Extractors with Weak Random Seeds

Ran Raz*
Weizmann Institute
ran.raz@weizmann.ac.il

Abstract

We show how to extract random bits from two or more independent weak random sources in cases where only one source is of linear min-entropy and all other sources are of logarithmic min-entropy. Our main results are as follows:

1. A long line of research, starting by Nisan and Zuckerman [15], gives explicit constructions of seeded-extractors, that is, extractors that use a short seed of truly random bits to extract randomness from a weak random source. For every such extractor E, with seed of length d, we construct an extractor E', with seed of length $d' = O(d)$, that achieves the same parameters as E but only requires the seed to be of min-entropy larger than $(1/2 + \delta) \cdot d'$ (rather than fully random), where δ is an arbitrary small constant.

2. Fundamental results of Chor and Goldreich and Vazirani [6, 22] show how to extract $\Omega(n)$ random bits from two (independent) sources of length n and min-entropy larger than $(1/2 + \delta) \cdot n$, where δ is an arbitrary small constant. We show how to extract $\Omega(n)$ random bits (with optimal probability of error) when only one source is of min-entropy $(1/2 + \delta) \cdot n$ and the other source is of logarithmic min-entropy.[1]

3. A recent breakthrough of Barak, Impagliazzo and Wigderson [4] shows how to extract $\Omega(n)$ random bits from a constant number of (independent) sources of length n and min-entropy larger than δn, where δ is an arbitrary small constant. We show how to extract $\Omega(n)$ random bits (with optimal probability of error) when only one source is of min-entropy δn and all other (constant number of) sources are of logarithmic min-entropy.

4. A very recent result of Barak, Kindler, Shaltiel, Sudakov and Wigderson [5] shows how to extract a constant number of random bits from three (independent) sources of length n and min-entropy larger than δn, where δ is an arbitrary small constant. We show how to extract $\Omega(n)$ random bits, with sub-constant probability of error, from one source of min-entropy δn and two sources of logarithmic min-entropy.

*Research supported by Israel Science Foundation (ISF) grant.

[1] We have learnt that the same result was obtained independently by Barak, Kindler, Shaltiel, Sudakov and Wigderson (private communication).

5. In the same paper, Barak, Kindler, Shaltiel, Sudakov and Wigderson [5] give an explicit coloring of the complete bipartite graph of size $2^n \times 2^n$ with two colors, such that there is no monochromatic subgraph of size larger than $2^{\delta n} \times 2^{\delta n}$, where δ is an arbitrary small constant. We give an explicit coloring of the complete bipartite graph of size $2^n \times 2^n$ with a constant number of colors, such that there is no monochromatic subgraph of size larger than $2^{\delta n} \times n^5$.

We also give improved constructions of mergers and condensers. In particular,

1. We show that using a constant number of truly random bits, one can condense a source of length n and min-entropy rate δ into a source of length $\Omega(n)$ and min-entropy rate $1 - \delta$, where δ is an arbitrary small constant.
2. We show that using a constant number of truly random bits, one can merge a constant number of sources of length n, such that at least one of them is of min-entropy rate $1 - \delta$, into one source of length $\Omega(n)$ and min-entropy rate slightly less than $1 - \delta$, where δ is any small constant.

1 Introduction

The problem of extracting pure randomness from weak sources of randomness has attracted a lot of attention in the last 20 years.

A *source of randomness* (or simply, a *source*) of length n is just a random variable X of length n bits. We say that the source is *weak* if its distribution is not uniform. The standard measure for the amount of randomness contained in a source is its *min-entropy*. We say that a random variable X (of length n bits) has min-entropy b if for every $a \in \{0,1\}^n$ the probability for $X = a$ is at most 2^{-b}. We say in this case that X is an (n, b)-*source*. We define the *min-entropy rate* of an (n, b)-source as the ratio b/n. Two or more sources are *independent* if they are independent as random variables.

Definition 1.1 ((n, b)-Source)
An (n, b)-source is a random variable of length n bits, with min-entropy $\geq b$.

Given an (n, b)-source X with an unknown distribution, it is easy to see that if $b \leq n - 1$ one cannot deterministically extract even one non-constant bit from X (unless additional information about the distribution of X is given). That is, no fixed function $E : \{0,1\}^n \to \{0,1\}$ produces a non-constant bit $E(X)$ for every such X. Hence, many works concentrated on the problem of extracting randomness from two or more independent sources.

Denote by U_n the uniform distribution over $\{0,1\}^n$. For a random variable X over $\{0,1\}^n$, denote by (X, U_m) the joint distribution of X and an independent random variable uniformly distributed over $\{0,1\}^m$, that is, (X, U_m) is the product of the distribution of X with the uniform distribution over $\{0,1\}^m$. In general, many times we will confuse notations between random variables and their distributions. We measure the distance between distributions by their $\mathcal{L}_1$ norm. Two distributions are ϵ-*close* if their $\mathcal{L}_1$ distance is at most ϵ.

1.1 Two-Sources-Extractors

Two-sources-extractors attempt to extract pure randomness from two independent weak sources.

Definition 1.2 (Two-Sources-Extractor)
A function $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is an $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma]$-two-sources-extractor if for every (n_1, b_1)-source X_1 and every independent (n_2, b_2)-source X_2, the distribution of the random variable $E(X_1, X_2)$ is γ-close to U_m (i.e., the uniform distribution over $\{0,1\}^m$). We say in this case that E extracts m bits with probability of error γ.

A two-sources-extractor is called *strong* if its output is almost independent of each one of the two inputs separately.[2]

Definition 1.3 (Strong-Two-Sources-Extractor)
An $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma]$-two-sources-extractor E is **strong in the first input** *if for every (n_1, b_1)-source X_1 and every independent (n_2, b_2)-source X_2, the distribution of $(X_1, E(X_1, X_2))$ is γ-close to (X_1, U_m). In the same way, E is* **strong in the second input** *if for X_1, X_2 as above, the distribution of $(X_2, E(X_1, X_2))$ is γ-close to (X_2, U_m). E is an $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma]$-strong-two-sources-extractor if it is strong in both inputs.*

A line of research constructed strong-two-sources-extractors based on the Hadamard matrix [21, 6, 22, 8, 9]. These extractors menage to extract random bits when $n_1 = n_2 = n$ and $b_1 + b_2 > n$. In particular, [9] gives an explicit $[(n, b_1), (n, b_2) \mapsto m \sim \gamma]$-strong-two-sources-extractor with $m = (b_1 + b_2 - n)/3$ and $\gamma = 2^{-m}$.

Can one explicitly extract random bits when $b_1 + b_2 < n$? It turns out that this can be done by constructions based on the Paley matrix. In particular, it was shown in [11, 1] how to extract one non-constant bit when $b_1 \geq n/2 + polylog(n)$ and $b_2 \geq \log n$, and similar methods also give a random bit with a polynomially small probability of error. Other constructions that work for $b_1 + b_2 < n$ (although with less tight parameters) are implicit in [19].

In this work, we give a more general construction, based on sample spaces that are ϵ-biased with respect to small linear tests (see [13, 2]). Our construction gives a strong extractor that outputs many output bits, and it performs well even when n_1 and n_2 are significantly different (which will be very important for some of the applications).

Roughly speaking (and for the important part of the range of the parameters), the following theorem shows that as long as $b_1 \geq (0.5 + \delta) \cdot n_1$ and $b_2 \geq 5 \log n_1$, one can (strongly) extract $\Omega(\delta b_2)$ random bits with an exponentially small probability of error.[3]

[2]The notion of strong extraction was the focus of several previous works. We note, however, that it can be proved that any two-sources-extractor, with small enough probability of error γ and small enough output length m, is a strong-two-sources-extractor with slightly worse parameters. We will not elaborate about this issue here, as it is not the focus of this work.

[3]Note that in the next subsection we will use these bits to extract much more bits out of the first source.

Theorem 1 (Strong-Two-Sources-Extractor)
For any n_1, n_2, b_1, b_2, m*, and any* $0 < \delta < 1/2$*, such that,*[4]

$$n_1 \geq 6 \log n_1 + 2 \log n_2,$$

$$b_1 \geq (0.5 + \delta) \cdot n_1 + 3 \log n_1 + \log n_2,$$
$$b_2 \geq 5 \log(n_1 - b_1),$$
$$m \leq \delta \cdot \min[n_1/8, b_2/40] - 1,$$

there exists an explicit[5] $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma]$*-strong-two-sources-extractor, with* $\gamma = 2^{-1.5 \cdot m}$.

1.1.1 Seeded-Extractors and Applications

Seeded-extractors attempt to extract pure randomness from one weak source, using an additional number of truly random bits, called *seed*. Obviously, this is interesting mainly when the length of the seed is smaller than the length of the weak source and the length of the output. A seeded-extractor is *strong* if its output is almost independent of the seed. Formally, a seeded-extractor can be presented as a two-sources-extractor, where the min-entropy of the first source is equal to its length.

Definition 1.4 (Seeded-Extractor)
A function $E : \{0, 1\}^d \times \{0, 1\}^n \to \{0, 1\}^m$ *is a* $[d, (n, b) \mapsto m \sim \gamma]$*-seeded-extractor if it is a* $[(d, d), (n, b) \mapsto m \sim \gamma]$*-two-sources-extractor. That is, for every* (n, b)*-source* X *and for an independent random variable* Z *uniformly distributed over* $\{0, 1\}^d$*, the distribution of* $E(Z, X)$ *is* γ*-close to* U_m*. A* $[d, (n, b) \mapsto m \sim \gamma]$*-seeded-extractor* E *is* **strong** *if it is strong in the first input as a two-sources-extractor, that is, if for* X, Z *as above, the distribution of* $(Z, E(Z, X))$ *is* γ*-close to* (U_d, U_m)*.*

Seeded-extractors and their applications have been studied in numerous of works. For excellent surveys of some of these works, see [17, 14, 20]. It was recently observed in [9] that given a strong-two-sources-extractor, the output of the extractor can be used as a seed for a seeded-extractor that is then applied on one of the two sources. In many cases, this composition results in a two-sources-extractor that outputs much more bits than the original one. Composing the strong-two-sources-extractor of Theorem 1 with a seeded-extractor that is applied on the first source, we obtain the following theorem.

Roughly speaking (and for the important part of the range of the parameters), the theorem shows that as long as $b_1 \geq (0.5 + \delta) \cdot n_1$ and $b_2 \geq 5 \log n_1$, if δb_2 is large enough (say, larger

[4]We have made no attempt to optimize the constants in the inequalities for b_2 and m, as they depend on each other.

[5]For simplicity, by *explicit* we mean: can be computed by a polynomial size circuit. In this paper, these circuits will always be uniform, in the sense that they can be computed by a polynomial time probabilistic Turing machine. In general, for our constructions, we will need to be able to do operations over finite fields. The "explicitness" of our constructions will hence be the same as the explicitness of the constructions of Alon, Goldreich, Hastad and Peralta [2] (see the discussion in [2, 3]).

than logarithmic in n_1), one can use the bits extracted by Theorem 1 as a seed for a seeded-extractor, and hence extract much more bits out of the first source.

Theorem 2 (Two-Sources-Extractor)
For any $n_1, n_2, b_1, b_2, d, m, \gamma$, and any $0 < \delta < 1/2$, such that,

$$n_1 \geq 6 \log n_1 + 2 \log n_2,$$

$$b_1 \geq (0.5 + \delta) \cdot n_1 + 3 \log n_1 + \log n_2,$$

$$b_2 \geq 5 \log(n_1 - b_1),$$

$$d \leq \delta \cdot \min[n_1/8, b_2/40] - 1,$$

if there exists an explicit $[d, (n_1, b_1) \mapsto m \sim \gamma]$-seeded-extractor, then there exists an explicit $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma']$-two-sources-extractor, with $\gamma' = \gamma + 2^{-1.5 \cdot d}$.

For example, using a seeded-extractor of Zuckerman [24], we obtain the following corollary. Roughly speaking, the corollary shows that if both sources are of length n, and the min-entropy rate of the first source is slightly more than a half and the min-entropy of the second source is logarithmic, then we are able to extract $\Omega(n)$ bits with a polynomially small error.[6]

Corollary 3 (Two-Sources-Extractor, Special Case)
For any constant $\delta > 0$, there exists an explicit family of $[(n, b_1), (n, b_2) \mapsto m \sim \gamma]$-two-sources-extractors, with

$$b_1 = (0.5 + \delta) \cdot n,$$

$$b_2 = O(\log n),$$

$$m = \Omega(n),$$

$$\gamma = 1/n^{\Omega(1)}.$$

In the same way, using known constructions of seeded-extractors (see for example [24, 23, 18, 16]), we can show that if both sources are of length n, and the min-entropy rate of the first source is slightly more than a half and the min-entropy of the second source is polylogarithmic, then we are able to extract all the min-entropy of the first source with a sub-polynomially small error.

1.1.2 Extractors with Weak Random Seeds

Composing the strong-two-sources-extractor of Theorem 1 with a seeded-extractor that is applied on the second source, we obtain the following theorem. Roughly speaking (and for the important part of the range of the parameters), the theorem shows that any seeded-extractor E, with seed of length d, can practically be operated with a seed of length $d' = O(d)$ that comes from a weak source of min-entropy rate slightly more than a half.[7]

[6] We have learnt that Corollary 3 was obtained independently by Barak, Kindler, Shaltiel, Sudakov and Wigderson (private communication). Their construction is based on the Paley matrix.

[7] We note that it follows easily from the definitions that any **strong**-seeded-extractor can be operated with seed that comes from a weak source. However, this typically gives a much weaker result than Theorem 4.

Theorem 4 (Extractors with Weak Seed)
There exists a (large enough) universal constant c, such that: For any $\delta > 0$, and any explicit $[d, (n,b) \mapsto m \sim \gamma]$-seeded-extractor E, such that $d \geq \log n$ and $b \geq cd/\delta$, there exists an explicit $[(d', b'), (n,b) \mapsto m \sim \gamma']$-two-sources-extractor E', with $d' \leq cd/\delta$, $b' = (0.5+\delta) \cdot d'$ and $\gamma' = \gamma + 2^{-1.5 \cdot d}$.

1.2 Multi-Sources-Extractors

Multi-sources-extractors attempt to extract pure randomness from several independent weak sources. This generalizes the notion of two-sources-extractors.

Definition 1.5 (Multi-Sources-Extractor)
A function $E : \{0,1\}^{n_1} \times \cdots \times \{0,1\}^{n_k} \to \{0,1\}^m$ is an $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma]$-multi-sources-extractor if for every independent random variables $X_1, ..., X_k$, such that each X_i is an (n_i, b_i)-source, the distribution of $E(X_1, ..., X_k)$ is γ-close to U_m.

A multi-sources-extractor is *strong* if its output is almost independent of every subset of all but one of the inputs.

Definition 1.6 (Strong-Multi-Sources-Extractor)
An $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma]$-multi-sources-extractor E is **strong in the j^{th} input** *if for every independent random variables $X_1, ..., X_k$, such that each X_i is an (n_i, b_i)-source, the distribution of $(X_j, E(X_1, ..., X_k))$ is γ-close to (X_j, U_m). More generally, E is* **strong in a subset $\sigma \subset \{1, ..., k\}$ of inputs** *if for $X_1, ..., X_k$ as above, the distribution of $(\{X_j\}_{j \in \sigma}, E(X_1, ..., X_k))$ is γ-close to $(\{X_j\}_{j \in \sigma}, U_m)$. E is an $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma]$-strong-multi-sources-extractor if it is strong in every subset $\sigma \subset \{1, ..., k\}$ of size $\leq k-1$.*

Barak, Impagliazzo and Wigderson recently presented new constructions of multi-sources-extractors, based on additive number theory [4]. In particular, for any constant $\delta > 0$ and for large enough n, they gave an explicit construction of an $[\{(n, \delta n)\}_1^k \mapsto n \sim 2^{-n}]$-multi-sources-extractor, where k is a constant depending only on δ. A more recent result of Barak, Kindler, Shaltiel, Sudakov and Wigderson shows that for any constant $\delta > 0$ and for large enough n, one can extract a constant number of random bits with a sub-constant probability of error, from only 3 $(n, \delta n)$-sources [5].

In this work, we improve both these results. Roughly speaking, our new constructions for multi-sources-extractors will work for $(n_1, b_1), ..., (n_k, b_k)$ that satisfy Property 1.7, with an arbitrary small constant $\delta > 0$ and a large enough constant c. Roughly speaking (and for the important part of the range of the parameters), the property requires that the first source is of min-entropy rate δ and all other sources are of logarithmic min-entropy.

We will show that for such sources one can extract $\Omega(n_1)$ bits with optimal probability of error, from a constant (depending on δ) number of sources, and one can extract $\Omega(n_1)$ bits with sub-constant probability of error, from only 3 sources. We will also show how to extract $\Omega(n_1)$ bits with a constant probability of error, from only 2 such sources, using an additional constant (depending on δ) number of truly random bits.

Property 1.7 *We say that $n_1, ..., n_k, b_1, ..., b_k > 0$ satisfy Property 1.7 with constants $c, \delta > 0$, if $n_1, ..., n_k > c$ and $b_1 \geq \delta n_1$, and for every $i \in \{2, ..., k\}$, $n_1 \geq c \log n_i$, and $b_i \geq 5 \log n_1$.*

1.2.1 Our Results

Our first result shows how to extract random bits, that are independent of the first source, from a constant number of sources that satisfy Property 1.7. Roughly speaking (and for the important part of the range of the parameters), the theorem shows that if one source of min-entropy rate δ is available, as well as a constant (depending on δ) number of sources of logarithmic min-entropy, then one can extract m bits, with an exponentially small probability of error, where m is of the order of the minimal min-entropy of all the sources.

Theorem 5 (Multi-Sources-Extractor)
For any constant $\delta > 0$, there exist constants $k, c, \alpha, \rho > 0$, such that for any $n_1, ..., n_k, b_1, ..., b_k$ that satisfy Property 1.7 with constants c, δ, there exists an explicit strong-in-the-first-input $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma]$-multi-sources-extractor, with

$$m \geq \min[\alpha n_1, b_2, ..., b_k]/200,$$

$$\gamma \leq 2^{-\rho \cdot m}.$$

Our second result shows how to (strongly) extract random bits, from two sources that satisfy Property 1.7, and a constant number of truly random bits. Roughly speaking (and for the important part of the range of the parameters), the theorem shows that if one source of min-entropy rate δ and one source of logarithmic min-entropy are available, as well as a constant (depending on δ) number of truly random bits, then one can extract m bits, with a constant probability of error, where m is of the order of the minimal min-entropy of the two sources.

Theorem 6 (Strong-Seeded-Two-Sources-Extractor)
For any constants $\delta, \gamma > 0$, there exist constants $n_3, c, \alpha > 0$, such that for any n_1, n_2, b_1, b_2 that satisfy Property 1.7 with constants c, δ, and for $b_3 = n_3$, there exists an explicit $[\{(n_i, b_i)\}_1^3 \mapsto m \sim \gamma]$-multi-sources-extractor E, with

$$m \geq \min[\alpha n_1, b_2]/200.$$

Moreover, E is strong in the sets $\{1,3\}$ and $\{2,3\}$.

Our third result shows how to extract random bits, that are independent of the first source, from three sources that satisfy Property 1.7. Roughly speaking (and for the important part of the range of the parameters), the theorem shows that if one source of min-entropy rate δ is available, as well as two sources of logarithmic min-entropy, then one can extract m bits, with a constant probability of error, where m is of the order of the minimal min-entropy of the three sources.

Theorem 7 (Three-Sources-Extractor)
For any constants $\delta, \gamma > 0$, there exist constants $c, \alpha > 0$, such that for any $n_1, n_2, n_3, b_1, b_2, b_3$ that satisfy Property 1.7 with constants c, δ, there exists an explicit strong-in-the-first-input $[\{(n_i, b_i)\}_1^3 \mapsto m \sim \gamma]$-multi-sources-extractor, with

$$m \geq \min[\alpha n_1, b_2]/200.$$

1.2.2 Extracting More Bits

Since the m output bits in Theorem 5, Theorem 6 and Theorem 7 are (almost) independent of the first source, they can be used as a seed for a seeded-extractor that is applied on the first source (as in Theorem 2). Hence, if m is large enough we are able to extract much more bits out of the first source. For example, if $m \geq c \cdot \log n_1$ (for a large enough constant c), we are able to extract $\Omega(n_1)$ random bits (as in Corollary 3), and if m is polylogarithmic in n_1 we are able to extract all the min-entropy of the first source.

1.3 Mergers and Condensers

In this work, we are interested in *mergers* and *condensers* mainly as tools for constructing multi-sources-extractors. Indeed, our constructions for multi-sources-extractors are based on new constructions for mergers and condensers. Nevertheless, the new constructions for mergers and condensers may be interesting in their own right and are described in this subsection.

1.3.1 Seeded-Condensers

Seeded-condensers generalize seeded-extractors, and attempt to transform a weak source with a relatively low min-entropy rate into a weak source with a much higher min-entropy rate, using an additional number of truly random bits (called *seed*). A seeded-condenser is *strong* if for almost all possible assignments to the seed, the output is close to be a source with high min-entropy.

Definition 1.8 (Seeded-Condenser)
A function $C : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^m$ is a $[d, (n, b_{\text{in}}) \mapsto (m, b_{\text{out}}) \sim \gamma]$-seeded-condenser if for every (n, b_{in})-source X, and for an independent random variable Z uniformly distributed over $\{0,1\}^d$, the distribution of $C(Z, X)$ is γ-close to a distribution of an (m, b_{out})-source. A $[d, (n, b_{\text{in}}) \mapsto (m, b_{\text{out}}) \sim \gamma]$-seeded-condenser C is **strong** *if for X as above, the average over $z \in \{0,1\}^d$ of the minimal distance between the distribution of $C(z, X)$ and a distribution of an (m, b_{out})-source is $\leq \gamma$.*

For any constants $\delta, \gamma > 0$, we give an explicit construction of $[d, (n, \delta n) \mapsto (m, \delta' m) \sim \gamma]$-strong-seeded-condenser, with $m = \Omega(n)$, $d = O(1)$ and $\delta' \geq 1 - \delta$. Roughly speaking, this shows that using a constant number of truly random bits, one can (strongly) condense a weak source with min-entropy rate close to 0 into a weak source with min-entropy rate close to 1.

Theorem 8 (Strong-Seeded-Condenser)
For any constants $\delta, \gamma > 0$, there exist constants $n_0, d, \alpha > 0$, such that for any $n \geq n_0$ there exists an explicit $[d, (n, \delta n) \mapsto (m, \delta' m) \sim \gamma]$-strong-seeded-condenser, such that,

$$m \geq \alpha \cdot n,$$

$$\delta' \geq 1 - \delta.$$

1.3.2 Somewhere-Random-Sources

Our new constructions for seeded-condensers are based on new constructions for, so called, *somewhere-condensers*, and new constructions for *mergers*. In the next subsections we will give the definitions of a merger and a somewhere-condenser. In order to give these definitions, we first need to give the definition of a *somewhere-random-source*, first introduced by Ta-Shma [18].

Definition 1.9 ($(n, b)^{1:k}$-Source)
A k places somewhere (n, b)-source, or shortly, an $(n, b)^{1:k}$-source, is a random variable $X = (X_1, ..., X_k)$, such that every X_i is of length n bits and at least one X_i is of min-entropy $\geq b$, that is, at least one of the random variables $X_1, ..., X_k$ is an (n, b)-source. Note that $X_1, ..., X_k$ are not necessarily independent.

1.3.3 Mergers

Mergers, first introduced by Ta-Shma [18], attempt to transform a k places somewhere (n, b)-source into one (m, b')-source, with a relatively high min-entropy b', using an additional number of truly random bits (called *seed*). In other words, we are given k random variables and we are guaranteed that at least one of them is an (n, b)-source. Our goal is to merge them into one source with high min-entropy, using an additional number of truly random bits. A merger is *strong* if for almost all possible assignments to the seed, the output is close to be a source with high min-entropy.

Definition 1.10 (Merger)
A function $M : \{0,1\}^d \times \{0,1\}^{n \cdot k} \to \{0,1\}^m$ is a $[d, (n, b_{\text{in}})^{1:k} \mapsto (m, b_{\text{out}}) \sim \gamma]$-merger if for every $(n, b_{\text{in}})^{1:k}$-source X, and for an independent random variable Z uniformly distributed over $\{0,1\}^d$, the distribution of $M(Z, X)$ is γ-close to a distribution of an (m, b_{out})-source. A $[d, (n, b_{\text{in}})^{1:k} \mapsto (m, b_{\text{out}}) \sim \gamma]$-merger M is **strong** *if for X as above, the average over $z \in \{0,1\}^d$ of the minimal distance between the distribution of $M(z, X)$ and a distribution of an (m, b_{out})-source is $\leq \gamma$.*

Lu, Reingold, Vadhan and Wigderson recently presented beautiful new constructions of strong-mergers that use only a constant number of truly random bits [12]. Roughly speaking, they showed how to merge (using a constant number of truly random bits) a k places somewhere (n, b)-source, where k is any constant, into one (n, b')-source, where b' is slightly less than $b/2$ (and where the probability of error γ is an arbitrary small constant).

The drawback of these constructions, however, (from our point of view), is that they loose a factor of 2 in the min-entropy rate, and hence the min-entropy rate decreases to below 0.5. In our work, we will need to keep the min-entropy rate above 0.5. We hence give here a generalization of their construction (using similar ideas) that (almost) preserves the original min-entropy rate, when the original min-entropy rate is close to 1.

Roughly speaking, we present constructions of strong-mergers that use a constant number of truly random bits and merge a k places somewhere (n, b)-source, where k is any constant and b/n is close to 1, into one (m, b')-source, where the min-entropy rate b'/m is only slightly lower than the min-entropy rate b/n, and where $m = \Omega(n)$, and where the probability of error γ is an arbitrary small constant.

Theorem 9 (Strong-Merger)
For any constants $\delta, \gamma', k > 0$, there exist constants $n_0, d, \alpha > 0$, such that for any $n \geq n_0$ there exists an explicit $[d, (n, b)^{1:k} \mapsto (m, b') \sim \gamma']$-strong-merger, such that,

$$b = n \cdot (1 - \delta),$$

$$m \geq \alpha \cdot n,$$

$$b' \geq m \cdot (1 - 4\delta/\gamma').$$

1.3.4 Somewhere-Condensers

Somewhere-condensers attempt to transform an (n, b)-source into a k places somewhere (m, b')-source, with a much higher min-entropy rate.

Note that any seeded-condenser, with seed of length d, gives a somewhere-condenser with $k = 2^d$. Thus, the notion of somewhere-condenser seems to be weaker than the one of seeded-condenser. Nevertheless, somewhere-condensers have the advantage that they may achieve a much smaller probability of error (e.g., much smaller than a constant when k is constant), and hence they may be interesting in their own right.

For technical reasons, in order to achieve a very small probability of error, we have to allow the distribution of the output of a somewhere-condenser to be a convex combination of distributions of k places somewhere (m, b')-sources, (rather than a distribution of one specific k places somewhere (m, b')-source).

Recall that a convex combination of probability distributions is an expression $\sum_j \alpha_j \mu_j$, where the coefficients α_j are positive real numbers such that $\sum_j \alpha_j = 1$, and every μ_j is a probability distribution over the same probability space. Note that a convex combination of probability distributions is a probability distribution (over the same probability space).

Definition 1.11 (Somewhere-Condenser)
A function $C : \{0,1\}^n \to \{0,1\}^{m \cdot k}$ is an $[(n, b_{\text{in}}) \mapsto (m, b_{\text{out}})^{1:k} \sim \gamma]$-somewhere-condenser if for every (n, b_{in})-source X, the distribution of the random variable $C(X)$ can be expressed as a convex combination of distributions, $\sum_j \alpha_j \mu_j + \gamma \mu'$, where μ' is an arbitrary probability distribution and every μ_j is a probability distribution of an $(m, b_{\text{out}})^{1:k}$-source.

Our constructions for somewhere-condensers are based on the recent constructions of multi-sources-extractors, by Barak, Impagliazzo and Wigderson [4].

For any constant $\delta > 0$, we give an explicit construction of $[(n, \delta n) \mapsto (m, \delta' m)^{1:k} \sim \gamma]$-somewhere-condenser, with $m = \Omega(n)$, $k = O(1)$, $\delta' \geq 1 - \delta$ and $\gamma \leq 2^{-\Omega(m)}$. Roughly speaking, this shows that one can condense an (n, b)-source with min-entropy rate close to 0 into a k places somewhere (m, b')-source with constant k and with min-entropy rate close to 1, and where the probability of error is exponentially small.[8]

Theorem 10 (Somewhere-Condenser)
For any constant $\delta > 0$, there exist constants $n_0, k, \alpha, \rho > 0$, such that for any $n \geq n_0$ there exists an explicit $[(n, \delta n) \mapsto (m, \delta' m)^{1:k} \sim \gamma]$-somewhere-condenser, such that,

$$m \geq \alpha \cdot n,$$
$$\delta' \geq 1 - \delta,$$
$$\gamma \leq 2^{-\rho \cdot m}.$$

1.4 Explicit Constructions of Ramsey Graphs

A recent breakthrough of Barak, Kindler, Shaltiel, Sudakov and Wigderson [5] gives an explicit coloring of the complete bipartite graph of size $2^n \times 2^n$ with two colors, such that there is no monochromatic subgraph of size larger than $2^{\delta n} \times 2^{\delta n}$, where δ is an arbitrary small constant.

Here we show (as an immediate corollary of Theorem 6) an explicit coloring of the complete bipartite graph of size $2^n \times 2^n$ with a constant number of colors, such that there is no monochromatic subgraph of size larger than $2^{\delta n} \times n^5$. Note that unlike the construction given in [5], the number of colors that we use is a constant larger than two. Moreover, that constant depends on δ. At the other hand, the sizes of the monochromatic subgraphs that we are able to exclude are much smaller than the ones in [5].

Our results are in fact more general and allow the sizes of the two sides of the graph to be significantly different.[9]

Corollary 11 (Ramsey-Graph)
For any constant $\delta > 0$, there exist constants $r, c > 0$, such that for any $n_2 > c$ and $n_1 > c \log n_2$, there exists an explicit coloring of the complete bipartite graph of size $2^{n_1} \times 2^{n_2}$ with r colors, such that there is no monochromatic subgraph of size larger than $2^{\delta n_1} \times (n_1)^5$.

1.5 Methods

For the proofs of our results we use a large number of new and borrowed methods. The new constructions for two-sources-extractors are based on the constructions of Alon, Gol-

[8] We have learnt that similar results were obtained independently by Barak, Kindler, Shaltiel, Sudakov and Wigderson [5]. Their proofs are based on similar methods.

[9] We note that the constant 5 can probably be improved to any constant larger than 1/2, using a method from [1].

dreich, Hastad and Peralta for sample spaces that are ϵ-biased with respect to small linear tests [2]. The new constructions for somewhere-condensers are based on the recent multi-sources-extractors of Barak, Impagliazzo and Wigderson [4]. The new constructions for mergers are based on the recent mergers of Lu, Reingold, Vadhan and Wigderson [12]. Other constructions are obtained by composing (in various ways) the above mentioned components. Many of the results are obtained by several steps of composition. Hence, in all parts of the work, special attention is given to the notion of strong extraction, and to the independence (or almost independence) of different random variables.

1.6 Related Works

Our results are are very related to recent results of Barak, Kindler, Shaltiel, Sudakov and Wigderson [5]. In particular, a result similar to Theorem 10 (Somewhere-Condenser) was proved independently in [5], and a result similar to Corollary 3 (Two-Sources-Extractor, Special Case) was also obtained independently by them (private communication).

While the two works are mostly independent, we stress that Theorem 7 (Three-Sources-Extractor) was only obtained after we heard a talk about their work[10], and our proof for that theorem uses ideas borrowed from their work. Our result on coloring of bipartite graphs was also added after we learnt about their results (although the proof is an easy corollary of our other results).

2 Preliminaries

The logarithm in this paper is always taken base 2. We assume for simplicity that the min-entropy b of an (n, b)-source is always an integer $\leq n$. We will usually denote by the letters a, b, d, k, l, m, n, p positive integers, and by Greek letters (e.g., $\alpha, \gamma, \delta, \epsilon, \rho$) positive reals (unless we say otherwise). We will usually denote by X, Y, Z random variables, and by a, x, y, z values that these variables can take.

2.1 Flat Sources

Let X be an (n, b)-source. We say that the source X is flat if it is uniformly distributed over a set $S_X \subset \{0,1\}^n$ of size 2^b. The following lemma, proved by Chor and Goldreich, shows that the distribution of any (n, b)-source is a convex combination of distributions of flat (n, b)-sources. Hence, as in [6], in most cases it will be enough to consider flat sources rather than general weak sources.

Lemma 2.1 *[6] The distribution of any (n, b)-source is a convex combination of distributions of flat (n, b)-sources.*

[10]The talk was given by Guy Kindler in a workshop on complexity theory (Banff, July 2004).

2.2 The Parity Lemma

A random variable Z over $\{0,1\}$ is *ϵ-biased* if $|\Pr[Z=0]-\Pr[Z=1]| \le \epsilon$, that is, if its distribution is ϵ-close to uniform. A sequence of 0-1 random variables $Z_1,...,Z_m$ is *ϵ-biased for linear tests* if the exclusive-or of any nonempty set of these variables is ϵ-biased, that is, for any nonempty $\tau \subset \{1,...,m\}$, the random variable $Z_\tau = \bigoplus_{i\in\tau} Z_i$ is ϵ-biased.

The following lemma is usually attributed to Vazirani. For the proof see for example [10].

Lemma 2.2 *Let $Z_1,...,Z_m$ be 0-1 random variables that are ϵ-biased for linear tests. Then, the distribution of $(Z_1,...,Z_m)$ is $\epsilon \cdot 2^{m/2}$-close to uniform.*

2.3 Entropy and Min-Entropy

The Shannon's entropy (or simply, *entropy*), $H(X)$, of a random variable X is defined by

$$H(X) = -\sum_a \Pr(X=a)\cdot \log \Pr(X=a).$$

The relations between the entropy and the min-entropy of a random variable are given by the following two lemmas.[11]

Lemma 2.3 *Let X be a random variable with min-entropy $\ge b$. Then, $H(X) \ \ge \ b$.*

Proof:
The proof is straight forward from the definitions. □

Lemma 2.4 *Let X be a random variable of length n bits, with $H(X) \ge n - \delta n$. Then, for any $\delta' \ge 2\delta$, the distribution of X is γ-close to a distribution of an $(n, n-\delta' n)$-source, where*

$$\gamma \le 2\delta/\delta'.$$

Proof:
Denote, $b = n - \delta n$ and $b' = n - \delta' n$. Denote by γ' the probability for $\Pr(X=a) \ge 2^{-b'}$, that is, $\sum_a \Pr(X=a)$, where the sum is taken over all elements a with $\Pr(X=a) \ge 2^{-b'}$.

By basic properties of the entropy function (see for example [7]), or alternatively, by a standard convexity argument,

$$H(X) \le (1-\gamma')\cdot n + \gamma' \cdot b'.$$

Hence,

$$b \le (1-\gamma')\cdot n + \gamma' \cdot b',$$

that is,

$$\gamma' \le (n-b)/(n-b') = \delta/\delta'.$$

By redistributing the probability mass of elements a with $\Pr(X=a) \ge 2^{-b'}$, we obtain an (n, b')-source which is $2\gamma'$-close to X. □

---

[11] For simplicity of the presentation, Lemma 2.4 is not given here in its tightest form.

3 Two-Sources-Extractors

Our main tool for constructing two-sources-extractors will be small probability spaces of 0-1 random variables that are ϵ-biased for small linear tests. We will show how to construct a two-sources-extractor from any such probability space.

Recall that a random variable Z over $\{0,1\}$ is ϵ-biased if $|\Pr[Z=0]-\Pr[Z=1]| \le \epsilon$, that is, if its distribution is ϵ-close to uniform. A sequence of 0-1 random variables $Z_1,...,Z_N$ is *ϵ-biased for linear tests of size k* if the exclusive-or of any k or less of these variables is ϵ-biased, that is, for any $r \in \{1,...,k\}$ and any different $i_1,...,i_r \in \{1,...,N\}$ the random variable $Z_{i_1} \oplus \cdots \oplus Z_{i_r}$ is ϵ-biased.

Explicit constructions for small probability spaces of N random variables that are ϵ-biased for linear tests of size k were given in [13, 2] (see also [3]). In particular, [2] showed that for every $k, N \ge 2$, variables $Z_1,...,Z_N$ as above can be explicitly constructed using $2\cdot\lceil\log(1/\epsilon)+\log k+\log\log N\rceil$ random bits.

3.1 Extracting One Bit

Let $N=2^{n_2}$. Let $Z_1,...,Z_N$ be 0-1 random variables that are ϵ-biased for linear tests of size k that can be constructed using n_1 random bits. We define $E:\{0,1\}^{n_1}\times\{0,1\}^{n_2}\to\{0,1\}$ by $E(x,y)=Z_y(x)$, that is, $E(x,y)$ is the random variable Z_y when using x as the value of the n_1 bits needed to produce $Z_1,...,Z_N$. In other words, x is used to choose the point in the probability space and y is used to choose the variable from $Z_1,...,Z_N$ that we evaluate.

The following lemma shows that if n_1 and ϵ are small enough and n_2 and k are large enough then the function E is a very good two-sources-extractor.

Lemma 3.1 *Let $N=2^{n_2}$. Let $Z_1,...,Z_N$ be 0-1 random variables that are ϵ-biased for linear tests of size k' that can be constructed using n_1 random bits. Define $E:\{0,1\}^{n_1}\times\{0,1\}^{n_2}\to\{0,1\}$ by $E(x,y)=Z_y(x)$. Then, for any even integer $k\le k'$ and any b_1,b_2, the function E is an $[(n_1,b_1),(n_2,b_2)\mapsto 1\sim\gamma]$-two-sources-extractor, with*

$$\gamma = 2^{(n_1-b_1)/k}\cdot\left[\epsilon^{1/k}+k\cdot 2^{-b_2/2}\right].$$

Proof:
Let X be an (n_1,b_1)-source and let Y be an independent (n_2,b_2)-source. We will show that the distribution of $E(X,Y)$ is γ-close to uniform. As in [6], it is enough to consider the case where X is uniformly distributed over a set $S_X\subset\{0,1\}^{n_1}$ of size 2^{b_1} and Y is uniformly distributed over a set $S_Y\subset\{0,1\}^{n_2}$ of size 2^{b_2}.

For every $x\in\{0,1\}^{n_1}$ and $y\in\{0,1\}^{n_2}$ denote

$$e(x,y) = -1^{E(x,y)} = -1^{Z_y(x)}.$$

Claim 3.2 *For any $r \in \{1, ..., k\}$ and any different $y_1, ..., y_r \in \{0,1\}^{n_2}$,*

$$\sum_{x \in \{0,1\}^{n_1}} \prod_{j=1}^{r} e(x, y_j) \leq 2^{n_1} \cdot \epsilon.$$

Proof:

$$\sum_{x \in \{0,1\}^{n_1}} \prod_{j=1}^{r} e(x, y_j) = \sum_{x \in \{0,1\}^{n_1}} \prod_{j=1}^{r} -1^{Z_{y_j}(x)} = \sum_{x \in \{0,1\}^{n_1}} -1^{Z_{y_1}(x) \oplus \cdots \oplus Z_{y_r}(x)},$$

and since $Z_{y_1} \oplus \cdots \oplus Z_{y_r}$ is ϵ-biased, the last sum is at most $2^{n_1} \cdot \epsilon$. $\square$

Denote by $\gamma(X, Y)$ the expectation of $e(X, Y)$. We will show that $|\gamma(X, Y)| \leq \gamma$. Obviously, this means that $E(X, Y)$ is γ-close to uniform, as required.

By the definition,

$$2^{b_1} \cdot 2^{b_2} \cdot \gamma(X, Y) = \sum_{x \in S_X} \sum_{y \in S_Y} e(x, y).$$

Hence, by a convexity argument and since k is even,

$$2^{b_1} \cdot \left(2^{b_2} \cdot \gamma(X, Y)\right)^k \leq \sum_{x \in S_X} \left(\sum_{y \in S_Y} e(x, y) \right)^k \leq$$

$$\sum_{x \in \{0,1\}^{n_1}} \left(\sum_{y \in S_Y} e(x, y) \right)^k = \sum_{x \in \{0,1\}^{n_1}} \sum_{y_1, ..., y_k \in S_Y} \prod_{j=1}^{k} e(x, y_j)$$

$$= \sum_{y_1, ..., y_k \in S_Y} \sum_{x \in \{0,1\}^{n_1}} \prod_{j=1}^{k} e(x, y_j).$$

We will break the sum over $y_1, ..., y_k \in S_Y$ into two sums. The first sum is over $y_1, ..., y_k \in S_Y$ such that at least one y_j is different than all other elements in $\{y_1, ..., y_k\}$, and the second sum is over $y_1, ..., y_k \in S_Y$ such that every y_j is identical to at least one other element in $\{y_1, ..., y_k\}$. The number of summands in the first sum is bounded by $2^{b_2 \cdot k}$, and by Claim 3.2 each summand is bounded by $2^{n_1} \cdot \epsilon$. The number of summands in the second sum is bounded by $2^{b_2 \cdot k/2} \cdot (k/2)^k$, and each summand is trivially bounded by 2^{n_1}. Hence,

$$2^{b_1} \cdot 2^{b_2 \cdot k} \cdot \gamma(X, Y)^k \leq 2^{n_1} \cdot \epsilon \cdot 2^{b_2 \cdot k} + 2^{n_1} \cdot 2^{b_2 \cdot k/2} \cdot (k/2)^k.$$

That is,

$$|\gamma(X, Y)| \leq 2^{(n_1 - b_1)/k} \cdot \epsilon^{1/k} + 2^{(n_1 - b_1)/k} \cdot 2^{-b_2/2} \cdot (k/2)$$
$$= 2^{(n_1 - b_1)/k} \cdot \left[\epsilon^{1/k} + (k/2) \cdot 2^{-b_2/2}\right].$$

$\square$

3.2 Extracting Many Bits

Let $N = m \cdot 2^{n_2}$. Let $Z_1, ..., Z_N$ be 0-1 random variables that are ϵ-biased for linear tests of size k that can be constructed using n_1 random bits. We think of the set of indices $\{1, ..., N\}$ as the set $\{(i, y) : i \in \{1, ..., m\}, y \in \{0,1\}^{n_2}\}$. We define $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ by $E_i(x, y) = Z_{(i,y)}(x)$, where $E_i(x, y)$ denotes the i^{th} bit of $E(x, y)$. In other words, x is used to choose the point in the probability space and i, y are used to choose the variable from $Z_1, ..., Z_N$ that we evaluate.

The following lemma shows that if n_1, m, ϵ are small enough and n_2, k are large enough then the function E is a very good two-sources-extractor.

Lemma 3.3 *Let $N = m \cdot 2^{n_2}$. Let $Z_1, ..., Z_N$ be 0-1 random variables that are ϵ-biased for linear tests of size k' that can be constructed using n_1 random bits. Define $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ by $E_i(x, y) = Z_{(i,y)}(x)$. Then, for any even integer $k \le k'/m$ and any b_1, b_2, the function E is an $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma 2^{m/2}]$-two-sources-extractor, where*

$$\gamma = 2^{(n_1-b_1)/k} \cdot \left[\epsilon^{1/k} + k \cdot 2^{-b_2/2}\right].$$

Proof:
Let X be an (n_1, b_1)-source and let Y be an independent (n_2, b_2)-source. We will show that the distribution of $E(X, Y)$ is $\gamma \cdot 2^{m/2}$-close to uniform.

For every nonempty $\tau \subset \{1, ..., m\}$, define $E_\tau : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}$, by

$$E_\tau(x, y) = \bigoplus_{i\in\tau} E_i(x, y) = \bigoplus_{i\in\tau} Z_{(i,y)}(x).$$

Since $|\tau| \le m$, the variables $\{Z'_y = \bigoplus_{i\in\tau} Z_{(i,y)} : y \in \{0,1\}^{n_2}\}$ are ϵ-biased for linear tests of size k'/m. Hence by Lemma 3.1, for every nonempty τ, the random variable $E_\tau(X, Y)$ is γ-close to uniform. Hence by Lemma 2.2, the distribution of $E(X, Y) = (E_1(X, Y), ..., E_m(X, Y))$ is $\gamma \cdot 2^{m/2}$-close to uniform. □

3.3 Strong Extraction

We will now show that if n_1, m, ϵ are small enough and n_2, k are large enough then the function E defined above is actually a very good strong-two-sources-extractor.

Lemma 3.4 *Let $N = m \cdot 2^{n_2}$. Let $Z_1, ..., Z_N$ be 0-1 random variables that are ϵ-biased for linear tests of size k' that can be constructed using n_1 random bits. Define $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ by $E_i(x, y) = Z_{(i,y)}(x)$. Then, for any even integer $k \le k'/m$ and any b_1, b_2, γ such that,*

$$\gamma \ge 2^{(n_1-b_1)/k} \cdot \left[\epsilon^{1/k} + k \cdot 2^{-b_2/2}\right],$$

the function E is an $[(n_1, b'_1), (n_2, b'_2) \mapsto m \sim \gamma']$-strong-two-sources-extractor, with

$$b'_1 = b_1 + m/2 + 2 - \log \gamma,$$

$$b'_2 = b_2 + m/2 + 2 - \log \gamma,$$
$$\gamma' = \gamma \cdot 2^{m/2+1}.$$

Proof:
Let X be an (n_1, b'_1)-source and let Y be an independent (n_2, b'_2)-source. We will show that the distribution of $(X, E(X,Y))$ is γ'-close to (X, U_m). The proof that the distribution of $(Y, E(X,Y))$ is γ'-close to (Y, U_m) is the same. As in [6], it is enough to consider the case where X is uniformly distributed over a set $S_X \subset \{0,1\}^{n_1}$ of size $2^{b'_1}$.

As before, for every nonempty $\tau \subset \{1, ..., m\}$, define $E_\tau : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}$, by

$$E_\tau(x,y) = \bigoplus_{i \in \tau} E_i(x,y) = \bigoplus_{i \in \tau} Z_{(i,y)}(x).$$

Since $|\tau| \le m$, the variables $\{Z'_y = \bigoplus_{i \in \tau} Z_{(i,y)} : y \in \{0,1\}^{n_2}\}$ are ϵ-biased for linear tests of size k'/m.

As before, by Lemma 3.1, for every nonempty τ, the random variable $E_\tau(X,Y)$ is γ-biased. For every nonempty τ, denote by B_τ the set of all $x \in S_X$, such that $E_\tau(x,Y)$ is not γ-biased.

Claim 3.5 *For every nonempty τ,*
$$|B_\tau| \le 2^{b_1+1}.$$

Proof:
Assume for a contradiction that $|B_\tau| > 2^{b_1+1}$. Denote by B^0_τ the set of all $x \in B_\tau$ such that $E_\tau(x,Y)$ is 0 with probability $> 1/2 + \gamma/2$, and denote by B^1_τ the set of all $x \in B_\tau$ such that $E_\tau(x,Y)$ is 0 with probability $< 1/2 - \gamma/2$. Since for every $x \in B_\tau$ the random variable $E_\tau(x,Y)$ is not γ-biased, we have $B_\tau = B^0_\tau \cup B^1_\tau$, and hence at least one of the sets B^0_τ, B^1_τ is of size larger than 2^{b_1}. W.l.o.g. assume that $|B^0_\tau| > 2^{b_1}$.

Let X' be a random variable uniformly distributed over B^0_τ. Then by the definition of B^0_τ, we know that $E_\tau(X',Y)$ is 0 with probability $> 1/2 + \gamma/2$. However, since X' is an (n_1, b_1)-source, by Lemma 3.1, $E_\tau(X',Y)$ is γ-close to uniform. $\square$

Define
$$B = \bigcup_\tau B_\tau,$$
where the union is over all nonempty $\tau \subset \{1, ..., m\}$. Then, by Claim 3.5,

$$|B|/|S_X| \le 2^m \cdot 2^{b_1+1}/2^{b'_1} = \gamma'/4.$$

For every $x \in S_X \setminus B$, the random variable $E_\tau(x,Y)$ is γ-biased for every nonempty τ. Hence, by Lemma 2.2, for every $x \in S_X \setminus B$, the distribution of $E(x,Y)$ is $\gamma'/2$-close to uniform. Thus, for $1 - \gamma'/4$ fraction of the elements in S_X, the distribution of $E(x,Y)$ is $\gamma'/2$-close to uniform. Hence, the distribution of $(X, E(X,Y))$ is γ'-close to (X, U_m). $\square$

3.4 Proof of Theorem 1

We will now use Lemma 3.4 and the construction given in [2] for random variables that are ϵ-biased for small linear tests, to give the proof for Theorem 1 (Strong-Two-Sources-Extractor). The proof will follow from the following lemma.

Lemma 3.6 *For any n_1, n_2, b_1, b_2, m, and any $0 < \delta < 1/2$, such that,*

$$n_1 \geq 6\log n_1 + 2\log n_2,$$

$$b_1 \geq n_1/2 + \delta n_1 + 3\log n_1 + \log n_2,$$
$$b_2 \geq 4\log(n_1 - b_1),$$
$$m \leq \delta \cdot \min[n_1/4, b_2/16] - 1,$$

there exists an explicit $[(n_1, b_1'), (n_2, b_2') \mapsto m \sim \gamma']$-strong-two-sources-extractor, with

$$b_1' = b_1 + 3(m+1),$$

$$b_2' = b_2 + 3(m+1),$$
$$\gamma' = 2^{-3m/2}.$$

Proof:
W.l.o.g. assume that $m \geq 1$. W.l.o.g. assume that $n_1 \geq 16$ and $b_2 \geq 64$ (as otherwise $m < 1$). Let $N = m \cdot 2^{n_2}$. Let $k' = m \cdot \max[(n_1 - b_1), 2]$. Let $\epsilon = 2^{-r}$, where $r = n_1/2 - 3\log n_1 - \log n_2$. Note that

$$n_1 \geq 2 \cdot \lceil \log(1/\epsilon) + \log k' + \log\log N \rceil.$$

Hence, by [2], 0-1 random variables $Z_1, ..., Z_N$ that are ϵ-biased for linear tests of size k' can be constructed using n_1 random bits. We will now consider two cases.

Case A: $b_2 \leq 4(n_1 - b_1)$.
In this case, we use Lemma 3.4 with $k =$ *the smallest even integer larger than* $8(n_1 - b_1)/b_2$. Hence, $k \leq n_1 - b_1$, and also

$$8(n_1 - b_1)/b_2 \leq k \leq 8(n_1 - b_1)/b_2 + 2 \leq 16(n_1 - b_1)/b_2 \leq 8n_1/b_2.$$

Note that

$$2^{(n_1-b_1)/k} \cdot \left[\epsilon^{1/k} + k \cdot 2^{-b_2/2}\right] \leq 2^{(n_1-b_1-r)/k} + 2^{(n_1-b_1)/k} \cdot (n_1 - b_1) \cdot 2^{-b_2/2} \leq$$

$$2^{-\delta n_1/k} + 2^{(n_1-b_1)/k} \cdot 2^{-b_2/4} \leq 2^{-\delta b_2/8} + 2^{b_2/8} \cdot 2^{-b_2/4} \leq 2 \cdot 2^{-\delta b_2/8} \leq 2^{-(2m+1)}.$$

Case B: $b_2 > 4(n_1 - b_1)$.
In this case, we use Lemma 3.4 with $k = 2$. Note that

$$2^{(n_1-b_1)/k} \cdot \left[\epsilon^{1/k} + k \cdot 2^{-b_2/2}\right] = 2^{(n_1-b_1-r)/2} + 2^{(n_1-b_1)/2} \cdot 2 \cdot 2^{-b_2/2} \leq$$

$$2^{-\delta n_1/2} + 2^{b_2/8} \cdot 2 \cdot 2^{-b_2/2} \leq 2^{-\delta n_1/2} + 2^{-b_2/4} \leq 2^{-(2m+1)}$$

Hence, in both cases the proof follows by Lemma 3.4, using $\gamma = 2^{-(2m+1)}$. □

Proof of Theorem 1: (Strong-Two-Sources-Extractor)
Let us first restate Theorem 1: For any n_1, n_2, b'_1, b'_2, m, and any $0 < \delta' < 1/2$, such that,

$$n_1 \geq 6 \log n_1 + 2 \log n_2,$$

$$b'_1 \geq n_1/2 + \delta' n_1 + 3 \log n_1 + \log n_2,$$

$$b'_2 \geq 5 \log(n_1 - b_1),$$

$$m \leq \delta' \cdot \min[n_1/8, b'_2/40] - 1,$$

there exists an explicit $[(n_1, b'_1), (n_2, b'_2) \mapsto m \sim \gamma']$-strong-two-sources-extractor, with $\gamma' = 2^{-3m/2}$.

Denote, $b_1 = b'_1 - 3(m+1)$ and $b_2 = b'_2 - 3(m+1)$. Denote, $\delta = \delta'/2$. Note that

$$b_1 \geq n_1/2 + \delta n_1 + 3 \log n_1 + \log n_2,$$

$$b_2 \geq 4 \log n_1,$$

$$m \leq \delta \cdot \min[n_1/4, b_2/16] - 1.$$

The proof hence follows by Lemma 3.6. □

3.5 Applying a Seeded-Extractor

For the proofs of Theorem 2 (Two-Sources-Extractor), Corollary 3 (Two-Sources-Extractor, Special Case) and Theorem 4 (Extractors with Weak Seed), we will need to compose the two-sources-extractors of Theorem 1 with seeded-extractors, as in [9]. Formally, we will need the following composition lemma.

Lemma 3.7 *Let $E_1 : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^d$ be an $[(n_1, b_1), (n_2, b_2) \mapsto d \sim \gamma_1]$-strong-two-sources-extractor, and let $E_2 : \{0,1\}^d \times \{0,1\}^{n_1} \to \{0,1\}^m$ be a $[d, (n_1, b_1) \mapsto m \sim \gamma_2]$-seeded-extractor. Denote by $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ the following composition of E_1 and E_2: for every $x \in \{0,1\}^{n_1}$ and $y \in \{0,1\}^{n_2}$, we define $E(x,y) = E_2(E_1(x,y), x)$. Then, E is an $[(n_1, b_1), (n_2, b_2) \mapsto m \sim \gamma_1 + \gamma_2]$-two-sources-extractor.*

Proof:
The proof is straight forward from the definitions. □

Proof of Theorem 2: (Two-Sources-Extractor)
The proof is straight forward from Theorem 1, using Lemma 3.7. By Theorem 1, there exists an explicit $[(n_1, b_1), (n_2, b_2) \mapsto d \sim 2^{-1.5 \cdot d}]$-strong-two-sources-extractor. If there exists an

explicit $[d,(n_1,b_1) \mapsto m \sim \gamma]$-seeded-extractor then by Lemma 3.7, there exists an explicit $[(n_1,b_1),(n_2,b_2) \mapsto m \sim \gamma']$-two-sources-extractor, with $\gamma' = \gamma + 2^{-1.5 \cdot d}$. $\square$

Proof of Corollary 3: (Two-Sources-Extractor, Special Case)
The proof is straight forward from Theorem 2, using the seeded-extractor of Zuckerman [24]. More precisely, we can use Theorem 1 to extract $d = O(\log n)$ bits that are (almost) independent of the first source, and then (by Lemma 3.7) we can use these bits as a seed for a seeded-extractor that extracts $\Omega(n)$ bits out of the first source (with a polynomially small probability of error). An explicit construction for such a seeded-extractor was given in [24]. $\square$

Proof of Theorem 4: (Extractors with Weak Seed)
The proof is straight forward from Theorem 1, using Lemma 3.7, where the roles of the two sources are exchanged (i.e., we think of the first source as the second and the second source as the first). More precisely, let $d' = \lfloor cd/\delta \rfloor$, where c is the (large enough) universal constant, and let $b' = (0.5+\delta) \cdot d'$. Given a (d',b')-source and an (n,b)-source, we can use Theorem 1 to extract d bits that are (almost) independent of the second source (with probability of error $2^{-1.5 \cdot d}$), and then (by Lemma 3.7) we can use these bits as a seed for the seeded-extractor E that extracts m bits out of the second source (with probability of error γ). $\square$

4 Mergers and Condensers

In this section, we describe our new constructions for mergers, somewhere-condensers and seeded-condensers and we give the proofs for Theorem 10, Theorem 9 and Theorem 8.

4.1 Somewhere-Condensers

Our construction for somewhere-condensers is based on the multi-sources-extractors of Barak, Impagliazzo and Wigderson [4]. The following lemma was proved in [4].

Lemma 4.1 *[4] For any constant $\delta_0 > 0$ there exist constants m_0, k, such that for any $m \geq m_0$, there exists an explicit $[\{(m,\delta_0 m)\}_1^k \mapsto m \sim 2^{-m}]$-multi-sources-extractor, E. Moreover, for any $x_1,...,x_{k-1} \in \{0,1\}^m$, there exists a unique $x_k \in \{0,1\}^m$ such that $E(x_1,...,x_k) = 0^m$, and that unique x_k can be explicitly computed as $x_k = f(x_1,...,x_{k-1})$.*

Recall that for two measures ψ, ψ' (over the same space), we say that $\psi < \psi'$ if for every event A we have $\psi(A) < \psi'(A)$. For a probability distribution ψ over a finite probability space, define by S_ψ the support of ψ, that is the set of all points with non-zero probability.

The following lemma (and its proof) gives our basic construction.

Lemma 4.2 *For any constant $\delta_0 > 0$ there exist constants n_0, k, such that for any $n \geq n_0$ and any $\delta > \delta_0 + 2k/n$, there exists an explicit $[(n,\delta n) \mapsto (m,\delta' m)^{1:k} \sim \gamma]$-somewhere-condenser,* *such that,*

$$m = \lceil n/(k-1) \rceil,$$
$$\delta' \geq \delta + (1-\delta)/(2k) - 5/m,$$
$$\gamma \leq 2^{-(1-\delta)m/(2k)}.$$

Proof:
Given δ_0, let m_0, k be the constants from Lemma 4.1, and let $n_0 = m_0 \cdot k$. Assume w.l.o.g. that n_0, m_0, k are large enough. Given n, δ, denote $m = \lceil n/(k-1) \rceil$ and $\delta' = \delta + (1-\delta)/(2k) - 5/m$. For simplicity, we assume that $\delta n, \delta' m$ are integers (otherwise, decrease δ by at most $1/n$ and increase δ' by at most $1/m$, and the same proof follows). For simplicity, we assume that $k-1$ divides n (otherwise, increase n by adding zeros, which decreases δ by at most k/n, and the same proof follows). Thus, $n = m \cdot (k-1)$. Let f be the function from Lemma 4.1 (applied for δ_0 and m). Define $C : \{0,1\}^{m \cdot (k-1)} \to \{0,1\}^{m \cdot k}$, by

$$C(x_1, ..., x_{k-1}) = (x_1, ..., x_{k-1}, f(x_1, ..., x_{k-1})).$$

Denote by $T \subset \{0,1\}^{m \cdot k}$ the image of C, that is,

$$T = \left\{ (x_1, ..., x_{k-1}, f(x_1, ..., x_{k-1})) : (x_1, ..., x_{k-1}) \in \{0,1\}^{m \cdot (k-1)} \right\}.$$

Let X be an $(n, \delta n)$-source. As in [6], it is enough to consider the case where X is uniformly distributed over a set $S_X \subset \{0,1\}^n$ of size $2^{\delta n}$. Denote by μ the distribution of $C(X)$. Then, obviously, μ is a uniform distribution over a set $S_\mu \subset \{0,1\}^{m \cdot k}$ of size $2^{\delta n}$.

Denote by $0 \leq \gamma' \leq 1$ the smallest number such that μ can be expressed as a convex combination of probability distributions, $\sum_j \alpha_j \mu_j + \gamma' \mu'$, where every μ_j is a probability distribution of an $(m, \delta' m)^{1:k}$-source (as in Definition 1.11). We will show that $\gamma' \leq 2^{-(1-\delta)m/(2k)}$, as required.

By the minimality of γ', for every $\alpha > 0$ and every probability distribution ψ, if $\alpha\psi < \mu'$ then ψ is not the distribution of an $(m, \delta' m)^{1:k}$-source. (Otherwise, we can express μ' as $\alpha \cdot \psi + (1-\alpha) \cdot \mu''$, which means that γ' can be decreased to $\gamma' \cdot (1-\alpha)$). Hence, the support of μ' is contained in a subset $B_1 \times \cdots \times B_k \subset \{0,1\}^{m \cdot k}$, where every $B_i \subset \{0,1\}^m$ is of size $2^{\delta' m}$. Note also that since $\gamma' \mu' < \mu$, the support of μ' is contained in the support of μ, and hence also in T. Therefore, by Lemma 4.1 (applied for random variables uniformly distributed over $B_1, ..., B_k$),

$$|S_{\mu'}| \leq |T \cap B_1 \times \cdots \times B_k| \leq 2^{\delta' m \cdot k} \cdot 2^{-m} \cdot 2.$$

Since μ is uniformly distributed over S_μ and since $\gamma' \mu' < \mu$,

$$\gamma' \leq |S_{\mu'}|/|S_\mu| \leq 2^{\delta' m \cdot k} \cdot 2^{-m} \cdot 2 \cdot 2^{-\delta m \cdot (k-1)} = 2^{(\delta' - \delta) \cdot m \cdot k} \cdot 2^{-(1-\delta) \cdot m} \cdot 2$$
$$= 2^{-(1-\delta) \cdot m/2} \cdot 2^{-5k} \cdot 2 < 2^{-(1-\delta) \cdot m/2}.$$

□

For the proof of Theorem 10 (Somewhere-Condenser), we will need to compose Lemma 4.2 with itself many times. Formally, we will need the following composition lemma.

Lemma 4.3 *Let $C_1 : \{0,1\}^{n_1} \to \{0,1\}^{n_2 \cdot k_1}$ be an $[(n_1, b_1) \mapsto (n_2, b_2)^{1:k_1} \sim \gamma_1]$-somewhere-condenser, and let $C_2 : \{0,1\}^{n_2} \to \{0,1\}^{n_3 \cdot k_2}$ be an $[(n_2, b_2) \mapsto (n_3, b_3)^{1:k_2} \sim \gamma_2]$-somewhere-condenser. Denote by $C : \{0,1\}^{n_1} \to \{0,1\}^{n_3 \cdot k_2 \cdot k_1}$ the following composition of C_2 and C_1: for every $x \in \{0,1\}^{n_1}$ we obtain $C(x)$ by applying C_2 on each of the k_1 coordinates of $C_1(x)$. Then, C is an $[(n_1, b_1) \mapsto (n_3, b_3)^{1:k_1 \cdot k_2} \sim \gamma_1 + \gamma_2]$-somewhere-condenser.*

Proof:
The proof is straight forward from the definitions. □

We are now ready to give the proof for Theorem 10.

Proof of Theorem 10: (Somewhere-Condenser)
The proof follows easily by compositions of Lemma 4.2 with itself (using Lemma 4.3), until the min-entropy is above $(1 - \delta) \cdot m$.

We start with an $(n, \delta n)$-source X. We apply Lemma 4.2, with δ_0 slightly smaller than δ, and get $X_1, ..., X_k$. We now apply Lemma 4.2 (with the original δ_0) on each one of the variables $X_1, ..., X_k$ separately. We keep doing that (with the original δ_0) until $\delta' \geq 1 - \delta$.

Note that since the min-entropy rate increases by a constant in each step, we stop after a constant number of steps. Hence, we end up with an $(m, \delta' m)^{1:k}$-source, with constant k and with $m = \Omega(n)$. Since we stop after a constant number of steps, the final γ is still exponentially small. The constant n_0 is chosen such that we can apply Lemma 4.2 in all steps. □

4.2 Mergers

Before giving our construction for mergers, we will need to prove the following lemma.

Lemma 4.4 *Let F be a finite field, and let $v_1, ..., v_r$ be linearly independent vectors in the vector space $\mathrm{F}^{k'}$. Let $S \subset \mathrm{F}^{k'}$ be such that for every $u \in \mathrm{F}^{k'}$ and every non-zero $\alpha_1, ..., \alpha_r \in \mathrm{F}$, at least one of the vectors $u, u + \alpha_1 v_1, ..., u + \alpha_r v_r$ is not in S. Then,*

$$|S| \leq r \cdot |\mathrm{F}|^{k'-1}.$$

Proof:
For every $i \in \{1, ..., r\}$, denote by S_i the set of all vectors $u \in S$, such that u is the unique vector from S in the line (i.e., affine subspace of dimension 1) $\{u + \alpha v_i : \alpha \in \mathrm{F}\}$. Since, for every i the number of lines of the form $\{u + \alpha v_i : \alpha \in \mathrm{F}\}$ is $|\mathrm{F}|^{k'-1}$, and since S_i contains at most one vector from each such line, we know that $|S_i| \leq |\mathrm{F}|^{k'-1}$.

Assume for a contradiction $|S| > r \cdot |\mathrm{F}|^{k'-1}$. Then, there exists $u \in S \setminus \bigcup_i S_i$. For every i, since $u \in S \setminus S_i$, there exists non-zero $\alpha_i \in \mathrm{F}$ such that $u + \alpha_i v_i \in S$ (by the definition of S_i). Thus, $u, u + \alpha_1 v_1, ..., u + \alpha_r v_r$ are all in S, which contradicts the requirement of the lemma. □

Our construction for mergers is based on the construction of Lu, Reingold, Vadhan and Wigderson [12]. The following lemma (and its proof) gives our basic construction.[12]

Lemma 4.5 *For any p, m, such that $p|m$, and any n, r, such that $n = m \cdot r$, and any b, k, γ, there exists an explicit $[d, (n, b)^{1:k} \mapsto (m, b') \sim \gamma']$-strong-merger, such that,*

$$d = k \cdot r \cdot p,$$

$$b' = m - (2/\gamma) \cdot (m + n - b)/(r + 1),$$

$$\gamma' = \gamma + 2r/2^p.$$

Proof:
Denote $l = m/p$. Let F be a finite field of size 2^p. Given $z \in \{0,1\}^d$, we think of z as a vector $(z_{1,1}, ..., z_{k,r}) \in \mathrm{F}^{kr}$. Given $x = (x_1, ..., x_k) \in \{0,1\}^{n \cdot k}$, we think of each $x_i \in \{0,1\}^n$ as a vector $(x_{i,1}, ..., x_{i,r})$, where each $x_{i,j}$ is in $\{0,1\}^m$. We think of each $x_{i,j} \in \{0,1\}^m$ as a vector in F^l. More generally, we think of $\{0,1\}^m$ as the vector space F^l.

Define $M : \{0,1\}^d \times \{0,1\}^{n \cdot k} \to \{0,1\}^m$ by,

$$M(z, x) = \sum_{i=1}^{k} \sum_{j=1}^{r} z_{i,j} \cdot x_{i,j} \in \mathrm{F}^l,$$

(where the operations are in the vector space F^l).

Let $X = (X_1, ..., X_k)$ be an $(n, b)^{1:k}$-source. Thus, every X_i is of length n bits and at least one X_i is of min-entropy $\geq b$. W.l.o.g., assume that $X_1 = (X_{1,1}, ..., X_{1,r})$ is of min-entropy $\geq b$. Hence, by Lemma 2.3, $H(X_{1,1}, ..., X_{1,r}) \geq b$, where H denotes the Shannon's entropy function.

Denote by $v_1, ..., v_{kr}$ the standard base for the vector space F^{kr}. In particular, $v_1, ..., v_r$ are the first r vectors in the standard base.

For every $z \in \mathrm{F}^{kr}$, denote

$$Y_z = M(z, X).$$

For every $z \in \mathrm{F}^{kr}$ and every non-zero $\alpha_1, ..., \alpha_r \in \mathrm{F}$, the values of the random variables $Y_z, Y_{z+\alpha_1 v_1}, ..., Y_{z+\alpha_r v_r}$ determine the values of $X_{1,1}, ..., X_{1,r}$ (by $X_{1,i} = (Y_{z+\alpha_i v_i} - Y_z)/\alpha_i$). Hence, by basic properties of the entropy function (see for example [7]),

$$H(Y_z) + H(Y_{z+\alpha_1 v_1}) + \cdots + H(Y_{z+\alpha_r v_r}) \geq$$

$$H(Y_z, Y_{z+\alpha_1 v_1}, ..., Y_{z+\alpha_r v_r}) \geq H(X_{1,1}, ..., X_{1,r}) \geq b.$$

Hence, at least one of the random variables $Y_z, Y_{z+\alpha_1 v_1}, ..., Y_{z+\alpha_r v_r}$ has entropy $\geq b/(r + 1)$, and by Lemma 2.4 that variable is γ-close to an (m, b')-source, where

$$b' = m - \frac{2}{\gamma} \cdot \left(m - \frac{b}{r+1} \right) = m - \frac{2}{\gamma} \cdot \frac{m \cdot (r+1) - b}{r+1} = m - \frac{2}{\gamma} \cdot \frac{m + n - b}{r+1}.$$

[12] We note that a better analysis of the same construction, using min-entropy rather than entropy, can possibly be done, and may be included in later versions of this work.

Denote by $S \subset \mathrm{F}^{kr}$ the set of all $z \in \mathrm{F}^{kr}$, such that, Y_z is not γ-close to an (m, b')-source. Then S satisfies the conditions of Lemma 4.4 (with $k' = kr$), and hence $|S| \leq r \cdot |\mathrm{F}|^{kr-1}$. That is, S is of fraction $\leq r/2^p$ of $z \in \mathrm{F}^{kr}$.

Thus, for at least $1 - r/2^p$ fraction of $z \in \mathrm{F}^{kr}$, the distribution of $M(z, X) = Y_z$ is γ-close to an (m, b')-source. Hence, the average over $z \in \mathrm{F}^{kr}$ of the minimal distance of the distribution of $M(z, X)$ and a distribution of an (m, b')-source is $\leq \gamma + 2r/2^p$. □

We are now ready to give the proof for Theorem 9.

Proof of Theorem 9: (Strong-Merger)
The proof follows immediately from Lemma 4.5. We choose in Lemma 4.5 a constant r, such that $1/(r+1)$ is negligible compared to δ, and we fix $m = \lceil n/r \rceil$. We then increase n to be exactly $m \cdot r$ by adding up to $r - 1$ zeros. (We choose n_0 to be large enough, such that adding at most $r - 1$ zeros affects δ in a negligible factor). We choose a constant p, such that $2r/2^p$ is negligible compared to γ', and we fix $\gamma = \gamma' - 2r/2^p$. We get in Lemma 4.5, $d = k \cdot r \cdot p$ (which is a constant), $b' \approx m - (2/\gamma) \cdot m \cdot \delta$ and $\gamma' \approx \gamma$ (where we use the sign $\approx$ to denote that we ignored negligible factors). Hence, $b' \approx m \cdot (1 - 2\delta/\gamma') \geq m \cdot (1 - 4\delta/\gamma')$. □

4.3 Seeded-Condensers

Theorem 8 (Strong-Seeded-Condenser) is proved by composing the somewhere-condenser of Theorem 10 and the merger of Theorem 9. Formally, we will need the following composition lemma.

Lemma 4.6 *Let $C : \{0,1\}^{n_1} \to \{0,1\}^{n_2 \cdot k}$ be an $[(n_1, b_1) \mapsto (n_2, b_2)^{1:k} \sim \gamma_1]$-somewhere-condenser, and let $M : \{0,1\}^d \times \{0,1\}^{n_2 \cdot k} \to \{0,1\}^m$ be a $[d, (n_2, b_2)^{1:k} \mapsto (m, b') \sim \gamma_2]$-strong-merger. Denote by $C' : \{0,1\}^d \times \{0,1\}^{n_1} \to \{0,1\}^m$ the following composition of M and C: for every $z \in \{0,1\}^d$ and $x \in \{0,1\}^{n_1}$, we define $C'(z, x) = M(z, C(x))$. Then, C' is a $[d, (n_1, b_1) \mapsto (m, b') \sim \gamma_1 + \gamma_2]$-strong-seeded-condenser.*

Proof:
The proof is straight forward from the definitions. □

We are now ready to give the proof for Theorem 8.

Proof of Theorem 8: (Strong-Seeded-Condenser)
The proof follows by composing Theorem 10 and Theorem 9, using Lemma 4.6. Given an $(n, \delta n)$-source, we use Theorem 10 to transform its distribution into a distribution that is, say, $\gamma/2$-close to a convex combination of distributions of $(n', \delta'' n')^{1:k}$-sources, with, say, $\delta'' \geq 1 - \delta\gamma/10$, and such that k is constant and $n' = \Omega(n)$. We can now use Theorem 9 to transform this distribution into a distribution that is γ-close to a distribution of an $(m, m - \delta m)$-source, such that $m = \Omega(n)$. By Theorem 9, we can do that using a seed of length $d = O(1)$.

Note that the merger of Theorem 9 functions well (i.e., with the parameters as above) on any $(n', \delta'' n')^{1:k}$-source, and hence it functions well (i.e., with the same parameters as above) also on a convex combination of distributions of $(n', \delta'' n')^{1:k}$-sources. This follows since a convex combination of distributions of $(m, m - \delta m)$-sources is also a distribution of an $(m, m - \delta m)$-source (as follows easily from the definitions).

Since the merger of Theorem 9 is strong, it can be verified (according to the same lines) that the seeded-condenser that we obtain is strong (as is stated in Lemma 4.6). $\square$

5 Multi-Sources-Extractors

Our results on multi-sources extractors are obtained by composing (in various ways) components that were derived in previous sections. A special attention is given to the notion of strong extraction, and to the independence (or almost independence) of different random variables.

5.1 Proof of Theorem 5

Theorem 5 (Multi-Sources-Extractor) is proved by composing the somewhere-condenser of Theorem 10 and the two-sources-extractor of Theorem 1. We will use the following composition lemma.

Lemma 5.1 *Let $C : \{0,1\}^{n_1} \to \{0,1\}^{n \cdot (k-1)}$ be an $[(n_1, b_1) \mapsto (n, b)^{1:k-1} \sim \gamma_1]$-somewhere-condenser. For every $i \in \{2, ..., k\}$, let $E_i : \{0,1\}^n \times \{0,1\}^{n_i} \to \{0,1\}^m$ be an $[(n, b), (n_i, b_i) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor. Denote by $E : \{0,1\}^{n_1} \times \cdots \times \{0,1\}^{n_k} \to \{0,1\}^m$ the following composition of C and $E_2, ..., E_k$: for every $x_1 \in \{0,1\}^{n_1}, ..., x_k \in \{0,1\}^{n_k}$, we define*

$$E(x_1, ..., x_k) = \bigoplus_{i=2}^{k} E_i(C(x_1)_{i-1}, x_i),$$

where $C(x_1)_1, ..., C(x_1)_{k-1} \in \{0,1\}^n$ denote the $k-1$ coordinates of $C(x_1)$ (i.e., $C(x_1) = (C(x_1)_1, ..., C(x_1)_{k-1})$). Then, E is a strong-in-the-first-input $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma_1 + \gamma_2]$-multi-sources-extractor.

Proof:
Let $X_1, ..., X_k$ be independent random variables, such that each X_i is an (n_i, b_i)-source.

First, assume that $C(X_1)$ is an $(n, b)^{1:k-1}$-source. Hence, one of the random variables $C(X_1)_1, ..., C(X_1)_{k-1}$ is an (n, b)-source. W.l.o.g., assume that $C(X_1)_1$ is an (n, b)-source. Since E_2 is an $[(n, b), (n_2, b_2) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor, the distribution of the random variable

$$(C(X_1)_1, E_2(C(X_1)_1, X_2))$$

is γ_2-close to $(C(X_1)_1, U_m)$. Hence, the distribution of the random variable

$$(X_1, C(X_1)_1, E_2(C(X_1)_1, X_2))$$

is γ_2-close to $(X_1, C(X_1)_1, U_m)$ (this follows since $C(x_1)_1$ is a function of x_1, or more precisely, since for every x_1, x'_1, such that $C(x_1)_1 = C(x'_1)_1$, the distributions of $E_2(C(x_1)_1, X_2)$ and $E_2(C(x'_1)_1, X_2)$ are the same). Hence, obviously, the distribution of the random variable

$$(X_1, E_2(C(X_1)_1, X_2))$$

is γ_2-close to (X_1, U_m). Hence, the distribution of the random variable

$$(X_1, X_3, ..., X_k, E_2(C(X_1)_1, X_2))$$

is γ_2-close to $(X_1, X_3, ..., X_k, U_m)$ (this follows since $X_3, ..., X_k$ are independent of X_1, X_2). Hence, the distribution of the random variable

$$(X_1, E_3(C(X_1)_2, X_3), ..., E_k(C(X_1)_{k-1}, X_k), E_2(C(X_1)_1, X_2))$$

is γ_2-close to $(X_1, E_3(C(X_1)_2, X_3), ..., E_k(C(X_1)_{k-1}, X_k), U_m)$. Hence, the distribution of the random variable

$$(X_1, \bigoplus_{i=2}^{k} E_i(C(X_1)_{i-1}, X_i))$$

is γ_2-close to (X_1, U_m).

Next, assume that the distribution of $C(X_1)$ is a convex combination of distributions of $(n, b)^{1:k-1}$-sources. Then, the same analysis as above, applied for each one of these distributions separately, shows that the random variable

$$(X_1, \bigoplus_{i=2}^{k} E_i(C(X_1)_{i-1}, X_i))$$

is γ_2-close to (X_1, U_m).

Since we know that the distribution of $C(X_1)$ is γ_1-close to a combination of distributions of $(n, b)^{1:k-1}$-sources, we can conclude that the random variable

$$(X_1, \bigoplus_{i=2}^{k} E_i(C(X_1)_{i-1}, X_i))$$

is $(\gamma_1 + \gamma_2)$-close to (X_1, U_m). Thus, E is a strong-in-the-first-input $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma_1 + \gamma_2]$-multi-sources-extractor. $\square$

Proof of Theorem 5: (Multi-Sources-Extractor)

Theorem 5 is proved by composing the somewhere-condenser of Theorem 10 and the two-sources-extractor of Theorem 1, using Lemma 5.1.

By Theorem 10, for the constant δ, there exist constants c, k, α, ρ_1, such that for $n_1 \geq c$ there exists an explicit $[(n_1, \delta n_1) \mapsto (n, b)^{1:k-1} \sim \gamma_1]$-somewhere-condenser, such that,

$$n \geq \alpha \cdot n_1,$$

$$b \geq 0.9 \cdot n,$$

$$\gamma_1 \leq 2^{-\rho_1 \cdot n}.$$

Assume that $n_1, ..., n_k, b_1, ..., b_k$ satisfy Property 1.7 with constants c, δ (where c is assumed to be large enough). Then, by Theorem 1, for every $i \in \{2, ..., k\}$, there exists an explicit $[(n, b), (n_i, b_i) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor such that,

$$m \geq \min[n, b_2, ..., b_k]/200,$$

$$\gamma_2 \leq 2^{-1.5 \cdot m}.$$

Hence, by Lemma 5.1, there exists an explicit strong-in-the-first-input $[\{(n_i, b_i)\}_1^k \mapsto m \sim \gamma_1 + \gamma_2]$-multi-sources-extractor. $\square$

5.2 Proof of Theorem 6

Theorem 6 (Strong-Seeded-Two-Sources-Extractor) is proved by composing the seeded-condenser of Theorem 8 and the two-sources-extractor of Theorem 1. We will use the following composition lemma.

Lemma 5.2 *Let $C : \{0,1\}^{n_3} \times \{0,1\}^{n_1} \to \{0,1\}^n$ be an $[n_3, (n_1, b_1) \mapsto (n, b) \sim \gamma_1]$-strong-seeded-condenser, and let $E : \{0,1\}^n \times \{0,1\}^{n_2} \to \{0,1\}^m$ be an $[(n, b), (n_2, b_2) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor. Denote by $E' : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \times \{0,1\}^{n_3} \to \{0,1\}^m$ the following composition of C and E: for every $x_1 \in \{0,1\}^{n_1}, x_2 \in \{0,1\}^{n_2}, x_3 \in \{0,1\}^{n_3}$, we define $E'(x_1, x_2, x_3) = E(C(x_3, x_1), x_2)$. Then, E' is an $[\{(n_i, b_i)\}_1^3 \mapsto m \sim \gamma_1 + \gamma_2]$-multi-sources-extractor, where $b_3 = n_3$. Moreover, E' is strong in the sets $\{1, 3\}$ and $\{2, 3\}$.*

Proof:
Let X_1, X_2, X_3 be independent random variables, such that each X_i is an (n_i, b_i)-source.

Since $C : \{0,1\}^{n_3} \times \{0,1\}^{n_1} \to \{0,1\}^n$ is an $[n_3, (n_1, b_1) \mapsto (n, b) \sim \gamma_1]$-strong-seeded-condenser, the average over $x_3 \in \{0,1\}^{n_3}$ of the minimal distance between the distribution of the random variable

$$C(x_3, X_1)$$

and a distribution of an (n, b)-source is $\leq \gamma_1$. Hence, since $E : \{0,1\}^n \times \{0,1\}^{n_2} \to \{0,1\}^m$ is an $[(n, b), (n_2, b_2) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor, the average over $x_3 \in \{0,1\}^{n_3}$ of the minimal distance between the distribution of the random variable

$$(X_2, E(C(x_3, X_1), X_2))$$

and the distribution (X_2, U_m) is $\leq \gamma_1 + \gamma_2$. Hence, since X_3 is uniformly distributed over $\{0,1\}^{n_3}$, the distribution of the random variable

$$(X_3, X_2, E(C(X_3, X_1), X_2))$$

is $(\gamma_1 + \gamma_2)$-close to (X_3, X_2, U_m). Thus, E' is an $[\{(n_i, b_i)\}_1^3 \mapsto m \sim \gamma_1 + \gamma_2]$-multi-sources-extractor, strong in the set $\{2, 3\}$.

Since $C : \{0,1\}^{n_3} \times \{0,1\}^{n_1} \to \{0,1\}^n$ is an $[n_3, (n_1, b_1) \mapsto (n, b) \sim \gamma_1]$-seeded-condenser, the distribution of the random variable

$$C(X_3, X_1)$$

is γ_1-close to a distribution of an (n, b)-source. Hence, since $E : \{0,1\}^n \times \{0,1\}^{n_2} \to \{0,1\}^m$ is an $[(n, b), (n_2, b_2) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor, the distribution of the random variable

$$(C(X_3, X_1), E(C(X_3, X_1), X_2))$$

is $(\gamma_1 + \gamma_2)$-close to $(C(X_3, X_1), U_m)$. Hence, the distribution of the random variable

$$(X_1, X_3, C(X_3, X_1), E(C(X_3, X_1), X_2))$$

is $(\gamma_1 + \gamma_2)$-close to $(X_1, X_3, C(X_3, X_1), U_m)$ (this follows as in the proof of Lemma 5.1, since $C(x_3, x_1)$ is a function of x_1, x_3, or more precisely, since for every x_1, x_3, x_1', x_3', such that $C(x_3, x_1) = C(x_3', x_1')$, the distributions of $E(C(x_3, x_1), X_2)$ and $E(C(x_3', x_1'), X_2)$ are the same). Hence, the distribution of the random variable

$$(X_1, X_3, E(C(X_3, X_1), X_2))$$

is $(\gamma_1 + \gamma_2)$-close to (X_1, X_3, U_m). Thus, E' is an $[\{(n_i, b_i)\}_1^3 \mapsto m \sim \gamma_1 + \gamma_2]$-multi-sources-extractor, strong in the set $\{1, 3\}$. □

Proof of Theorem 6: (Strong-Seeded-Two-Sources-Extractor)
Theorem 6 is proved by composing the seeded-condenser of Theorem 8 and the two-sources-extractor of Theorem 1, using Lemma 5.2.

By Theorem 8, for the constants δ, γ, there exist constants $c, n_3, \alpha > 0$, such that for $n_1 \geq c$ there exists an explicit $[n_3, (n_1, \delta n_1) \mapsto (n, b) \sim \gamma/2]$-strong-seeded-condenser, such that,

$$n \geq \alpha \cdot n_1,$$

$$b \geq 0.9 \cdot n.$$

Assume that n_1, n_2, b_1, b_2 satisfy Property 1.7 with constants c, δ (where c is assumed to be large enough). Then, by Theorem 1, there exists an explicit $[(n, b), (n_2, b_2) \mapsto m \sim \gamma/2]$-strong-two-sources-extractor such that,

$$m \geq \min[n, b_2]/200.$$

Hence, by Lemma 5.2, there exists an explicit $[\{(n_i, b_i)\}_1^3 \mapsto m \sim \gamma]$-multi-sources-extractor, strong in the sets $\{1, 3\}$ and $\{2, 3\}$ (where $b_3 = n_3$). □

5.3 Proof of Theorem 7

Before proving Theorem 7 (Three-Sources-Extractor), we will need to prove the following theorem. The theorem shows how to extract a constant number of random bits from three sources that satisfy Property 1.7. Moreover, the extracted bits are independent of the sets of sources $\{1,2\}$ and $\{1,3\}$. Roughly speaking (and for the important part of the range of the parameters), the theorem shows that if one source of min-entropy rate δ is available, as well as two sources of logarithmic min-entropy, then one can extract a constant number of bits, with a constant probability of error, and these bits are independent of the sets of sources $\{1,2\}$ and $\{1,3\}$.

Theorem 12 *For any constants $\delta, \gamma > 0$ and any constant $m' > 0$, there exists a constant $c > 0$, such that for any $n_1, n_2, n_3, b_1, b_2, b_3 > 0$ that satisfy Property 1.7 with constants c, δ, there exists an explicit $[\{(n_i, b_i)\}_1^3 \mapsto m' \sim \gamma]$-multi-sources-extractor, strong in the sets $\{1,2\}$ and $\{1,3\}$.*

Theorem 12 is proved by composing the somewhere-condenser of Theorem 10, the two-sources-extractor of Theorem 1, and an optimal strong-two-sources-extractor (whose existence is guaranteed by a probabilistic argument) and that acts on a constant number of bits (and hence it can be found in constant time). The idea for this composition is borrowed from [5]. We will use the following composition lemma.

Lemma 5.3 *Let $C : \{0,1\}^{n_1} \to \{0,1\}^{n \cdot k}$ be an $[(n_1, b_1) \mapsto (n,b)^{1:k} \sim \gamma_1]$-somewhere-condenser. Let $E_2 : \{0,1\}^n \times \{0,1\}^{n_2} \to \{0,1\}^m$ be an $[(n,b),(n_2,b_2) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor, and let $E_3 : \{0,1\}^n \times \{0,1\}^{n_3} \to \{0,1\}^m$ be an $[(n,b),(n_3,b_3) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor. Let $E' : \{0,1\}^{m \cdot k} \times \{0,1\}^{m \cdot k} \to \{0,1\}^{m'}$ be an $[(mk,m),(mk,m) \mapsto m' \sim \gamma_3]$-strong-two-sources-extractor. Denote by $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \times \{0,1\}^{n_3} \to \{0,1\}^{m'}$ the following composition of C, E_2, E_3, E': for every $x_1 \in \{0,1\}^{n_1}, x_2 \in \{0,1\}^{n_2}, x_3 \in \{0,1\}^{n_3}$, we define*

$$y_2 = (E_2(C(x_1)_1, x_2), \ldots, E_2(C(x_1)_k, x_2)) \in \{0,1\}^{m \cdot k},$$
$$y_3 = (E_3(C(x_1)_1, x_3), \ldots, E_3(C(x_1)_k, x_3)) \in \{0,1\}^{m \cdot k},$$
$$E(x_1, x_2, x_3) = E'(y_2, y_3),$$

where $C(x_1)_1, ..., C(x_1)_k \in \{0,1\}^n$ denote the k coordinates of $C(x_1)$ (i.e., $C(x_1) = (C(x_1)_1, ..., C(x_1)_k)$). Then, E is an $[\{(n_i, b_i)\}_1^3 \mapsto m' \sim \gamma_1 + 2\gamma_2 + \gamma_3]$-multi-sources-extractor. Moreover, E is strong in the sets $\{1,2\}$ and $\{1,3\}$.

Proof:
Let X_1, X_2, X_3 be independent random variables, such that each X_i is an (n_i, b_i)-source. Let

$$Y_2 = (E_2(C(X_1)_1, X_2), \ldots, E_2(C(X_1)_k, X_2)),$$
$$Y_3 = (E_3(C(X_1)_1, X_3), \ldots, E_3(C(X_1)_k, X_3)).$$

For every $x_1 \in \{0,1\}^{n_1}$, let

$$Y_2|_{X_1 = x_1} = (E_2(C(x_1)_1, X_2), \ldots, E_2(C(x_1)_k, X_2)),$$

$$Y_3|_{X_1=x_1} = (E_3(C(x_1)_1, X_3), \ldots, E_3(C(x_1)_k, X_3)).$$

First, assume that $C(X_1)$ is an $(n,b)^{1:k}$-source. Hence, one of the random variables $C(X_1)_1, ..., C(X_1)_k$ is an (n,b)-source. W.l.o.g., assume that $C(X_1)_1$ is an (n,b)-source. Since E_2 is an $[(n,b),(n_2,b_2) \mapsto m \sim \gamma_2]$-strong-two-sources-extractor, the distribution of the random variable

$$(C(X_1)_1, E_2(C(X_1)_1, X_2))$$

is γ_2-close to $(C(X_1)_1, U_m)$. Hence, the distribution of the random variable

$$(X_1, C(X_1)_1, E_2(C(X_1)_1, X_2))$$

is γ_2-close to $(X_1, C(X_1)_1, U_m)$ (this follows as in the proof of Lemma 5.1, since $C(x_1)_1$ is a function of x_1, or more precisely, since for every x_1, x_1', such that $C(x_1)_1 = C(x_1')_1$, the distributions of $E_2(C(x_1)_1, X_2)$ and $E_2(C(x_1')_1, X_2)$ are the same). Hence, obviously, the distribution of the random variable

$$(X_1, E_2(C(X_1)_1, X_2))$$

is γ_2-close to (X_1, U_m).

Hence, the expectation over $X_1 = x_1$ of the distance between the distribution of the random variable $E_2(C(x_1)_1, X_2)$ and the uniform distribution U_m is $\leq \gamma_2$. Hence, the expectation over $X_1 = x_1$ of the minimal distance between the distribution of the random variable $Y_2|_{X_1=x_1}$ and a distribution of an (mk,m)-source is $\leq \gamma_2$. In the same way, the expectation over $X_1 = x_1$ of the minimal distance between the distribution of the random variable $Y_3|_{X_1=x_1}$ and a distribution of an (mk,m)-source is $\leq \gamma_2$. Since for every x_1, the random variables $Y_2|_{X_1=x_1}$ and $Y_3|_{X_1=x_1}$ are independent, the expectation over $X_1 = x_1$ of the minimal distance between the distribution of the random variable $(Y_2|_{X_1=x_1}, Y_3|_{X_1=x_1})$ and a distribution of a pair of independent (mk,m)-sources is $\leq 2\gamma_2$.

Therefore, since E' is an $[(mk,m),(mk,m) \mapsto m' \sim \gamma_3]$-strong-two-sources-extractor, the expectation over $X_1 = x_1$ of the distance between the distribution of the random variable

$$(Y_2|_{X_1=x_1}, E'(Y_2|_{X_1=x_1}, Y_3|_{X_1=x_1}))$$

and the distribution $(Y_2|_{X_1=x_1}, U_{m'})$ is $\leq 2\gamma_2 + \gamma_3$. Hence, the distribution of the random variable

$$(X_1, Y_2, E'(Y_2, Y_3))$$

is $(2\gamma_2 + \gamma_3)$-close to $(X_1, Y_2, U_{m'})$. This implies that the distribution of the random variable

$$(X_1, X_2, Y_2, E'(Y_2, Y_3))$$

is $(2\gamma_2 + \gamma_3)$-close to $(X_1, X_2, Y_2, U_{m'})$ (as before and as in the proof of Lemma 5.1, this follows since for a fixed $X_1 = x_1$ the random variable Y_2 is a function of X_2 (and Y_3 is independent of X_2), or more precisely, since for every x_1, x_2, x_2', such that the value of Y_2 when $X_1 = x_1, X_2 = x_2$ is the same as its value when $X_1 = x_1, X_2 = x_2'$, the distribution of $E'(Y_2, Y_3)$ conditioned on $X_1 = x_1, X_2 = x_2$ is the same as its distribution conditioned on $X_1 = x_1, X_2 = x'_2$). We can hence conclude that the distribution of the random variable

$$(X_1, X_2, E(X_1, X_2, X_3))$$

is $(2\gamma_2 + \gamma_3)$-close to $(X_1, X_2, U_{m'})$.

Next, assume that the distribution of $C(X_1)$ is a convex combination of distributions of $(n, b)^{1:k}$-sources. Then, the same analysis as above, applied for each one of these distributions separately, shows that the random variable

$$(X_1, X_2, E(X_1, X_2, X_3))$$

is $(2\gamma_2 + \gamma_3)$-close to $(X_1, X_2, U_{m'})$.

Since we know that the distribution of $C(X_1)$ is γ_1-close to a combination of distributions of $(n, b)^{1:k}$-sources, we can conclude that the random variable

$$(X_1, X_2, E(X_1, X_2, X_3))$$

is $(\gamma_1 + 2\gamma_2 + \gamma_3)$-close to $(X_1, X_2, U_{m'})$. Thus, E is an $[\{(n_i, b_i)\}_1^3 \mapsto m' \sim \gamma_1 + 2\gamma_2 + \gamma_3]$-multi-sources-extractor, strong in the set $\{1, 2\}$. In the same way, E is also strong in the set $\{1, 3\}$. $\square$

Proof of Theorem 12:
Theorem 12 is proved using Lemma 5.3, by composing the somewhere-condenser of Theorem 10, the two-sources-extractor of Theorem 1, and an optimal strong-two-sources-extractor that acts on a constant number of bits.

By Theorem 10, for the constants δ, γ, there exist constants c, k, α, such that for $n_1 \geq c$ there exists an explicit $[(n_1, \delta n_1) \mapsto (n, b)^{1:k} \sim \gamma/4]$-somewhere-condenser, such that,

$$n \geq \alpha \cdot n_1,$$

$$b \geq 0.9 \cdot n.$$

By a standard probabilistic argument, for the constants k, m', γ, there exists a (large enough) constant m, such that there exists an $[(mk, m), (mk, m) \mapsto m' \sim \gamma/4]$-strong-two-sources-extractor, E'. Since E' acts on a constant number of bits, it can be found in constant time by an exhaustive search.

Assume that $n_1, n_2, n_3, b_1, b_2, b_3$ satisfy Property 1.7 with constants c, δ (where c is assumed to be large enough). Then, by Theorem 1, for every $i \in \{2, 3\}$, there exists an explicit $[(n, b), (n_i, b_i) \mapsto m \sim \gamma/4]$-strong-two-sources-extractor.

Hence, by Lemma 5.3, there exists an explicit $[\{(n_i, b_i)\}_1^3 \mapsto m' \sim \gamma]$-multi-sources-extractor, strong in the sets $\{1, 2\}$ and $\{1, 3\}$. $\square$

Proof of Theorem 7: (Three-Sources-Extractor)
Theorem 7 is proved by composing the multi-sources-extractor of Theorem 12 and the multi-sources-extractor of Theorem 6.

Let X_1, X_2, X_3 be independent random variables, such that each X_i is an (n_i, b_i)-source, and such that the requirements of Theorem 7 are satisfied (for a large enough constant c).

By Theorem 12, for any constant m' (that may depend on the constants δ, γ), if we assume that the constant c is large enough then we can extract from X_1, X_2, X_3, a string Z' of m' random bits, with distribution that is $\gamma/2$-close to the uniform distribution. Moreover, the distribution of (X_1, X_2, Z') is $\gamma/2$-close to $(X_1, X_2, U_{m'})$.

By Theorem 6, if we assume that the constants m' and c are large enough then we can extract from X_1, X_2, Z', a string Z of m random bits, with distribution that is γ-close to the uniform distribution, where $m \geq \min[\alpha n_1, b_2]/200$ (where $\alpha > 0$ is a small enough constant, that may depend on the constants δ, γ). Moreover, the distribution of (X_1, Z) is γ-close to (X_1, U_m). □

5.4 Proof of Corollary 11

Corollary 11 is an easy corollary of Theorem 6.

Proof of Corollary 11: (Ramsey-Graph)
We fix the constant γ in Theorem 6 to be 0.1, and we let the constant c to be the one from Theorem 6, and the constant r to be $2^{2^{n_3}}$, (where n_3 is the constant from Theorem 6). We only consider the first bit extracted by the multi-sources-extractor of Theorem 6, (i.e., we reduce m to be 1). We think of the multi-sources-extractor of Theorem 6, $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \times \{0,1\}^{n_3} \rightarrow \{0,1\}$, as a function $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \rightarrow \{0,1\}^{2^{n_3}}$. We think of this function as a coloring of the the complete bipartite graph of size $2^{n_1} \times 2^{n_2}$ with r colors. By Theorem 6 we know that there is no monochromatic subgraph of size larger than $2^{\delta n_1} \times (n_1)^5$, as such a subgraph implies the existence of independent X_1, X_2, X_3, such that X_1 is an $(n_1, \delta n_1)$-source, X_2 is an $(n_2, 5 \log n_1)$-source, and X_3 is an (n_3, n_3)-source, and such that the first output bit of the multi-sources-extractor of Theorem 6 is constant on these sources. □

Acknowledgment

I would like to thank Noga Alon, Boaz Barak, Ariel Gabizon, Oded Goldreich, Omer Reingold, Ronen Shaltiel, Amir Shpilka and avi Wigderson for very helpful conversations.

References

[1] Noga Alon. Tools from Higher Algebra. In *Handbook of Combinatorics, R.L. Graham, M. Grotschel and L. Lovasz, eds, North Holland* (1995), Chapter 32: 1749-1783

[2] Noga Alon, Oded Goldreich, Johan Hastad, Rene Peralta. Simple Construction of Almost k-wise Independent Random Variables. *Random Struct. Algorithms* 3(3): 289-304 (1992)

[3] Noga Alon, Oded Goldreich, Johan Hastad, Rene Peralta. Addendum to "Simple Construction of Almost k-wise Independent Random Variables". *Random Struct. Algorithms* 4(1): 119-120 (1993)

[4] Boaz Barak, Russell Impagliazzo, Avi Wigderson. Extracting Randomness from Few Independent Sources. FOCS 2004

[5] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, Avi Wigderson. Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers and Extractors. In preparation, 2004

[6] Benny Chor, Oded Goldreich. Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. *SIAM J. Comput.* 17(2): 230-261 (1988)

[7] Thomas M. Cover, Joy A. Thomas. *Elements of Information Theory.* John Wiley and Sons, Inc., (1991)

[8] Yevgeniy Dodis, Roberto Oliveira. On Extracting Private Randomness over a Public Channel. RANDOM-APPROX 2003: 252-263

[9] Yevgeniy Dodis, Ariel Elbaz, Roberto Oliveira, Ran Raz. Improved Randomness Extraction from Two Independent Sources. RANDOM-APPROX 2004

[10] Oded Goldreich. Three XOR-Lemmas - An Exposition. Electronic Colloquium on Computational Complexity (ECCC) 2(56): (1995)

[11] Ronald Graham, Joel Spencer. A Constructive Solution to a Tournament Problem. *Canad. Math. Bull.* 14: 45-48 (1971)

[12] Chi-Jen Lu, Omer Reingold, Salil P. Vadhan, Avi Wigderson. Extractors: Optimal up to Constant Factors. STOC 2003: 602-611

[13] Joseph Naor, Moni Naor. Small-bias Probability Spaces: Efficient Constructions and Applications. *SIAM J. Comput.* 22(4): 838-856 (1993)

[14] Noam Nisan, Amnon Ta-Shma. Extracting Randomness: A Survey and New Constructions. *J. Comput. Syst. Sci.* 58(1): 148-173 (1999)

[15] Noam Nisan, David Zuckerman. Randomness is Linear in Space. *J. Comput. Syst. Sci.* 52(1): 43-52 (1996)

[16] Ran Raz, Omer Reingold, Salil P. Vadhan. Error Reduction for Extractors. FOCS 1999: 191-201

[17] Ronen Shaltiel. Recent Developments in Explicit Constructions of Extractors. *Bulletin of the EATCS* 77: 67-95 (2002)

[18] Amnon Ta-Shma. On Extracting Randomness From Weak Random Sources. STOC 1996: 276-285

[19] Luca Trevisan, Salil P. Vadhan. Extracting Randomness from Samplable Distributions. FOCS 2000: 32-42

[20] Salil P. Vadhan. Randomness Extractors and their Many Guises (Tutorial given at FOCS 2002). http://www.eecs.harvard.edu/∼salil/extractors-focs02.ppt

[21] Umesh V. Vazirani. Strong Communication Complexity or Generating Quasirandom Sequences form Two Communicating Semi-Random Sources. *Combinatorica* 7(4): 375-392 (1987)

[22] Umesh V. Vazirani. Efficiency Considerations in Using Semi-Random Sources. STOC 1987: 160-168

[23] Avi Wigderson, David Zuckerman. Expanders That Beat the Eigenvalue Bound: Explicit Construction and Applications. *Combinatorica* 19(1): 125-138 (1999)

[24] David Zuckerman. Randomness-Optimal Oblivious Sampling. *Random Struct. Algorithms* 11(4): 345-367 (1997)