Linial [KKL88] implies that the largest q one could hope to handle is $O(n/\log n)$.

1.6 Organization

We introduce some preliminaries in Section 2. In Section 3, we reduce the problem of constructing extractors for two independent sources to the problem of extracting from (q,t,γ)-bit-fixing sources. We use Section 4 and 5 to prove Theorem 4. We use Section 6 to wrap up the proofs of Theorem 1 and Theorem 6. Finally, we present a proof sketch of Theorem 2 in Section 7.

2 Preliminaries

We reserve the letter e for the base of the natural logarithm. We use $\ln(x)$ for $\log_e(x)$, and $\log(x)$ for $\log_2(x)$.
We use $\mathbf{U}_m$ to denote the uniform distribution on $\{0,1\}^m$.
For any integer $t > 0$, $[t]$ denotes the set $\{1,\dots,t\}$.
For a string y of length n, and any subset $S \subseteq [n]$, we use y_S to denote the projection of y onto the coordinates indexed by S.
Without explicitly stating it, we sometimes assume when needed that n is sufficiently large so that asymptotic statements imply concrete inequalities, e.g., if $\ell = o(n)$ then we may assume that $\ell < n/10$.

2.1 Seeded Extractors

We use the following strong seeded extractor constructed by Trevisan [Tre01], with subsequent improvements by Raz, Reingold and Vadhan [RRV02].

Theorem 2.1 ([Tre01] [RRV02])**.** *For every $n,k,m \in \mathbb{N}$ and $\epsilon > 0$, with $m \le k \le n$, there exists an explicit strong-seeded extractor* $\text{TExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for min-entropy k and error ϵ, where $d = O\left(\frac{\log^2(n/\epsilon)}{\log(k/m)}\right)$.*

We also use optimal constructions of strong-seeded extractors.

Theorem 2.2 ([GUV09])**.** *For any constant $\alpha > 0$, and all integers $n,k > 0$ there exists a polynomial time computable strong-seeded extractor* $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with $d = O(\log n + \log(1/\epsilon))$ and $m = (1-\alpha)k$.*

To ensure that for each $x \in \{0,1\}^n$, $\text{Ext}(x,s_1) \ne \text{Ext}(x,s_2)$ whenever $s_1 \ne s_2$, we can concatenate the seed to the output of Ext, though it is no longer strong.

Corollary 2.3. *For any constant $\alpha > 0$, and all integers $n,k > 0$ there exists a polynomial time computable seeded extractor* $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with $d = O(\log n + \log(1/\epsilon))$ and $m = (1-\alpha)k$. Further for all $x \in \{0,1\}^n$, $\text{Ext}(x,s_1) \ne \text{Ext}(x,s_2)$ whenever $s_1 \ne s_2$.*

2.2 Sampling Using Weak Sources

A well known way of sampling using weak sources uses randomness extractors. We first introduce a graph-theoretic view of extractors. Any seeded extractor $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ can also be viewed as an unbalanced bipartite graph G_{Ext} with 2^n left vertices (each of degree 2^d) and 2^m right vertices. We use $\mathcal{N}(x)$ to denote the set of neighbours of x in G_{Ext}. We call G_{Ext} the graph corresponding to Ext.

Theorem 2.4 ([Zuc97])**.** *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a seeded extractor for min-entropy* k *and error* ϵ*. Let* $D = 2^d$*. Then for any set* $R \subseteq \{0,1\}^m$*,*

$$|\{x \in \{0,1\}^n : ||\mathcal{N}(x) \cap R| - \mu_R D| > \epsilon D\}| < 2^k,$$

where $\mu_R = |R|/2^m$*.*

Theorem 2.5 ([Zuc97])**.** *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a seeded extractor for min-entropy* k *and error* ϵ*. Let* $\{0,1\}^d = \{r_1, \ldots, r_D\}$*,* $D = 2^d$*. Define* $\mathrm{Samp}(x) = \{\mathrm{Ext}(x, r_1), \ldots, \mathrm{Ext}(x, r_D)\}$*. Let* $\mathbf{X}$ *be an* $(n, 2k)$*-source. Then for any set* $R \subseteq \{0,1\}^m$*,*

$$\mathbf{Pr}_{\mathbf{x} \sim \mathbf{X}}[||\mathrm{Samp}(\mathbf{x}) \cap R| - \mu_R D| > \epsilon D] < 2^{-k},$$

where $\mu_R = |R|/2^m$*.*

2.3 An Inequality

We frequently use the following inequality.

Claim 2.6. *For any* $n > 1$ *and* $0 \leq x \leq n$*, we have*

$$e^{-x}\left(1 - \frac{x^2}{n}\right) \leq \left(1 - \frac{x}{n}\right)^n \leq e^{-x}.$$

2.4 Some Probability Lemmas

Lemma 2.7 ([GRS06])**.** *Let* $\mathbf{X}$ *be a random variable taking values in a set* S*, and let* $\mathbf{Y}$ *be a random variable on* $\{0,1\}^t$*. Assume that* $|(\mathbf{X}, \mathbf{Y}) - (\mathbf{X}, \mathbf{U}_t)| \leq \epsilon$*. Then for every* $y \in \{0,1\}^t$*,*

$$|(\mathbf{X}|Y = y) - \mathbf{X}| \leq 2^{t+1}\epsilon.$$

Lemma 2.8 ([Sha08])**.** *Let* $\mathbf{X}_1, \mathbf{Y}_1$ *be random variables taking values in a set* S_1*, and let* $\mathbf{X}_2, \mathbf{Y}_2$ *be random variables taking values in a set* S_2*. Suppose that*

1. $|\mathbf{X}_2 - \mathbf{Y}_2| \leq \epsilon_2$*.*
2. *For every* $s_2 \in S_2$*,* $|(\mathbf{X}_1|\mathbf{X}_2 = s_2) - (\mathbf{Y}_1|Y_2 = s_2)| \leq \epsilon_1$*.*

Then

$$|(\mathbf{X}_1, \mathbf{X}_2) - (\mathbf{Y}_1, \mathbf{Y}_2)| \leq \epsilon_1 + \epsilon_2.$$

Using the above results, we record a useful lemma.

Lemma 2.9. *Let $\mathbf{X}_1, \ldots, \mathbf{X}_t$ be random variables, such that each $\mathbf{X}_i$ takes values 0 and 1. Further suppose that for any subset $S = \{s_1, \ldots, s_r\} \subseteq [t]$,*

$$(\mathbf{X}_{s_1}, \mathbf{X}_{s_2} \ldots, \mathbf{X}_{s_r}) \approx_\epsilon (\mathbf{U}_1, \mathbf{X}_{s_2} \ldots, \mathbf{X}_{s_r}).$$

Then

$$(\mathbf{X}_1, \ldots, \mathbf{X}_t) \approx_{5t\epsilon} \mathbf{U}_t.$$

Proof. We prove this by induction on t. The base case when $t = 1$ is direct. Thus, suppose $t \geq 2$. It follows that

$$(\mathbf{X}_t, \mathbf{X}_1, \ldots, \mathbf{X}_{t-1}) \approx_\epsilon (\mathbf{U}_1, \mathbf{X}_1, \ldots, \mathbf{X}_{t-1}).$$

By an application of Lemma 2.7, for any value of the bit b,

$$|(\mathbf{X}_1, \ldots, \mathbf{X}_{t-1} | \mathbf{X}_t = b) - (\mathbf{X}_1, \ldots, \mathbf{X}_{t-1})| \leq 4\epsilon.$$

Further, by the induction hypothesis, we have

$$|(\mathbf{X}_1, \ldots, \mathbf{X}_{t-1}) - \mathbf{U}_{t-1}| \leq 5(t-1)\epsilon.$$

Thus, by the triangle inequality for statistical distance, it follows that for any value of the bit b,

$$|(\mathbf{X}_1, \ldots, \mathbf{X}_{t-1} | \mathbf{X}_t = b) - \mathbf{U}_{t-1}| \leq (5t-1)\epsilon.$$

Using Lemma 2.8 and the fact that $|\mathbf{X}_t - \mathbf{U}_1| \leq \epsilon$, it follows that

$$|(\mathbf{X}_1, \ldots, \mathbf{X}_t) - \mathbf{U}_t| \leq (5t-1)\epsilon + \epsilon = 5t\epsilon.$$

This completes the induction, and the lemma follows. □

2.5 Extractors for Bit-fixing Sources via Resilient Functions

The following lemma connects the problem of constructing extractors for (q, t, γ)-non-oblivious bit-fixing sources and constructing (t, γ)-independent (q, ϵ_1)-resilient functions.

Lemma 2.10. *Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function that is (t, γ)-independent (q, ϵ_1)-resilient. Further suppose that for any (t, γ)-wise independent distribution $\mathcal{D}$, $|\mathbf{E}_{\mathbf{x} \sim \mathcal{D}}[f(\mathbf{x})] - \frac{1}{2}| \leq \epsilon_2$. Then f is an extractor for (q, t, γ)-non-oblivious bit-fixing sources with error $\epsilon_1 + \epsilon_2$.*

Proof. Let $\mathbf{X}$ be a (q, t, γ)-non-oblivious bit-fixing source on n bits. Then $\mathbf{X}$ is sampled in the following way: For some fixed subset $Q \subset \{x_1, \ldots, x_n\}$ of q variables, the variables $\overline{Q} = [n] \setminus Q$ are drawn from some fixed (t, γ)-wise independent distribution $\mathcal{D}_1$ on $n - q$ bits, and the variables in Q are chosen arbitrarily depending on the values of the variables in $\overline{Q}$.

Let E be the following event: f is determined on fixing the variables in $\overline{Q}$ by sampling from $\mathcal{D}_1$ and leaving the remaining variables free. Since f is (t, γ)-independent (q, ϵ_1)-resilient, we have $\mathbf{Pr}[E] \geq 1 - \epsilon_1$. Let $\mathcal{D}$ be any (t, γ)-wise independent distribution on n bits whose projection on to $\overline{Q}$ matches $\mathcal{D}_1$. It follows that

$$\left| \mathbf{Pr}_{\mathbf{x} \sim \mathcal{D}}[f(\mathbf{x}) = 1] - \frac{1}{2} \right| \leq \epsilon_2.$$

We have,

$$\begin{aligned}
\mathbf{Pr}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})=1] &= \mathbf{Pr}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})=1|E]\mathbf{Pr}[E] + \mathbf{Pr}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})=1|\overline{E}]\mathbf{Pr}[\overline{E}] \\
&= \mathbf{Pr}_{\mathbf{x}\sim\mathbf{X}}[f(\mathbf{x})=1|E]\mathbf{Pr}[E] + \mathbf{Pr}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})=1|\overline{E}]\mathbf{Pr}[\overline{E}] \\
&= \mathbf{Pr}_{\mathbf{x}\sim\mathbf{X}}[f(\mathbf{x})=1] + \mathbf{Pr}[\overline{E}]\left(\mathbf{Pr}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})=1|\overline{E}] - \mathbf{Pr}_{\mathbf{x}\sim\mathbf{X}}[f(\mathbf{x})=1|\overline{E}]\right)
\end{aligned}$$

Hence,

$$|\mathbf{Pr}_{\mathbf{x}\sim\mathcal{D}}[f(\mathbf{x})=1] - \mathbf{Pr}_{\mathbf{x}\sim\mathbf{X}}[f(\mathbf{X})=1]| \leq \mathbf{Pr}[\overline{E}] \leq \epsilon_1.$$

Thus,

$$\left|\mathbf{Pr}_{\mathbf{x}\sim\mathbf{X}}[f(\mathbf{x})=1] - \frac{1}{2}\right| \leq \epsilon_1 + \epsilon_2.$$

□

3 Reduction to a NOBF Source

The main result in this section is a reduction from the problem of extracting from two independent (n,k)-sources to the task of extracting from a single (q,t,γ)-NOBF source on $n^{O(1)}$ bits. We formally state the reduction in the following theorem.

Theorem 3.1. *There exist constants $\delta, c' > 0$ such that for every $n, t > 0$ there exists a polynomial time computable function* reduce : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^D$, *$D = n^{O(1)}$, satisfying the following property: if $\mathbf{X}, \mathbf{Y}$ are independent (n,k)-sources with $k \geq c't^4 \log^2 n$, then*

$$\mathbf{Pr}_{\mathbf{y}\sim\mathbf{Y}}[\mathrm{reduce}(\mathbf{X},\mathbf{y}) \textit{ is a } (q,t,\gamma)\textit{-NOBF source}] \geq 1 - n^{-\omega(1)}$$

where $q = D^{1-\delta}$ and $\gamma = 1/D^{t+1}$.

Li had earlier proved a similar theorem with $q = D/3$, and his methods would extend to achieve a similar bound as we achieve.

The δ we obtain in Theorem 3.1 is a small constant. Further, it can be shown that for our reduction method, it is not possible to achieve $\delta > 1/2$. Thus, we cannot use the majority function as the extractor for the resulting (q,t,γ)-NOBF source.

The reduction in Theorem 3.1 is based on explicit constructions of non-malleable extractors (introduced in the following section) from the recent work of Chattopadhyay, Goyal and Li [CGL16].

3.1 Non-Malleable Extractors

Non-malleable extractors were introduced by Dodis and Wichs [DW09] as a generalization of strong-seeded extractors. Recently, Chattopadhyay, Goyal and Li [CGL16] constructed an explicit t-non-malleable extractor for polylogarithmic min-entropy. This is a crucial component in our reduction.

Theorem 3.2 ([CGL16])**.** *There exists a constant $c' > 0$ such that for all $n, t > 0$ there exists an explicit (t,k,ϵ)-non-malleable extractor* nmExt : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}$, *where $k \geq c't\log^2(n/\epsilon)$ and $d = O\left(t^2 \log^2(n/\epsilon)\right)$.*

3.2 The Reduction

In the following lemma, we reduce extracting from two independent sources to extracting from a (q, t, γ)-NOBF source using non-malleable extractors and seeded extractors in a black-box way. Theorem 3.1 then follows by plugging in explicit constructions of these components.

Lemma 3.3. *Let* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}$ *be a* (t, k, ϵ_1)*-non-malleable extractor and let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^{d_2} \to \{0,1\}^{d_1}$ *be a seeded extractor for min-entropy* $k/2$ *with error* ϵ_2*. Let* $\{0,1\}^{d_2} = \{s_1, \ldots, s_{D_2}\}$*,* $D_2 = 2^{d_2}$*. Suppose that* Ext *satisfies the property that for all* $y \in \{0,1\}^n$*,* $\mathrm{Ext}(y, s) \neq \mathrm{Ext}(y, s')$ *whenever* $s \neq s'$*. Define the function:*

$$\mathrm{reduce}(x, y) = \mathrm{nmExt}(x, \mathrm{Ext}(y, s_1)) \circ \ldots \circ \mathrm{nmExt}(x, \mathrm{Ext}(y, s_{D_2})).$$

If $\mathbf{X}$ *and* $\mathbf{Y}$ *are independent* (n, k)*-sources, then*

$$\mathbf{Pr}_{\mathbf{y}\sim\mathbf{Y}}[\mathrm{reduce}(\mathbf{X}, \mathbf{y}) \textit{ is a } (q, t, \gamma)\textit{-NOBF source}] \geq 1 - n^{-\omega(1)},$$

where $q = (\sqrt{\epsilon_1} + \epsilon_2)D_2$ *and* $\gamma = 5t\sqrt{\epsilon_1}$*.*

We prove a lemma about t-non-malleable extractors from which Lemma 3.3 is easy to obtain.

Lemma 3.4. *Let* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}$ *be a* (t, k, ϵ)*-non-malleable extractor. Let* $\{0,1\}^d = \{s_1, \ldots, s_D\}$*,* $D = 2^d$*. Let* $\mathbf{X}$ *be any* (n, k)*-source. There exists a subset* $R \subseteq \{0,1\}^d$*,* $|R| \geq (1 - \sqrt{\epsilon})D$ *such that for any distinct* $r_1, \ldots, r_t \in R$*,*

$$(\mathrm{nmExt}(\mathbf{X}, r_1), \ldots, \mathrm{nmExt}(\mathbf{X}, r_t)) \approx_{5t\sqrt{\epsilon}} \mathbf{U}_t.$$

Proof. Let

$$\begin{aligned} BAD = \{r \in \{0,1\}^d : \exists \text{ distinct } r_1, \ldots, r_t \in \{0,1\}^d,\\ \forall i \in [t]\ r_i \neq r, \text{ s.t } |(\mathrm{nmExt}(\mathbf{X}, r), \mathrm{nmExt}(\mathbf{X}, r_1), \ldots, \mathrm{nmExt}(\mathbf{X}, r_t)) -\\ (\mathbf{U}_1, \mathrm{nmExt}(\mathbf{X}, r_1), \ldots, \mathrm{nmExt}(\mathbf{X}, r_t))| > \sqrt{\epsilon}\} \end{aligned}$$

We define adversarial functions $f_1, \ldots, f_t$ as follows. For each $r \in BAD$, set $f_i(r) = r_i$, $i = 1, \ldots, t$ (the f_i's are defined arbitrarily for $r \notin BAD$, only ensuring that there are no fixed points). Let $\mathbf{Y}$ be uniform on $\{0,1\}^d$. It follows that

$$|(\mathrm{nmExt}(\mathbf{X}, \mathbf{Y}), \mathrm{nmExt}(\mathbf{X}, f_1(\mathbf{Y})), \ldots, \mathrm{nmExt}(\mathbf{X}, f_t(\mathbf{Y}))) -$$
$$(\mathbf{U}_1, \mathrm{nmExt}(\mathbf{X}, f_1(\mathbf{Y})), \ldots, \mathrm{nmExt}(\mathbf{X}, f_t(\mathbf{Y})))| \geq \frac{\sqrt{\epsilon}}{2^d}|BAD|$$

Thus $|BAD| \leq \sqrt{\epsilon}2^d$ using the property that nmExt is a (k, t, ϵ)-non-malleable extractor. Define $R = \{0,1\}^d \setminus BAD$. Using Lemma 2.9, it follows that R satisfies the required property. □

of Lemma 3.3. Let $R \subseteq \{0,1\}^{d_1}$ be such that for any distinct $r_1, \ldots, r_t \in R$,

$$(\mathrm{nmExt}(\mathbf{X}, r_1), \ldots, \mathrm{nmExt}(\mathbf{X}, r_t)) \approx_{5t\sqrt{\epsilon_1}} \mathbf{U}_t.$$

It follows by Lemma 3.4 that $|R| \geq (1 - \sqrt{\epsilon_1})D_1$. Define $\mathrm{Samp}(y) = \{\mathrm{Ext}(y, s_1), \ldots, \mathrm{Ext}(y, s_{D_2})\} \subset \{0,1\}^{d_1}$. Using Theorem 2.5, we have

$$\Pr_{\mathbf{y}\sim\mathbf{Y}}[|\mathrm{Samp}(\mathbf{y}) \cap R| \leq (1 - \sqrt{\epsilon_1} - \epsilon_2)D_2] \leq 2^{-k/2}. \tag{1}$$

Consider any $\mathbf{y}$ such that $|\mathrm{Samp}(\mathbf{y}) \cap R| \geq (1 - \sqrt{\epsilon_1} - \epsilon_2)D_2$, and let $\mathbf{Z_y} = \mathrm{reduce}(\mathbf{X}, \mathbf{y})$. Since the output bits of nmExt corresponding to seeds in $\mathrm{Samp}(\mathbf{y}) \cap R$ are $(t, 5t\sqrt{\varepsilon_1})$-wise independent, we have that $\mathbf{Z_y}$ is a $((\sqrt{\epsilon_1} + \epsilon_2)D_2, t, 5t\sqrt{\varepsilon_1})$-NOBF source on D_2 bits.

Thus using (1), it follows that with probability at least $1 - 2^{-k/2}$ over $\mathbf{y} \sim \mathbf{Y}$, $\mathrm{reduce}(\mathbf{X}, \mathbf{y})$ is a $((\sqrt{\epsilon_1} + \epsilon_2)D_2, t, 5t\sqrt{\epsilon_1})$-NOBF source on D_2 bits. □

of Theorem 3.1. We derive Theorem 3.1 from Lemma 3.3 by plugging in explicit non-malleable extractors and seeded extractors as follows:

1. Let $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}$ be an explicit (t, k, ϵ_1)-non-malleable extractor from Theorem 3.2. Thus $d_1 = c_1 t^2 \log^2(n/\epsilon_1)$, for some constant c_1. Such an extractor exists as long as $k \geq \lambda_1 t \log^2(n/\epsilon_1)$ for some constant λ_1.

2. Let $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{d_1}$ be the extractor from Corollary 2.3 set to extract from min-entropy $k/2$ with error ϵ_2. Thus $d = c_2 \log(n/\epsilon_2)$ for some constant c_2. Let $D = 2^d = (n/\epsilon_2)^{c_2}$. Such an extractor exists as long as $k \geq 3d_1$.

3. We choose $\epsilon_1, \epsilon_2, \delta$ such that the following hold:

   - $(\sqrt{\epsilon_1} + \epsilon_2)D \leq D^{1-\delta}$.
   - $\sqrt{\epsilon_1} \leq 1/(5tD^{t+1})$.
   - $\delta' = \delta c_2 < 9/10$.

   To satisfy the above requirements, we pick ϵ_1, ϵ_2 as follows: Let $\epsilon_2 = 1/n^{C_2}$ where C_2 is fixed such that $\epsilon_2 D \leq D^{1-\delta}/2$. Thus, we need to ensure that
   $\epsilon_2 \leq 1/(2D^\delta)$. Substituting $D = (n/\epsilon_2)^{c_2}$ and simplifying, we have

   $$\begin{aligned} \epsilon_2 &\leq \epsilon_2^{c_2\delta}/2n^{c_2\delta} \\ \text{i.e.,} \qquad \epsilon_2^{1-c_2\delta} &\leq 1/2n^{c_2\delta} \\ \text{i.e.,} \qquad \epsilon_2 &\leq 1/(2n)^{\delta'/(1-\delta')}. \end{aligned}$$

   We note that $1 - \delta' > 1/10$. Thus, we can choose $C_2 = 10$.

   We now set $\epsilon_1 = 1/n^{C_1 t}$, where we choose the constant C_1 such that $\sqrt{\epsilon_1} \leq 1/(5tD^{t+1})$. Simplifying, we have

   $$\epsilon_1 \leq \frac{\epsilon_2^{2c_2(t+1)}}{25t^2 n^{2c_2(t+1)}} \leq \frac{1}{25t^2 n^{2c_2(C_2+1)(t+1)}} \leq \frac{1}{n^{23c_2(t+1)}}.$$

   Thus, we can choose $C_1 = 24c_2$.

4. We note that for the above choice of parameters, nmExt and Ext indeed work for min-entropy $k \geq c' t^4 \log^2 n$, for some large constant c'.

5. Let $\{0,1\}^d = \{s_1, \ldots, s_D\}$.

Define the function:

$$\mathrm{reduce}(x, y) = \mathrm{nmExt}(x, \mathrm{Ext}(y, s_1)) \circ \ldots \circ \mathrm{nmExt}(x, \mathrm{Ext}(y, s_D)).$$

Let $\mathbf{X}$ and $\mathbf{Y}$ be independent (n,k)-sources. By Lemma 3.3, it follows that

$$\mathbf{Pr}_{\mathbf{y} \sim \mathbf{Y}}[\mathrm{reduce}(\mathbf{X}, \mathbf{y}) \text{ is a } (q, t, \gamma)\text{-NOBF source}] \geq 1 - n^{-\omega(1)},$$

where $q = (\sqrt{\epsilon_1} + \epsilon_2)D$ and $\gamma = 5t\sqrt{\epsilon_1}$. Theorem 3.1 now follows by our choice of parameters. □

4 Monotone Constant-Depth Resilient Functions are t-Independent Resilient

Using the reduction from Section 3, we have now reduced the problem of extracting from two independent sources to extracting from a (q, t, γ)-NOBF source. By Lemma 4.1 this translates to constructing a nearly balanced function f with small $\mathbf{I}_{q,t,\gamma}(f)$. We show if f is a constant depth monotone circuit, then in order to prove an upper bound for $\mathbf{I}_{q,t,\gamma}(f)$, it is in fact enough to upper bound $\mathbf{I}_q(f)$, which is a simpler quantity to handle.

Theorem 4.1. *There exists a constant $b > 0$ such that the following holds: Let $\mathcal{C} : \{0,1\}^n \to \{0,1\}$ be a monotone circuit in AC^0 of depth d and size m such that $|\mathbf{E}_{\mathbf{x}\sim\mathbf{U}_n}[\mathcal{C}(x)] - \frac{1}{2}| \leq \epsilon_1$. Suppose $q > 0$ is such that $\mathbf{I}_q(\mathcal{C}) \leq \epsilon_2$. If $t \geq b(\log(5m/\epsilon_3))^{3d+6}$, then $\mathbf{I}_{q,t}(\mathcal{C}) \leq \epsilon_2 + \epsilon_3$ and $\mathbf{I}_{q,t,\gamma}(\mathcal{C}) \leq \epsilon_2 + \epsilon_3 + \gamma n^t$. Further, for any distribution $\mathcal{D}$ that is (t, γ)-wise independent, $|\mathbf{E}_{x\sim\mathcal{D}}[\mathcal{C}(x)] - \frac{1}{2}| \leq \epsilon_1 + \epsilon_3 + \gamma n^t$.*

We first briefly sketched the main ideas of the proof in the introduction.

We now formally prove Theorem 4.1. We recall the result of Braverman [Bra10], which was recently refined by Tal [Tal14].

Theorem 4.2 ([Bra10] [Tal14])**.** *Let $\mathcal{D}$ be any $t = t(m, d, \epsilon)$-wise independent distribution on $\{0,1\}^n$. Then for any circuit $\mathcal{C} \in AC^0$ of depth d and size m,*

$$|\mathbf{E}_{\mathbf{x}\sim\mathbf{U}_n}[\mathcal{C}(\mathbf{x})] - \mathbf{E}_{\mathbf{x}\sim\mathcal{D}}[\mathcal{C}(\mathbf{x})]| \leq \epsilon$$

where $t(m, d, \epsilon) = O(\log(m/\epsilon))^{3d+3}$.

We also recall a result about almost t-wise independent distributions.

Theorem 4.3 ([AGM03])**.** *Let $\mathcal{D}$ be a (t, γ)-wise independent distribution on $\{0,1\}^n$. Then there exists a t-wise independent distribution that is $n^t\gamma$-close to $\mathcal{D}$.*

of Theorem 4.1. The bound on $\mathbf{E}_{\mathbf{x}\sim\mathcal{D}}[\mathcal{C}(\mathbf{x})]$ is direct from Theorem 4.2 and Theorem 4.3. We now proceed to prove the influence property.

Consider any set Q of variables, $|Q| = q$. Let $\overline{Q} = [n] \setminus Q$. We construct a function $\mathcal{E}_Q : \{0,1\}^{n-q} \to \{0,1\}$ such that $\mathcal{E}_Q(y) = 1$ if and only if $\mathcal{C}$ is undetermined when $x_{\overline{Q}}$ is set to y. Thus, it follows that

$$\mathbf{E}_{\mathbf{y}\sim\mathbf{U}_{n-q}}[\mathcal{E}_Q(\mathbf{y})] = \mathbf{Pr}_{\mathbf{y}\sim\mathbf{U}_{n-q}}[\mathcal{E}_Q(\mathbf{y}) = 1] = \mathbf{I}_Q(\mathcal{C}) \leq \epsilon_2.$$

Let $\mathcal{D}$ be any t-wise independent distribution. We have,

$$\mathbf{E}_{\mathbf{y}\sim\mathcal{D}}[\mathcal{E}_Q(\mathbf{y})] = \mathbf{Pr}_{\mathbf{y}\sim\mathcal{D}}[\mathcal{E}_Q(\mathbf{y}) = 1] = \mathbf{I}_{Q,\mathcal{D}}(\mathcal{C}).$$

Thus to prove that $\mathbf{I}_{Q,\mathcal{D}}(\mathcal{C}) \leq \epsilon_2 + \epsilon_3$, it is enough to prove that

$$|\mathbf{E}_{\mathbf{y}\sim\mathbf{U}_{n-q}}[\mathcal{E}_Q(\mathbf{y})] - \mathbf{E}_{\mathbf{y}\sim\mathcal{D}}[\mathcal{E}_Q(\mathbf{y})]| \leq \epsilon_3. \tag{2}$$

We construct $\mathcal{E}_Q$ as follows: Let $\mathcal{C}_0$ be the circuit obtained from $\mathcal{C}$ by setting all variables in Q to 0. Let $\mathcal{C}_1$ be the circuit obtained from $\mathcal{C}$ by setting all variables in Q to 1. Define $\mathcal{E}_Q := \neg(\mathcal{C}_0 = C_1)$. Since $\mathcal{C}$ is monotone, $\mathcal{E}_Q$ satisfies the required property. Further $\mathcal{E}_Q$ can be computed by a circuit in AC^0 of depth $d + 2$ and size $4m + 3$. It can be checked that the depth of $\mathcal{E}_Q$ can be reduced to $d + 1$ by combining two layers. Thus (2) now directly follows from Theorem 4.2. The bound on $\mathbf{I}_{\mathcal{C},t,\gamma}(q)$ follows from an application of Theorem 4.3. $\square$

5 Monotone Boolean functions in AC^0 Resilient to Coalitions

The main result in this section is an explicit construction of a constant depth monotone circuit f which is resilient to coalitions and is almost balanced under the uniform distribution. This is the final ingredient in our construction of a 2-source extractor.

Theorem 5.1. *For any $\delta > 0$, and every large enough integer n, there exists a polynomial time computable monotone Boolean function $f : \{0,1\}^n \to \{0,1\}$ satisfying:*

- *f is a depth 4 circuit in AC^0 of size $n^{O(1)}$.*
- $\left|\mathbf{E}_{\mathbf{x}\sim\mathbf{U}_n}[f(\mathbf{x})] - \frac{1}{2}\right| \leq \frac{1}{n^{\Omega(1)}}$.
- *For any $q > 0$, $\mathbf{I}_q(f) \leq q/n^{1-\delta}$.*

We first prove Theorem 4, which follows easily from the above theorem.

Proof of Theorem 4. Let $f : \{0,1\}^n \to \{0,1\}$ be the function from Theorem 5.1 such that for any $q > 0$, $\mathbf{I}_q(f) \leq q/n^{1-\frac{\delta}{2}}$. Also we have that f is monotone and is a depth 4 AC^0 circuit.

Fix $\epsilon_3 = 1/n$. Thus by Theorem 4.1, it follows that there exists a constant b such that for any $t \geq b(\log(5n/\epsilon_3))^{18}$, $q > 0$,

$$\mathbf{I}_{q,t,\gamma}(f) \leq \epsilon_3 + \frac{q}{n^{1-\frac{\delta}{2}}} \leq \frac{q}{n^{1-\delta}}.$$

Further, using Theorem 4.1, for any t-wise independent distribution $\mathcal{D}$, we have

$$\left|\mathbf{E}_{\mathbf{x}\sim\mathcal{D}}[f(x)] - \frac{1}{2}\right| \leq \frac{1}{n} + \frac{1}{n^{\Omega(1)}}.$$

□

The remainder of this section is used to prove Thereom 5.1. Our starting point is the work of Ajtai and Linial [AL93], who proved the existence of functions computable by linear sized depth 3 circuits in AC^0 that are $(\Omega(n/\log^2 n), \epsilon)$-resilient. However, this construction is probabilistic, and deterministically finding such functions requires time $n^{O(n^2)}$. Further these functions are not guaranteed to be monotone (or even unate). We provide some intuition of our construction in the introduction.

We initially construct a depth 3 circuit which works, but then the inputs have to be chosen from independent Bernoulli distributions where the probability p of 1 is very different from 1/2. By observing that we can approximate this Bernoulli distribution with a CNF on uniform bits, we obtain a depth 4 circuit which works for uniformly random inputs.

5.1 Our Construction and Key Lemmas

Construction 1: Let $\mathrm{Ext} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be a strong-seeded extractor set to extract from min-entropy $k = 2\delta r$ with error $\epsilon \leq \delta/4, b = \delta_1 m$, $\delta_1 = \delta/20$, and output length $m = \delta r$. Assume that Ext is such that $\epsilon > 1/M^{\delta_1}$. Let $R = 2^r$, $B = 2^b$, $M = 2^m$ and $K = 2^k$. Let $s = BM$. Thus $s = M^{1+\delta_1}$.

Let $\{0,1\}^r = \{v_1, \dots, v_R\}$. We define a collection of R equi-partitions of $[s]$, $\mathcal{P} = \{P^{v_1}, \dots, P^{v_R}\}$ as follows: Let G_{Ext} be the bipartite graph corresponding to Ext and let $\mathcal{N}(x)$, for any $x \in \{0,1\}^r$, denote the neighbours of x in G_{Ext}. For some $v \in \{0,1\}^r$, let $\mathcal{N}(v) = \{z_1, \ldots, z_B\}$. For each $w \in \{0,1\}^m$, the set $\{(j, z_j \oplus w) : j \in \{0,1\}^b\}$ is defined to be a block in P^v, where $\oplus$ denotes the bit-wise XOR of the two strings. Note that P^v indeed forms an equi-partition of $[s]$ with M blocks of size B.

Define the function $f_{\mathrm{Ext}} : \{0,1\}^s \to \{0,1\}$ as:

$$f_{\mathrm{Ext}}(y) = \bigwedge_{1 \le i \le R} \bigvee_{1 \le j \le M} \bigwedge_{\ell \in P^i_j} y_\ell.$$

Let

$$\gamma = \frac{\ln M - \ln \ln(R/\ln 2)}{B}.$$

We prove the following lemmas from which the proof of Theorem 5.1 is straightforward. We first introduce some definitions.

Definition 5.2 ((n,τ)-Bernoulli distribution)**.** *A distribution on n bits is an (n,τ)-Bernoulli distribution, denoted by $\mathbf{Ber}(n,\tau)$, if each bit is independently set to 1 with probability τ and set to 0 with probability $1-\tau$.*

Lemma 5.3. *Let $\mathrm{Ext} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be the extractor used in Construction 1. For any constant $\epsilon_1 > 0$, let $(1 - B^{-\epsilon_1})\gamma \le p_1 \le \gamma$. Then there exists a constant $\delta > 0$ such that for any $q > 0$,*

$$\mathbf{I}_{q,\mathbf{Ber}(s,1-p_1)}(f_{\mathrm{Ext}}) \le \frac{q}{s^{1-\delta}}.$$

The following generalizes the notion of a design extractor which was introduced by Li [Li12a].

Definition 5.4 (Shift-design extractor)**.** *Let $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be a strong-seeded extractor. Let $D = 2^d$. If for any distinct $x, x' \in \{0,1\}^n$, and arbitrary $y, y' \in \{0,1\}^m$*

$$|\{(h, \mathrm{Ext}(x,h) \oplus y) : h \in \{0,1\}^d\} \cap \{(h, \mathrm{Ext}(x',h) \oplus y') : h \in \{0,1\}^d\}| \le (1-\eta)D,$$

then Ext is called an η-shift-design extractor.

Lemma 5.5. *Let $\mathrm{Ext} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be the extractor used in Construction 1. Suppose Ext is a $\frac{1}{10}$-shift-design extractor. For any constant $\epsilon_1 > 0$, let $(1 - B^{-\epsilon_1})\gamma \le p_1 \le \gamma$. Then, the following holds:*

$$\left| \mathbf{E}_{\mathbf{y} \sim \mathbf{Ber}(s,1-p_1)}[f_{\mathrm{Ext}}(\mathbf{y})] - \frac{1}{2} \right| \le B^{-\Omega(1)}.$$

Lemma 5.6. *Let $\mathrm{TExt} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be the Trevisan extractor from Theorem 2.1 with parameters as in Construction 1. Then, TExt is a $\frac{1}{10}$-shift-design extractor.*

Lemma 5.7. *Suppose $\gamma < 9/10$. Then for any $\nu > 0$, there exists an explicit size h monotone CNF $\mathcal{C}$ on h bits, where $h = O\left(\frac{1}{\nu} \ln\left(\frac{1}{\nu}\right)\right)$, such that $\gamma - \nu \le \mathbf{Pr}_{\mathbf{x} \sim \mathbf{U}_h}[\mathcal{C}(\mathbf{x}) = 0] < \gamma$.*

We first show how to derive Theorem 5.1 from the above lemmas.

Proof of Theorem 5.1. Let $\mathrm{TExt} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$ be the Trevisan extractor from Theorem 2.1 with parameters as in Construction 1: $k = 2\delta r, m = \delta r, \delta_1 = \delta/20$ and $\epsilon = 2^{-\delta_2 \sqrt{r}}$ where δ_2

is chosen appropriately such that the seed length of TExt from Theorem 2.1 is (for some constant λ)

$$b = \frac{\lambda \log^2(r/\epsilon)}{\log(k/m)} = \frac{\lambda \log^2(r/2^{-\delta_2\sqrt{r}})}{\log 2} = \lambda(\delta_2^2 r + \log^2 r + 2\delta_2\sqrt{r}\log r) = \delta_1 \delta r = \delta_1 m.$$

Thus, indeed $M^{-\delta_1} < \epsilon < \delta/4$.

We now fix the parameter r as follows. Let the parameter ν in Lemma 5.7 be set to γ/B^{ϵ_1}, where $\epsilon_1 = \delta/4$ and let $\mathcal{C}$ be the size h monotone CNF circuit guaranteed by Lemma 5.7, where $h < B^{1+2\epsilon_1}$. Thus, $(1 - B^{-\epsilon_1})\gamma \leq \mathbf{Pr}_{\mathbf{x}\sim\mathbf{U}_h}[\mathcal{C}(\mathbf{x}) = 0] < \gamma$.

Choose the largest integer r such that for $m = \delta r$, we have $n' = sh = BMh < n$. It follows that for this choice of r, $n' = \Omega(n)$. We construct our function on n' bits. The size of the coalition is at most $n^{1-\delta} = (n')^{1-\delta'}$, where $\delta' = \delta - o(1)$. Thus, we may assume $n = n' = BMh$ and $\delta = \delta'$. Thus $n = BMh < M^{1+\delta_1+(1+2\epsilon_1)\delta_1}$ and $B = n^{\Omega(1)}$.

We now use Construction 1 and construct the function $f_{\mathrm{TExt}} : \{0,1\}^s \to \{0,1\}$, where we instantiate Ext with extractor TExt as set up above. Let f be the function derived from f_{TExt} by replacing each variable y_i by a copy of the monotone CNF $\mathcal{C}$ set up above. Since TExt is a polynomial time function, f_{TExt} can be constructed in polynomial time. Thus f is computable by a polynomial time algorithm. Further, f is an $O(RMBh) = n^{O(1)}$ sized monotone circuit in AC^0 of depth 4.

We observe that,

$$\begin{aligned}
s^{1-\frac{\delta}{2}} &= (MB)^{1-\frac{\delta}{2}} \\
&> (MB)^{\left(1+\frac{\delta}{2}\right)(1-\delta)} \\
&> (MB^3)^{1-\delta} && \text{(since } M^{\delta/2} > B^2\text{)} \\
&\geq (MBh)^{1-\delta} = n^{1-\delta}.
\end{aligned}$$

This calculation and Lemma 5.7 yields that

$$\mathbf{I}_{n^{1-\delta}}(f) \leq \mathbf{I}_{s^{1-\frac{\delta}{2}},\mathbf{Ber}(s,1-p_1)}(f_{\mathrm{TExt}}).$$

Using Lemma 5.3, it follows that

$$\mathbf{I}_{q,\mathbf{Ber}(s,1-p_1)}(f_{\mathrm{Ext}}) \leq \frac{q}{s^{1-\frac{\delta}{2}}} < \frac{q}{n^{1-\delta}}.$$

We now bound the bias of f. By Lemma 5.6, we have that TExt is a $\frac{1}{10}$-shift-design extractor. Thus by Lemma 5.5, we have

$$\left|\mathbf{E}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f_{\mathrm{TExt}}(\mathbf{y})] - \frac{1}{2}\right| \leq B^{-\Omega(1)} = n^{-\Omega(1)}.$$

Finally, using Lemma 5.7, it follows that

$$\left|\mathbf{E}_{\mathbf{x}\sim\mathbf{U}_n}[f(\mathbf{x})] - \frac{1}{2}\right| \leq \frac{1}{n^{\Omega(1)}}$$

. ∎

Proof of Lemma 5.6. To prove that TExt is a $\frac{1}{10}$-shift-design extractor, we first recall the construction of the Trevisan extractor $\mathrm{TExt} : \{0,1\}^r \times \{0,1\}^b \to \{0,1\}^m$.

For any input $y \in \{0,1\}^r$, we describe the construction of the Trevisan extractor [Tre01,RRV02] to obtain the first bit of the output since this is enough for the purpose of this proof. Fix an asymptotically good binary linear error correcting code $\mathcal{C}'$ with constant relative rate α, block length $\bar{r} = (r+1)/\alpha$, and relative distance $\frac{1}{2} - \beta$, where $\beta < \epsilon$. Further assume that $\mathcal{C}'$ contains the all 1's string $\vec{1}$. Let $\{v_1, \ldots, v_{r+1}\}$ be a basis of C' with $v_{r+1} = \vec{1}$. Let $\mathcal{C}$ be the binary linear code generated by $\{v_1, \ldots, v_r\}$ i.e., $\mathcal{C} = \mathrm{span}\{v_1, \ldots, v_r\}$. It follows that $\mathcal{C}$ does not contain $\vec{1}$, has relative rate $\alpha(1 - \frac{1}{\bar{r}}) > 0.9\alpha$ and relative distance $\frac{1}{2} - \beta$. Let $\mathrm{Enc} : \{0,1\}^r \to \{0,1\}^{\bar{r}}$ be the encoding function of $\mathcal{C}$.

Further fix a subset $S_1 \subset [b]$ of size $\log(\bar{r})$. Then the first bit of the output of TExt on input y and seed z is the bit at the z_{S_1}'th coordinate of the string $c_y = \mathrm{Enc}(y)$. Thus, as we cycle over all seeds z, each bit of the string c_y appears equally often.

For any $x \in \{0,1\}^r$, define

$$T_x^0 = \{(h, \mathrm{TExt}(x,h)_{[1]}) : h \in \{0,1\}^b\}, \qquad T_x^1 = \{(h, \mathrm{TExt}(x,h)_{[1]} \oplus 1) : h \in \{0,1\}^b\}.$$

Let x, x' be any two distinct r bit strings. It follows by our argument above, and the fact that C' is a linear code with distance $\frac{1}{2} - \beta$ containing $\vec{1}$ that $|T_x^{b_1} \cap T_{x'}^{b_2}| \leq (\frac{1}{2} + \beta)B < 0.9B$ for any two bits b_1 and b_2.

Let $y, y' \in \{0,1\}^m$. Let the first bit of y be b_1 and the first bit of y' be b_2. Thus,

$$|\{(h, \mathrm{TExt}(x,h) \oplus y) : h \in \{0,1\}^b\} \cap \{(h, \mathrm{TExt}(x',h) \oplus y') : h \in \{0,1\}^b\}| \leq |T_x^{b_1} \cap T_{x'}^{b_2}| \leq 0.9B.$$

□

Proof of Lemma 5.7. Let $h_2 = \lceil \log(2/\nu) \rceil$, and let h_1 be the largest integer such that $(1-2^{-h_2})^{h_1} \geq 1 - \gamma$. Thus,

$$\begin{aligned}(1-\gamma) \leq (1-2^{-h_2})^{h_1} &\leq (1-\gamma)/(1-2^{-h_2}) \\ &< (1-\gamma)(1+2^{1-h_2}) \\ &\leq (1-\gamma)(1+\nu) \\ &< 1-\gamma+\nu\end{aligned}$$

and $h_1 = O(2^{h_2})$.

Define

$$\mathcal{C}(x) = \bigwedge_{g_1=1}^{h_1} \bigvee_{g_2=1}^{h_2} x_{g_1,g_2}.$$

and $h = h_1 h_2 = O(h_2 2^{h_2}) = O\left(\frac{1}{\nu}\log\left(\frac{1}{\nu}\right)\right)$.

Thus $\mathbf{Pr}_{\mathbf{x}\sim\mathbf{U}_h}[\mathcal{C}(\mathbf{x}) = 0] = 1 - (1-2^{-h_2})^{h_1}$, and hence

$$\gamma - \nu \leq \mathbf{Pr}_{\mathbf{x}\sim\mathbf{U}_h}[\mathcal{C}(\mathbf{x}) = 0] \leq \gamma.$$

□

We now proceed to prove Lemma 5.3 and Lemma 5.5.

For convenience, define

$$f^i_{\text{Ext}}(y) = \bigvee_{1\le j\le M} \bigwedge_{\ell\in P^i_j} y_\ell$$

where $i \in \{0,1\}^r$. Further, let

$$p_2 = (1-p_1)^B, \quad p_3 = (1-p_2)^M.$$

We record two easy claims.

Claim 5.8. *For any $i \in \{0,1\}^r, j \in \{0,1\}^m$, $\mathbf{Pr}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[\bigwedge_{\ell\in P^i_j} \mathbf{y}_\ell = 1] = (1-p_1)^B = p_2$.*

Claim 5.9. *For any $i \in \{0,1\}^r$, $\mathbf{Pr}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f^i_{\text{Ext}}(\mathbf{y}) = 0] = (1-p_2)^M = p_3$.*

We frequently use the following bounds.

Claim 5.10. *The following inequalities hold: Let $\epsilon_2 = \epsilon_1/2$. Then,*

1. $\frac{\ln R - \ln\ln 2}{M}\left(1-\frac{1}{B^{\epsilon_2}}\right) \le p_2 \le \frac{\ln R-\ln\ln 2}{M}\left(1+\frac{1}{B^{\epsilon_2}}\right) \le \frac{r}{M}$.
2. $\frac{1}{2R} \le \left(\frac{\ln 2}{R}\right)\left(1-\frac{2r}{B^{\epsilon_2}}\right) \le p_3 \le \left(\frac{\ln 2}{R}\right)\left(1+\frac{r}{B^{\epsilon_2}}\right) \le \frac{0.9}{R}$.

Proof. We have,

$$\begin{aligned} p_2 = (1-p_1)^B \ge (1-\gamma)^B \ge e^{-\gamma B}(1-\gamma^2 B) && \text{(by Claim 2.6)} \\ \ge \frac{\ln R - \ln\ln 2}{M}\left(1-\frac{r^2}{B}\right) && \text{(since } \gamma < (\ln M)/B < r/B) \end{aligned}$$

We now upper bound p_2. We have,

$$\begin{aligned} p_2 &\le (1-\gamma(1-B^{-\epsilon_1}))^B \le e^{-\gamma B(1-B^{-\epsilon_1})} && \text{(by Claim 2.6)} \\ &< \left(\frac{\ln R - \ln\ln 2}{M}\right) M^{B^{-\epsilon_1}} < \left(\frac{\ln R-\ln\ln 2}{M}\right) e^{\delta r B^{-\epsilon_1}} \\ &\le \frac{\ln R - \ln\ln 2}{M}\left(1+\frac{r}{B^{\epsilon_1}}\right) \end{aligned}$$

Thus,

$$\frac{\ln R - \ln\ln 2}{M}\left(1-\frac{1}{B^{\epsilon_2}}\right) \le p_2 \le \frac{\ln R - \ln\ln 2}{M}\left(1+\frac{1}{B^{\epsilon_2}}\right),$$

since $\epsilon_2 = \epsilon_1/2$.

Estimating similarly as above, we have

$$
\begin{aligned}
p_3 &= (1-p_2)^M \\
&\geq \left(1-\left(\frac{\ln R - \ln\ln 2}{M}\right)\left(1+\frac{1}{B^{\epsilon_2}}\right)\right)^M \\
&\geq \left(1-\frac{(\ln R - \ln\ln 2)^2}{M}\left(1+\frac{1}{B^{\epsilon_2}}\right)^2\right)\left(\frac{\ln 2}{R}\right)e^{\frac{-(\ln R-\ln\ln 2)}{B^{\epsilon_2}}} && \text{(by Claim 2.6)} \\
&\geq \left(1-\frac{2r^2}{M}\right)\left(\frac{\ln 2}{R}\right)e^{-r/B^{\epsilon_2}} \\
&\geq \left(1-\frac{2r^2}{M}\right)\left(\frac{\ln 2}{R}\right)\left(1-\frac{r}{B^{\epsilon_2}}\right) \\
&\geq \left(1-\frac{2r}{B^{\epsilon_2}}\right)\left(\frac{\ln 2}{R}\right).
\end{aligned}
$$

Finally, we have

$$
\begin{aligned}
p_3 &\leq \left(1-\left(\frac{\ln R - \ln\ln 2}{M}\right)\left(1-\frac{1}{B^{\epsilon_2}}\right)\right)^M \\
&\leq \left(\frac{\ln 2}{R}\right)^{1-B^{-\epsilon_2}} && \text{(by Claim 2.6)} \\
&\leq \left(\frac{\ln 2}{R}\right)2^{r/B^{\epsilon_2}} \leq \left(\frac{\ln 2}{R}\right)\left(1+\frac{r}{B^{\epsilon_2}}\right).
\end{aligned}
$$

Thus,

$$\left(\frac{\ln 2}{R}\right)\left(1-\frac{2r}{B^{\epsilon_2}}\right) \leq p_3 \leq \left(\frac{\ln 2}{R}\right)^{1-\frac{r}{B}} \leq \left(\frac{\ln 2}{R}\right)\left(1+\frac{r}{B^{\epsilon_2}}\right).$$

□

5.2 Proof of Lemma 5.3 : Bound on Influence of Coalitions on f_{Ext}

We now proceed to bound the influence of coalitions of variables on f_{Ext}.

Claim 5.11. *For any $i \in \{0,1\}^r$ and $q \leq s^{1-\delta}$, $\mathbf{I}_{q,\mathbf{Ber}(s,1-p_1)}(f^i_{\text{Ext}}) \leq \frac{1}{R}$.*

Proof. Let Q be any set of variables of size q, $q \leq s^{1-\delta}$. There are at most q blocks of P^i which contain a variable from Q. By Claim 5.8, it follows that the probability that for a y sampled from $\mathbf{Ber}(s, 1-p_1)$, there is no AND gate at depth 1 in f^i_{Ext} which outputs 1 is at most

$$
\begin{aligned}
(1-p_2)^{M-q} &\leq p_3^{1-\frac{s^{1-\delta}}{M}} \\
&\leq p_3(2R)^{\frac{s^{1-\delta}}{M}} && \text{(since } p_3 > 1/(2R) \text{ by Claim 5.10)} \\
&\leq p_3 e^{r/M^{\delta/2}} && \text{(since } s = M^{1+\delta_1} < M^{1+\frac{\delta}{2}}/2) \\
&< \frac{1}{R} && \text{(since } p_3 < 0.9/R \text{ by Claim 5.10)}
\end{aligned}
$$

Thus the influence of Q is bounded by $\frac{1}{R}$. □

Definition 5.12. *For any $i \in \{0,1\}^r$ and $j \in \{0,1\}^m$, define a block P^i_j to be bad with respect to a subset of variables Q if $|P^i_j \cap Q| \geq 2\epsilon B$. Further call a partition P^i bad with respect to Q if it has a block which is bad. Otherwise, P^i is good.*

Claim 5.13. *Consider any subset of variables Q of size q. If $q \leq s^{1-\delta}$, then there are less than KM bad partitions with respect to Q.*

Proof. Suppose to the contrary that there are at least KM bad partitions. It follows by an averaging argument that there exists $j \in \{0,1\}^m$ such that the number of bad blocks among the $\{P^i_j : i \in \{0,1\}^r\}$ is at least K. Define the function $\mathrm{Ext}_j(x,y) = \mathrm{Ext}(x,y) \oplus j$. Observe that Ext_j is a seeded extractor for min-entropy k with error ϵ.

Let $\mathcal{N}_j(x)$ denote the set of neighbours of x in the graph corresponding to Ext_j. It follows that $|\{|\mathcal{N}_j(x) \cap Q| \geq 2\epsilon B|\}| \geq K$. We note that $q/M = s^{1-\delta}/M = (MB)^{1-\delta}/M < 1/M^{\delta/19} < \epsilon$, since $\epsilon > 1/M^{\delta_1} = 1/M^{\delta/20} > 1/M^{\delta/19}$. Thus, we have

$$|\{|\mathcal{N}_j(x) \cap Q| \geq (\epsilon + \mu_Q)B\}| \geq K,$$

where $\mu_Q = q/M$. However this contradicts Theorem 2.4. Thus the number of bad blocks is bounded by KM. $\square$

Claim 5.14. *Let P^i be a partition that is good with respect to a subset of variables Q, $|Q| = q$. If $q \leq s^{1-\delta}$, then $\mathbf{I}_{Q,\mathbf{Ber}(s,1-p_1)}(f_{\mathrm{Ext}}) \leq \frac{q}{2s^{1-\delta}}$.*

Proof. We note that there are at least $M - q$ blocks in P^i that do not have any variables from Q. Each of the remaining blocks have at most $2\epsilon B$ variables from Q. An assignment of x leaves f^i_{Ext} undetermined only if: (a) there is no AND gate at depth 1 in f^i_{Ext} which outputs 1 and (b) There is at least one block with a variable from Q such that the non-Q variables are all set to 1. These two events are independent. Further, by Claim 5.11, the probability of (a) is bounded by $1/R$. We now bound the probability of (b). If there are h variables of Q in P^i_j, the probability that the non-Q variables are all 1's is exactly $(1-p_1)^{B-h}$. Thus the probability of event (b) is bounded by

$$\begin{aligned}
q(1-p_1)^{B(1-2\epsilon)} &= qp_2^{1-2\epsilon} \\
&\leq \frac{qr}{M^{1-2\epsilon}} && \text{(since } p_2 < r/M \text{ by Claim 5.10)} \\
&= \frac{qr}{M^{1-\frac{\delta}{2}}} && \text{(since } \epsilon < \delta/4) \\
&< \frac{q}{M^{1-\frac{2\delta}{3}}} && \text{(using } r = M^{o(1)}) \\
&< \frac{q}{2s^{1-\delta}} && \text{(since } s = M^{1+\delta_1} < M^{1+\frac{\delta}{4}}).
\end{aligned}$$

$\square$

Thus for any $q \leq s^{1-\delta}$,

$$\mathbf{I}_{q,\mathbf{Ber}(s,1-p_1)}(f_{\mathrm{Ext}}) \leq \frac{KM}{R} + \frac{q}{2s^{1-\delta}} = \frac{1}{R^{1-3\delta}} + \frac{q}{2s^{1-\delta}} < \frac{q}{s^{1-\delta}}.$$

$\square$

5.3 Proof of Lemma 5.5: Bound on the Bias of f_{Ext}

We now proceed to show that f_{Ext} is almost balanced. For ease of presentation, we slightly abuse notation and relabel the partitions in Construction 1 as $P^1, \ldots, P^R$, where for any $i \in [R]$, P^i corresponds to the partition P^{v_i} with v_i being the r bit string for the integer $i-1$.

Claim 5.15. *There exists a small constant $\epsilon_3 > 0$ such that for any $i \in \{0,1\}^r$, $\mathbf{Pr}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f^i_{\text{Ext}}(\mathbf{y}) = 1] = 1 - \frac{\alpha}{R}$, where $1 - \frac{1}{B^{\epsilon_3}} \leq \frac{\alpha}{\ln 2} \leq 1 + \frac{1}{B^{\epsilon_3}}$.*

Proof. Directly follows from Claim 5.10. $\square$

We now estimate the probability $\mathbf{Pr}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f_{\text{Ext}}(\mathbf{y}) = 0]$. This is not direct since the f^i_{Ext}'s are on the same set of variables, and can be correlated in general. Towards estimating this, we introduce some definitions.

Definition 5.16. *Let P^i, P^j be two equi-partitions of $[s]$ with blocks of size B. Then (P^i, P^j) is said to be pairwise-good if the size of the intersection of any block of P^i and any block of P^j is at most $0.9B$.*

Definition 5.17. *Let $P^1, \ldots, P^R$ be equi-partitions of $[s]$ with blocks of size B. A collection of partitions $\mathcal{P} = \{P^1, \ldots, P^R\}$ is pairwise-good if for any distinct $i, j \in \{0,1\}^r$, (P^i, P^j) is pairwise-good.*

Lemma 5.18. *If $\mathcal{P}$ is pairwise-good, then $|\mathbf{E}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f_{\text{Ext}}(\mathbf{y})] - \frac{1}{2}| \leq \frac{1}{B^{\Omega(1)}}$.*

Lemma 5.19. *The set of partitions $\mathcal{P} = \{P^1, \ldots, P^R\}$ in Construction 1 is pairwise-good.*

It is clear that the above two lemmas directly imply that $|\mathbf{E}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f_{\text{Ext}}(\mathbf{y})] - \frac{1}{2}| \leq \frac{1}{B^{\Omega(1)}}$.

Proof of Lemma 5.19. Let $P^{i_1}_{j_1}$ and $P^{i_2}_{j_2}$ be any two blocks such that $i_1 \neq i_2$. We need to prove that $|P^{i_1}_{j_1} \cap P^{i_2}_{j_2}| \leq 0.9B$. Recall that $P^{i_1}_{j_1} = \{(z, \text{Ext}(i_1, z) \oplus j_1) : z \in \{0,1\}^b\}$, and similarly $P^{i_2}_{j_2} = \{(z, \text{Ext}(i_2, z) \oplus j_2) : z \in \{0,1\}^b\}$. The bound on $|P^{i_1}_{j_1} \cap P^{i_2}_{j_2}|$ now directly follows from the fact that Ext is a $\frac{1}{10}$-shift-design extractor. $\square$

Proof of Lemma 5.18. Let $\mathcal{P} = \{P^1, \ldots, P^R\}$ be pairwise-good.

Recall that
$$p_3 = \mathbf{Pr}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f^i_{\text{Ext}}(\mathbf{y}) = 0] = \frac{\alpha}{R}.$$

Let y be sampled from $\mathbf{Ber}(s, 1-p_1)$. Let E_i be the event $f^i_{\text{Ext}}(y) = 0$. We have,

$$p = \mathbf{Pr}_{\mathbf{y}\sim\mathbf{Ber}(s,1-p_1)}[f_{\text{Ext}}(\mathbf{y}) = 0] = \mathbf{Pr}\left[\bigvee_{1\leq i\leq R} E_i\right].$$

For $1 \leq c \leq R$, let

$$S_c = \sum_{1\leq i_1<\ldots<i_c\leq R} \mathbf{Pr}\left[\bigwedge_{1\leq g\leq c} E_{i_g}\right].$$

Using the Bonferroni inequalities, it follows that for any even $a \in [R]$,

$$\sum_{c=1}^{a} (-1)^{(c-1)} S_c \leq p \leq \sum_{c=1}^{a+1} (-1)^{(c-1)} S_c. \tag{3}$$

Towards proving a tight bound on p using (3), we prove the following lemma.

Lemma 5.20. *There exist constants $\beta_1, \beta_2 > 0$ such that for any $c \leq s^{\beta_1}$, and arbitrary $1 \leq i_1 < \ldots < i_c \leq R$, the following holds:*

$$\left(\frac{\alpha}{R}\right)^c \leq \mathbf{Pr}\left[\bigwedge_{1 \leq g \leq c} E_{i_g}\right] \leq \left(\frac{\alpha}{R}\right)^c \left(1 + \frac{1}{M^{\beta_2}}\right).$$

To prove the above lemma, we recall Janson's inequality [Jan90, BS89]. We follow the presentation in [AS92].

Theorem 5.21 (Janson's Inequality [Jan90, BS89, AS92])**.** *Let Ω be a finite universal set and let $\mathcal{O}$ be a random subset of Ω constructed by picking each $h \in \Omega$ independently with probability p_h. Let $Q_1, \ldots, Q_\ell$ be arbitrary subsets of Ω, and let $\mathcal{E}_i$ be the event $Q_i \subseteq \mathcal{O}$. Define*

$$\Delta = \sum_{i<j : Q_i \cap Q_j \neq \emptyset} \mathbf{Pr}\left[\mathcal{E}_i \wedge \mathcal{E}_j\right], \qquad D = \prod_{i=1}^{\ell} \mathbf{Pr}\left[\overline{\mathcal{E}_i}\right].$$

Assume that $\mathbf{Pr}[\mathcal{E}_i] \leq \tau$ for all $i \in [\ell]$. Then

$$D \leq \mathbf{Pr}\left[\bigwedge \overline{\mathcal{E}_i}\right] \leq D e^{\frac{\Delta}{1-\tau}}.$$

$\square$

Proof of Lemma 5.20. We set $\beta_1 = 1/90$ with foresight. Without loss of generality suppose $i_g = g$ for $g \in [c]$. We use Janson's inequality with $\Omega = [s]$, and $\mathcal{O}$ constructed by picking each $h \in [s]$ with probability $1 - p_1$. Further let $\mathcal{E}_{i,j}$ be the event that $P_j^i \subseteq \mathcal{O}$. Intuitively, $\mathcal{O}$ denotes the set of coordinates in y that are set to 1 for a sample y from $\mathbf{Ber}(s, 1 - p_1)$. With this interpretation, the event $f^i_{\mathrm{Ext}}(y) = 0$ exactly corresponds to the event $\bigwedge_{1 \leq j \leq M} \overline{\mathcal{E}_{i,j}}$. Thus, we have

$$\mathbf{Pr}\left[\bigwedge_{1 \leq g \leq c} E_g\right] = \mathbf{Pr}\left[\bigwedge_{i \in [c], j \in \{0,1\}^m} \overline{\mathcal{E}_{i,j}}\right].$$

We now estimate D, Δ, γ to apply Janson's inequality. For any $i \in [c], j \in \{0,1\}^m$, we have $\mathbf{Pr}[\mathcal{E}_{i,j}] = \mathbf{Pr}[P_j^i \subseteq \mathcal{O}] = (1 - p_1)^B = p_2$. Note that $\tau = p_2 < \frac{1}{2}$. Further

$$D = \prod_{i \in [c], j \in \{0,1\}^m} \mathbf{Pr}\left[\overline{\mathcal{E}_{i,j}}\right] = (1 - p_2)^{Mc} = p_3^c = \left(\frac{\alpha}{R}\right)^c.$$

Finally, we have

$$\Delta = \sum_{i_1 < i_2 \in [c], j_1, j_2 \in \{0,1\}^m : P_{j_1}^{i_1} \cap P_{j_1}^{i_1} \neq \emptyset} \mathbf{Pr}[\mathcal{E}_{i_1, j_1} \wedge \mathcal{E}_{i_2, j_2}]$$

We observe that any P_j^i can intersect at most B blocks of another partition $P^{i'}$. Thus, the total number of blocks that intersect between two partitions P^i and P^j is bounded by $MB = s$. Further, recall that $\mathcal{P}$ is pairwise-good. Thus it follows that for any distinct $i_1, i_2 \in [c]$, and $j_1, j_2 \in \{0,1\}^m$, $|P_{j_1}^{i_1} \cap P_{j_2}^{i_2}| \leq 0.9B$. Thus, $|P_{j_1}^{i_1} \cup P_{j_2}^{i_2}| \geq 1.1B$ and hence for any $i_1 < i_2 \in [c], j_1, j_2 \in \{0,1\}^m$,

$$\mathbf{Pr}[\mathcal{E}_{i_1,j_1} \wedge \mathcal{E}_{i_2,j_2}] \leq (1-p_1)^{\frac{11B}{10}} = p_2^{\frac{11}{10}}.$$

By Claim 5.10, $p_2 \leq \frac{r}{M}$. Thus,

$$\Delta \leq \binom{c}{2} s p_2^{\frac{11}{10}} < \frac{s^{1+2\beta_1} r^2}{M^{\frac{11}{10}}} = \frac{(MB)^{1+2\beta_1} r^2}{M^{\frac{11}{10}}} = \frac{B^{1+2\beta_1} r^2}{M^{\frac{1}{10}-2\beta_1}} = \frac{M^{\delta_1(1+2\beta_1)} r^2}{M^{\frac{1}{10}-2\beta_1}} < \frac{r^2}{M^{\frac{1}{20}-3\beta_1}}.$$

Recall $\beta_1 = 1/90$. It follows that

$$\Delta < M^{-\beta'},$$

where $\beta' = 1/70$.

Invoking Janson's inequality, we have

$$\left(\frac{\alpha}{R}\right)^c \leq \mathbf{Pr}\left[\bigwedge_{1 \leq g \leq c} E_g\right] \leq \left(\frac{\alpha}{R}\right)^c e^{2M^{-\beta'}} \leq \left(1 + \frac{3}{M^{\beta'}}\right)\left(\frac{\alpha}{R}\right)^c.$$

This concludes the proof. □

Fix $a = s^{\beta_3}$ (assume that a is even), $\beta_3 = \min\{\beta_1/2, \beta_2/1000\}$, where β_1, β_2 are the constants in Lemma 5.20.

The following lemma combined with (3) proves a tight bound on p (recall that $p = \mathbf{Pr}_{\mathbf{y} \sim \mathbf{Ber}(s, 1-p_1)}[f_{\text{Ext}}(\mathbf{y}) = 0]$).

Claim 5.22. $e^{-\alpha} - \frac{1}{M^{\beta_2/2}} \leq \sum_{c=1}^{a} (-1)^{c-1} S_c < \sum_{c=1}^{a+1} (-1)^{c-1} S_c \leq e^{-\alpha} + \frac{1}{M^{\beta_2/2}}$.

Proof. For any $c \leq a+1$, using Lemma 5.20, we have

$$\binom{R}{c}\left(\frac{\alpha}{R}\right)^c \leq S_c \leq \binom{R}{c}\left(\frac{\alpha}{R}\right)^c \left(1 + \frac{1}{M^{\beta_2}}\right).$$

We have,

$$\begin{aligned} \binom{R}{c}\left(\frac{\alpha}{R}\right)^c &\leq \frac{R^c}{c!}\frac{\alpha^c}{R^c} \\ &= \frac{\alpha^c}{c!} \end{aligned}$$

and

$$\begin{aligned} \binom{R}{c}\left(\frac{\alpha}{R}\right)^c &= \frac{R(R-1)\dots(R-c+1)}{R^c}\frac{\alpha^c}{c!} \\ &\geq \left(1 - \frac{a^2}{R}\right)\frac{\alpha^c}{c!} && \text{(by Weierstrass product inequality)} \\ &\geq \left(1 - \frac{1}{R^{1-\beta_2}}\right)\frac{\alpha^c}{c!} \end{aligned}$$

by our choice of a.

Thus, for any $c \leq a$, we have

$$\left| S_c - \frac{\alpha^c}{c!} \right| \leq \frac{1}{M^{\beta_2}} \tag{4}$$

It also follows that

$$S_{a+1} \leq \frac{1}{a!} + \frac{1}{M^{\beta_2}} < \frac{2}{M^{\beta_2}}, \tag{5}$$

using $a = s^{\beta_3}$.

Finally, by the classical Taylor's theorem, we have

$$\left| e^{-\alpha} - \sum_{c=1}^{a} (-1)^{c-1} \frac{\alpha^c}{c!} \right| < \frac{1}{a!} < \frac{1}{M^{\beta_2}}. \tag{6}$$

Claim 5.22 is now direct from the inequalities (4), (5), (6) and the fact that $aM^{-\beta_2} \leq M^{-\beta_2/2}$. □

The next claim is a restatement of Lemma 5.18.

Claim 5.23. *$|p - \frac{1}{2}| \leq B^{-\Omega(1)}$, where $p = \mathbf{Pr}_{\mathbf{y} \sim \mathbf{Ber}(s, 1-p_1)}[f_{\text{Ext}}(\mathbf{y}) = 0]$.*

Proof. Using (3) and Claim 5.22, we have

$$|p - e^{-\alpha}| \leq \frac{1}{M^{\beta_2/2}}.$$

Recall that from Claim 5.15, we have

$$\ln 2 \left(1 - \frac{1}{B^{\epsilon_3}}\right) \leq \alpha \leq \ln 2 \left(1 + \frac{1}{B^{\epsilon_3}}\right).$$

Thus,

$$\left| e^{-\alpha} - \frac{1}{2} \right| \leq \frac{2}{B^{\epsilon_3}}$$

and hence, we have

$$\left| p - \frac{1}{2} \right| \leq \frac{3}{B^{\epsilon_3}}.$$

□

□

6 Wrapping Up the Proofs of Theorem 1 and Theorem 6

Proof of Theorem 6. Let $f : \{0,1\}^n \to \{0,1\}$ be the explicit function constructed in Theorem 4 satisfying: For any $q > 0$, $t \geq c(\log n)^{18}$ (c is the constant from Theorem 4) and $\gamma \leq 1/n^{t+1}$,

- $\mathbf{I}_q(f) \leq q/n^{1-\frac{\delta}{2}}$

- For any (t, γ)-wise independent distribution $\mathcal{D}$, $\left|\mathbf{E}_{\mathbf{x}\sim\mathcal{D}}[f(x)] - \frac{1}{2}\right| \leq \frac{1}{n^{\Omega(1)}}$.

Using Lemma 2.10, it follows that f is an extractor for $(n^{1-\delta}, t, \gamma)$-non-oblivious bit-fixing sources with error $1/n^{\Omega(1)}$. □

Proof of Theorem 1. Let reduce : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^D$ be the function from Theorem 3.1 with $t = c(\log n)^{18}$, where c is the constant from Theorem 6. Set the constant $C = 74$ and $C_1 = c'$, where c' is the constant from Theorem 3.1. We note that $D = n^{O(1)}$.

Let bitExt : $\{0,1\}^D \to \{0,1\}$ be the explicit extractor from Theorem 6 set to extract from (q, t, γ)-non-oblivious bit-fixing source on D bits with error $\frac{1}{n^{\Omega(1)}}$, where $q = D^{1-\delta}$ and $\gamma \leq 1/D^{t+1}$.

Define

$$\text{2Ext}(x, y) = \text{bitExt}(\text{reduce}(x, y)).$$

Let $\mathbf{X}$ and $\mathbf{Y}$ be any two independent (n, k)-sources, where $k \geq C_1(\log n)^C$. We prove that

$$|(\text{2Ext}(\mathbf{X}, \mathbf{Y}), \mathbf{Y}) - (\mathbf{U}_1, \mathbf{Y})| \leq \frac{1}{n^{\Omega(1)}}.$$

Let $\mathbf{Z} = \text{reduce}(\mathbf{X}, \mathbf{Y})$. Theorem 3.1 implies that with probability at least $1 - n^{-\omega(1)}$ (over $\mathbf{y} \sim \mathbf{Y}$), the conditional distribution $\mathbf{Z}|\mathbf{Y} = \mathbf{y}$ is a (q, t, γ)-non-oblivious bit-fixing source on M bits. Thus, for each such $\mathbf{y}$,

$$|\text{bitExt}(\text{reduce}(\mathbf{X}, \mathbf{y})) - \mathbf{U}_1| \leq \frac{1}{n^{\Omega(1)}}.$$

Thus, we have

$$|(\text{2Ext}(\mathbf{X}, \mathbf{Y}), \mathbf{Y}) - (\mathbf{U}_1, \mathbf{Y})| \leq \frac{1}{n^{\omega(1)}} + \frac{1}{n^{\Omega(1)}}.$$

□

7 Achieving Smaller Error

We show that it is indeed possible to achieve an extractor with smaller error at the expense of increasing min-entropy requirement and the running time of the extractor by a slight modification of our construction.

Informally, we achieve this by using the sources $\mathbf{X}$ and $\mathbf{Y}$ to generate a much longer string $\mathbf{Z}$ with the property that most of the bits are t-wise independent. This allows us to achieve smaller error in the reduction, and now applying the extractor for (q, t, γ)-sources developed in Theorem 6, the result follows.

Theorem 7.1 (Theorem 2 restated)**.** *There exists a constant $C > 0$ such that for all $n \in \mathbb{N}$ and any $\epsilon > 0$, there exists a 2-source extractor* 2Ext : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *computable in time* $\text{poly}(n, 1/\epsilon)$ *for min-entropy at least* $\log^C(n/\epsilon)$ *and error* ϵ*.*

Proof sketch. We provide the details of the construction and omit the proof since it is very similar to the proof of Theorem 1.

We set up the required ingredients as follows:

- Let $t = b(\log(5D/\epsilon))^{18}$, where b is the constant from Theorem 4.1.

- Let $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}$ be a (t, k, ϵ_1)-non-malleable extractor from Theorem 3.2. Thus $d_1 = c_1 t^2 \log^2(n/\epsilon_1)$, for some constant c_1. For such an extractor to exists, we require $k \geq \lambda_1 t \log^2(n/\epsilon_1)$.
- Let $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{d_1}$ be the seeded extractor from Theorem 2.3 set to extract from min-entropy $k/2$ with error ϵ_2. Thus, $d = c_2 \log(n/\epsilon_2)$, for some constant c_2. Let $D = 2^d = (n/\epsilon_2)^{c_2}$. Such an extractor exists for $k \geq 3d_1$.
- Choose $\delta > 0$, such that $\delta' = \delta c_2 < 9/10$.
- Let $f : \{0,1\}^D \to \{0,1\}$ be the function from Theorem 5.1 such that f is $\mathbf{I}_q(f) \leq q/D^{1-\frac{\delta}{2}}$ and $\left|\mathbf{E}_{v\sim\mathbf{U}_D}[f(v)] - \frac{1}{2}\right| \leq D^{-\beta}$ for some small constant β.
- Pick ϵ_1, ϵ_2 such that the following inequalities are satisfied:
  - $D = (n/\epsilon_2)^{c_2} \geq \max\{1/\epsilon^{1/\beta}, 1/\epsilon^{2/\delta}\}$,
  - $\epsilon_2 \leq D^{-\delta}/2 = (\epsilon_2/n)^{\delta'}$,
  - $\sqrt{\epsilon_1} \leq \frac{1}{5tD^{t+1}}$.

  Thus, we can pick $\epsilon_2 = \min\{n\epsilon^{\frac{1}{c_2\beta}}, n\epsilon^{\frac{2}{c_2\delta}}, 1/n^{\delta'/(1-\delta')}\}$ and $\epsilon_1 = 1/(5tD^{t+1})$.
- With this setting of parameters, we require $k \geq (\log(n/\epsilon))^{c'}$, where c' is a large enough constant, for nmExt and Ext to work.

Let $\{0,1\}^{d_2} = \{r_1, \ldots, r_{D_2}\}$. Define

$$\mathrm{reduce}(x,y) = \mathrm{nmExt}(x, \mathrm{Ext}(y, r_1)) \circ \ldots \circ \mathrm{nmExt}(x, \mathrm{Ext}(y, r_{D_2}))$$

and

$$2\mathrm{Ext}(x,y) = f(\mathrm{reduce}(x,y)).$$

Using arguments similar to the proof of Theorem 1, it can be shown that 2Ext is an extractor for min-entropy k with error $O(\epsilon)$. Further, the extractor runs in time $\mathrm{poly}(n, 1/\epsilon)$. □

Acknowledgments

We thank anonymous referees for valuable comments that led to improvements in the presentation of the paper. We are grateful to Xin Li for an observation which led to Theorem 2. We also thank Ran Raz for reminding us that every 2-source extractor is strong.

References

[AGM03] Noga Alon, Oded Goldreich, and Yishay Mansour. Almost k-wise independence versus k-wise independence. *Inf. Process. Lett.*, 88(3):107–110, 2003.

[AL93] Miklós Ajtai and Nathan Linial. The influence of large coalitions. *Combinatorica*, 13(2):129–145, 1993.

[Alo98] Noga Alon. The Shannon capacity of a union. *Combinatorica*, 18(3):301–310, 1998.

[AN93] Noga Alon and Moni Naor. Coin-flipping games immune against linear-sized coalitions. *SIAM J. Comput.*, 22(2):403–417, 1993.

[AS92] Noga Alon and Joel Spencer. *The Probabilistic Method*. John Wiley, 1992.

[Bar06] Boaz Barak. A Simple Explicit Construction of an $n^{\tilde{O}(\log n)}$-Ramsey Graph. Technical report, Citeseer, 2006.

[BH05] Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to/dev/random. In *Proceedings of the 12th ACM conference on Computer and communications security*, pages 203–212, 2005.

[BIW06] Boaz Barak, Russell Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. *SIAM J. Comput.*, 36(4):1095–1118, December 2006.

[BKS+10] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. *J. ACM*, 57(4), 2010.

[BL85] Michael Ben-Or and Nathan Linial. Collective coin flipping, robust voting schemes and minima of Banzhaf values. In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*, pages 408–416, 1985.

[BN96] Ravi B. Boppana and Babu O. Narayanan. The biased coin problem. *SIAM J. Discrete Math.*, 9(1):29–36, 1996.

[Bou05] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *International Journal of Number Theory*, 01(01):1–32, 2005.

[Bra10] Mark Braverman. Polylogarithmic independence fools AC^0 circuits. *J. ACM*, 57(5), 2010.

[BRSW12] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson. 2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction. *Annals of Mathematics*, 176(3):1483–1543, 2012. Preliminary version in STOC '06.

[BS89] Ravi Boppona and Joel Spencer. A useful elementary correlation inequality. *Journal of Combinatorial Theory, Series A*, 50(2):305 – 307, 1989.

[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.

[CGH+85] Benny Chor, Oded Goldreich, Johan Hastad, Joel Friedman, Steven Rudich, and Roman Smolensky. The bit extraction problem of t-resilient functions (preliminary version). In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*, pages 396–407, 1985.

[CGL16] Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. In *STOC*, 2016.

[CL16] Eshan Chattopadhyay and Xin Li. Extractors for sumset sources. In *STOC*, 2016.

[Coh15] Gil Cohen. Local correlation breakers and applications to three-source extractors and mergers. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[Coh16] Gil Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. In *STOC*, 2016.

[DKSS09] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 181–190, 2009.

[DO03] Y. Dodis and R. Oliveira. On extracting private randomness over a public channel. In *RANDOM 2003, 7th International Workshop on Randomization and Approximation Techniques in Computer Science*, pages 252–263, 2003.

[Dod06] Yevgeniy Dodis. Fault-tolerant leader election and collective coin-flipping in the full information model, 2006.

[DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *STOC*, pages 601–610, 2009.

[Fei99] Uriel Feige. Noncryptographic selection protocols. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science*, pages 142–153, 1999.

[FW81] P. Frankl and R.M. Wilson. Intersection theorems with geometric consequences. *Combinatorica*, 1(4):357–368, 1981.

[Gop14] Parikshit Gopalan. Constructing Ramsey graphs from boolean function representations. *Combinatorica*, 34(2):173–206, 2014.

[Gro00] Vince Grolmusz. Low rank co-diagonal matrices and Ramsey graphs. *Electr. J. Comb.*, 7, 2000.

[GRS06] Ariel Gabizon, Ran Raz, and Ronen Shaltiel. Deterministic extractors for bit-fixing sources by obtaining an independent seed. *SIAM J. Comput.*, 36(4):1072–1094, 2006.

[GSV05] S. Goldwasser, M. Sudan, and V. Vaikuntanathan. Distributed computing with imperfect randomness. In P. Fraigniaud, editor, *Proceedings of the 19th International Symposium on Distributed Computing DISC 2005*, volume 3724 of *Lecture Notes in Computer Science*, pages 288–302. Springer, 2005.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *J. ACM*, 56(4), 2009.

[Jan90] Svante Janson. Poisson approximation for large deviations. *Random Structures & Algorithms*, 1(2):221–229, 1990.

[JK99] Benjamin Jun and Paul Kocher. The Intel random number generator. *Cryptography Research Inc. white paper*, 1999.

[KKL88] Jeff Kahn, Gil Kalai, and Nathan Linial. The influence of variables on boolean functions (extended abstract). In *29th Annual Symposium on Foundations of Computer Science, White Plains, New York, USA, 24-26 October 1988*, pages 68–80, 1988.

[KLR09] Y. Kalai, X. Li, and A. Rao. 2-source extractors under computational assumptions and cryptography with defective randomness. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 617–626, 2009.

[KLRZ08] Y. Kalai, X. Li, A. Rao, and D. Zuckerman. Network extractor protocols. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 654–663, 2008.

[KZ07] Jesse Kamp and David Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. *SIAM J. Comput.*, 36(5):1231–1247, 2007.

[Li11] Xin Li. Improved constructions of three source extractors. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, June 8-10, 2011*, pages 126–136, 2011.

[Li12a] Xin Li. Design extractors, non-malleable condensers and privacy amplification. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, pages 837–854, 2012.

[Li12b] Xin Li. Non-malleable extractors, two-source extractors and privacy amplification. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science*, pages 688–697, 2012.

[Li13a] Xin Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science*, pages 100–109, 2013.

[Li13b] Xin Li. New independent source extractors with exponential improvement. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 783–792, 2013.

[Li15a] Xin Li. Extractors for affine sources with polylogarithmic entropy. Technical Report TR15-121, ECCC, 2015.

[Li15b] Xin Li. Improved constructions of two-source extractors. *Electronic Colloquium on Computational Complexity (ECCC)*, 2015.

[Li15c] Xin Li. Three-source extractors for polylogarithmic min-entropy. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[LRVW03] Chi-Jen Lu, Omer Reingold, Salil P. Vadhan, and Avi Wigderson. Extractors: optimal up to constant factors. In *STOC*, pages 602–611, 2003.

[Mek15] R. Meka. Explicit resilient functions matching Ajtai-Linial. Technical Report TR15-144, ECCC, 2015.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43–52, 1996.

[PR04] P. Pudlak and V. Rodl. Pseudorandom sets and explicit constructions of Ramsey graphs, 2004.

[Rao09a] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. *SIAM J. Comput.*, 39(1):168–194, 2009.

[Rao09b] Anup Rao. Extractors for low-weight affine sources. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity*, 2009.

[Raz05] Ran Raz. Extractors with weak random seeds. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 11–20, 2005.

[RRV02] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. *JCSS*, 65(1):97–128, 2002.

[RSZ02] Alexander Russell, Michael E. Saks, and David Zuckerman. Lower bounds for leader election and collective coin-flipping in the perfect information model. *SIAM J. Comput.*, 31(6):1645–1662, 2002.

[RZ01] A. Russell and D. Zuckerman. Perfect-information leader election in $\log^* n + O(1)$ rounds. *JCSS*, 63:612–626, 2001.

[RZ08] Anup Rao and David Zuckerman. Extractors for three uneven-length sources. In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques, 11th International Workshop, APPROX 2008, and 12th International Workshop, RANDOM 2008, Boston, MA, USA, August 25-27, 2008. Proceedings*, pages 557–570, 2008.

[Sak89] Michael Saks. A robust noncryptographic protocol for collective coin flipping. *SIAM Journal on Discrete Mathematics*, 2(2):240–244, 1989.

[Sha02] Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[Sha08] Ronen Shaltiel. How to get more mileage from randomness extractors. *Random Struct. Algorithms*, 33(2):157–186, 2008.

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

[Tal14] Avishay Tal. Tight bounds on the Fourier spectrum of AC^0. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:174, 2014.

[Tre01] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, pages 860–879, 2001.

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

[Zuc97] David Zuckerman. Randomness-optimal oblivious sampling. *Random Structures and Algorithms*, 11:345–367, 1997.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de