Electronic Colloquium on Computational Complexity, 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

July 24, 2015

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 other main contribution is a reduction showing how such a resilient function gives a two-source extractor. This relies heavily on the new non-malleable extractor of Chattopadhyay, Goyal and Li [CGL15].

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 [Coh15b].

*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.

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 $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ 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 get past 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.

We use the notion statistical distance to measure the error of the extractor.

Definition 1.2. *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 1.3 (Two-source extractor)**.** *A function $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is called a two-source extractor for min-entropy k and error ϵ if for any independent (n,k)-sources $\mathbf{X}$ and $\mathbf{Y}$*

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

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 $|(\mathrm{Ext}(\mathbf{X},\mathbf{Y}),\mathbf{Y}) - (\mathbf{U}_m,\mathbf{Y})| \leq \epsilon$, where $\mathbf{U}_m$ is independent from $\mathbf{Y}$.

A simple probabilistic argument shows the existence of 2-source extractors for min-entropy $k \geq 2\log n + 10\log(1/\epsilon)$. 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 progress was made on this problem 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 [Li15]. Recently Cohen [Coh15a] 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 $n^{-\Omega(1)}$. Further, the extractor is strong in the second source.*

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.

We 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 composition with a strong-seeded extractor.

1.1 Ramsey Graphs

Definition 1.4 (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 $K = (2 + o(1)) \log N$. 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][1] achieving the same bound. An explanation to why these approaches were stuck at this bound was discovered by Gopalan [Gop14], who showed 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 1.5 (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.*

[1] The construction in [Bar06] achieves a weaker notion of explicitness, and runs in time poly(N) to compute edge relations.

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, and we refer the reader to [BRSW12] for a proof.

Lemma 1.6. *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, as an immediate consequence of Theorem 1, we obtain the following result.

Theorem 2. *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 1.7. *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[2], Cohen [Coh15b] used the challenge-response mechanism introduced in [BKS+10] with new advances in constructions of extractors and obtained 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

We now describe a high-level overview of our construction. First, let's try to build a 1-source extractor, even though it's impossible. Let X have min-entropy k that is polylogarithmic. Let's cycle over all seeds of a strong extractor SExt that extracts from min-entropy k with error ε, and concatenate the outputs to obtain an D-bit string where most individual bits are close to uniform. If we take the majority of these D bits we might hope that the output is close to uniform. However, the outputs with different seeds may be correlated in arbitrary ways, so this approach doesn't work.

We can try to fix this approach by using the new non-malleable extractor of Chattopadhyay, Goyal, and Li [CGL15]. Such a non-malleable extractor strengthens the strong extractor so that the output bits are almost t-wise independent as long as we use a seed of length $O(t^2 \log^2 n/\varepsilon)$. Now if we try applying the majority to the D-bit string it still doesn't work, even if the uniform bits were completely independent. This is because an $\alpha \approx \sqrt{\varepsilon}$ fraction of the bits may not be uniform, and as this is greater than $\sqrt{D}$, these bad bits may completely bias the majority.

We can therefore look at more "resilient" functions – ones which tolerate more than $\sqrt{D}$ bad bits. In particular, we could hope that the Ajtai-Linial function [AL93] suffices, since it can tolerate

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

about $D/\log^2 D$ bad bits. However, this still doesn't work, as the parameters are still not strong enough. (Besides, it can't work since we're only using one source.)

Our approach is to use the second source to sample $D' < D$ bits from the first source, using an extractor-based sample. Now we may have, say, $2\alpha D'$ bad bits, because of sampler errors, but this is still a more favorable function of D'. We then apply a suitable function f to the output bits, where f is a derandomized monotone version of the Ajtai-Linial function to get our output.

There are still three issues to resolve. First, we need f to have constant depth, as we will use Braverman's result [Bra10] that polylog-wise independence fools AC^0. While the Ajtai-Linial function has constant depth, the only derandomization of Ajtai-Linial that we know, which is unpublished work by Meka [Mek09], does not.

Second, we need f to be monotone, as we really need a different function to be in AC^0, namely, the function that tests whether a set of variables Q can influence the function. We only know how to do this when f is monotone, by checking whether f changes when the variables in Q are all set to 0 versus when they are all set to 1. However, the Ajtai-Linial function and Meka's derandomization are not monotone.

Third and related, we need a new way to derandomize Ajtai-Linial to achieve the above constraints. Meka's derandomization uses small versions of Ajtai-Linial and thus cannot be made monotone without making Ajtai-Linial monotone.

Therefore, most of our work is spent achieving these goals. The Ajtai-Linial function uses a family of partitions obtained by the probabilistic method. We show how to use extractors to construct such partitions.

Thus, our new function f is an explicit resilient function, which is interesting in its own right. We now explain some applications of it.

1.3 Resilient Functions

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.

To state our results more formally, we introduce some definitions.

Definition 1.8. *Let $f : \{0,1\}^n \to \{0,1\}$ be any boolean function on variables $x_1, \ldots, x_n$. The* *influence of a set $Q \subseteq \{x_1, \ldots, x_n\}$ 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 $\mathbf{I}_q(f) = \max_{Q \subseteq \{x_1,\ldots,x_n\}, |Q|=q} \mathbf{I}_Q(f)$.*

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 $\mathbf{I}_{Q,t}(f) = \max_{\mathcal{D} \in \mathcal{D}_k} \mathbf{I}_{Q,\mathcal{D}}(f)$, 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 independent distributions (see Section 2 for definition of a (t,γ)-wise independent distribution). Finally, for any integer q define $\mathbf{I}_{q,t}(f) = \max_{Q \subseteq \{x_1,\ldots,x_n\}, |Q|=q} \mathbf{I}_{Q,t}(f)$ and $\mathbf{I}_{q,t,\gamma}(f) = \max_{Q \subseteq \{x_1,\ldots,x_n\}, |Q|=q} \mathbf{I}_{Q,t,\gamma}(f)$.

Definition 1.9. *Let $f : \{0,1\}^n \to \{0,1\}$ be any boolean function on variables $x_1, \ldots, x_n$ 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 $\mathbf{I}_{q,t,\gamma}(f) \le \epsilon$.*

For $t < \sqrt{n}$, the only known function that is t-independent (q,ϵ_1)-resilient function is the majority function [Vio14] for $t = \log^c(n)$ and $q < n^{\frac{1}{2}-\tau}$, $\tau > 0$. The iterated majority function of Ben-Or and Linial mentioned in the previous section handles a larger $q = O(n^{0.63})$ for $t = n$, but it is not clear if it remains resilient for smaller t. Further, for $t = n$, Ajtai and Linial showed the existence of functions that are resilient for $q = O(n/\log^2 n)$. However, their functions are not explicit and require time $n^{O(n^2)}$ to deterministically construct.

Our main contribution here is the following.

Theorem 3. *There exists a constant c such that for any $\delta > 0$ and every large enough integer $n \in \mathbb{N}$, there exists an efficiently computable monotone boolean function $f : \{0,1\}^n \to \{0,1\}$ satisfying: For any $q > 0, t \ge c(\log n)^{18}$ and $\gamma < 1/n^{t+1}$,*

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

The following theorem is direct from Theorem 3, even ignoring the t-wise independent part; see e.g., Lemma 2 in [Dod06].

Theorem 4. *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.*

1.4 Bit-Fixing Sources

Another use of resilient functions is to build extractors for bit-fixing sources. We first formally define the notion of a deterministic extractor for a class of sources.

Definition 1.10. *We say that 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 $\mathbf{X} \in \mathcal{X}$, $|f(\mathbf{X}) - \mathbf{U}_m| \le \epsilon$.*

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.

In this work we are interested in designing extractors for a generalization of non-oblivious bit-fixing sources, where the random bits are guaranteed to be only almost t-wise independent. We introduce these sources more formally.

Definition 1.11. *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 a (t, ϵ)-wise independent distribution if the distribution obtained by restricting $\mathcal{D}$ to any t coordinates is ϵ-close to uniform.*

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

If the joint distribution of the bits indexed by $\overline{Q}$ is (t, γ)-wise independent then $\mathbf{X}$ is said to be a (q, t, γ)-non-oblivious bit-fixing source.

For $t < \sqrt{n}$, the only known extractor for this class of sources was by Viola [Vio14], who showed that the majority function extracts from (q, t)-independent non-oblivious sources on n bits, with $t = \log^c(n), q = n^{\frac{1}{2} - \tau}$ for any $\tau > 0$. As an open question, Viola asked how to construct extractors for this class of sources for larger q. We improve q to $n^{1-\delta}$ for any $\delta > 0$ and obtain the following theorem.

Theorem 5. *There exists a constant c such that for any constant $\delta > 0$, and for all $n \in \mathbb{N}$, there exists an explicit extractor* $\mathrm{bitExt} : \{0,1\}^n \to \{0,1\}$ *for the class of (q, t, γ)-non-oblivious bit-fixing sources with error $n^{-\Omega(1)}$, where $q \leq n^{1-\delta}, t \geq c \log^{18}(n)$ and $\gamma \leq 1/n^{t+1}$.*

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

1.5 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 3. We use Section 6 to wrap up the proofs of Theorem 1 and Theorem 5.

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 $\{1, \ldots, t\}$.
For a string y of length n, and any subset $S \subseteq [n]$, we use y_S to denote the projection of y to 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 $\ell < n/10$.
A distribution $\mathcal{D}$ on $\{0,1\}^n$ is called a (t, γ)-wise independent distribution if the restriction of $\mathcal{D}$ to every t distinct co-ordinates is γ-close to $\mathbf{U}_t$.

2.1 Seeded Extractors

Definition 2.1. *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, $|\mathrm{Ext}(\mathbf{X}, \mathbf{U}_d) - \mathbf{U}_m| \leq \epsilon$. *Further,* Ext *is called a strong-seeded extractor if* $|(\mathrm{Ext}(\mathbf{X}, \mathbf{U}_d), \mathbf{U}_d) - (\mathbf{U}_m, \mathbf{U}_d)| \leq \epsilon$, *where* $\mathbf{U}_m$ *and* $\mathbf{U}_d$ *are independent.*

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

Theorem 2.2 ([Tre01] [RRV02])**.** *For every* $n, k, m \in \mathbb{N}$ *and* $\epsilon > 0$, *with* $m \leq k \leq n$, *there exists an explicit strong-seeded extractor* $\mathrm{TExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *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 2.3 ([GUV09])**.** *For any constant* $\alpha > 0$, *and all integers* $n, k > 0$ *there exists a polynomial time computable strong-seeded extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with* $d = O(\log n + \log(1/\epsilon))$ *and* $m = (1-\alpha)k$.

To ensure that for each $x \in \{0,1\}^n$, $\mathrm{Ext}(x, s_1) \neq \mathrm{Ext}(x, s_2)$ whenever $s_1 \neq s_2$, we can concatenate the seed to the output of Ext.

Corollary 2.4 ([GUV09])**.** *For any constant* $\alpha > 0$, *and all integers* $n, k > 0$ *there exists a polynomial time computable seeded extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with* $d = O(\log n + \log(1/\epsilon))$ *and* $m = (1-\alpha)k$. *Further for all* $x \in \{0,1\}^n$, $\mathrm{Ext}(x, s_1) \neq \mathrm{Ext}(x, s_2)$ *whenever* $s_1 \neq s_2$.

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 a (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}, for any $x \in \{0,1\}^n$. We call G_{Ext} the graph corresponding to Ext.

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* $D = 2^d$. *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 2.6 ([Zuc97]). *Let* $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a seeded extractor for min-entropy* k *and error* ϵ. *Let* $\{0,1\}^d = \{r_1, \ldots, r_D\}$, $D = 2^d$. *Define* $\text{Samp}(x) = \{\text{Ext}(x, r_1), \ldots, \text{Ext}(x, r_D)\}$. *Let* $\mathbf{X}$ *be a* $(n, 2k)$*-source. Then for any set* $R \subseteq \{0,1\}^m$,

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

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

2.3 An Inequality

We frequently use the following inequality.

Claim 2.7. *For any* $n > 1$ *and* $0 \le x \le n$, *we have*

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

2.4 Some Probability Lemmas

Lemma 2.8 ([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* $|(\mathbf{X}, \mathbf{Y}) - (\mathbf{X}, \mathbf{U}_t)| \le \epsilon$. *Then for every* $y \in \{0,1\}^t$,

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

Lemma 2.9 ([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. $|\mathbf{X}_2 - \mathbf{Y}_2| \le \epsilon_2$.
2. *For every* $s_2 \in S_2$, $|(\mathbf{X}_1|\mathbf{X}_2 = s_2) - (\mathbf{Y}_1|Y_2 = s_2)| \le \epsilon_1$.

Then

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

Using the above results, we record a useful lemma.

Lemma 2.10. *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 $t \ge 2$. 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 2.8, for any value of the bit b,

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

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 2.9 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. $\square$

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 2.11. *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,

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

$\square$

3 Reducing Two Independent Sources to a (q,t,γ)-Independent Non-Oblivious Bit-Fixing 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)-non-oblivious bit-fixing 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* $\text{reduce} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^D$, $D = n^{O(1)}$, *satisfying the following property: if $\mathbf{X}, \mathbf{Y}$ are independent (n,k)-sources with $k \geq c't^4 \log^2 n$, then*

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

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

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)-non-oblivious bit-fixing 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 [CGL15].

3.1 Non-Malleable Extractors

Non-malleable extractors were introduced by Dodis and Wichs [DW09] as a generalization of the notion of a strong-seeded extractor. 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 now introduce this notion more formally.

Definition 3.2. *A function* $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *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*[3]*, then*

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

In a recent work, Chattopadhyay, Goyal and Li [CGL15] constructed an explicit t-non-malleable extractor for polylogarithmic min-entropy. This is a crucial component in our reduction.

Theorem 3.3 ([CGL15])**.** *There exists a constant $c' > 0$ such that for all $n, t > 0$ there exists an explicit (t,k,ϵ)-non-malleable extractor* $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}$, *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 show a way to reduce extracting from two independent sources to extracting from a (q,t,γ)-non-oblivious bit-fixing 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.

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

Lemma 3.4. *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:*

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

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

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

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 3.4 is easy to obtain.

Lemma 3.5. *Let* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}$ *be a* (t, k, ϵ)*-non-malleabale 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

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

We define adversarial functions $f_1, \ldots, f_t$ in the following way. For each $r \in BAD$, set $f_i(r) = r_i$, $i = 1, \ldots, t$ (the f_i's are arbitrarily defined 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 2.10, it follows that R satisfies the required property. □

Proof of Lemma 3.4. 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 3.5 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 2.6, 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 $((\sqrt{\epsilon_1} + \epsilon_2) D_2, t, 5t\sqrt{\varepsilon_1})$-non-oblivious bit-fixing 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 $((\sqrt{\epsilon_1} + \epsilon_2) D_2, t, 5t\sqrt{\epsilon_1})$-non-oblivious bit-fixing source on D_2 bits. □

Proof of Theorem 3.1. We derive Theorem 3.1 from Lemma 3.4 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 3.3. 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 2.4 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

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

   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 3.4, it follows that

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

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

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)-non-oblivious bit-fixing source. By Lemma 2.11 this translates to constructing a 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 $|\mathbf{E}_{\mathbf{x}\sim\mathbf{U}_n}[\mathcal{C}(x)] - \frac{1}{2}| \le \epsilon_1$. Suppose $q > 0$ is such that $\mathbf{I}_q(\mathcal{C}) \le \epsilon_2$. If $t \ge b(\log(5m/\epsilon_3))^{3d+6}$, then $\mathbf{I}_{q,t}(\mathcal{C}) \le \epsilon_2 + \epsilon_3$ and $\mathbf{I}_{q,t,\gamma}(\mathcal{C}) \le \epsilon_2 + \epsilon_3 + \gamma n^t$. Further, for any distribution $\mathcal{D}$ that is (t,γ)-wise independent, $|\mathbf{E}_{x\sim\mathcal{D}}[\mathcal{C}(x)] - \frac{1}{2}| \le \epsilon_1 + \epsilon_3 + \gamma n^t$.*

We first briefly sketch the main ideas involved in proving the above theorem. 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 $\mathcal{C}$ is undetermined for some setting of the variables outside Q. This crucially relies on the fact that $\mathcal{C}$ is a monotone function. Next, using the result of Braverman [Bra10] that small AC^0 circuits are fooled by bounded independence, 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 result now follows using the bound on $\mathbf{I}_Q(\mathcal{C})$.

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,*

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

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 $\mathcal{D}$.*

Proof of Therorem 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

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

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

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

We construct $\mathcal{E}_Q$ as follows: Let $\mathcal{C}_0$ be the circuit obtained from $\mathcal{C}$ by setting all the variables in Q to 0. Let $\mathcal{C}_1$ be the circuit obtained from $\mathcal{C}$ by setting all the variables in Q to 1. Define $\mathcal{E}_Q \coloneqq \neg(\mathcal{C}_0 = C_1)$. It is easy to check that $\mathcal{E}_Q$ satisfies the required property (using the fact that $\mathcal{C}$ is monotone). 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. □

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 3, which is easy to obtain from the above theorem.

Proof of Theorem 3. 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 $t \geq b(\log(5n/\epsilon_3))^{18}$, $q > 0$ and $\gamma \leq 1/n^{t+1}$,

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

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

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

□

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 resilient to $\Omega(n/\log^2 n)$ adversaries. 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).

The high level idea is to derandomize the construction of [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 use partitions chosen according to an extractor, although it's not obvious how an extractor defines these partitions. We also suitably modify the construction to ensure that the resulting function is monotone, which is crucial in light of Theorem 4.1.

5.1 Our Construction and Main 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 $\epsilon \leq \delta/4$ set such that $b = \delta_1 m$, $\delta_1 = \delta/20$, 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 $\{0,1\}^r = \{v_1, \ldots, v_R\}$. We define a collection of R equi-partitions of $[s]$, $\mathcal{P} = \{P^{v_1}, \ldots, P^{v_R}\}$ in the following way: 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:

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

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 called 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 $(1 - B^{-\epsilon_1})\gamma \leq p_1 \leq \gamma$. Then there exists a constant $\delta' > 0$ such that for any $q > 0$,*

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

The following generalizes the notion of a design extractor which was introduced by Li [Li12].

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 $y, y' \in \{0,1\}^m$*

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

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* 2.2 *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 monotone* CNF $\mathcal{C}$ *on* h *bits of size* h*, 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 2.2 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 2.2 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, $(1 - B^{-\epsilon_1})\gamma \le \mathbf{Pr}_{\mathbf{x} \sim \mathbf{U}_h}[\mathcal{C}(\mathbf{x}) = 0] < \gamma$.

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,

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

Thus the above calculation and Lemma 5.7 yields that

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

Using Lemma 5.3, it follows that

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

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 $\overline{r} = (r+1)/\alpha$, 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 $\alpha(1 - \frac{1}{\overline{r}}) > 0.9\alpha$ and relative distance $\frac{1}{2} - \beta$. Let $\mathrm{Enc} : \{0,1\}^r \to \{0,1\}^{\overline{r}}$ be the encoding function of $\mathcal{C}$.

Further fix a subset $S_1 \subset [b]$ of size $\log(\overline{r})$. 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

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

□

We now proceed to prove Lemma 5.3 and Lemma 5.5.

For convenience, define

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

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

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,

$$\begin{aligned} p_2 &= (1-p_1)^B \ge (1-\gamma)^B \ge e^{-\gamma B}(1-\gamma^2 B) && \text{(by Claim 2.7)} \\ &\ge \frac{\ln R - \ln\ln 2}{M}\left(1 - \frac{r^2}{B}\right) && \text{(since } \gamma < (\ln M)/B < r/B\text{)} \end{aligned}$$

We now upper bound p_2. We have,

$$\begin{aligned} p_2 &\le (1-\gamma(1-B^{-\epsilon_1}))^B \le e^{-\gamma B(1-B^{-\epsilon_1})} && \text{(by Claim 2.7)} \\ &< \left(\frac{\ln R - \ln\ln 2}{M}\right) M^{B^{-\epsilon_1}} < \left(\frac{\ln R - \ln\ln 2}{M}\right) e^{\delta r B^{-\epsilon_1}} \\ &\le \frac{\ln R - \ln\ln 2}{M}\left(1 + \frac{r}{B^{\epsilon_1}}\right) \end{aligned}$$

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

$$\begin{aligned}
p_3 &= (1-p_2)^M \\
&\geq \left(1 - \left(\frac{\ln R - \ln\ln 2}{M}\right)\left(1+\frac{1}{B^{\epsilon_2}}\right)\right)^M \\
&\geq \left(1 - \frac{(\ln R - \ln\ln 2)^2}{M}\left(1+\frac{1}{B^{\epsilon_2}}\right)^2\right)\left(\frac{\ln 2}{R}\right)e^{\frac{-(\ln R - \ln\ln 2)}{B^{\epsilon_2}}} && \text{(by Claim 2.7)} \\
&\geq \left(1-\frac{2r^2}{M}\right)\left(\frac{\ln 2}{R}\right)e^{-r/B^{\epsilon_2}} \\
&\geq \left(1-\frac{2r^2}{M}\right)\left(\frac{\ln 2}{R}\right)\left(1-\frac{r}{B^{\epsilon_2}}\right) \\
&\geq \left(1-\frac{2r}{B^{\epsilon_2}}\right)\left(\frac{\ln 2}{R}\right).
\end{aligned}$$

Finally, we have

$$\begin{aligned}
p_3 &\leq \left(1 - \left(\frac{\ln R - \ln\ln 2}{M}\right)\left(1-\frac{1}{B^{\epsilon_2}}\right)\right)^M \\
&\leq \left(\frac{\ln 2}{R}\right)^{1-B^{-\epsilon_2}} && \text{(by Claim 2.7)} \\
&\leq \left(\frac{\ln 2}{R}\right)2^{r/B^{\epsilon_2}} \leq \left(\frac{\ln 2}{R}\right)\left(1+\frac{r}{B^{\epsilon_2}}\right).
\end{aligned}$$

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_j^i to be bad with respect to a subset of variables Q if $|P_j^i \cap Q| \geq 2\epsilon B$. 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 $\{P_j^i : i \in \{0,1\}^r\}$ 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 2.5. 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_j^i, 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 $1 - \frac{1}{B^{\epsilon_3}} \le \frac{\alpha}{\ln 2} \le 1 + \frac{1}{B^{\epsilon_3}}$.*

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

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

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 $|P^{i_1}_{j_1} \cap P^{i_2}_{j_2}| \le 0.9B$. 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,

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

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

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

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

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

□

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 $P^i_j \subseteq \mathcal{O}$. 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 $f^i_{\text{Ext}}(y) = 0$ 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 $\mathbf{Pr}[\mathcal{E}_{i,j}] = \mathbf{Pr}[P^i_j \subseteq \mathcal{O}] = (1-p_1)^B = p_2$. 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

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

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 $p = \mathbf{Pr}_{\mathbf{y} \sim \mathbf{Ber}(s, 1-p_1)}[f_{\mathrm{Ext}}(\mathbf{y}) = 0]$).

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 $c \le a$, we have

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

It also follows that

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

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 $aM^{-\beta_2} \le M^{-\beta_2/2}$. ☐

The next claim is a restatement of Lemma 5.18.

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

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

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

Recall that from Claim 5.15, we have

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

Thus,

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

and hence, we have

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

☐

☐

6 Wrapping Up the Proofs of Theorem 1 and Theorem 5

Proof of Theorem 5. Let $f : \{0,1\}^n \to \{0,1\}$ be the explicit function constructed in Theorem 3 satisfying: For any $q > 0$, $t \ge c(\log n)^{18}$ (c is the constant from Theorem 3) and $\gamma \le 1/n^{t+1}$,

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

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

Using Lemma 2.11, 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 5. 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 5 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 $\gamma \le 1/D^{t+1}$.

Define

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

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

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

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

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

Thus, we have

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

□

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. 2006.

[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.

[CGL15] Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. *CoRR*, abs/1505.00107, 2015.

[Coh15a] Gil Cohen. Local correlation breakers and applications to three-source extractors and mergers, 2015. *To appear in FOCS 2015.*

[Coh15b] Gil Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 2015.

[DKSS09] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *FOCS*, pages 181–190, 2009.

[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 *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*, 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.

[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.

[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.

[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.

[Li12] 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.

[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 Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 783–792. ACM, 2013.

[Li15] Xin Li. Three-source extractors for polylogarithmic min-entropy. 2015. *To appear in FOCS 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.

[Mek09] Raghu Meka. Explicit coin flipping protocols. Unpublished manuscript, 2009.

[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