Two-Source Condensers with Low Error and Small Entropy Gap via Entropy-Resilient Functions

Avraham Ben-Aroya
The Blavatnik School of Computer Science, Tel-Aviv University, Tel Aviv, Israel

Gil Cohen
The Blavatnik School of Computer Science, Tel-Aviv University, Tel Aviv, Israel
https://www.gilcohen.org
gil@tauex.tau.ac.il

Dean Doron
Department of Computer Science, University of Texas at Austin, USA
deandoron@utexas.edu

Amnon Ta-Shma
The Blavatnik School of Computer Science, Tel-Aviv University, Tel Aviv, Israel
https://www.cs.tau.ac.il/~amnon
amnon@tau.ac.il

Abstract

In their seminal work, Chattopadhyay and Zuckerman (STOC'16) constructed a two-source extractor with error ε for n-bit sources having min-entropy $\text{polylog}(n/\varepsilon)$. Unfortunately, the construction's running-time is $\text{poly}(n/\varepsilon)$, which means that with polynomial-time constructions, only polynomially-small errors are possible. Our main result is a $\text{poly}(n, \log(1/\varepsilon))$-time computable two-source *condenser*. For any $k \geq \text{polylog}(n/\varepsilon)$, our condenser transforms two independent (n, k)-sources to a distribution over $m = k - O(\log(1/\varepsilon))$ bits that is ε-close to having min-entropy $m - o(\log(1/\varepsilon))$. Hence, achieving entropy gap of $o(\log(1/\varepsilon))$.

The bottleneck for obtaining low error in recent constructions of two-source extractors lies in the use of resilient functions. Informally, this is a function that receives input bits from r players with the property that the function's output has small bias even if a bounded number of corrupted players feed adversarial inputs after seeing the inputs of the other players. The drawback of using resilient functions is that the error cannot be smaller than $\ln r/r$. This, in return, forces the running time of the construction to be polynomial in $1/\varepsilon$.

A key component in our construction is a variant of resilient functions which we call *entropy-resilient functions*. This variant can be seen as playing the above game for several rounds, each round outputting one bit. The goal of the corrupted players is to reduce, with as high probability as they can, the min-entropy accumulated throughout the rounds. We show that while the bias decreases only polynomially with the number of players in a one-round game, their success probability decreases *exponentially* in the entropy gap they are attempting to incur in a repeated game.

2012 ACM Subject Classification Theory of computation → Pseudorandomness and derandomization

Keywords and phrases Condensers, Extractors, Resilient functions, Explicit constructions

Digital Object Identifier 10.4230/LIPIcs.APPROX-RANDOM.2019.43

Category RANDOM

Funding *Avraham Ben-Aroya*: Israel Science Foundation Grant 994/14 and by Len Blavatnik and the Blavatnik Family Foundation.
Dean Doron: Israel Science Foundation Grant 994/14 and by Len Blavatnik and the Blavatnik Family Foundation. This work was done while being at Tel-Aviv University.
Amnon Ta-Shma: Israel Science Foundation Grant 994/14.

1 Introduction

The problem of extracting randomness from imperfect random sources can be traced back to von Neumann [45]. Ideally, and somewhat informally, a randomness extractor is an algorithm that produces, or extracts, truly random bits from an imperfect source of randomness. Going beyond that particular task, randomness extractors have found dozens of applications for error correcting codes, cryptography, combinatorics, and circuit lower bounds to name a few.

An imperfect source of randomness is modelled by a random variable X that, for convenience sake, is assumed to be supported on n-bit strings. The standard measure for the amount of randomness in X is its *min-entropy* [18], which is the maximum $k \geq 0$ for which one cannot guess X with probability larger than 2^{-k}. For any such k, we say that X is an (n, k)-*source*, or a k-*source* for short.

Ideally, a randomness extractor would have been defined as a function $\mathsf{Ext}\colon \{0,1\}^n \to \{0,1\}^m$ with the property that for every random variable X with sufficiently high min-entropy, the output $\mathsf{Ext}(X)$ is ε-close to the uniform distribution on $\{0,1\}^m$ in the statistical distance, which we write as $\mathsf{Ext}(X) \approx_\varepsilon U_m$. Unfortunately, such a function Ext, even for very high min-entropy $k = n - 1$ and, when set with a modest error guarantee $\varepsilon = 1/4$ and a single output bit $m = 1$, does not exist. In light of that, several types of randomness extractors, that relax in different ways the above ideal definition, have been introduced and studied in the literature. In this work, we focus on one such well-studied instantiation.

▶ **Definition 1** (Two-source extractors [18]). *A function* $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ *is a* two-source extractor for min-entropy k with error guarantee ε *if for every pair of independent* (n, k)*-sources* X, Y*, the output distribution* $\mathsf{Ext}(X, Y) \approx_\varepsilon U_m$.

The existence of a two-source extractor for any min-entropy $k = \Omega(\log(n/\varepsilon))$ with $m = 2k - O(\log(1/\varepsilon))$ output bits was proved in [18]. In the same paper, an explicit construction of a two-source extractor for min-entropy $k > n/2$ was obtained. Remarkably, despite much attention [13, 42, 12, 31] and progress on relaxed settings [6, 41, 33, 32, 34, 20], the problem of constructing two-source extractors even for min-entropy as high as $k = 0.1n$ with $m = 1$ output bits remained open for 30 years. To appreciate the difficulty of constructing two-source extractors, we remark that such constructions yield explicit constructions of Ramsey graphs, a notoriously hard problem in combinatorics [1, 38, 25, 19, 26, 3, 27, 39, 5, 6, 7, 23].

In their breakthrough result, Chattopadhyay and Zuckerman [17] were finally able to obtain an explicit two-source extractor for min-entropy $k = \mathrm{polylog}(n/\varepsilon)$. Partially motivated by the problem of constructing Ramsey graphs, a line of followup works [24, 16, 21, 9, 22, 35, 36] focused on the case of constant error ε and was devoted for reducing the min-entropy requirement as a function of n. The state of the art result in this line of work is due to Li [36] and requires min-entropy $\frac{\log n \cdot \log\log n}{\log\log\log n} \cdot \mathrm{poly}(1/\varepsilon)$.

1.1 Resilient Functions – The Barrier for Obtaining Extractors With Low Error

Unfortunately, despite the fact that the dependence of the min-entropy of the Chattopadhyay-Zuckerman extractor on ε is polynomially-close to optimal, the running-time of their construction depends polynomially on $1/\varepsilon$ rather than the desired $\mathrm{polylog}(1/\varepsilon)$ dependence. The same holds for all subsequent constructions. That is, these constructions are not strongly polynomial-time and, in particular, the error guarantee cannot be taken to be sub-polynomial in n while maintaining running-time $\mathrm{poly}(n)$. This stands in contrast to classical extractors for high min-entropy [18, 42, 13, 31] that are strongly polynomial-time, and can support exponentially-small error.

Informally speaking, the reason for this undesired dependence of the running-time on ε lies in the use of a so-called *resilient function* [11]. A q-resilient function $f\colon \{0,1\}^r \to \{0,1\}$ can be thought of as an r-player game. If all players feed uniform and independent inputs to f, the output distribution has small bias, and, furthermore, this property is retained even if any q players decide to deviate from the rules of the game and choose their inputs as a function of all other inputs to f.

Majority on r input bits is an example of a q-resilient function with $q = O(\sqrt{r})$. Ajtai and Linial proved, using the probabilistic method, the existence of a q-resilient function for $q = O(\frac{r}{\log^2 r})$ [2]. The KKL Theorem [30] implies that the Ajtai-Linial function is tight up to a $\log r$ factor. Chattopadhyay and Zuckerman [17] constructed a derandomized version of the Ajtai-Linial function with $q = r^{1-\delta}$, for any constant $\delta > 0$. Their construction has further desirable properties. In a subsequent work, Meka obtained a derandomized version of the Ajtai-Linial function with the same parameters as the randomized construction [37]. However, no matter what function is chosen, [30] showed that there is always a single corrupted player that has influence $p = \Omega(\frac{\log r}{r})$, i.e., with probability p over the input fed by the other players, the single corrupted player can fully determine the result.

Almost all constructions of randomness extractors following [17] can be divided into two steps. First, the two n-bit sources X, Y are "transformed" to a single r-bit source $Z = h(X,Y)$ with some structure, called a *non-oblivious bit-fixing source*. A resilient function $f\colon \{0,1\}^r \to \{0,1\}$ is then applied to Z so to obtain the output $\mathsf{Ext}(X,Y) = f(h(X,Y))$. In all works, the function h is based on non-malleable extractors or on related primitives such as correlation breakers. As mentioned above, the use of the resilient function implies that even a single corrupted player has influence $\Omega(\frac{\log r}{r})$ and so to obtain an error guarantee ε, the number of players r must be taken larger than $1/\varepsilon$. This results in running-time $\Omega(1/\varepsilon)$.[1]

1.2 Entropy-Resilient Functions

To obtain our condenser, we extend the notion of resilient functions to functions outputting many bits. Informally speaking, instead of considering an r-player game in which the bad players try to bias the output, we study a repeated game version in which the r players play for m rounds. The bad players attempt to decrease, with as high probability as they can, the min-entropy of the m-bit outcome (and we will even allow the bad players to cast their votes after the good players played all rounds).

Recall that, by [30], when $m = 1$, even a single player can bias the result by $\Omega(\frac{\log r}{r})$. Put differently, viewing this bias as the error of a deterministic extractor, the error is bound to be at least polynomially-small in the number of players. Our key insight is that when m becomes large, the probability that the bad players can reduce g bits of entropy from the output (creating an "entropy gap" of g) is *exponentially small* in g. We further show that this holds for a specific function f, induced by the Ajtai-Linial function, even when the honest players are only t-wise independent (for $t = \mathrm{polylog}(r/\varepsilon)$). Our analysis uses and extends ideas from the work of Chattopadhyay and Zuckerman [17].

[1] There is one exception to the above scheme. In [8], it is shown that if very strong t-non-malleable extractors can be explicitly constructed then the function f can be replaced with the parity function (which is not resilient at all) and low error two-source extractors with low min-entropy requirement can be obtained. However, it is not known how to explicitly construct such t-non-malleable extractors.

1.3 The Two-Source Condensers We Obtain

The main contribution of this work is an explicit construction of a two-source *condenser* with low error and small entropy gap, outputting almost all of the entropy from one source.

▶ **Definition 2** (Two-source condensers). *A function* $\mathsf{Cond}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ *is a* two-source condenser for min-entropy k with min-entropy gap g and error guarantee ε *if for every pair of independent* (n,k)*-sources,* $\mathsf{Cond}(X,Y)$ *is* ε*-close to an* $(m, m-g)$*-source.*

Note that a two-source extractor is a two-source condenser with entropy gap $g = 0$. Thus, condensers can be seen as a relaxation of extractors in which some, hopefully small, "gap" of min-entropy in the output distribution is allowed. Despite having a weaker guarantee, condensers play a key role in the construction of many types of randomness extractors, including two-source extractors [9], their variants [42, 6, 47, 41, 32], and seeded-extractors [28]. Most related to our work is a paper by Rao [40] that, for every $\delta > 0$, constructed a $\mathrm{poly}(n, \log(1/\varepsilon))$-time computable two-source condenser[2] for min-entropy $k = \delta n$ having $m = \Omega(\delta n)$ output bits with entropy gap $g = \mathrm{poly}(1/\delta, \log(1/\varepsilon))$.

In this work, we obtain a strongly polynomial-time construction of a two-source condenser with low error and small min-entropy gap.

▶ **Theorem 3** (Main result). *For all integers* n, k *and every* $\varepsilon > 0$ *such that* $n \geq k \geq \mathrm{polylog}(\frac{n}{\varepsilon})$*, there exists a* $\mathrm{poly}(n, \log(1/\varepsilon))$*-time computable two-source condenser*

$$\mathsf{Cond}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$$

for min-entropy k*, with error guarantee* ε*, min-entropy gap* $g = o(\log \frac{1}{\varepsilon})$*, and* $m = k - O(\log(1/\varepsilon))$ *output bits.*

Note that the entropy gap g is independent of the entropy k and scales *sub*-logarithmically with $1/\varepsilon$. We prove Theorem 3, whose formal statement is given in Theorem 31, in two steps. First, we construct a two-source condenser with the same guarantees as provided by Theorem 3, though only with $m = k^\alpha$ output bits, where $0 < \alpha < 1$ is some small universal constant (see Theorem 27). This part of the construction is based on our study of entropy-resilient functions (Section 3) and on the adaptation of the Chattopadhyay-Zuckerman construction for entropy-resilient functions. To reduce the huge entropy-loss we incur (i.e., to increase the output length from k^α to $k - O(\log(1/\varepsilon))$), in the second step, we construct a seedless condenser for block-sources–a result that we believe is of independent interest on which we now elaborate.

1.4 Seedless Condensers for a Single Block-Source

A (k_1, k_2)*-block-source* is a pair of random variables X_1, X_2 that, although may be dependent, have the following guarantee. First, X_1 is a k_1-source, and second, conditioned on any fixing of X_1, the random variable X_2 has min-entropy k_2. Throughout this section, we denote the length of X_1 by n_1 and the length of X_2 by n_2. Informally, the notion of a block-source "lies between" a single source and two independent sources. Indeed, any (k_1, k_2)-block-source is a $(k_1 + k_2)$-source. Moreover, if X_1 is a k_1-source and X_2 is an independent k_2-source then X_1, X_2 is a (k_1, k_2)-block-source.

[2] To the matter of fact, Rao entitled his construction a "two-source almost extractor" – a suitable name given its small entropy gap.

Block-sources are key to almost all constructions of seeded extractors as well as to the construction of Ramsey graphs. As mentioned above, there is no one-source extractor, whereas two-source extractors exist even for very low min-entropy. Despite being more structured than a general source, it is a well-known fact that there is no extractor for a single block-source (with non-trivial parameters).

A key component that allows us to increase the output length of our condenser discussed above is a seedless condenser for a single block-source. Let X_1, X_2 be a (k_1, k_2)-block-source. Write $g = n_2 - k_2$ for the entropy gap of X_2. For any given $\varepsilon > 0$, we show how to *deterministically* transform X_1, X_2 to a single m-bit random variable, where $m = k_1 - g - O(\log(1/\varepsilon))$, that is ε-close to having min-entropy $m - g - 1$. That is, informally, we are able to condense X_1 roughly to its entropy content k_1 using (the dependent random variable) X_2 while inheriting the entropy gap of X_2 both in the resulted entropy gap and entropy loss. We stress that this transformation is deterministic. This demonstrates that despite the well-known fact that a block-source extractor does not exist, a block-source condenser does. For a formal treatment, see Section 5.

1.5 A Three-Source Extractor

An immediate implication of Theorem 3 are low error three-source extractors supporting min-entropies $k_1 = k_2 = \text{polylog}(n/\varepsilon)$ and $k_3 = \Omega(\log(1/\varepsilon))$. This is achieved by feeding our condenser's output $Y = \mathsf{Cond}(X_1, X_2)$ as a seed to a seeded extractor that supports small entropies (see, e.g., Theorem 10), outputting $\mathsf{Ext}(X_3, Y)$.

▶ **Corollary 4.** *For all integers n, k, k' and every $\varepsilon > 0$ such that $n \geq k \geq \text{polylog}(\frac{n}{\varepsilon})$ and $n \geq k' \geq \Omega(\log \frac{1}{\varepsilon})$ there exists a $\text{poly}(n, \log(1/\varepsilon))$-time computable three-source extractor*

$$\mathsf{3Ext}\colon \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$$

for min-entropies k, k, k' and error guarantee ε, where $m = k' - O(\log(1/\varepsilon))$.

Proof. Set $\varepsilon' = \varepsilon^2$, let $k' \geq 2\log(1/\varepsilon') + O(1)$ and let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be the (k', ε')-strong-seeded-extractor guaranteed to us by Theorem 10, where $m = k' - 2\log(1/\varepsilon) - O(1)$ and $d = O(\log n \log(n/\varepsilon'))$.

Let k be large enough for $\mathsf{Cond}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^d$ given to us by Theorem 31 to output d bits with error $\varepsilon/2$ and entropy gap $g = o(\log(1/\varepsilon))$, so indeed $k \geq \text{polylog}(\frac{n}{\varepsilon})$.

Denote $Y = \mathsf{Cond}(X_1, X_2)$, so Y is $(\varepsilon/2)$-close to some random variable Y' having min-entropy at least $d - g$. Then:

$$\begin{aligned}
|\mathsf{Ext}(X_3, Y) - U_m \times Y| &\leq |\mathsf{Ext}(X_3, Y') - U_m \times Y'| + \frac{\varepsilon}{2} \\
&= \sum_{y \in \mathsf{supp}(Y')} \Pr[Y' = y] \cdot |\mathsf{Ext}(X_3, y) - U_m| + \frac{\varepsilon}{2} \\
&\leq \sum_{y \in \{0,1\}^d} 2^{-(d-g)} \cdot |\mathsf{Ext}(X_3, y) - U_m| + \frac{\varepsilon}{2} \\
&\leq 2^g \sum_{y \in \{0,1\}^d} 2^{-d} |\mathsf{Ext}(X_3, y) - U_m| + \frac{\varepsilon}{2} \\
&= 2^g \cdot |\mathsf{Ext}(X_3, U_d) - U_m \times U_d| + \frac{\varepsilon}{2} \;\leq\; 2^g \varepsilon' + \frac{\varepsilon}{2} \;\leq\; \varepsilon,
\end{aligned}$$

thereby also showing that $\mathsf{3Ext}(X_1, X_2, X_3) = \mathsf{Ext}(X_3, Y)$ is strong in Y. ◀

When ε is sub-polynomial in n (which is an interesting regime of parameters because then the two-source extractor of [17] is not polynomial-time computable) Corollary 4 improves upon known three-source extractors that either require all three-sources to have min-entropy $\text{polylog}(\frac{n}{\varepsilon})$ [34] or require, for any parameter of choice $\delta > 0$, min-entropies δn, $\text{poly}(\frac{1}{\delta})\log(\frac{n}{\varepsilon})$, $\text{poly}(\frac{1}{\delta})\log(\frac{\log n}{\varepsilon})$ [20].

We remark that the proof of Corollary 4 goes through because the tiny entropy gap g of $Y = \mathsf{Cond}(X_1, X_2)$ (where $g = o(\log \frac{1}{\varepsilon})$) allows us to use Y as a replacement to a truly uniform seed with only a minor loss in parameters. We believe this should also be true in other circumstances where random variables with a negligible entropy gap can replace uniform random variables. A recent example to this is the use of samplers with multiplicative error instead of standard samplers in [9].

To conclude, we believe that the use of entropy-resilient functions as a tool to extract almost all the entropy from bit-fixing sources while suffering only a small error is both natural and interesting on its own. We hope the tools and constructions developed in this paper will be of further use, possibly for constructing low error two-source extractors. In particular, we have seen in Corollary 4 that by using an independent third source and outputting $\mathsf{Ext}(X_3, \mathsf{Cond}(X_1, X_2))$ we get an excellent three-source extractor. An open problem left by our work is whether outputting $\mathsf{Ext}(X_2, \mathsf{Cond}(X_1, X_2))$ gives a low-error two-source extractor. We remark that a similar idea has been used in previous constructions [34, 10] and elsewhere. We were not able to prove that $\mathsf{Ext}(X_2, \mathsf{Cond}(X_1, X_2))$ gives a low-error two-source extractor and we leave this as an intriguing open problem.

2 Preliminaries

We use $\log(x)$ for $\log_2(x)$. For an integer n, we denote by $[n]$ the set $\{1, \ldots, n\}$. The density of a subset $B \subseteq A$ is denoted by $\mu(B) = \frac{|B|}{|A|}$.

2.1 Random Variables, Min-Entropy

The *statistical distance* between two distributions X and Y over the same domain Ω is defined by $\mathsf{SD}(X, Y) = \max_{A \subseteq \Omega}(\Pr[X \in A] - \Pr[Y \in A])$. If $\mathsf{SD}(X, Y) \leq \varepsilon$ we say X is ε-close to Y and denote it $X \approx_\varepsilon Y$. We denote by U_n the random variable distributed uniformly over $\{0,1\}^n$.

For a function $f\colon \Omega_1 \to \Omega_2$ and a random variable X distributed over Ω_1, $f(X)$ is the random variable distributed over Ω_2 obtained by choosing $x \sim X$ and outputting $f(x)$. For every $f\colon \Omega_1 \to \Omega_2$ and two random variables X, Y over Ω_1 it holds that $\mathsf{SD}(f(X), f(Y)) \leq \mathsf{SD}(X, Y)$.

The *min-entropy* of a random variable X is defined by

$$H_\infty(X) \;=\; \min_{x \in \mathsf{supp}(X)} \log \frac{1}{\Pr[X = x]}.$$

A random variable X is an (n, k)-source if X is distributed over $\{0,1\}^n$ and has min-entropy at least k. When n is clear from the context we sometimes omit it and simply say that X is a k-source.

2.2 Limited Independence

▶ **Definition 5.** *A distribution X over $\{0,1\}^n$ is called* (t, γ)-wise independent *if the restriction of X to every t coordinates is γ-close to U_t.*

▶ **Lemma 6** ([4])**.** *Let $X = X_1, \ldots, X_n$ be a distribution over $\{0,1\}^n$ that is (t, γ)-wise independent. Then, X is $(n^t\gamma)$-close to a t-wise independent distribution.*

2.3 Seeded Extractors

▶ **Definition 7** (Seeded extractors). *A function*

$$\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

is a (k,ε)-seeded-extractor if the following holds. For every (n,k)-source X, the output $\mathsf{Ext}(X,Y) \approx_\varepsilon U_m$, where Y is uniformly distributed over $\{0,1\}^d$ and is independent of X. Further, Ext is a (k,ε)-strong-seeded-extractor if $(\mathsf{Ext}(X,Y),Y) \approx_\varepsilon (U_m,Y)$.

▶ **Theorem 8** ([28]). *There exists a universal constant $c_{\mathsf{GUV}} \geq 2$ for which the following holds. For every integers $n \geq k$ and $\varepsilon > 0$ there exists a $\mathrm{poly}(n, \log(1/\varepsilon))$-time computable (k,ε)-strong-seeded-extractor*

$$\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

with seed length $d = c_{\mathsf{GUV}} \log(n/\varepsilon)$ and $m = k/2$ output bits.

Extractors can be used for sampling using weak sources.

▶ **Theorem 9** ([46]). *Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be a (k_1,ε)-seeded-extractor. Identify $\{0,1\}^d$ with $[2^d]$ and let $S(X) = \left\{\mathsf{Ext}(X,1),\ldots,\mathsf{Ext}(X,2^d)\right\}$. Then, for every (n,k_2)-source X and any set $T \subseteq \{0,1\}^m$,*

$$\Pr_{x\sim X}\left[\left|\frac{|S(x)\cap T|}{2^d} - \mu(T)\right| > \varepsilon\right] \;\leq\; 2^{-(k_2-k_1)}.$$

The following extractor allows us to extract all the min-entropy, at the cost of a larger seed-length.

▶ **Theorem 10** ([28]). *There exists a universal constant c such that the following holds. For all integers $n \geq k$ and any $\varepsilon > 0$ such that $k \geq 2\log(1/\varepsilon) + O(1)$, there exists a $\mathrm{poly}(n, \log(1/\varepsilon))$-time computable (k,ε)-strong-seeded-extractor*

$$\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

with seed length $d = c\log n \cdot \log\frac{n}{\varepsilon}$ and $m = k - 2\log\frac{1}{\varepsilon} - O(1)$ output bits.

2.4 Two-Source Condensers

▶ **Definition 11** (Condensers). *A function*

$$\mathsf{Cond}\colon \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$$

is an $((n_1,k_1),(n_2,k_2)) \to_\varepsilon (m, k' = m-g)$ condenser *if the following holds. For every (n_1,k_1)-source X_1 and an independent (n_2,k_2)-source X_2, the output $\mathsf{Cond}(X_1,X_2)$ is ε-close to an (m,k')-source. We refer to ε as the* error guarantee *and to g as the* entropy gap *of* Cond.

▶ **Definition 12** (Strong condensers). *A function*

$$\mathsf{Cond}\colon \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$$

is a $((n_1,k_1),(n_2,k_2)) \to_{\varepsilon_1,\varepsilon_2} (m,k')$-strong-condenser (in the first source) *if the following holds. For every (n_1,k_1)-source X_1 and an independent (n_2,k_2)-source X_2, with probability $1-\varepsilon_1$ over $x_1 \sim X_1$, the output $\mathsf{Cond}(x_1,X_2)$ is ε_2-close to an (m,k')-source.*

Similarly, one can define, in the natural way, a condenser that is strong in the second source.

2.5 Non-Malleable Extractors

▶ **Definition 13.** *A function* $\mathsf{nmExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a* (k,ε) t-non-malleable extractor*, if for every* (n,k)*-source* X*, for every independent random variable* Y *that is uniform over* $\{0,1\}^d$ *and every functions* $f_1,\ldots,f_t\colon \{0,1\}^d \to \{0,1\}^d$ *with no fixed-points*[3] *it holds that:*

$$(\mathsf{nmExt}(X,Y),\mathsf{nmExt}(X,f_1(Y)),\ldots,\mathsf{nmExt}(X,f_t(Y),Y) \approx_\varepsilon (U_m,\mathsf{nmExt}(X,f_1(Y)),\ldots,\mathsf{nmExt}(X,f_t(Y),Y)).$$

We will need the following lemma concerning the existence of a set of good seeds of a non-malleable extractor, given in [17].

▶ **Lemma 14** ([17])**.** *Let* $\mathsf{nmExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a* (k,ε) t*-non-malleable extractor. Let* X *be any* (n,k)*-source. Let* BAD *be the set defined by*

$$\mathrm{BAD} = \{r \in [D] \mid \exists \text{ distinct } r_1,\ldots,r_t \in [D], \forall i \in [t]\ r_i \neq r,\ |(\mathsf{nmExt}(X,r), \mathsf{nmExt}(X,r_1),\ldots,\mathsf{nmExt}(X,r_t)) - (U_m,\mathsf{nmExt}(X,r_1),\ldots,\mathsf{nmExt}(X,r_t))| > \sqrt{\varepsilon}\}.$$

Then, $\mu(\mathrm{BAD}) \leq \sqrt{\varepsilon}$*. We refer to the set* $[D] \setminus \mathrm{BAD}$ *as the set of* good seeds *(with respect to the underlying distribution of* X*).*

▶ **Lemma 15.** *Let* $X_1,\ldots,X_t$ *be random variables over* $\{0,1\}^m$*. Further suppose that for any* $i \in [t]$*,*

$$\left(X_i, \{X_j\}_{j\neq i}\right) \approx_\varepsilon \left(U_m, \{X_j\}_{j\neq i}\right).$$

Then, $(X_1,\ldots,X_t) \approx_{t\varepsilon} U_{tm}$*.*

Finally, good explicit constructions of t-non-malleable extractors exist. The following choice of parameters will be sufficient for us.

▶ **Theorem 16** ([15, 22, 35])**.** *There exists a universal constant* $c_{\mathsf{nm}} \geq 2$ *such that for all integers* n,k,t*, and every* $\varepsilon > 0$ *such that* $n \geq k \geq c_{\mathsf{nm}} t^2 \log^2(n/\varepsilon)$*, there exists a* $\mathrm{poly}(n,\log(1/\varepsilon))$*-time computable* (k,ε) t*-non-malleable extractor*

$$\mathsf{nmExt}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

with $m = \frac{k}{3t}$ *output bits and seed length* $d = c_{\mathsf{nm}} t^2 \log^2(n/\varepsilon)$*.*

2.6 Fooling AC Circuits

A Boolean circuit is an $\mathsf{AC}[d,s]$ circuit if it has depth d, size s and unbounded fan-in. We say that a circuit C with n input bits is ε*-fooled* by a distribution D if $\mathsf{SD}(C(D),D(U_n)) \leq \varepsilon$.

Harsha and Srinivasan [29], improving upon Braverman's seminal result [14] (see also [44]) proved:

▶ **Theorem 17** ([29])**.** *There exists a constant* $c > 0$ *such that the following holds. For every integers* s,d,t*, any* $\mathsf{AC}[d,s]$ *circuit is* ε*-fooled by any* t*-wise independent distribution, where* $\varepsilon = 2^{-\frac{t}{(\log s)^{c\cdot d}}}$*.*

[3] That is, for every i and every x, we have $f_i(x) \neq x$.

We need a slight generalization of Theorem 17:

▶ **Lemma 18.** *There exists a constant $c > 0$ such that the following holds for every integers n, m, d, s, where $m \leq s$. Let $C\colon \{0,1\}^n \to \{0,1\}^m$ be an $\mathsf{AC}[d,s]$ circuit. Then, C is ε-fooled by any t-wise independent distribution, where $\varepsilon = 2^{m - \frac{t}{(\log s)^{c \cdot d}}}$.*

Proof. Fix some $z \in \{0,1\}^m$ and consider the circuit $C_z\colon \{0,1\}^n \to \{0,1\}$ that given an input $x \in \{0,1\}^n$ checks whether $C(x) = z$. C_z can be constructed by adding an AND gate and m comparators on top of C, so clearly C_z is an $\mathsf{AC}[d+2, s']$ circuit for $s' = s + O(m)$. By Theorem 17, every t-wise distribution ε'-fools C_z, where

$$\varepsilon' = 2^{-\frac{t}{(\log s')^{c' \cdot (d+2)}}} \leq 2^{-\frac{t}{(\log s)^{c \cdot d}}}$$

for some universal constants $c, c' > 0$ (using the fact that $m \leq s$). That is, for every t-wise distribution D and $z \in \{0,1\}^m$, $\mathsf{SD}(C_z(D), C_z(U_n)) \leq \varepsilon'$. Now,

$$\begin{aligned}\varepsilon = \mathsf{SD}(C(D), C(U_n)) &= \frac{1}{2} \sum_{z \in \{0,1\}^m} |\Pr[C(D) = z] - \Pr[C(U_n) = z]| \\ &= \sum_{z \in \{0,1\}^m} \frac{1}{2} |\mathbb{E}[C_z(D)] - \mathbb{E}[C_z(U_n)]| \leq 2^m \varepsilon',\end{aligned}$$

as desired. ◀

3 Entropy-Resilient Functions

▶ **Definition 19** (Non-oblivious sources). *Let $\Sigma = \{0,1\}^m$. A (q,t)-non-oblivious Σ-fixing source $X = (X_1, \ldots, X_r)$ is a random variable over $\Sigma^r = \{0,1\}^{rm}$ for which there exists a set $R_{\mathsf{bad}} \subseteq [r]$ of cardinality $q' \leq q$ such that:*

- *The joint distribution of $\{(X_i)_j \mid i \in [r] \setminus R_{\mathsf{bad}}, j \in [m]\}$, denoted by G_X, is t-wise independent over $\{0,1\}^{(r-q')m}$; and*
- *Each of the random variables in $B_X \triangleq \{(X_i)_j\}$ with $i \in R_{\mathsf{bad}}$ and $j \in [m]$ may depend arbitrarily on all other random variables in G_X and B_X.*

If $t = (r-q')m$ we say X is a q-non-oblivious Σ-fixing source. If $m = 1$ we say X is a bit-fixing source and the definition coincides with the standard definition of non-oblivious bit-fixing sources [11]. When X is clear from context, we write G and B for G_X and B_X, respectively.

▶ **Definition 20** (Entropy-resilient functions). *Let $\Sigma = \{0,1\}^m$. A function $f\colon \Sigma^r \to \Sigma$ is a* (q,t,g,ε)-entropy-resilient function *if for every (q,t)-non-oblivious Σ-fixing source X over Σ^r, the output $f(X)$ is ε-close to an $(m, m-g)$-source. If $g = 0$ we say f is (q,t,ε)-resilient.*

3.1 Functions With One Output Bit

▶ **Definition 21.** *Let $f\colon \{0,1\}^r \to \{0,1\}$ be an arbitrary function. Let X be a (q,t)-non-oblivious bit-fixing source over $\{0,1\}^r$. Define $E(f)$ to be the event in which the bits tossed by the good players do not determine the value of the function f. We define the influence of the bad players by $I(f) = \Pr[E(f)]$.*

Balanced resilient functions can be seen as deterministic extractors against non-oblivious bit-fixing sources outputting one bit. Chattopadhyay and Zuckerman [17], followed by an improvement by Meka [37], derandomized the Ajtai-Linial function [2] and obtained an explicit construction of an almost-balanced resilient function which is also computable by monotone AC^0 circuits.

▶ **Theorem 22** ([17, 37]). *For every constant $0 < \delta < 1$, there exists a constant $c_\delta \geq 1$ such that for every constant $c \geq c_\delta$ and integer r there exists a monotone function $\mathsf{Res}\colon \{0,1\}^r \to \{0,1\}$ such that for every $t \geq c \log^4 r$,*

- *For every (q,t)-non-oblivious bit-fixing source X, $I(\mathsf{Res}) \leq c \cdot \frac{q}{r^{1-\delta}}$.*
- *For every t-wise independent distribution D, $\mathrm{bias}(\mathsf{Res}(D)) \leq r^{-1/c}$.*

The function Res is computable by a uniform depth 3 monotone circuit of size r^c. Further, the function $c_\delta(\delta)$ is continuous and monotonically decreasing.

Throughout the paper we make use of the following corollary.

▶ **Corollary 23.** *For every constant $0 < \gamma < 1$ there exist constants $0 < \alpha < \beta < 1$ such that for every integer r there exists a function $\mathsf{Res}\colon \{0,1\}^r \to \{0,1\}$ which for every $t \geq \frac{1}{\beta} \log^4 r$ satisfies: For every $(r^{1-\gamma}, t)$-non-oblivious bit-fixing source X,*

$$I(\mathsf{Res}) \leq \frac{1}{\beta} \cdot r^{-\alpha},$$
$$\mathrm{bias}\left(\mathsf{Res}(X) \mid \neg E(\mathsf{Res})\right) \leq \frac{3}{\beta} \cdot r^{-\alpha}.$$

The function Res is computable by a uniform depth 3 monotone circuit of size $r^{\frac{1}{\beta}}$.

Proof. Using the notations of Theorem 22, assume that for every η, $c_\eta > \frac{1}{2\eta}$ (if not, we can always increases c_η). Given $\gamma > 0$, set δ to be the constant satisfying the equation $f(\delta) = \delta - \gamma + \frac{1}{2c_\delta} = 0$. Such a δ exists, as $f(\delta) \leq 2\delta - \gamma$ and therefore $f(\delta) < 0$ when δ approaches 0, and $f(\delta) > 0$ when δ approaches γ. Note that by our choice of δ, it holds that

$$\delta < \gamma = \delta + \frac{1}{2c_\delta} < \delta + \frac{1}{c_\delta}.$$

Set $\alpha = \gamma - \delta > 0$ and $\beta = \frac{1}{c_\delta}$. Note that indeed $\beta > \alpha$.

By Theorem 22, applied with the constant δ, it holds that $I(\mathsf{Res}) \leq c_\delta \frac{r^{1-\gamma}}{r^{1-\delta}} = \frac{1}{\beta} r^{-\alpha}$. Further, $\mathrm{bias}(\mathsf{Res}(D)) \leq r^{-\beta}$.

Following similar arguments as in [17], we have that $\mathrm{bias}(\mathsf{Res}(X)) \leq \frac{1}{\beta} r^{-\alpha} + r^{-\beta}$, so

$$\mathrm{bias}\left(\mathsf{Res}(X) \mid \neg E(\mathsf{Res})\right) \leq \frac{\frac{1}{\beta} r^{-\alpha} + r^{-\beta}}{1 - \frac{1}{\beta} r^{-\alpha}} \leq \frac{3}{\beta} r^{-\alpha}. \qquad \blacktriangleleft$$

3.2 Functions With Multiple Output Bits

The output bit of a (q,t,ε)-resilient function $f\colon \{0,1\}^r \to \{0,1\}$ applied to a (q,t)-non-oblivious bit-fixing source is indeed ε-close to uniform, but, as shown by [30] even when $q = 1$, ε cannot be smaller that $\frac{\ln r}{r}$ (and the simpler bound $\varepsilon \geq \frac{1}{r}$ is almost trivial). We show that when we output many bits, and allow $o(\log \frac{1}{\varepsilon})$ entropy gap, we may obtain much smaller error. We do that by exhibiting an entropy-resilient function based on a parallel application of the (derandomized version of the) Ajtai-Linial function.

A construction of an entropy-resilient function. Given a constant $0 < \gamma < 1$ and integers $r \geq m$ let $\mathsf{Res}\colon \{0,1\}^r \to \{0,1\}$ be the function guaranteed by Corollary 23 with respect to γ. Define $\Sigma = \{0,1\}^m$ and $\mathsf{EntRes}\colon \Sigma^r \to \Sigma$ as follows. On input $x \in \Sigma^r$,

$$\mathsf{EntRes}(x) = (\mathsf{Res}(x^{(1)}), \ldots, \mathsf{Res}(x^{(m)})),$$

where x_i stands for the i-th column of x, when we view x as a $r \times m$ table.

▶ **Theorem 24.** *For every constant $0 < \gamma < 1$ there exist constants $0 < \alpha < 1$ and $c' \geq 1$ such that the following holds. For every integers r, $m \leq r^{\alpha/2}$, every $\varepsilon > 0$, and for every integer $t \geq m \cdot (\log r)^{c'}$, the function $\mathsf{EntRes}\colon \Sigma^r \to \Sigma$ is $(q = r^{1-\gamma}, t, g, \varepsilon)$-entropy-resilient with entropy gap $g = o(\log(1/\varepsilon))$.*

The proof of Theorem 24 is done in two steps. First, in Section 3.2.1, we analyze the theorem for the special case in which the distribution G_X of the given non-oblivious Σ-fixing source X is uniform. Then, based on that result, in Section 3.2.2 we prove Theorem 24.

3.2.1 The Uniform Case

In this section, we prove the following lemma.

▶ **Lemma 25.** *Keeping the notations of Theorem 24, the function $\mathsf{EntRes}\colon \Sigma^r \to \Sigma$ is $(q = r^{1-\gamma}, g, \varepsilon)$-entropy-resilient with entropy gap*

$$g = c_{\mathsf{ent}_1} \frac{\ln \frac{1}{\varepsilon}}{\ln \ln \frac{1}{\varepsilon} + c_{\mathsf{ent}_2} \ln r} = o(\log(1/\varepsilon))$$

for some universal constant $c_{\mathsf{ent}_1} > 0$ and a constant $c_{\mathsf{ent}_2} > 0$ that depends only on γ.

Proof of Lemma 25. Let X be a $(q = r^{1-\gamma})$-non-oblivious Σ-fixing source. Let $R_{\mathsf{bad}} \subseteq [r]$ be the set of bad players, and E_i the event that the values of the good players in $X^{(i)}$ do not determine the value of Res. Note that we shall also denote E_i as an indicator for that event.

By Corollary 23, there exists constants $0 < \alpha < \beta < 1$ such that $\Pr[E_i = 1] \leq \frac{1}{\beta} \cdot r^{-\alpha}$ for every $i \in [m]$. Observe that the random variables $E_1, \ldots, E_m$ are independent, as the value of E_i depends only on the values of the good players in the i-th column, and by assumption all these values are independent of the corresponding values in the other columns. Write $\mu = m \cdot \frac{1}{\beta} \cdot r^{-\alpha}$ and note that since $m \leq r^{\alpha/2}$, $\mu < 1$. Set

$$c = \frac{4 \ln \frac{1}{\varepsilon}}{\mu} \cdot \frac{1}{\ln \frac{\ln \frac{1}{\varepsilon}}{\mu}}$$

and observe that $c > 1$. By the Chernoff bound,

$$\Pr\left[\sum_{i=1}^{m} E_i > c\mu\right] \leq \left(\frac{e^{c-1}}{c^c}\right)^{\mu} \leq e^{-\frac{1}{2}\mu c \ln c} \leq \varepsilon,$$

where the last inequality follows from the fact that $c \ln c \geq \frac{2 \ln \frac{1}{\varepsilon}}{\mu}$.

By Corollary 23, for every $i \in [m]$,

$$\mathrm{bias}\left(\mathsf{Res}(X_i) \mid E_i = 0\right) \leq \frac{3}{\beta} \cdot r^{-\alpha}.$$

Assume that the event $\sum_{i=1}^{m} E_i \leq c\mu$ holds, and let $I \subseteq [m]$, $|I| \geq m - c\mu$ be the set of good columns I for which $E_i = 0$. For every $w \in \{0,1\}^m$, since the random variables $\{\mathsf{EntRes}(X)_i\}_{i \in I}$ are independent, we have:

$$\Pr[\mathsf{EntRes}(X) = w] \leq \Pr[\mathsf{EntRes}(X)_I = w_I] \leq \left(\frac{1}{2} + \frac{3}{\beta} \cdot r^{-\alpha}\right)^{m-c\mu}$$
$$\leq 2^{-m+c\mu} e^{\frac{6}{\beta} r^{-\alpha} m} \leq 2^{-m+c\mu} 2^{10\mu}.$$

Now, we have

$$c\mu + 10\mu \;\leq\; 2c\mu \;\leq\; \frac{8 \ln \frac{1}{\varepsilon}}{\ln \ln \frac{1}{\varepsilon} + \ln \frac{1}{\mu}} \;\leq\; \frac{8 \ln \frac{1}{\varepsilon}}{\ln \ln \frac{1}{\varepsilon} + \frac{4}{\alpha} \ln r} \;=\; o\left(\log \frac{1}{\varepsilon}\right).$$

We have shown that except with probability ε, the output $\mathsf{EntRes}(X)$ has min-entropy $m - o(\log(1/\varepsilon))$, as desired. More specifically, the min-entropy in the good columns alone is at least $m - o(\log(1/\varepsilon))$, and we stress that the good columns are not fixed but depend on the sample itself. ◀

3.2.2 The Bounded-Independence Case – Proof of Theorem 24

Throughout this section, we use the same notations as in Lemma 25. We are given X that is a (q,t)-non-oblivious Σ-fixing source. We use a similar approach to the one taken in [17]. For the sake of the proof, we:

- Let GU be the distribution in which the good players are jointly uniform, and the bad players are arbitrary.
- Define a small-depth circuit C' that is related to EntRes so that $H_\infty(\mathsf{EntRes}(X)) \geq H_\infty(C'(X))$.

We will show that $C'(X)$ and $C'(GU)$ are statistically close to each other. Finally, the results of Section 3.2.1 proves that except for a small probability, $H_\infty(C'(GU)) \geq m - o(\log(1/\varepsilon))$.

Proof of Theorem 24. Fix a (q,t)-non-oblivious Σ-fixing source X. Let GU be the distribution where the good players are jointly uniform, and the bad players are arbitrary. We construct a circuit $C' \colon \{0,1\}^{rm} \to \{0,1\}^m$ such that:

$$(C'(x))_i = \begin{cases} \mathsf{EntRes}(x)_i & \text{If } E_i(x) = 0, \\ 0 & \text{Otherwise.} \end{cases}$$

Recall that E_i is *fully determined* by the good players, and so does $\mathsf{EntRes}(X)_i$ when $E_i = 0$. Hence, C' is fully determined by the good players.

We can write a small-depth circuit computing C'. Let C be the depth-3 size $r^{1/\beta}$ circuit that computes the function $\mathsf{Res} \colon \{0,1\}^r \to \{0,1\}$ as guaranteed by Theorem 22. Construct a circuit for C' as follows:

- For $i \in [m]$ and $b \in \{0,1\}$ let $C_{i,b}$ be a copy of C where we wire $(x_i)_j$ for every good player $j \in [r]$, and the value b for every bad player.
- The top part contains m comparators, outputting the output of $C_{i,0}$ if the output of $C_{i,0}$ is the same as the output of $C_{i,1}$, and 0 otherwise.

The circuit has depth 4 and size $s'' = O(mr^{1/\beta})$ and its correctness is guaranteed by the fact that Res is monotone (so it is sufficient to consider the case where the bad players voted unanimously).

By Lemma 18, $\mathsf{SD}(C'(GU), C'(X)) \leq 2^{m - \frac{t}{(\log(mr))^{c''}}}$ for some large enough universal constant $c'' > 0$. For every $w \in \{0,1\}^m$:

$$\begin{aligned}\Pr\left[\mathsf{EntRes}(X) = w\right] &\leq \Pr\left[\mathsf{EntRes}(X)_I = w_I\right] = \Pr\left[C'(X)_I = w_I\right] \\ &\leq \Pr\left[C'(GU)_I = w_I\right] + 2^{m - \frac{t}{(\log(mr))^{c''}}} \\ &\leq 2^{-m + \frac{8\ln\frac{1}{\varepsilon}}{\ln\ln\frac{1}{\varepsilon} + \frac{4}{\alpha}\ln r}} + 2^{m - \frac{t}{(\log(mr))^{c''}}},\end{aligned}$$

where in the last inequality we have used Lemma 25. We can set the constant c' stated in the theorem to be larger than c'' and get that

$$\Pr\left[\mathsf{EntRes}(X) = w\right] \;\leq\; 2 \cdot 2^{-m + \frac{8\ln\frac{1}{\varepsilon}}{\ln\ln\frac{1}{\varepsilon} + \frac{4}{\alpha}\ln r}}.$$

To conclude, note that the above holds with probability at least $1-\varepsilon$, and then $\mathsf{EntRes}(X)$ has min-entropy at least $-1 + m - \frac{8\ln\frac{1}{\varepsilon}}{\ln\ln\frac{1}{\varepsilon} + \frac{4}{\alpha}\ln r} = m - o(\log(1/\varepsilon))$, as desired. ◀

4 Low Error Two-Source Condensers With High Entropy Loss

Chattopadhyay and Zuckerman [17] showed a reduction from two independent sources to non-oblivious bit-fixing sources. In Section 4.1 we extend this to many output bits and show a reduction from two independent sources to non-oblivious Σ-fixing sources. Our reduction is similar to the one in [17], and here:

- We let the non-malleable extractors output m bits rather than a single bit, obtaining a non-oblivious Σ-fixing source for $\Sigma = \{0,1\}^m$.
- Correspondingly, we apply our entropy-resilient function EntRes whereas in [17] the function Res is applied.

In Section 4.2 we use this together with the results of Section 3 to get a low error two-source condenser with many output bits, yet still far from getting almost all of the possible entropy from the two sources.

4.1 From Two Independent Sources to a Non-Oblivious Σ-Fixing Source

In this section, we revisit the [17] transformation of two independent sources to a non-oblivious bit-fixing source (i.e., with $m = 1$), and extend it to sources with several bits. Throughout this section, we refer to $c_{\mathsf{GUV}}, c_{\mathsf{nm}}$ as the constants that appear in Theorem 8 and Theorem 16, respectively.

▶ **Theorem 26.** *For every integers n, t, m, k, with $n \geq k \geq (tm\log n)^5$ and set $\Sigma = \{0,1\}^m$, there exists a $\mathrm{poly}(n)$-time computable function $\mathsf{TwoSourcesToNOF}\colon \{0,1\}^n \times \{0,1\}^n \to \Sigma^r$, where $r = n^{2c_{\mathsf{GUV}}}$ such that the following holds. Let X_1, X_2 be a pair of independent (n,k)-sources. Then, with probability at least $1 - 2^{-k/2}$ over $x_2 \sim X_2$, the output*

$$\mathsf{TwoSourcesToNOF}(X_1, x_2)$$

is (n^{-mt})-close to an $\left(r^{1-\frac{1}{4c_{\mathsf{GUV}}}}, t\right)$-non-oblivious Σ-fixing source.

Proof. We start by setting the following parameters:

Setting of parameters.

- Set $\varepsilon_{\mathsf{GUV}} = \frac{1}{n}$.
- Set $d_{\mathsf{GUV}} = c_{\mathsf{GUV}} \log\left(\frac{n}{\varepsilon_{\mathsf{GUV}}}\right) = 2c_{\mathsf{GUV}} \log n$.
- Set $\varepsilon_{\mathsf{nm}} = 2^{-4mt(d_{\mathsf{GUV}}+\log m)}$.
- Set $d_{\mathsf{nm}} = c_{\mathsf{nm}} t^2 \log^2\left(\frac{n}{\varepsilon_{\mathsf{nm}}}\right)$.

Note that $\varepsilon_{\mathsf{nm}} = 2^{-\Theta(mt\log n)}$ and that $d_{\mathsf{nm}} = \Theta(t^4 m^2 \log^2 n)$.

Building blocks. For the construction of $\mathsf{TwoSourcesToNOF}$, we make use of the following ingredients:

- Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^{d_{\mathsf{GUV}}} \to \{0,1\}^{d_{\mathsf{nm}}}$ be the $(k/2, \varepsilon_{\mathsf{GUV}})$-strong-seeded-extractor, guaranteed by Theorem 8. One can verify that $k/2 \geq 2d_{\mathsf{nm}}$ as required by Theorem 8.
- Let $\mathsf{nmExt}\colon \{0,1\}^n \times \{0,1\}^{d_{\mathsf{nm}}} \to \{0,1\}^m$ be the $(k, \varepsilon_{\mathsf{nm}})$ t-non-malleable extractor, guaranteed by Theorem 16. Note that $k \geq 3tm$ so the hypothesis of Theorem 16 is met with our choice of parameters.

The construction. We identify $[r]$ with $\{0,1\}^{d_{\mathsf{GUV}}}$. On inputs $x_1, x_2 \in \{0,1\}^n$, we define $\mathsf{TwoSourcesToNOF}(x_1, x_2)$ to be the $r \times m$ matrix whose i-th row is given by

$$\mathsf{TwoSourcesToNOF}(x_1, x_2)_i = \mathsf{nmExt}(x_1, \mathsf{Ext}(x_2, i)).$$

Analysis. Write $D_{\mathsf{nm}} = 2^{d_{\mathsf{nm}}}$ and identify $[D_{\mathsf{nm}}]$ with $\{0,1\}^{d_{\mathsf{nm}}}$. Let $G \subseteq [D_{\mathsf{nm}}]$, $|G| \geq (1 - \sqrt{\varepsilon_{\mathsf{nm}}})D_{\mathsf{nm}}$, be the set of good seeds guaranteed by Lemma 14. By Lemma 15, for any distinct $r_1, \ldots, r_t \in G$,

$$(\mathsf{nmExt}(X_1, r_1), \ldots, \mathsf{nmExt}(X_1, r_t)) \approx_{t\sqrt{\varepsilon_{\mathsf{nm}}}} U_{tm}.$$

Let $S(X_2) = \left\{\mathsf{Ext}(X_2, 1), \ldots, \mathsf{Ext}(X_2, 2^{d_{\mathsf{nm}}})\right\}$. By Theorem 9,

$$\Pr_{x_2 \sim X_2}\left[|S(x_2) \cap G| \leq (1 - \sqrt{\varepsilon_{\mathsf{nm}}} - \varepsilon_{\mathsf{GUV}}) \cdot r\right] \leq 2^{-k/2}.$$

We say that $x_2 \in \mathsf{supp}(X_2)$ is good if it induces a good sample, that is if $|S(x_2) \cap G| > (1 - \sqrt{\varepsilon_{\mathsf{nm}}} - \varepsilon_{\mathsf{GUV}})r$. Fix a good x_2 and let $Z = \mathsf{TwoSourcesToNOF}(X_1, x_2)$. In the good seeds, every t elements of Z are $(t\sqrt{\varepsilon_{\mathsf{nm}}})$-close to uniform, and there are at most $q \leq (\sqrt{\varepsilon_{\mathsf{nm}}} + \varepsilon_{\mathsf{GUV}})r$ bad rows. Applying Lemma 6, we get that Z is $\zeta = t\sqrt{\varepsilon_{\mathsf{nm}}}(rm)^{mt}$-close to a (q,t)-non-oblivious bit-fixing source. By our choice of $\varepsilon_{\mathsf{nm}}$,

$$\zeta = 2^{-2mt(d_{\mathsf{GUV}}+\log m)} 2^{mt\log(rm)} \leq 2^{-mt\log r} \leq n^{-mt}.$$

Further,

$$q \leq (\sqrt{\varepsilon_{\mathsf{nm}}} + \varepsilon_{\mathsf{GUV}})r \leq 2\varepsilon_{\mathsf{GUV}} r = 2r^{-\frac{1}{2c_{\mathsf{GUV}}}+1} \leq r^{1-\frac{1}{4c_{\mathsf{GUV}}}}.$$

We now analyse the running-time. We first apply Ext to compute $S(x_2)$, which takes time $\mathrm{poly}(n, \log(1/\varepsilon_{\mathsf{GUV}})) = \mathrm{poly}(n)$. Then, applying each nmExt takes $\mathrm{poly}(n, \log(1/\varepsilon_{\mathsf{nm}})) = \mathrm{poly}(n, m, t, d_{\mathsf{GUV}}) = \mathrm{poly}(n)$ time and we do it for $r = \mathrm{poly}(n)$ times. Overall, the running time is $\mathrm{poly}(n)$, as required. In particular, as $n \geq k \geq m$, the running time is also poly-logarithmic in the errors of the construction, $2^{-k/2}$ and n^{-mt}. ◀

4.2 Low Error Condensers With High Entropy Loss

▶ **Theorem 27.** *There exists a universal constant $c \geq 1$ such that the following holds. For every integers n, k, m and every $\varepsilon > 0$ such that $n \geq k \geq (m \log(n/\varepsilon))^c$ there exists a* $\mathrm{poly}(n)$*-time computable* $((n,k),(n,k)) \to_{\varepsilon, 2^{-k/2}} (m, m-g)$*-condenser*

$$\mathsf{Cond}' \colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m ,$$

that is strong in the second source, with entropy gap $g = o(\log(1/\varepsilon))$.

Proof. We start by describing the construction of our condenser Cond' and then turn to the analysis. As usual, we let c_{GUV} be the constant that is given by Theorem 8.

Setting of parameters.

- Set $\gamma = \frac{1}{4c_{\mathsf{GUV}}}$ and let $0 < \alpha < \beta < 1$ and c' be the constants from Theorem 24 with respect to this γ.
- Set $r = n^{2c_{\mathsf{GUV}}}$.
- Set $t = m \cdot (\log(r/\varepsilon))^{c'}$.
- Set c, the constant stated in this theorem, to $c = \max(10c', 2/\alpha)$.

Building blocks.

- Let $\mathsf{TwoSourcesToNOF} \colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{r \times m}$ be the function that is given by Theorem 26. We are about to apply $\mathsf{TwoSourcesToNOF}$ to (n,k)-sources, and indeed k is large enough to satisfy the hypothesis of Theorem 26.
- Let $\mathsf{EntRes} \colon \{0,1\}^{r \times m} \to \{0,1\}^m$ be the function from Theorem 24 when set with the parameter γ as defined above. Note that the hypothesis of Theorem 24 holds, as since $c \geq 2/\alpha$ we have that $m < r^{\alpha/2}$, and t is large enough.

The construction. On inputs $x_1, x_2 \in \{0,1\}^n$, we define

$$\mathsf{Cond}'(x_1, x_2) = \mathsf{EntRes}\left(\mathsf{TwoSourcesToNOF}(x_1, x_2)\right).$$

Analysis. Clearly, EntRes is computable in $\mathrm{poly}(m, r) = \mathrm{poly}(n)$ time. Let X_1, X_2 be a pair of independent (n,k)-sources. By Theorem 26, except with probability $2^{-k/2}$ over $x_2 \sim X_2$, the output $\mathsf{TwoSourcesToNOF}(X_1, x_2)$ is n^{-mt}-close to an $(r^{1-\gamma}, t)$-non-oblivious bit-fixing source. For every x_2 for which this event holds, the output $\mathsf{EntRes}(\mathsf{TwoSourcesToNOF}(X_1, x_2))$ is $(n^{-mt} + \varepsilon)$-close to an $(m, m - o(\log(1/\varepsilon)))$-source, and $n^{-mt} \leq \varepsilon$. ◀

5 Deterministically Condensing a Single Block-Source

A distribution (X, Y) is a blockwise source if both X has sufficient min-entropy and also for every $x \in \mathsf{supp}(X)$, $(Y \mid X = x)$ has sufficient min-entropy. In this section we show how to deterministically condense a blockwise source into a source having very small entropy gap, using the connection between condensers with small entropy gap and samplers with multiplicative error and ideas from [43]. In the next section we will use it to significantly increase the output length of the condenser from Section 4.2.

▶ **Lemma 28** (Deterministically condensing a blockwise source)**.** *Let X be an (n,k)-source. Let Y be a d-bit random variable (that may depend on X) such that for every $x \in \mathsf{supp}(X)$, the random variable $(Y \mid X = x)$ is ε_{B}-close to a $(d, d-g)$-source.*

Let $\mathsf{Ext} \colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be a $(k_{\mathsf{Ext}}, \varepsilon_{\mathsf{Ext}})$-seeded-extractor. Suppose $k \geq k_{\mathsf{Ext}} + \log(1/\varepsilon_{\mathsf{Ext}})$. Then, $\mathsf{Ext}(X, Y)$ is $(2^{g+2}\varepsilon_{\mathsf{Ext}} + 2\varepsilon_{\mathsf{B}})$-close to an $(m, m-g-1)$-source.

Proof. Fix any $T \subseteq \{0,1\}^m$. Define the set

$$\mathsf{OverHit}_T \;=\; \left\{ x \in \{0,1\}^n : \Pr_{y \sim U_d}[\mathsf{Ext}(x,y) \in T] > \mu(T) + \varepsilon_{\mathsf{Ext}} \right\}.$$

▷ Claim 29. $|\mathsf{OverHit}_T| < 2^{k_{\mathsf{Ext}}}$.

Proof. Suppose towards a contradiction that $|\mathsf{OverHit}_T| \geq 2^{k_{\mathsf{Ext}}}$ and let B denote the random variable that is uniform over the set $\mathsf{OverHit}_T$. Since B has min-entropy at least k_{Ext}, the output $\mathsf{Ext}(B, U_d)$ is $\varepsilon_{\mathsf{Ext}}$-close to uniform, and therefore $\Pr_{x \sim B, y \sim U_d}[\mathsf{Ext}(x,y) \in T] \;\leq\; \mu(T) + \varepsilon_{\mathsf{Ext}}$. This stands in contradiction to the definition of B. ◁

Now,

$$\Pr\left[\mathsf{Ext}(X,Y) \in T\right] \leq \Pr[\mathsf{Ext}(X,Y) \in T \mid X \notin \mathsf{OverHit}_T] + \Pr[X \in \mathsf{OverHit}_T].$$

By Claim 29, $\Pr[X \in \mathsf{OverHit}_T] \leq 2^{k_{\mathsf{Ext}} - k}$. Also, for every $x \notin \mathsf{OverHit}_T$ let

$$GY_x = \left\{ y \in \{0,1\}^d : \mathsf{Ext}(x,y) \in T \right\}.$$

By definition, $\mu(GY_x) \leq \mu(T) + \varepsilon_{\mathsf{Ext}}$. Also, $Y|(X=x)$ is ε_{B}-close to some random variable Y'_x having support size at least 2^{d-g}. Therefore,

$$\begin{aligned}\Pr_{y \sim (Y|X=x)}[\mathsf{Ext}(x,y) \in T] &= \Pr_{y \sim (Y|X=x)}[y \in GY_x] \;\leq\; \varepsilon_{\mathsf{B}} + \Pr[Y'_x \in GY_x] \\ &\leq \varepsilon_{\mathsf{B}} + \frac{|GY_x|}{2^{d-g}} \;\leq\; \varepsilon_{\mathsf{B}} + 2^g(\mu(T) + \varepsilon_{\mathsf{Ext}}).\end{aligned}$$

Thus,

$$\begin{aligned}\Pr\left[\mathsf{Ext}(X,Y) \in T\right] &\leq \Pr[\mathsf{Ext}(X,Y) \in T \mid X \notin \mathsf{OverHit}_T] + \Pr[X \in \mathsf{OverHit}_T] \\ &\leq 2^g\mu(T) + 2^g\varepsilon_{\mathsf{Ext}} + \varepsilon_{\mathsf{B}} + 2^{k_{\mathsf{Ext}} - k} \leq 2^g\mu(T) + (2^g+1)\varepsilon_{\mathsf{Ext}} + \varepsilon_{\mathsf{B}}.\end{aligned}$$

But,

▷ Claim 30. Let Z be a random variable over n-bit strings such that for every $T \subseteq \{0,1\}^n$, $\Pr[Z \in T] \leq 2^g\mu(T) + \varepsilon$. Then, Z is 2ε-close to an $(n, n-g-1)$-source.

Proof. Set $H = \left\{ x : \Pr[Z = x] > 2^{-(n-g-1)} \right\}$. On the one hand,

$$\Pr\left[Z \in H\right] = \sum_{x \in H} \Pr\left[Z = x\right] \geq 2^{g+1}\mu(H).$$

On the other hand, by our assumption, $\Pr\left[Z \in H\right] \leq 2^g\mu(H) + \varepsilon$. Together, we get that $2^g\mu(H) \leq \varepsilon$. Thus, $\Pr\left[Z \in H\right] \leq 2\varepsilon$. As H are all the heavy elements, we conclude that Z is 2ε-close to a distribution with $n-g-1$ min-entropy. ◁

We can therefore summarize that $\mathsf{Ext}(X,Y)$ is $(2^{g+2}\varepsilon_{\mathsf{Ext}} + 2\varepsilon_{\mathsf{B}})$-close to an $(m, m-g-1)$-source. ◀

6 Low Error Two-Source Condensers

In this section we will construct our low error condenser, with small entropy gap outputting many bits, by exploiting the block-wise structure of our previous construction. Roughly speaking, we are close to a scenario in which X_2 has sufficient min-entropy and also for every fixing of $x_2 \in \mathsf{supp}(X_2)$, the random variable $\mathsf{Cond}'(X_1, x_2)$ is close to uniform. The result of Section 5 can then be applied – allowing us to extract almost all the entropy from one of the sources. To that end, we prove the following theorem, which readily implies Theorem 3.

▶ **Theorem 31** (Main theorem). *There exists a universal constant $c \geq 1$ such that the following holds. For every integers $n \geq k$ and every $\varepsilon > 0$ such that $k \geq \log^c(n/\varepsilon)$ there exists a $\mathrm{poly}(n, \log(1/\varepsilon))$-time computable $((n,k),(n,k)) \to_\varepsilon (m, m-g)$ two-source condenser*

$$\mathsf{Cond}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$$

with $m = k - 5\log(1/\varepsilon) - O(1)$ and $g = o(\log(1/\varepsilon))$.

Proof. We start by setting some parameters.

Parameters.

- Set $\varepsilon_{\mathsf{Cond}'} = \varepsilon/8$.
- Set $\varepsilon_{\mathsf{Ext}} = \varepsilon^2/32$.
- Set $k_{\mathsf{Ext}} = k - \log(2/\varepsilon)$.
- Set $d_{\mathsf{Ext}} = c' \log n \cdot \log(n/\varepsilon_{\mathsf{Ext}})$ where c' is the constant that is given by Theorem 10.

For the construction we make use of the following building blocks.

- Let $\mathsf{Ext}\colon \{0,1\}^n \times \{0,1\}^{d_{\mathsf{Ext}}} \to \{0,1\}^m$ be the $(k_{\mathsf{Ext}}, \varepsilon_{\mathsf{Ext}})$-strong-seeded-extractor that is given by Theorem 10. By that theorem, $m = k_{\mathsf{Ext}} - 2\log(1/\varepsilon_{\mathsf{Ext}}) - O(1)$.
- Let $\mathsf{Cond}'\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{d_{\mathsf{Ext}}}$ be the $((n,k),(n,k)) \to_{\varepsilon_{\mathsf{Cond}'}, 2^{-k/2}} (d_{\mathsf{Ext}}, d_{\mathsf{Ext}} - g')$-condenser, strong in the second source, that is given by Theorem 27, with $g' = o(\log(1/\varepsilon_{\mathsf{Cond}'}))$. Note that our choice of parameters satisfies the hypothesis of Theorem 27 for a large enough constant c.

The construction. On inputs $x_1, x_2 \in \{0,1\}^n$, we define

$$\mathsf{Cond}(x_1, x_2) = \mathsf{Ext}(x_2, \mathsf{Cond}'(x_1, x_2)).$$

Analysis. Let X_1, X_2 be a pair of independent (n,k)-sources. By Theorem 27, with probability at least $1 - 2^{-k/2}$ over $x_2 \sim X_2$, the random variable $\mathsf{Cond}'(X_1, x_2)$ is $\varepsilon_{\mathsf{Cond}'}$-close to a $(d, d-g')$-source. Lemma 28 implies that $\mathsf{Ext}(X_2, \mathsf{Cond}'(X_1, X_2))$ is $2^{-k/2} + (2^{g'+2}\varepsilon_{\mathsf{Ext}} + 2\varepsilon_{\mathsf{Cond}'})$-close to an $(m, m-g'-1)$-source.

By our choice of parameters, $2^{-k/2} + 2^{g'+1}\varepsilon_{\mathsf{Ext}} + 2\varepsilon_{\mathsf{Cond}'} \leq \varepsilon$. Note that $k - m = \log(2/\varepsilon) + 2\log(1/\varepsilon_{\mathsf{Ext}}) = 5\log(1/\varepsilon) + O(1)$. The running-time of the construction readily follows from the running-times of Cond' and Ext. ◀

References

1 H. L. Abbott. Lower bounds for some Ramsey numbers. *Discrete Mathematics*, 2(4):289–293, 1972.

2 M. Ajtai and N. Linial. The influence of large coalitions. *Combinatorica*, 13(2):129–145, 1993.

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

4 N. Alon, O. Goldreich, and Y. Mansour. Almost k-wise independence versus k-wise independence. *Information Processing Letters*, 88(3):107–110, 2003.

5 B. Barak. A simple explicit construction of an $n^{\widetilde{O}(\log n)}$-Ramsey graph. *arXiv preprint*, 2006. arXiv:math/0601651.

6 B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. *Journal of the ACM (JACM)*, 57(4):20, 2010.

7 B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction. *Annals of Mathematics*, 176(3):1483–1544, 2012.

8 A. Ben-Aroya, E. Chattopadhyay, D. Doron, X. Li, and A. Ta-Shma. A New Approach for Constructing Low-Error, Two-Source Extractors. In *LIPIcs-Leibniz International Proceedings in Informatics*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

9 A. Ben-Aroya, D. Doron, and A. Ta-Shma. An efficient reduction from two-source to non-malleable extractors: achieving near-logarithmic min-entropy. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 1185–1194. ACM, 2017.

10 A. Ben-Aroya, D. Doron, and A. Ta-Shma. Near-Optimal Erasure List-Decodable Codes. In *Electronic Colloquium on Computational Complexity (ECCC)*, 2018.

11 M. Ben-Or and N. Linial. Collective coin flipping, robust voting schemes and minima of Banzhaf values. In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 408–416. IEEE, 1985.

12 E. Ben-Sasson and N. Zewi. From affine to two-source extractors via approximate duality. In *Proceedings of the 43rd annual ACM Symposium on Theory of computing (STOC)*, pages 177–186. ACM, 2011.

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

14 M. Braverman. Polylogarithmic independence fools AC0 circuits. *Journal of the ACM (JACM)*, 57(5):28, 2010.

15 E. Chattopadhyay, V. Goyal, and X. Li. Non-malleable extractors and codes, with their many tampered extensions. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 285–298. ACM, 2016.

16 E. Chattopadhyay and X. Li. Explicit Non-Malleable Extractors, Multi-Source Extractors and Almost Optimal Privacy Amplification Protocols. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 158–167. IEEE, 2016.

17 E. Chattopadhyay and D. Zuckerman. Explicit two-source extractors and resilient functions. In *Proceedings of the 48th Annual ACM Symposium on Theory of Computing (STOC)*, pages 670–683. ACM, 2016.

18 B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

19 F. R. K. Chung. A note on constructive methods for Ramsey numbers. *Journal of Graph Theory*, 5(1):109–113, 1981.

20 G. 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 (FOCS)*, pages 845–862. IEEE, 2015.

21 G. Cohen. Making the Most of Advice: New Correlation Breakers and Their Applications. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 188–196. IEEE, 2016.

22 G. Cohen. Two-source extractors for quasi-logarithmic min-entropy and improved privacy amplification protocols. In *Electronic Colloquium on Computational Complexity (ECCC)*, 2016.

23 G. Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 278–284. ACM, 2016.

24 G. Cohen and L. Schulman. Extractors for Near Logarithmic Min-Entropy. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, page 14, 2016.

25 P. Frankl. A constructive lower bound for Ramsey numbers. *Ars Combinatoria*, 3(297-302):28, 1977.

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

27 V. Grolmusz. Low rank co-diagonal matrices and Ramsey graphs. *Journal of combinatorics*, 7(1):R15–R15, 2001.

28 V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):20, 2009.

29 P. Harsha and S. Srinivasan. On Polynomial Approximations to AC0. *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, 2016.

30 K. Kahn, G. Kalai, and N. Linial. The influence of variables on Boolean functions. In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 68–80. IEEE, 1988.

31 Mark Lewko. An explicit two-source extractor with min-entropy near 4/9. *arXiv preprint*, 2018. `arXiv:1804.05451`.

32 X. 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 (FOCS)*, pages 100–109, 2013.

33 X. Li. New independent source extractors with exponential improvement. In *Proceedings of the 45th annual ACM Symposium on Theory of Computing (STOC)*, pages 783–792. ACM, 2013.

34 X. Li. Three-source extractors for polylogarithmic min-entropy. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 863–882. IEEE, 2015.

35 X. Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 1144–1156. ACM, 2017.

36 X. Li. Non-malleable extractors and non-malleable codes: Partially optimal constructions. In *Electronic Colloquium on Computational Complexity (ECCC)*, 2018.

37 R. Meka. Explicit resilient functions matching Ajtai-Linial. In *Proceedings of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1132–1148. SIAM, 2017.

38 Zs. Nagy. A constructive estimation of the Ramsey numbers. *Mat. Lapok*, 23:301–302, 1975.

39 M. Naor. Constructing Ramsey graphs from small probability spaces. *IBM Research Report RJ*, 8810, 1992.

40 A. Rao. A 2-source almost-extractor for linear entropy. In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques*, pages 549–556. Springer, 2008.

41 A. Rao. Extractors for a constant number of polynomially small min-entropy independent sources. *SIAM Journal on Computing*, 39(1):168–194, 2009.

42 R. Raz. Extractors with weak random seeds. In *Proceedings of the 37th annual ACM Symposium on Theory of Computing (STOC)*, pages 11–20. ACM, 2005.

43 R. Raz, O. Reingold, and S. Vadhan. Error reduction for extractors. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 191–201. IEEE, 1999.

44 A. Tal. Tight bounds on the Fourier spectrum of AC0. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 79. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

45 John von Neumann. Various techniques used in connection with random digits. *John von Neumann, Collected Works*, 5:768–770, 1963.

46 D. Zuckerman. Randomness-optimal oblivious sampling. *Random Structures and Algorithms*, 11(4):345–367, 1997.

47 D. Zuckerman. Linear Degree Extractors and the Inapproximability of Max Clique and Chromatic Number. *Theory of Computing*, 3:103–128, 2007.