Electronic Colloquium on Computational Complexity, Report No. 190 (2010)

Improved Constructions of Three Source Extractors

Xin Li [*]
University of Texas at Austin
lixints@cs.utexas.edu

Abstract

We study the problem of constructing extractors for independent weak random sources. The probabilistic method shows that there exists an extractor for two independent weak random sources on n bits with only logarithmic min-entropy. However, previously the best known explicit two source extractor only achieves min-entropy $0.499n$ [Bou05], and the best known three source extractor only achieves min-entropy $n^{0.9}$ [Rao06]. It is a long standing open problem to construct extractors that work for smaller min-entropy.

In this paper we construct an extractor for three independent weak random sources on n bits with min-entropy $n^{1/2+\delta}$, for any constant $0 < \delta < 1/2$. This improves the previous best result of [Rao06]. In addition, we consider the problem of constructing extractors for three independent weak sources, such that one of the sources is significantly shorter than the min-entropy of the other two, in the spirit of [RZ08]. We give an extractor that works in the case where the longer, n-bit sources only have min-entropy $\mathrm{polylog}(n)$, and the shorter source also has min-entropy $\mathrm{polylog}(n)$. This improves the result of [RZ08].

We also study the problem of constructing extractors for affine sources over GF(2). Previously the best known deterministic extractor for n-bit affine sources in this case achieves entropy $n/\sqrt{\log\log n}$ [Yeh10, Li10]. In this paper we construct an extractor for two independent affine sources with entropy $n^{1/2+\delta}$, for any constant $0 < \delta < 1/2$.

Our constructions mainly use the extractors for somewhere random sources in [Rao06, Rao09] and the lossless condenser in [GUV07].

[*] Supported in part by NSF Grant CCF-0634811, NSF grant CCF-0916160 and THECB ARP Grant 003658-0113-2007.

ISSN 1433-8092

1 Introduction

Randomness has played an important role in computer science, with applications in many areas such as algorithm design, distributed computing and cryptography. These applications generally either provide solutions that are much more efficient than their deterministic counterparts (e.g., in algorithm design), or solve problems that would otherwise be impossible in the deterministic case (e.g., in distributed computing and cryptography).

However, to ensure their performances these applications need to rely on the assumption that they have access to uniformly random bits, while in practice it is not clear how to obtain such high quality sources of randomness. Instead, it may be the case that only imperfect random sources with highly biased random bits are available. Therefore an important problem is to study how to use imperfect random sources in these applications.

The study of this problem has led to the introduction of *randomness extractors*[NZ96]. Informally, a randomness extractor is a function $\mathsf{Ext} : \{0,1\}^n \to \{0,1\}^m$ such that given any imperfect random source as the input, the output is statistically close to uniform. If such functions can be computed efficiently then they can be used to convert imperfect random sources into nearly uniform random bits, and the problem of using imperfect randomness in randomized applications can be solved. Since the introduction of extractors, a lot of research work has been conducted on this object, and extractors are found to have applications in many other problems in computer science. We refer the reader to [FS02] for a survey on this subject.

In the context of extractors, an imperfect random source is modeled by an arbitrary probability distribution with a certain amount of entropy. The entropy used here is the *min-entropy*. A probability distribution (or equivalently, a random variable) on n bits is said to have min-entropy k if the probability of getting any particular string is at most 2^{-k}, and the distribution is called an (n, k)-weak random source. Unfortunately, it is not hard to show that no deterministic extractor exists even for $(n, n-1)$ weak random sources. Given this negative result, the study of extractors has been pursued in two different directions.

One direction is to give the function Ext an additional independent small seed of uniform random bits. Such extractors are thus called *seeded extractors*. Seeded extractors provide an optimal solution to the problem of simulating randomized algorithms using weak random sources, and a long line of research has resulted in seeded extractors with almost optimal parameters [LRVW03, GUV07, DW08, DKSS09].

Another direction is to study extractors for special classes of sources. These include for example samplable sources [TV00], bit-fixing sources [KZ07, GRS04], affine sources [GR05, Bou07], independent sources [BIW04, BKS$^+$05, Raz05, Rao06, BRSW06] and small space sources [KRVZ06].

The results of this paper fall into the second kind. Specifically, in this paper we study the problem of constructing extractors for independent sources and affine sources.

1.1 Extractors for Independent Sources

Using the probabilistic method, it is not hard to show that there exists an extractor for just two independent weak random sources, with only logarithmic min-entropy. However, despite considerable efforts on this problem [BIW04, BKS$^+$05, Raz05, Bou05, Rao06, BRSW06], the known constructions are far from achieving these parameters. Currently the best explicit extractor for two independent (n, k) sources only achieves min-entropy $k = 0.499n$ [Bou05], and the best explicit extractor for independent (n, n^α) sources requires $O(1/\alpha)$ sources [Rao06, BRSW06]. Given this embarrassing situation, in this paper we ask a slightly less ambitious question: how well can we do with three independent sources? That is, we want to construct an explicit extractor for three independent (n, k) sources, with k as small as possible.

Currently, the best known extractor for three independent sources achieves min-entropy $k = n^{0.9}$ [Rao06]. In this paper we improve this result. In addition, we consider the problem of building extractors for three independent sources with uneven lengths as in [RZ08]. There the authors gave an extractor for three independent sources, where two of them can have any polynomially small min-entropy and the third can have polylogarithmic entropy, as long as the length of the third source is much smaller than the min-entropy of the other two. In this paper we also improve this result in various aspects, and our construction is simpler than that of [RZ08].

1.2 Extractors for Affine Sources

An affine source is the uniform distribution over some affine subspace of a vector space.

Definition 1.1. (affine source) Let $\mathbb{F}_q$ be the finite field with q elements. Denote by $\mathbb{F}_q^n$ the n-dimensional vector space over $\mathbb{F}_q$. A distribution X over $\mathbb{F}_q^n$ is an $(n, k)_q$ affine source if there exist linearly independent vectors $a_1, \cdots, a_k \in \mathbb{F}_q^n$ and another vector $b \in \mathbb{F}_q^n$ s.t. X is sampled by choosing $x_1, \cdots, x_k \in \mathbb{F}$ uniformly and independently and computing

$$X = \sum_{i=1}^{k} x_i a_i + b.$$

In the case of affine sources, the min-entropy coincides with the standard Shannon entropy, and we will just call it entropy.

An affine extractor is a deterministic function such that given any affine source as the input, the output of the function is statistically close to the uniform distribution.

Definition 1.2. (affine extractor) A function $\mathsf{AExt} : \mathbb{F}_q^n \to \{0, 1\}^m$ is a deterministic (k, ϵ)-affine extractor if for every $(n, k)_q$ affine source X,

$$|\mathsf{AExt}(X) - U_m| \leq \epsilon.$$

Here U_m is the uniform distribution over $\{0, 1\}^m$ and $| \cdot |$ stands for the statistical distance.

In this paper we focus on the case where $q = 2$ and we will just write (n, k) affine sources instead of $(n, k)_2$ affine sources. Using the probabilistic method, it is not hard to show that there exists a deterministic affine extractor, as long as $k > 2 \log n$ and $m < k - O(1)$. However, again the known constructions are far from achieving these parameters. Currently the best explicit extractor for an (n, k) affine source only achieves entropy $k = n/\sqrt{\log \log n}$ [Yeh10, Li10]. Thus in this paper we also ask a slightly less ambitious question: how well can we do with two independent affine sources? That is, we want to construct an explicit extractor for two independent (n, k) affine sources, with k as small as possible. To our best knowledge there has been no result on this problem before, although a result in [Li10] implies such an extractor with $k = \delta n$ for any constant $0 < \delta < 1$. In this paper we also improve this result.

1.3 Our Results

For the problem of constructing three source extractors, we achieve min-entropy $k = n^{1/2+\delta}$, for any constant $0 < \delta < 1/2$. This improves the previous best result of [Rao06], where the min-entropy is required to be at least $n^{0.9}$. Specifically, we have the following theorem.

Theorem 1.3. *For every constant $0 < \delta < 1/2$, there exists a polynomial time computable function $\mathsf{THExt} : (\{0,1\}^n)^3 \to \{0,1\}^m$ such that if X, Y, Z are three independent (n, k) sources with $k = n^{1/2+\delta}$, then*

$$|\mathsf{THExt}(X, Y, Z) - U_m| < n^{-\Omega(\delta)}$$

with $m = \Omega(k)$.

The following table summarizes recent results on extractors for independent sources.

Number of Sources	Min-Entropy	Output	Error	Ref
$O(\mathrm{poly}(1/\delta))$	δn	$\Theta(n)$	$2^{-\Omega(n)}$	[BIW04]
3	δn, any constant δ	$\Theta(1)$	$O(1)$	[BKS$^+$05]
3	One source: δn, any constant δ. Other sources may have $k \geq \mathrm{polylog}(n)$.	$\Theta(1)$	$O(1)$	[Raz05]
2	One source: $(1/2 + \delta)n$, any constant δ. Other source may have $k \geq \mathrm{polylog}(n)$	$\Theta(k)$	$2^{-\Omega(k)}$	[Raz05]
2	$(1/2 - \alpha_0)n$ for some small universal constant $\alpha_0 > 0$	$\Theta(n)$	$2^{-\Omega(n)}$	[Bou05]
$O(1/\delta)$	$k = n^{\delta}$	$\Theta(k)$	$k^{-\Omega(1)}$	[Rao06]
$O(1/\delta)$	$k = n^{\delta}$	$\Theta(k)$	$2^{-k^{\Omega(1)}}$	[BRSW06]
3	One source: δn, any constant δ. Other sources may have $k \geq \mathrm{polylog}(n)$.	$\Theta(k)$	$2^{-k^{\Omega(1)}}$	[Rao06]
3	$k = n^{1-\alpha_0}$ for some small universal constant $\alpha_0 > 0$	$\Theta(k)$	$2^{-k^{\Omega(1)}}$	[Rao06]
3	$k = n^{1/2+\delta}$, any constant δ	$\Theta(k)$	$k^{-\Omega(1)}$	This work

Table 1: **Summary of Results on Extractors for Independent Sources.**

For three independent sources with uneven lengths, we have the following theorem.

Theorem 1.4. *For every constant $0 < \gamma < 1$, there exists a polynomial time computable function $\mathsf{UExt} : \{0,1\}^{n_1} \times \{0,1\}^{n_1} \times \{0,1\}^{n_3} \to \{0,1\}^m$ such that if X is an (n_1, k_1) source, Y is an (n_2, k_2) source, Z is an (n_3, k_3) source and X, Y, Z are independent, then*

$$|\mathsf{UExt}(X, Y, Z) - U_m| < 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}$$

with $m = \Omega(k_3)$, as long as the following hold:

- $n_1 < k_2^{\gamma}$ *and* $k_2 \leq k_3$.
- $k_1 > 2\log^2 n_1$, $k_1 > 2\log^2 n_2$ *and* $k_1 > 2\log^2 n_3$.
- $k_2^{\frac{1-\gamma}{4}} > \log^2 n_2$ *and* $k_2^{\frac{1-\gamma}{4}} > \log^2 n_3$.

By setting the parameters appropriately, we get the following two corollaries.

Corollary 1.5. *For all constants $0 < \beta, \gamma < 1$ there is a polynomial time computable function* $\mathsf{UExt} : \{0,1\}^{n^{\beta\gamma}} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{\Omega(n^\beta)}$ *which is an extractor for three independent sources with min-entropy requirement $k = \log^3 n, n^\beta, n^\beta$, and error $2^{-\log^{\Omega(1)} n}$.*

This result improves that of [RZ08] in the sense that the length of the short source can be $n^{\beta\gamma}$ for any constant $0 < \gamma < 1$. In particular, γ can be arbitrarily close to 1, while in [RZ08] it has to be $1/h$ for some constant $h > 1$.

Corollary 1.6. *For every constant $c > 3$ there is a constant $d > c$ and a polynomial time computable function* $\mathsf{UExt} : \{0,1\}^{\log^c n} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{\Omega(\log^d n)}$ *which is an extractor for three independent sources with min-entropy requirement $k = \log^3 n, \log^d n, \log^d n$, and error $2^{-\log^{\Omega(1)} n}$.*

This result gives an extractor for three independent sources, such that two of them have only polylogarithmic min-entropy, and the third one has polynomially small min-entropy while the length is only polylogarithmic of the other two. It appears that the result in [RZ08] cannot handle this situation.

For two independent affine sources, we have the following theorem.

Theorem 1.7. *For every constant $0 < \delta < 1/2$, there exists a polynomial time computable function* $\mathsf{TAExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ *such that if X, Y are two independent affine (n,k) sources with $k = n^{1/2+\delta}$, then*

$$|\mathsf{TAExt}(X,Y) - U_m| < n^{-\Omega(\delta)}$$

with $m = \Omega(k)$.

Remark 1.8.

- In this paper we do not optimize the length of the output, but it is not hard to show that in all our constructions the output length can be made to $k - o(k)$, by using a seeded extractor that extracts almost all randomness from a weak source in our constructions.
- In fact, our extractor for two independent affine sources works for one affine block source with two blocks of length n, as long as the first block has entropy $n^{1/2+\delta}$, and the second has entropy $n^{1/2+\delta}$ even conditioned on the fixing of the first one.

1.4 Overview of the Constructions and Techniques

Here we give a brief description of our constructions and the techniques used. For clarity and simplicity we shall be imprecise sometimes.

1.4.1 The three source extractor

Our construction of the three source extractor mainly uses somewhere random sources and the extractor for such sources in [Rao06]. Informally, a somewhere random source is a matrix of random variables such that at least one of the rows is uniform. If we have two independent somewhere random sources $X = X_1 \circ \cdots \circ X_t$ and $Y = Y_1 \circ \cdots \circ Y_t$ with the same number of rows t, and there exists an i such that both X_i and Y_i are uniform, then we call X and Y independent *aligned* somewhere random sources. In [Rao06] it is shown that if we have two independent aligned somewhere random sources X, Y with t rows and each row has n bits, such that $t < n^\gamma$ for some arbitrary constant $0 < \gamma < 1$, then we can efficiently extract random bits from X and Y.

Now given three independent (n, k) sources X, Y, Z with $k = n^{1/2+\delta}$, our construction uses X to convert Y and Z into two somewhere random sources, such that with high probability over the fixing of X (and some additional random variables), they are independent aligned somewhere random sources, and the number of rows is significantly smaller than the length of each row. Then we will be done by using the extractor in [Rao06] described above.

To illustrate how we do this, first assume that we have a strong seeded extractor that only uses $\log n$ additional random bits and can extract almost all the entropy from an (n, k)-source with error $1/100$. A strong seeded extractor is a seeded extractor such that with high probability over the fixing of the seed, the output is still close to uniform. We now try this extractor on X, Y and Z with all $2^{\log n} = n$ possibilities of the seed and output $n^{\delta/2}$ bits. Thus we obtain three $n \times n^{\delta/2}$ matrices. Now we divide each matrix into $\sqrt{n}$ blocks with each block consisting of $\sqrt{n}$ rows. Therefore we get $X^1 \circ \cdots \circ X^t$, $Y^1 \circ \cdots \circ Y^t$ and $Z^1 \circ \cdots \circ Z^t$, where $t = \sqrt{n}$ and each X^i, Y^i, Z^i is a block. By a standard property of strong seeded extractors, with probability $1 - 1/10 = 9/10$ over the fixing of the seed, the output is $1/10$-close to uniform. Therefore in each matrix, at least $9/10$ fraction of the rows are close to uniform. We say a block is "good" if it contains at least one such row. Thus in each matrix at least $9/10$ fraction of the blocks are good.

Now it's easy to see that there exists an i such that all X^i, Y^i and Z^i are good. In other words, in some sense the matrices are already "aligned". Next, for each i we compute an output R_i from (X^i, Y^i, X, Y) and an output R'_i from (X^i, Z^i, X, Z), with the property that if X^i, Y^i are good, then R_i is (close to) uniform, and if X^i, Z^i are good, then R'_i is (close to) uniform. We then concatenate $\{R_i\}$ to form a matrix SR_y and concatenate $\{R'_i\}$ to form a matrix SR_z. Since there exists an i such that all X^i, Y^i and Z^i are good, SR_y and SR_z are (close to) aligned somewhere random sources.

In the analysis below we consider a particular i such that all X^i, Y^i and Z^i are good (though we may not know what i is).

Now let's consider computing R_i from (X^i, Y^i, X, Y) (R'_i is computed the same way from (X^i, Z^i, X, Z)). Here we use a two-source extractor Raz in [Raz05]. This extractor is strong and it works as long as one of the source has min-entropy rate (the ratio between min-entropy and the length of the source) $> 1/2$, and even if the two sources have different lengths. We first apply Raz to Y^i and each row of X^i (note Y^i is treated as a whole) to obtain a matrix M. Note that if X^i, Y^i are good then they are both somewhere random, and thus Y^i has min-entropy at least $n^{\delta/2}$. Thus M is also a somewhere random source. Since Raz is a strong two-source extractor, we can fix X^i, and conditioned on this fixing M is still a somewhere random source. Moreover now M is a deterministic function of Y^i and is thus independent of X. Next note that the size of X^i is $\sqrt{n} \cdot n^{\delta/2} = n^{1/2+\delta/2}$ while the min-entropy of X is $n^{1/2+\delta}$. Thus with high probability over the fixings of X^i, X still has min-entropy at least $0.9n^{1/2+\delta}$. Therefore now we can apply a strong seeded extractor to X and each row of M and output $0.8n^{1/2+\delta}$ bits. Thus we obtain a $(\sqrt{n} \times 0.8n^{1/2+\delta})$ somewhere random source $\bar{X}^i$. Furthermore, since we applied a strong seeded extractor and now M is a deterministic function of Y^i, we can further fix Y^i and $\bar{X}^i$ is still somewhere random, meanwhile it is now a deterministic function of X.

Similarly, we can compute a somewhere random source $\bar{Y}^i$. Specifically, Since Raz is a strong two-source extractor, we can fix Y^i, and conditioned on this fixing M is still a somewhere random source. Moreover now M is a deterministic function of X^i and is thus independent of Y. Next note that the size of Y^i is $\sqrt{n} \cdot n^{\delta/2} = n^{1/2+\delta/2}$ while the min-entropy of Y is $n^{1/2+\delta}$. Thus with high probability over the fixings of Y^i, Y still has min-entropy at least $0.9n^{1/2+\delta}$. Therefore now we can apply a strong seeded extractor to Y and each row of M and output $0.8n^{1/2+\delta}$ bits. Thus we obtain a $(\sqrt{n} \times 0.8n^{1/2+\delta})$ somewhere random source $\bar{Y}^i$. Furthermore, since we applied a strong seeded extractor and now M is a deterministic function of X^i, we can further fix X^i and $\bar{Y}^i$ is still somewhere random, meanwhile it is now a deterministic function of X.

Therefore now after the fixings of (X^i, Y^i), we get two independent $(\sqrt{n} \times 0.8n^{1/2+\delta})$ somewhere random sources $(\bar{X}^i, \bar{Y}^i)$. It is easy to check that they are aligned. Note that the number of rows is significantly less than the length of each row, thus we can apply the extractor in [Rao06] to get a random string R_i with say $0.7n^{1/2+\delta}$ bits. Further notice that the extractor in [Rao06] is strong, thus we can fix X and R_i is still (close to) uniform. This means that we can fix X and SR_y is still somewhere random (recall that SR_y is the concatenation of $\{R_i\}$), moreover it is now a deterministic function of Y.

Similarly we can compute SR_z, and by the same argument we can fix X and SR_z is still somewhere random, moreover it is now a deterministic function of Z. Therefore now after we fix (X, Y^i, Z^i), we get two independent aligned $(\sqrt{n} \times 0.7n^{1/2+\delta})$ somewhere random sources, and again the extractor in [Rao06] can be used to obtain an output that is (close to) uniform.

The above argument works even if the seed length of the strong seeded extractor that we use on X, Y, Z (try all possibilities of the seed) is $(1 + \alpha)\log n$ instead of $\log n$, as long as α can be an arbitrarily small constant. However, currently we don't have such extractors for min-entropy $k = n^{1/2+\delta}$. Fortunately, we have condensers with such short seed length. A (seeded) condenser is a generalization of a seeded extractor, such that the output is close to having high min-entropy instead of being uniform. In this paper we use the condenser built in [GUV07]. For any constant $\alpha > 0$ and any (n, k') source, this condenser uses $d = (1 + 1/\alpha) \cdot (\log n + \log k' + \log(1/\epsilon)) + O(1)$ additional random bits to convert the source roughly into a $((1+\alpha)k', k')$ source with error ϵ. Now we can take α to be a sufficiently large constant, say $10/\delta$, take k' to be small, say $n^{\delta/10}$ (note that an $(n, n^{1/2+\delta})$ source is also an $(n, n^{\delta/10})$ source), and take ϵ to be something like $n^{-\delta/10}$. This gives us a small seed length, such that $2^d = O(n^{1+\delta/3})$. Therefore the number of blocks is $O(n^{1/2+\delta/3})$, which is significantly less than $n^{1/2+\delta}$.

Now we can repeat the argument before. The condenser can also be shown to be strong, in the sense that with probability $1 - 2\sqrt{\epsilon}$ over the fixing of the seed, the output is $\sqrt{\epsilon}$-close to having min-entropy $k' - d$ (intuitively, this is because the seed length is d, thus conditioned on the seed the output can lose at most d bits of entropy). Now define a block to be "good" if it contains at least one "good" row that is $\sqrt{\epsilon}$-close to having min-entropy $k' - d$. Again we can show there is an i such that all X^i, Y^i and Z^i are good.

To finish the argument, we need to apply Raz to Y^i and each row of X^i. However now the good row in X^i is not uniform, in fact it may not even have min-entropy rate $> 1/2$. On the other hand, it does have a constant min-entropy rate. Therefore we now first apply the somewhere condenser from [BKS+05, Zuc07] to each row of X^i to boost the min-entropy rate to 0.9. The somewhere condenser outputs another constant number of rows for each row of X^i, and if the row of X^i is good, then one of the outputs is close to having min-entropy rate 0.9. Now we can apply Raz to Y^i and each output of the somewhere condenser, and proceed as before. Since this only increases the number of rows in $(\bar{X}^i, \bar{Y}^i)$ by a constant factor, it does not affect our analysis. Thus we obtain a three source extractor for min-entropy $k = n^{1/2+\delta}$.

1.4.2 The extractor for three sources with uneven lengths

If we do not try to optimize the parameters here, our construction for this extractor is quite simple. Assume that we have three independent sources X, Y, Z such that X is an (n_1, k_1) source, Y is an (n_2, k_2) source, Z is an (n_3, k_3) source and n_1 is significantly smaller than k_2 and k_3. We can do the following. First take a strong seeded extractor that uses $O(\log n_1)$ additional random bits, and try this extractor on X with all possibilities of the seed. Then we get a somewhere random source $\bar{X}$ with n_1^c rows for some constant $c > 1$. Now we apply a strong seeded extractor to Y and each row of $\bar{X}$ and output $\Omega(k_2)$ bits. Thus we get a $n_1^c \times \Omega(k_2)$ somewhere random source. We do the same thing to Z and each row of $\bar{X}$ and we get a $n_1^c \times \Omega(k_3)$ somewhere random source. Note that these two somewhere random sources are aligned. Moreover since the extractor is strong, we can fix X and conditioned on this fixing, the two sources are still aligned somewhere random sources, and they are now independent (because they are now deterministic functions of Y and Z respectively). Thus if $n_1^c < min[k_2, k_3]$, we can use the extractor in [Rao06] to extract random bits from these two sources.

There are two small disadvantages with the above construction. First, it requires that $n_1 < min[k_2, k_3]^{1/c}$ for some constant $c > 1$ instead of $n_1 < min[k_2, k_3]^{\gamma}$ for any constant $0 < \gamma < 1$. Second, the error of the construction is only $1/\text{poly}(n_1)$. We deal with these problems as follows.

For the first problem, as before, instead of using a seeded extractor on X (trying all possibilities of the seed), we use the seeded condenser in [GUV07] and the somewhere condenser in [BKS+05, Zuc07]. This gives us a short seed whose length is arbitrarily close to $\log n_1$, thus we can achieve $n_1 < min[k_2, k_3]^{\gamma}$ for any constant $0 < \gamma < 1$. However, now the "good" row in $\bar{X}$ only has min-entropy rate 0.9 and we cannot apply a seeded extractor to Y and each row of $\bar{X}$. We can use the strong two source extractor Raz here, but then the length of the output is at most k_1, and is smaller than n_1. So instead we do the following.

For each row $\bar{X}_i$ in $\bar{X}$, assume the length is m_1. We first take a substring S_i of $\bar{X}_i$ with length $0.3m_1$, and apply Raz to S_i and Y to get V_i. We then apply a strong seeded extractor to $\bar{X}_i$ and V_i to get R_i, and apply a strong seeded extractor to Y and R_i to get the final output H_i. We concatenate $\{H_i\}$ to get a matrix SR_y. Now if $\bar{X}_i$ has min-entropy rate 0.9, then S_i has min-entropy rate at least $2/3$ and thus the two source extractor Raz works. Since Raz is strong, we can fix S_i and V_i is still (close to) uniform, and it is a deterministic function of Y and thus independent of $\bar{X}_i$. Note that S_i has length $0.3m_1$ thus with high probability over the fixing of S_i, $\bar{X}_i$ still has min-entropy at least say $0.5m_1$. Therefore R_i is (close to) uniform. Since the seeded extractor is also strong, we can further fix V_i and R_i is still uniform, and it is now a deterministic function of $\bar{X}_i$ and thus independent of Y. Note that the length of V_i is at most $k_1 < n_1$ and is much smaller than k_2, thus with high probability over the fixing of V_i, Y still has min-entropy at least $0.9k_2$. Therefore now H_i is (close to) uniform and can output $0.8k_2$ bits. Moreover since the seeded extractor is strong, H_i is (close to) uniform even conditioned on the fixing of X. Thus we obtain a somewhere random source SR_y with the number of rows significantly smaller than the length of each row, and it is somewhere random even conditioned on the fixing of X.

We can now do the same thing to X and Z to obtain a somewhere random source SR_z, and apply the extractor in [Rao06] to (SR_y, SR_z) to extract random bits.

For the second problem, we use similar techniques as those in [BRSW06] to show that, when the extractor is run on three sources with larger min-entropy, the error must become much smaller.

1.4.3 The affine two source extractor

Here we mainly use affine somewhere random sources, the extractor for such sources in [Rao09], and strong linear seeded extractors. An affine somewhere random source is an affine source that is also a somewhere random source. In [Rao09] it is shown that if we have an affine somewhere random sources X with t rows and each row has n bits, such that $t < n^{\gamma}$ for some arbitrary constant $0 < \gamma < 1$, then we can efficiently extract random bits from X. A strong linear seeded extractor is a strong seeded extractor such that for any fixing of the seed, the output is a linear function of the weak source. Such extractors are known to exist, for example Trevisan's extractor [Tre01].

Given two independent (n, k) affine sources X, Y with $k = n^{1/2+\delta}$ for any constant $0 < \delta < 1/2$, our extractor works as follows. We first convert X into a somewhere random source $\bar{X}$ (not necessarily affine) with $\sqrt{n}$ rows. We then apply a strong linear seeded extractor to Y and each row of $\bar{X}$ and output $\Omega(n^{1/2+\delta})$ bits. Thus we obtain a $(\sqrt{n} \times \Omega(n^{1/2+\delta}))$ somewhere random source H. By the property of the strong linear seeded extractor, we can fix X, and with high probability over this fixing, H is still somewhere random. Moreover now it is affine, since conditioned on the fixing of X, the extractor is a linear function. Thus we can now apply the extractor in [Rao09] to extract random bits from H.

Now let us see how we can convert X into a somewhere random source with $\sqrt{n}$ rows. To do this, we first divide X into $\sqrt{n}$ blocks $X^1 \circ \cdots \circ X^t$ where $t = \sqrt{n}$ and each block has $\sqrt{n}$ bits. By Lemma 2.15, the sum of the entropies of these blocks is at least $k = n^{1/2+\delta}$. Therefore at least one block must have entropy at least n^{δ}. Now for each X^i we do the following. We take the condenser from [GUV07] and try it on X^i with all possibilities of the seed. Next we take a strong seeded extractor that uses $O(\log n)$ additional random bits, and for each possible output of the condenser, try the extractor with all possibilities of the seed. We concatenate all these outputs to get a somewhere random source M^i. Note that X^i has length $\sqrt{n}$, the condenser has seed length $d_1 = (1 + 1/\alpha) \cdot (\log n_1 + \log k_1 + \log(1/\epsilon_1)) + O(1)$ and the extractor has seed length $d_2 = O(\log n_2)$. Thus M^i has $2^{d_1+d_2}$ rows. Now note that $n_1 = \sqrt{n}$, and n_2 is the length of the output of the condenser, which is roughly $(1 + \alpha)k_1$. Thus we can choose α to be a large enough constant, choose k_1 to be n^{δ_1} for a small enough constant δ_1 and choose $\epsilon_1 = n^{-\delta_2}$ for a small enough constant δ_2, such that $d_1 + d_2 \leq (1/2 + \delta/2) \log n$. Hence M^i has at most $n^{1/2+\delta/2}$ rows.

Now for each M^i, we apply a strong linear seeded extractor to X and each row of M^i to get a matrix $\bar{X}^i$. Now assume X^i has entropy at least n^{δ} (recall that we know there exists such a block). Then M^i is a somewhere random source. We want to argue that $\bar{X}^i$ is also a somewhere random source. At first this may seem unreasonable because M^i and X are correlated. However note that M^i is a deterministic function of X^i, and X^i is a linear function of X. Also note that since X^i only has $\sqrt{n}$ bits, conditioned on the fixing of X^i, X has entropy at least $n^{1/2+\delta} - \sqrt{n} > 0.9n^{1/2+\delta}$ by Lemma 2.14. Now the property of strong linear seeded extractor and the structure of affine sources guarantee that in this case, with high probability over the fixing of X^i, $\bar{X}^i$ is also a somewhere random source. Moreover, each row in $\bar{X}^i$ can have length $\Omega(n^{1/2+\delta})$. Furthermore, conditioned on the fixing of X^i, X is still an affine source. Thus conditioned on the fixing of X^i, $\bar{X}^i$ is also an affine source, since the extractor is a linear seeded extractor. Thus now conditioned on the fixing of X^i, $\bar{X}^i$ is an affine somewhere random source with at most $n^{1/2+\delta/2}$ rows and each row has length $\Omega(n^{1/2+\delta})$. Therefore we can use the extractor in [Rao09] to extract random bits from $\bar{X}^i$. Since we try this for every X^i, we end up with a somewhere random source with $\sqrt{n}$ rows.

Roadmap. The rest of the paper is organized as follows. In Section 2 we give the preliminaries and previous work that we use. Section 3 gives the formal description of our three source extractor, and its analysis. Section 4 gives the formal description of our extractor for three independent sources with uneven lengths, and the analysis of the extractor. Section 5 gives our extractor for two independent affine sources, and the analysis of the extractor. Finally in Section 6 we conclude with some open problems.

2 Preliminaries

We use common notations such as $\circ$ for concatenation and $[n]$ for $\{1, 2, \cdots, n\}$. All logarithms are to the base 2. We often use capital letters for random variables and corresponding small letters for their instantiations.

2.1 Basic Definitions

Definition 2.1 (statistical distance)**.** Let D and F be two distributions on a set S. Their **statistical distance** is

$$|D - F| \overset{def}{=} \max_{T \subseteq S}(|D(T) - F(T)|) = \frac{1}{2}\sum_{s \in S}|D(s) - F(s)|$$

If $|D - F| \leq \epsilon$ we say that D is ϵ-*close* to F.

Definition 2.2. The *min-entropy* of a random variable X is defined as

$$H_\infty(X) = min_{x \in \mathsf{supp}(X)}\{-\log_2 \Pr[X = x]\}.$$

We say X is an (n, k)-source if X is a random variable on $\{0,1\}^n$ and $H_\infty(X) \geq k$. When n is understood from the context we simply say that X is a k-source.

2.2 Somewhere Random Sources, Extractors and Condensers

Definition 2.3 (Somewhere Random sources)**.** A source $X = (X_1, \cdots, X_t)$ is $(t \times r)$ *somewhere-random* (SR-source for short) if each X_i takes values in $\{0,1\}^r$ and there is an i such that X_i is uniformly distributed.

Definition 2.4. An elementary somewhere-k-source is a vector of sources $(X_1, \cdots, X_t)$, such that some X_i is a k-source. A somewhere k-source is a convex combination of elementary somewhere-k-sources.

Definition 2.5. A function $C : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a $(k \to l, \epsilon)$-condenser if for every k-source X, $C(X, U_d)$ is ϵ-close to some l-source. When convenient, we call C a rate-$(k/n \to l/m, \epsilon)$-condenser.

Definition 2.6. A function $C : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a $(k \to l, \epsilon)$-somewhere-condenser if for every k-source X, the vector $(C(X, y)_{y \in \{0,1\}^d})$ is ϵ-close to a somewhere-l-source. When convenient, we call C a rate-$(k/n \to l/m, \epsilon)$-somewhere-condenser.

Definition 2.7. A function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *strong seeded extractor* for min-entropy k and error ϵ if for every min-entropy k source X,

$$|(\mathsf{Ext}(X,R),R) - (U_m,R)| < \epsilon,$$

where R is the uniform distribution on d bits independent of X, and U_m is the uniform distribution on m bits independent of R.

Definition 2.8. A function $\mathsf{TExt} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ is a *strong two source extractor* for min-entropy k_1, k_2 and error ϵ if for every independent (n_1,k_1) source X and (n_2,k_2) source Y,

$$|(\mathsf{TExt}(X,Y),X) - (U_m,X)| < \epsilon$$

and

$$|(\mathsf{TExt}(X,Y),Y) - (U_m,Y)| < \epsilon,$$

where U_m is the uniform distribution on m bits independent of (X,Y).

Definition 2.9. (aligned SR-source) [Rao06] We say that a collection of SR-sources $X_1, \cdots, X_u$ is *aligned* if there is some i such that the i'th row of every SR-source in the collection is uniformly distributed.

We also need the definition of a subsource.

Definition 2.10 (Subsource)**.** Given random variables X and X' on $\{0,1\}^n$ we say that X' is a *deficiency-d subsource* of X and write $X' \subseteq X$ if there exits a set $A \subseteq \{0,1\}^n$ such that $(X|A) = X'$ and $\Pr[x \in A] \geq 2^{-d}$.

We have the following lemma.

Lemma 2.11 ([BRSW06])**.** *Let X be a random variable over $\{0,1\}^n$ such that X is ϵ-close to an (n,k) source with $\epsilon \leq 1/4$. Then there is a deficiency 2 subsource $X' \subseteq X$ such that X' is a $(n,k-3)$ source.*

2.3 Strong Linear Seeded Extractors

We need the following definition and property of a specific kind of extractors.

Definition 2.12. A function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *strong seeded extractor* for min-entropy k and error ϵ if for every min-entropy k source X,

$$\Pr_{u \leftarrow_R U_d}[|\mathsf{Ext}(X,u) - U_m| \leq \epsilon] \geq 1 - \epsilon,$$

where U_m is the uniform distribution on m bits. We say that the function is a *linear strong seeded extractor* if the function $\mathsf{Ext}(\cdot,u)$ is a linear function over $\mathsf{GF}(2)$, for every $u \in \{0,1\}^d$.

Proposition 2.13 ([Rao09])**.** *Let $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be a linear strong seeded extractor for min-entropy k with error $\epsilon < 1/2$. Let X be any affine source with entropy k. Then,*

$$\Pr_{u \leftarrow_R U_d}[|\mathsf{Ext}(X,u) - U_m| = 0] \geq 1 - \epsilon$$

2.4 The Structure of Affine Sources

The following lemma explains the behavior of a linear function acting on an affine source.

Lemma 2.14 ([Rao09, Li10]). *(Affine Conditioning) . Let X be any affine source on $\{0,1\}^n$. Let $L : \{0,1\}^n \to \{0,1\}^m$ be any linear function. Then there exist independent affine sources A, B such that:*

- $X = A + B$.
- *For every* $b \in \mathsf{Supp}(B)$, $L(b) = 0$.
- $H(A) = H(L(A))$ *and there exists an affine function* $L^{-1} : \{0,1\}^m \to \{0,1\}^n$ *such that* $A = L^{-1}(L(A))$.

We have the following lemma that exhibits a nice structure of affine sources.

Lemma 2.15 ([Li10]). *Let X be any affine source on $\{0,1\}^n$. Divide X into t arbitrary blocks $X = X_1 \circ X_2 \circ ... \circ X_t$. Then there exist positive integers $k_1, ..., k_t$ such that,*

- $\forall j, 1 \leq j \leq t$ *and* $\forall (x_1, .., x_{j-1}) \in \mathsf{Supp}(X_1, .., X_{j-1})$, $H(X_j|_{X_1=x_1,...,X_{j-1}=x_{j-1}}) = k_j$.
- $\sum_{i=1}^{t} k_i = H(X)$.

2.5 Previous Work that We Use

We are going to use condensers recently constructed based on the sum-product theorem. The following construction is due to Zuckerman [Zuc07].

Theorem 2.16 ([BKS+05, Zuc07]). *For any constant $\beta, \delta > 0$, there is an efficient family of rate-$(\delta \to 1-\beta, \epsilon = 2^{-\Omega(n)})$-somewhere condensers $\mathsf{Zuc} : \{0,1\}^n \to (\{0,1\}^m)^D$ where $D = O(1)$ and $m = \Omega(n)$.*

We need the following two source extractor from [Raz05].

Theorem 2.17 ([Raz05]). *For any n_1, n_2, k_1, k_2, m and any $0 < \delta < 1/2$ with*

- $n_1 \geq 6 \log n_1 + 2 \log n_2$
- $k_1 \geq (0.5 + \delta) n_1 + 3 \log n_1 + \log n_2$
- $k_2 \geq 5 \log(n_1 - k_1)$
- $m \leq \delta \min[n_1/8, k_2/40] - 1$

There is a polynomial time computable strong 2-source extractor $\mathsf{Raz} : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ for min-entropy k_1, k_2 with error $2^{-1.5m}$.

We need the following theorem from [Rao06].

Theorem 2.18 ([Rao06]). *For every constant $\gamma < 1$ and integers n, n', t s.t. $t < n^\gamma$ and $t < n'^\gamma$ there exists a constant $\alpha < 1$ and a polynomial time computable function* $\mathsf{2SRExt} : \{0,1\}^{tn} \times \{0,1\}^{tn'} \to \{0,1\}^m$ *s.t. if X is a $(t \times n)$ SR-source and Y is an independent aligned $(t \times n')$ SR-source,*

$$|(\mathsf{2SRExt}(X,Y), Y) - (U_m, Y)| < \epsilon$$

and

$$|(\mathsf{2SRExt}(X,Y), X) - (U_m, X)| < \epsilon,$$

where U_m is independent of X, Y, $m = min[n,n'] - min[n,n']^\alpha$ and $\epsilon = 2^{-min[n,n']^{\Omega(1)}}$.

We use the following lossless condenser constructed in [GUV07].

Theorem 2.19 ([GUV07]). *For all constants $\alpha > 0$, and every $n \in \mathbb{N}$, $k \le n$ and $\epsilon > 0$, there is an explicit $(k \to k + d, \epsilon)$ (lossless) condenser* $\mathsf{Cond} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with $d = (1 + 1/\alpha) \cdot (\log n + \log k + \log(1/\epsilon)) + O(1)$ and $m \le 2d + (1 + \alpha)k$.*

We use the following strong seeded extractor in [GUV07].

Theorem 2.20 ([GUV07]). *For every constant $\alpha > 0$, and all positive integers n, k and $\epsilon > \exp(-n/2^{O(\log^* n)})$, there is an explicit construction of a strong (k, ϵ) extractor* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with $d = O(\log n + \log(1/\epsilon))$ and $m \ge (1 - \alpha)k$.*

We need the following simple lemma about statistical distance.

Lemma 2.21 ([MW97]). *Let X and Y be random variables and let $\mathcal{Y}$ denote the range of Y. Then for all $\epsilon > 0$*

$$\Pr_Y\left[H_\infty(X|Y = y) \ge H_\infty(X) - \log|\mathcal{Y}| - \log\left(\frac{1}{\epsilon}\right)\right] \ge 1 - \epsilon$$

We need the following lemma about conditioning on the seed of a condenser.

Lemma 2.22. *Let* $\mathsf{Cond} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a $(k \to l, \epsilon)$-condenser. For any (n,k)-source X, let R be the uniform distribution over d bits independent of X. With probability $1 - 2\sqrt{\epsilon}$ over the fixings of $R = r$,* $\mathsf{Cond}(X, r)$ *is $\sqrt{\epsilon}$-close to being an $l - 2d$ source.*

Proof. Let $W = \mathsf{Cond}(X, R)$. We know that W is ϵ close to having min-entropy l. Now for a fixed $R = r$, let $S_r = \{w \in \mathsf{Supp}(W) : \Pr[W = w|_{R=r}] > 2^{-l+2d}\}$. Note that if $\Pr[W = w|_{R=r}] > 2^{-l+2d}$ then $\Pr[W = w] \ge \Pr[W = w|_{R=r}] \Pr[R = r] > 2^{-l+d}$. Pick $\epsilon_1 > 0$ and let $\Pr_R[\Pr[W|_{R=r} \in S_r] > \epsilon_1] = \epsilon_2$, then $\Pr_W[\Pr[W = w] > 2^{-l+d}] > \epsilon_1\epsilon_2$. Thus the statistical distance between W and any l-source is at least $(1 - 2^{-d})\epsilon_1\epsilon_2 > \epsilon_1\epsilon_2/2$. Therefore $\epsilon_1\epsilon_2 < 2\epsilon$.

Therefore with probability $1 - 2\sqrt{\epsilon}$ over R, $\epsilon_1 < \sqrt{\epsilon}$. This implies that $W|_{R=r}$ is $\sqrt{\epsilon}$-close to having min-entropy $l - 2d$. □

Our extractor for affine sources use strong linear seeded extractors as ingredients. Specifically, we use the construction of Trevisan [Tre01] and the improvement by Raz et al. [RRV02].

Theorem 2.23 ([Tre01, RRV02]). *For every $n, k \in \mathbb{N}$ with $k < n$ and any $0 < \epsilon < 1$ there is an explicit (k, ϵ)-strong linear seeded extractor* $\mathsf{LExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{\Omega(k)}$ *with $d = O(\log^2(n/\epsilon))$.*

We need to use the following extractor for an affine somewhere random source.

Theorem 2.24 ([Rao09])**.** *For every constant $\gamma < 1$ and integers n, t s.t. $t < n^{\gamma}$ there exists a constant $\alpha < 1$ and a polynomial time computable function* $\mathsf{ASRExt} : \{0,1\}^{tn} \to \{0,1\}^{n-n^{\alpha}}$ *s.t. for every $(t \times n)$ affine-SR-source X,* $\mathsf{ASRExt}(X)$ *is $2^{-n^{\Omega(1)}}$-close to uniform.*

3 The Three Source Extractor

In this section we present our three source extractor. We have the following algorithm.

Algorithm 3.1 ($\mathsf{THExt}(x, y, z)$)**.**

Input: x, y, z — a sample from three independent (n, k)-sources with $k = n^{1/2+\delta}$, for some arbitrary constant $0 < \delta < 1/2$.
Output: w — an m bit string.

Sub-Routines and Parameters:
Let Cond be a $(k_1 \to k_1 + d, \epsilon_1)$ condenser from Theorem 2.19, such that $k_1 = n^{\delta/10}$, $\epsilon_1 = n^{-\delta/10}$ and $\alpha = 10/\delta$ where α is the parameter α in Theorem 2.19.
Let Zuc be a rate-$(0.09\delta \to 0.9, 2^{-\Omega(n)})$-somewhere-condenser form Theorem 2.16.
Let Raz be the strong 2-source extractor from Theorem 2.17.
Let Ext be the strong extractor from Theorem 2.20.
Let $\mathsf{2SRExt}$ be the extractor for two independent aligned SR-source from Theorem 2.18.

1. For every $s \in \{0,1\}^d$ compute $x_s = \mathsf{Cond}(x, s)$. Concatenate $\{x_s\}$ in the binary order of s to form a matrix of 2^d rows. Divide the rows of the matrix sequentially into blocks $x^1, \cdots x^t$ with each block consisting of $\sqrt{n}$ rows. Do the same things to y and z and obtain blocks $y^1, \cdots, y^t$ and $z^1, \cdots, z^t$.

2. (Compute an SR-source from x and y). For $i = 1$ to t do the following.

   - For each row x^i_j in block x^i (there are $\sqrt{n}$ rows), apply Zuc to get a constant number of outputs $\{x^i_{j\ell}\}$.
   - For each $x^i_{j\ell}$ compute $v^i_{j\ell} = \mathsf{Raz}(x^i_{j\ell}, y_i)$ and output $m_2 = \Omega(k_1)$ bits.
   - For each $v^i_{j\ell}$ compute $\mathsf{Ext}(x, v^i_{j\ell})$, output $0.9n^{1/2+\delta}$ bits and concatenate these strings to form a matrix $\bar{x}^i$. Similarly for each $v^i_{j\ell}$ compute $\mathsf{Ext}(y, v^i_{j\ell})$, output $0.9n^{1/2+\delta}$ bits and concatenate these strings to form a matrix $\bar{y}^i$.
   - Compute $r_i = \mathsf{2SRExt}(\bar{x}^i, \bar{y}^i)$ and output $m_3 = 0.8n^{1/2+\delta}$ bits.

3. Concatenate $\{r_i, i = 1, \cdots, t\}$ to form a matrix sr_y.

4. Repeat step 2 and step 3 above for x and z to obtain a matrix sr_z.

5. Output $w = \mathsf{2SRExt}(sr_y, sr_z)$.

3.1 Analysis of the extractor

In this section we analyze the three source extractor. Specifically, we prove the following theorem.

Theorem 3.2. *For any constant $0 < \delta < 1/2$, let X, Y, Z be three independent (n, k) sources with $k = n^{1/2+\delta}$. Then*

$$|\mathsf{THExt}(X, Y, Z) - U_m| < n^{-\Omega(\delta)}$$

with $m = \Omega(k)$.

Proof. Our goal is to show that SR_y and SR_z is (close to) a convex combination of independent aligned SR-sources with few rows. Then we'll be done by Theorem 2.18.

First note that $k > k_1$, thus an (n, k)-source is also an (n, k_1) source. Let S be the uniform distribution over d bits independent of (X, Y, Z). By Theorem 2.19 we have that $X_S = \mathsf{Cond}(X, S)$ is ϵ_1-close to being an $(m_1, k_1 + d)$ source with $m_1 \leq 2d + (1 + \alpha)k_1 < (2 + \alpha)k_1$, since $d = (1 + 1/\alpha) \cdot (\log n + \log k + \log(1/\epsilon)) + O(1) = O(\log n) = O(\log k_1)$.

Now by Lemma 2.22, with probability $1 - 2\sqrt{\epsilon_1}$ over the fixings of $S = s$, X_s is $\sqrt{\epsilon_1}$-close to being an $(m_1, k_1 - d)$ source. We say that a row X_s is good if it is $\sqrt{\epsilon_1}$-close to being an $(m_1, k_1 - d)$ source, and we say that a block X^i is good if it contains at least one good row. It's easy to see that the fraction of "bad" blocks in $\{X^i\}$ is at most $2\sqrt{\epsilon_1}$. Similarly this is also true for the blocks $\{Y^i\}$ and $\{Z^i\}$.

Now since $2\sqrt{\epsilon_1} < 1/3$, by the union bound there exists an i s.t. X^i, Y^i and Z^i are all good blocks. Without loss of generality assume that X^1, Y^1 and Z^1 are all good blocks. We are going to show that the first rows of SR_y and SR_z are close to uniform, thus SR_y and SR_z are aligned somewhere random sources.

We first show this for SR_y. Note that X^1 is a good block and Y^1 is also a good block. Therefore at least one row in X^1 is good. Without loss of generality assume that X^1_1 is a good row. Thus X^1_1 is $\sqrt{\epsilon_1}$-close to being an $(m_1, k_1 - d)$ source. Note that $k_1 - d > 0.99k_1$ since $d = O(\log k_1)$ and $m_1 < (2 + \alpha)k_1$. Thus X^1_1 is close to having min-entropy rate $0.99/(2 + \alpha) = 0.99/(2 + 10/\delta) = 0.99\delta/(10 + 2\delta) > 0.09\delta$ since $\delta < 1/2$.

Therefore by Theorem 2.16, $\mathsf{Zuc}(X^1_1)$ is $\sqrt{\epsilon_1} + 2^{-\Omega(m_1)} = n^{-\Omega(\delta)}$-close to being a somewhere rate 0.9 source with $O(1)$ rows, and the length of each row is $\Omega(m_1) = \Omega(k_1)$.

We now have the following claim.

Claim 3.3. *With probability $1 - n^{-\Omega(\delta)}$ over the fixings of X^1 and Y^1, $\bar{X}^1$ is a deterministic function of X, $\bar{Y}^1$ is a deterministic function of Y, and they are $2^{-n^{\Omega(1)}}$-close to being two aligned $(O(\sqrt{n}) \times 0.9n^{1/2+\delta})$ SR-sources.*

proof of the claim. Note that $\mathsf{Zuc}(X^1_1)$ is $n^{-\Omega(\delta)}$-close to being a somewhere rate 0.9 source with $O(1)$ rows, and each row has length $\Omega(k_1)$. For simplicity, consider the case where $\mathsf{Zuc}(X^1_1)$ is close to an elementary somewhere rate 0.9 source (since $\mathsf{Zuc}(X^1_1)$ is $n^{-\Omega(\delta)}$-close to being a convex combination of such sources, this increases the error by at most $n^{-\Omega(\delta)}$). Without loss of generality assume that the first row X^1_{11} is $n^{-\Omega(\delta)}$-close to having rate 0.9. Since Y^1 is a good block Y^1 is $\sqrt{\epsilon_1}$-close to having min-entropy at least $k_1 - d > 0.99k_1$, and Y^1 has length $m_1\sqrt{n} = \mathrm{poly}(k_1)$. Therefore by Theorem 2.17 we have

$$|(V^1_{11}, X^1_{11}) - (U_{m_2}, X^1_{11})| < n^{-\Omega(\delta)} + 2^{-\Omega(k_1)} = n^{-\Omega(\delta)}$$

and

$$|(V^1_{11}, Y^1) - (U_{m_2}, Y^1)| < n^{-\Omega(\delta)} + 2^{-\Omega(k_1)} = n^{-\Omega(\delta)}.$$

Therefore with probability $1 - n^{-\Omega(\delta)}$ over the fixing of X^1_{11}, V^1_{11} is $n^{-\Omega(\delta)}$-close to uniform. Since X^1_{11} is a deterministic function of X^1, this also implies that with probability $1 - n^{-\Omega(\delta)}$ over the fixing of X^1, V^1_{11} is $n^{-\Omega(\delta)}$-close to uniform. Note that after this fixing, V^1_{11} is a deterministic function of Y^1, and is thus independent of X. Moreover, note that the length of X^1 is $m_1\sqrt{n} = O(k_1\sqrt{n}) = O(n^{1/2+\delta/10})$. Thus by Lemma 2.21, with probability $1 - 2^{-n^{\delta/10}}$ over the fixing of X^1, X has min-entropy at least $n^{1/2+\delta} - O(n^{1/2+\delta/10}) - n^{\delta/10} > 0.99n^{1/2+\delta}$.

Therefore, now by the strong extractor property of Ext from Theorem 2.20, with probability $1 - n^{-\Omega(\delta)}$ over the fixing of V^1_{11}, $\mathsf{Ext}(X, V^1_{11})$ is $2^{-n^{\Omega(1)}}$-close to uniform. Since now V^1_{11} is a deterministic function of Y^1, this also implies that with probability $1 - n^{-\Omega(\delta)}$ over the fixing of Y^1, $\mathsf{Ext}(X, V^1_{11})$ is $2^{-n^{\Omega(1)}}$-close to uniform. Note also that after this fixing $\mathsf{Ext}(X, V^1_{11})$ is a deterministic function of X. Therefore we have shown that with probability $1 - n^{-\Omega(\delta)}$ over the fixing of X^1 and Y^1, $\bar{X}^1$ is a deterministic function of X and is $2^{-n^{\Omega(1)}}$-close to an SR-source.

By symmetry we can also show that with probability $1 - n^{-\Omega(\delta)}$ over the fixing of X^1 and Y^1, $\bar{Y}^1$ is a deterministic function of Y and is $2^{-n^{\Omega(1)}}$-close to an SR-source.

Since both in $\bar{X}^1$ and $\bar{Y}^1$, the first row is close to uniform, they are close to being aligned SR-sources. ■

Now we have the following claim.

Claim 3.4. *With probability $1 - n^{-\Omega(\delta)}$ over the fixing of X, Y^1, Z^1, SR_y and SR_z are two independent aligned somewhere random sources.*

proof of the claim. Note that $\bar{X}^1$ and $\bar{Y}^1$ each has $\sqrt{n}$ rows, and each row has $0.9n^{1/2+\delta}$ bits. Thus by Claim 3.3 and Theorem 2.18, we have

$$|(R_1, \bar{X}^1) - (U_{m_3}, \bar{X}^1)| < n^{-\Omega(\delta)}.$$

This means that with probability $1 - n^{-\Omega(\delta)}$ over the fixing of $\bar{X}^1$, R_1 is $n^{-\Omega(\delta)}$-close to uniform. Since we have fixed X^1 and Y^1 before, now $\bar{X}^1$ is a deterministic function of X. Thus this also implies that with probability $1 - n^{-\Omega(\delta)}$ over the fixing of X, R_1 is $n^{-\Omega(\delta)}$-close to uniform. Moreover, now R_1 (and all the other R_i's) is a deterministic function of Y. Therefore with probability $1 - n^{-\Omega(\delta)}$ over the fixing of X, SR_y is $n^{-\Omega(\delta)}$-close to an SR-source. Moreover, after this fixing SR_y is a deterministic function of Y.

By the same argument, it follows that with probability $1 - n^{-\Omega(\delta)}$ over the fixings of X and Z^1, SR_z is $n^{-\Omega(\delta)}$-close to an SR-source, and SR_z is a deterministic function of Z. Thus SR_y and SR_z are independent.

Since both in SR_y and SR_z, the first row is close to uniform, they are close to being aligned independent SR-sources. ■

Now note that

$$2^d = O((nk_1/\epsilon_1)^{1+1/\alpha}) = O(n^{(1+\delta/5)(1+\delta/10)}) = O(n^{1+\delta/3}).$$

Thus SR_y and SR_z each has $2^d/\sqrt{n} = O(n^{1/2+\delta/3})$ rows, and each row has $0.8n^{1/2+\delta}$ bits. Therefore again by Theorem 2.18 we have

$$|\mathsf{THExt}(X,Y,Z) - U_m| < n^{-\Omega(\delta)} + 2^{-n^{\Omega(1)}} = n^{-\Omega(\delta)},$$

and $m = \Omega(k)$. ■

4 Extractor for Three Sources with Uneven Lengths

In this section we give our extractor for three independent sources with uneven lengths. Our extractor improves that of [RZ08].

First we have the following algorithm.

Algorithm 4.1 ($\mathsf{UExt}(x, y, z)$)**.**

Input: x, y, z — a sample from three independent sources X, Y, Z, where X is an (n_1, k_1) source, Y is an (n_2, k_2) source and Z is an (n_3, k_3) source s.t. $k_2 \leq k_3$ and $n_1 < k_2^{\gamma}$ for some arbitrary constant $0 < \gamma < 1$.
Output: w — an m bit string.

Sub-Routines and Parameters:
Let Cond be a $(k_4 \to k_4 + d, \epsilon_4)$ condenser from Theorem 2.19, with parameters $\alpha = \frac{1+3\gamma}{1-\gamma}$, $k_4 = min[k_1, k_2^{\frac{1-\gamma}{4}}]$ and $\epsilon_4 = 1/100$.
Let Zuc be a rate-$(0.9/(2+\alpha) \to 0.9, 2^{-\Omega(n)})$-somewhere-condenser form Theorem 2.16.
Let Raz be the strong 2-source extractor from Theorem 2.17.
Let Ext be the strong extractor from Theorem 2.20.
Let $\mathsf{2SRExt}$ be the extractor for two independent aligned SR-source from Theorem 2.18.

1. For every $s \in \{0,1\}^d$ compute $x_s = \mathsf{Cond}(x, s)$. Concatenate $\{x_s\}$ to form a matrix of $t = 2^d$ rows.
2. (Compute an SR-source from x and y). For $i = 1$ to t do the following.
    - For each row x_i, apply Zuc to get a constant number of outputs $\{x_{ij}\}$. Each x_{ij} has m_1 bits.
    - For each x_{ij}, take a substring $\bar{x}_{ij}$ with $0.3m_1$ bits. Compute $v_{ij} = \mathsf{Raz}(\bar{x}_{ij}, y)$, $r_{ij} = \mathsf{Ext}(x_{ij}, v_{ij})$ and $h_{ij} = \mathsf{Ext}(y, r_{ij})$.
3. Concatenate $\{h_{ij}\}$ to form a matrix sr_y.
4. Repeat step 2 and step 3 above for x and z to obtain a matrix sr_z.
5. Compute $\bar{w} = \mathsf{2SRExt}(sr_y, sr_z)$.
6. Output $w = \mathsf{Ext}(sr_z, \bar{w})$.

4.1 Analysis of the extractor

First we prove the following theorem.

Theorem 4.2. *For every constant $0 < \gamma < 1$, assume that X is an (n_1, k_1) source, Y is an (n_2, k_2) source and Z is an (n_3, k_3) source such that X, Y, Z are independent, and the following hold:*

- $n_1 < k_2^{\gamma}$ *and* $k_2 \leq k_3$.
- $k_1 > \log^2 n_1$, $k_1 > \log^2 n_2$ *and* $k_1 > \log^2 n_3$.
- $k_2^{\frac{1-\gamma}{4}} > \log^2 n_2$ *and* $k_2^{\frac{1-\gamma}{4}} > \log^2 n_3$.

Then there exists a deficiency 2 subsouce $X' \subseteq X$ such that

$$|(\mathsf{UExt}(X', Y, Z), X') - (U_m, X')| < 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}$$

with $m = \Omega(k_3)$.

Proof. As usual, the goal is to show that SR_y and SR_z is (close to) a convex combination of aligned SR-sources with few rows.

First note that $k_4 \leq k_1$, thus X is also an (n_1, k_4) source. Therefore by Lemma 2.22, with probability $1 - 2\sqrt{\epsilon_4} = 4/5$ over the fixings of $S = s$, $\mathsf{Cond}(X, s)$ is $\sqrt{\epsilon_4} = 1/10$-close to having min-entropy $k_4 - d$. Without loss of generality assume that the first row X_1 is $1/10$-close to having min-entropy $k_4 - d$.

Now note that

$$d = (1 + 1/\alpha) \cdot (\log n_1 + \log k_4 + \log(1/\epsilon_4)) + O(1).$$

Since we take $k_4 = min[k_1, k_2^{\frac{1-\gamma}{4}}]$, we have $d = O(\log n_1)$. Note that $k_1 > \log^2 n_1$ and $n_1 < k_2^{\gamma}$, thus $d = o(k_4)$. Now by Lemma 2.11 there is a deficiency 2 subsource $X' \subseteq X$ such that X'_1 has min-entropy $k_4 - d - 3 > 0.9k_4$ while the length of X'_1 is at most $2d + (1 + \alpha)k_4 < (2 + \alpha)k_4$. Thus X'_1 has min-entropy rate at least $0.9/(2 + \alpha)$. Note that $k_2^{\frac{1-\gamma}{4}} = n_1^{\Omega(1)} = k_1^{\Omega(1)}$. Thus $k_4 = k_1^{\Omega(1)}$. Therefore now by Theorem 2.16, $\mathsf{Zuc}(X'_1)$ is $2^{-k_1^{\Omega(1)}}$-close to a somewhere rate 0.9 source.

For simplicity, consider the case where $\mathsf{Zuc}(X'_1)$ is close to an elementary somewhere rate 0.9 source (since $\mathsf{Zuc}(X'_1)$ is $2^{-k_1^{\Omega(1)}}$-close to being a convex combination of such sources, this increases the error by at most $2^{-k_1^{\Omega(1)}}$).Without loss of generality assume that X'_{11} is $2^{-k_1^{\Omega(1)}}$-close to having min-entropy rate 0.9. Note that $k_1 > \log^2 n_2$ and $k_2^{\frac{1-\gamma}{4}} > \log^2 n_2$. Thus X'_{11} has length $m_1 = \Omega(k_4) = \Omega(\log^2 n_2)$. Since X'_{11} has min-entropy $0.9m_1$, $\bar{X}'_{11}$ has min-entropy at least $0.2m_1$. Therefore $\bar{X}'_{11}$ has entropy rate at least 2/3. Thus by Theorem 2.17, with probability $1 - 2^{-k_1^{\Omega(1)}}$ over the fixings of $\bar{X}'_{11}$, $V_{11} = \mathsf{Raz}(\bar{X}'_{11}, Y)$ is $2^{-k_1^{\Omega(1)}}$-close to uniform and has length $\Omega(m_1)$.

Note that after the fixing of $\bar{X}'_{11}$, V_{11} is a deterministic function of Y and is thus independent of X'_{11}. Moreover by Lemma 2.21 with probability $1 - 2^{-0.1m_1} = 1 - 2^{-k_1^{\Omega(1)}}$ over the fixings of $\bar{X}'_{11}$, X'_{11} has min-entropy at least $0.9m_1 - 0.3m_1 - 0.1m_1 = 0.6m_1$. Thus by Theorem 2.20, with probability $1 - 2^{-k_1^{\Omega(1)}}$ over the further fixings of V_{11}, $R_{11} = \mathsf{Ext}(X'_{11}, V_{11})$ is $2^{-k_1^{\Omega(1)}}$-close to uniform and has length $\Omega(m_1)$. Note that after this fixing, R_{11} is a deterministic function of X'

and is thus independent of Y. Moreover since V_{11} has length at most $m_1 = O(k_1) = O(n_1) = o(k_2)$, by Lemma 2.21 with probability $1 - 2^{m_1} = 1 - 2^{-k_1^{\Omega(1)}}$ over the fixings of V_{11}, Y has min-entropy at least $k_2 - m_1 - m_1 > 0.9k_2$. Therefore again by Theorem 2.20, with probability $1 - 2^{-k_1^{\Omega(1)}}$ over the further fixings of R_{11}, $H_{11} = \mathsf{Ext}(Y, R_{11})$ is $2^{-k_1^{\Omega(1)}}$-close to uniform and has length $\Omega(k_2)$. Since now R_{11} is a deterministic function of X', this also implies that with probability $1 - 2^{-k_1^{\Omega(1)}}$ over the fixings of X', H_{11} is $2^{-k_1^{\Omega(1)}}$-close to uniform. Note that after the fixing of X', SR_y is a deterministic function of Y. Thus we have shown the following claim.

Claim 4.3. *With probability $1-2^{-k_1^{\Omega(1)}}$ over the fixings of X', V_{11}, SR_y is a deterministic function of Y and is $2^{-k_1^{\Omega(1)}}$-close to an SR-source.*

Similarly, we can also show that with probability $1 - 2^{-k_1^{\Omega(1)}}$ over the fixings of X' and some other random variable (which is a deterministic function of Z), SR_z is a deterministic function of Z and is $2^{-k_1^{\Omega(1)}}$-close to an SR-source.

Since both the first rows in SR_y and SR_z are close to uniform (we assumed that X'_{11} is close to having min-entropy rate 0.9), SR_y and SR_z are $2^{-k_1^{\Omega(1)}}$-close to a convex combination of two independent aligned SR-sources.

Now note that

$$2^d = (O(n_1k_4))^{1+1/\alpha} < (O(k_2^{\gamma}k_2^{\frac{1-\gamma}{4}}))^{1+\frac{1-\gamma}{1+3\gamma}} = O(k_2^{\frac{1+\gamma}{2}}).$$

Thus the number of rows in SR_y and SR_z is $O(2^d) = O(k_2^{\frac{1+\gamma}{2}})$. Since $\gamma < 1$, $\frac{1+\gamma}{2} < 1$. Note that each row in SR_y has length $\Omega(k_2)$ and each row in SR_z has length $\Omega(k_3)$ with $k_3 \geq k_2$. Therefore by Theorem 2.18,

$$|(\bar{W}, SR_z) - (U_{m'}, SR_z)| < 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}},$$

where $m' = \Omega(k_2)$. Therefore by Theorem 2.20, $W = \mathsf{Ext}(SR_z, \bar{W})$ is $2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}$-close to uniform with $m = \Omega(k_3)$. Since this is true with probability $1 - 2^{-k_1^{\Omega(1)}}$ over the fixings of X', we have that

$$|(\mathsf{UExt}(X', Y, Z), X') - (U_m, X')| < 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}.$$

■

Now we have the following theorem.

Theorem 4.4. *For every constant $0 < \gamma < 1$, there exists a polynomial time computable function $\mathsf{UExt} : \{0,1\}^{n_1} \times \{0,1\}^{n_1} \times \{0,1\}^{n_3} \to \{0,1\}^m$ such that if X is an (n_1, k_1) source, Y is an (n_2, k_2) source, Z is an (n_3, k_3) source and X, Y, Z are independent, then*

$$|\mathsf{UExt}(X, Y, Z) - U_m| < 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}$$

with $m = \Omega(k_3)$, as long as the following hold:

- *$n_1 < k_2^{\gamma}$ and $k_2 \leq k_3$.*

- $k_1 > 2\log^2 n_1$, $k_1 > 2\log^2 n_2$ *and* $k_1 > 2\log^2 n_3$.
- $k_2^{\frac{1-\gamma}{4}} > \log^2 n_2$ *and* $k_2^{\frac{1-\gamma}{4}} > \log^2 n_3$.

Proof. Let UExt be the algorithm from Algorithm 4.1, set up to work for an $(n_1, k_1/2)$ source, an (n_2, k_2) source and an (n_3, k_3) source. Let $m = \Omega(k_3)$ be the output length and $\epsilon = 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}$ be the error in Theorem 4.2. Now run UExt on X, Y, Z. Define

$$B_X = \{x \in \mathsf{Supp}(X) : |\mathsf{UExt}(x, Y, Z) - U_m| \geq \epsilon\}.$$

We have the following claim:

Claim 4.5. $|B_X| < 2^{k_1/2}$.

The proof of the claim is by contradiction. Assume that $|B_X| \geq 2^{k_1/2}$. Then we define a weak random source $\bar{X}$ to be the uniform distribution on B_X. Thus $\bar{X}$ is an $(n_1, k_1/2)$ source and is indepedent of Y, Z. Note that $k_1/2 > \log^2 n_1$, $k_1/2 > \log^2 n_2$ and $k_1/2 > \log^2 n_3$. Thus by Theorem 4.2 there exists a deficiency 2 subsouce $X' \subseteq \bar{X}$ such that

$$|(\mathsf{UExt}(X', Y, Z), X') - (U_m, X')| < \epsilon.$$

However by the definition of B_X any subsource $X' \subseteq \bar{X}$ must have

$$|(\mathsf{UExt}(X', Y, Z), X') - (U_m, X')| \geq \epsilon,$$

which is a contradiction. Therefore we must have that $|B_X| < 2^{k_1/2}$.

Thus,

$$|(\mathsf{UExt}(X, Y, Z) - U_m| < 2^{k_1/2} \cdot 2^{-k_1} + \epsilon = 2^{-k_1^{\Omega(1)}} + 2^{-k_2^{\Omega(1)}}.$$

■

5 The Affine Two Source Extractors

In this section we give an extractor for two independent affine sources with entropy $k = n^{1/2+\delta}$. We have the following algorithm.

Algorithm 5.1 ($\mathsf{TAExt}(x, y)$).

Input: x, y — a sample from two independent (n, k) affine sources with $k = n^{1/2+\delta}$, for some constant $0 < \delta < 1/2$.
Output: w — an m bit string.

Sub-Routines and Parameters:
Let Cond be a $(k_1 \to k_1 + d_1, \epsilon_1)$ condenser from Theorem 2.19, with parameters $\alpha = 10/\delta$ and $k_1 = n^{\Omega(\delta)} < n^\delta, \epsilon_1 = n^{-\Omega(\delta)}$ to be chosen later. The output has length $m_1 \leq 2d_1 + (1+\alpha)k_1$.
Let Ext be the strong extractor from Theorem 2.20, set up to extract from a $(m_1, k_1 - d_1)$ source using d_2 bits, with error $\epsilon_2 = n^{-\Omega(\delta)}$ to be chosen later.
Let LExt be the strong linear seeded extractor from Theorem 2.23.
Let ASRExt be the extractor for an affine SR-source from Theorem 2.24.

1. Divide x into $\sqrt{n}$ blocks $x^1, \cdots, x^t$ where $t = \sqrt{n}$ and each block has $\sqrt{n}$ bits.

2. (Compute an SR-source from x and y). For $i = 1$ to t do the following.

   - For every $s \in \{0,1\}^{d_1}$, $v \in \{0,1\}^{d_2}$ compute $x^i_s = \mathsf{Cond}(x^i, s)$ and $x^i_{sv} = \mathsf{Ext}(x^i_s, v)$ with output length $n^{\Omega(1)}$. Concatenate $\{x^i_{sv}\}$ to form a matrix of $2^{d_1+d_2}$ rows.
   - For each row x^i_{sv} (there are $2^{d_1+d_2}$ rows), compute $z^i_{sv} = \mathsf{LExt}(x, x^i_{sv})$ and output $m_2 = \Omega(k)$ bits. Concatenate all z^i_{sv} to form a matrix x^i of $2^{d_1+d_2}$ rows.
   - Compute $r_i = \mathsf{ASRExt}(\bar{x}^i)$ and output $\Omega(k)$ bits.
   - Compute $h_i = \mathsf{LExt}(y, r_i)$ and output $m_3 = \Omega(k)$ bits with error $\epsilon_3 = n^{-\Omega(\delta)}$.

3. Concatenate $\{h_i\}$ to form a matrix h_{xy} with $t = \sqrt{n}$ rows.

4. Output $w = \mathsf{ASRExt}(h_{xy})$.

5.1 Analysis of the extractor

In this section we prove the following theorem.

Theorem 5.2. *For any constant $0 < \delta < 1/2$, let X, Y be two independent affine (n, k) sources with $k = n^{1/2+\delta}$. Then*

$$|\mathsf{TAExt}(X, Y) - U_m| < n^{-\Omega(\delta)},$$

and $m = \Omega(k)$.

Proof. Our goal is to show that H_{xy} is (close to) a convex combination of affine SR-sources with few rows. Then we'll be done by Theorem 2.24.

First note that by Lemma 2.15, the sum of the entropies of X^i is at least $k = n^{1/2+\delta}$. Thus at least one block has entropy at least n^δ. Without loss of generality assume that $H(X^1) \geq n^\delta$.

Note that we choose $k_1 < n^\delta$. Thus an affine source with entropy n^δ is also a source with min-entropy k_1. Now by Lemma 2.22, with probability $1 - 2\sqrt{\epsilon_1}$ over S, X^1_S is $\sqrt{\epsilon_1}$-close to being an

(m_1, k_1-d_1) source. Therefore there exists an i such that X_i^1 is $\sqrt{\epsilon_1}$-close to being an (m_1, k_1-d_1) source. Without loss of generality assume X_1^1 is $\sqrt{\epsilon_1}$-close to being an (m_1, k_1-d_1) source. Now by the strong extractor property of Ext (Theorem 2.20), there exists a j such that X_{1j}^1 is $\sqrt{\epsilon_1}+\sqrt{\epsilon_2}$-close to uniform. Without loss of generality assume that X_{11}^1 is $\sqrt{\epsilon_1}+\sqrt{\epsilon_2}$-close to uniform.

Now we count the number of elements in $\{X_{sv}^i\}$. This number is equal to $2^{d_1+d_2}$. Note that

$$d_1 = (1+1/\alpha)\cdot(\log(\sqrt{n})+\log k_1+\log(1/\epsilon_1))+O(1)$$

and

$$d_2 = O(\log m_1+\log(1/\epsilon_2)),$$

where $m_1 \le 2d_1+(1+\alpha)k_1$.

Since we choose $k_1 = n^{\Omega(\delta)}$ and $\epsilon_1, \epsilon_2 = n^{-\Omega(\delta)}$, we have $d_1 = O(\log n) = O(\log k_1)$. Thus $m_1 \le (2+\alpha)k_1$ and $k_1 - d_1 > 0.99k_1$.

Therefore

$$d_1+d_2 = (1+1/\alpha)(\log(\sqrt{n}))+(1/\alpha+O(1))\log k_1+(1+1/\alpha)\log(1/\epsilon_1)+O(\log(1/\epsilon_2))+O(1).$$

Since $\alpha = 10/\delta$, we can choose $k_1 = n^{\Omega(\delta)}$ and $\epsilon_1, \epsilon_2 = n^{-\Omega(\delta)}$ such that

$$d_1+d_2 \le (1/2+\delta/2)\log n.$$

Thus $2^{d_1+d_2} \le n^{1/2+\delta/2}$ and each X_{sv}^i outputs $\Omega(k_1) = n^{\Omega(\delta)}$ bits by Theorem 2.20.

Now we know that X_{11}^1 is $n^{-\Omega(\delta)}$-close to uniform. We have the following claim.

Claim 5.3. *With probability $1-n^{-\Omega(\delta)}$ over the fixing of $X^1 = x^1$, $Z_{11}^1 = \mathsf{LExt}(X, x_{11}^1)$ is uniform.*

proof of the claim. At first it seems that X and X_{11}^1 are correlated, so it is not clear that LExt can work. However in our case we are going to use the fact that X is an affine source and LExt is a strong linear seeded extractor.

Specifically, note that X_{11}^1 is a deterministic function of X^1, which is in turn a linear function of X. Let L stand for this linear function, i.e. $L(x) = x^1$. By Lemma 2.14, there exist independent affine sources A and B such that $X = A+B$ and for every $b \in \mathsf{Supp}(B)$, $L(b) = 0$. Thus $X^1 = L(X) = L(A+B) = L(A)$. Therefore by Lemma 2.14 $H(A) = H(X^1) \le \sqrt{n}$. Thus the entropy of B is

$$H(B) = H(X)-H(A) \ge n^{1/2+\delta}-n^{1/2} > 0.9n^{1/2+\delta} = 0.9k.$$

Note that X_{11}^1 is a deterministic function of X^1, thus it is also a deterministic function of A, and is therefore independent of B. Since X_{11}^1 has $n^{\Omega(\delta)}$ bits and $\epsilon_2 = n^{-\Omega(\delta)}$, by Theorem 2.23 and Proposition 2.13 we have

$$\Pr_{u \leftarrow_R X_{11}^1}[|\mathsf{LExt}(B,u)-U_{m_2}| = 0] \ge 1-\epsilon_2-n^{-\Omega(\delta)} = 1-n^{-\Omega(\delta)}.$$

Since X_{11}^1 is a deterministic function of A, this also implies that

$$\Pr_{a \leftarrow_R A, u = x_{11}^1(a)}[|\mathsf{LExt}(B,u)-U_{m_2}| = 0] \ge 1-n^{-\Omega(\delta)}.$$

Now note that conditioned on a fixed $A = a$, u is also fixed, and

$$\mathsf{LExt}(X, u) = \mathsf{LExt}(a + B, u) = \mathsf{LExt}(a, u) + \mathsf{LExt}(B, u)$$

since LExt is a linear seeded extractor. Thus if for a fixed $A = a$ and $u = x^1_{11}(a)$, $\mathsf{LExt}(B, u) = U_{m_2}$, then $\mathsf{LExt}(X, u)$ is also uniform.

Therefore

$$\Pr_{a \leftarrow_R A, u = x^1_{11}(a)}[|\mathsf{LExt}(X, u) - U_{m_2}| = 0] \geq 1 - n^{-\Omega(\delta)}.$$

Note that by Lemma 2.14 there exists an affine function L^{-1} such that $A = L^{-1}(L(A)) = L^{-1}(X^1)$. Thus A is also a deterministic function of X^1 (in fact, there is a bijection between X^1 and A). Therefore this also implies that

$$\Pr_{x \leftarrow_R X^1, u = x^1_{11}(x)}[|\mathsf{LExt}(X, u) - U_{m_2}| = 0] \geq 1 - n^{-\Omega(\delta)}.$$

$\blacksquare$

Therefore, with probability $1 - n^{-\Omega(\delta)}$ over the fixing of $X^1 = x^1$, $\bar{X}^1$ is an SR-source. Moreover, since X^1 is a linear function of X, conditioned on $X^1 = x^1$, X is still an affine source. Next note that conditioned on $X^1 = x^1$, $\mathsf{LExt}(X, x^1_{sv})$ is a linear function of X. Thus conditioned on $X^1 = x^1$, $\bar{X}^1$ is an affine source. Therefore with probability $1 - n^{-\Omega(\delta)}$ over the fixing of $X^1 = x^1$, $\bar{X}^1$ is an affine SR-source. Note that the number of rows is $2^{d_1 + d_2} \leq n^{1/2 + \delta/2}$ and each row has length $m_2 = \Omega(k) = \Omega(n^{1/2+\delta})$, by Theorem 2.24 we have that R_1 is $n^{-\Omega(\delta)}$ close to uniform.

Note R_1 has $\Omega(k)$ bits and R_1 is a deterministic function of X and is independent of Y, thus again by Theorem 2.23 and Proposition 2.13 we have

$$\Pr_{r \leftarrow_R R_1}[|\mathsf{LExt}(Y, r) - U_{m_3}| = 0] \geq 1 - \epsilon_3 - n^{-\Omega(\delta)} = 1 - n^{-\Omega(\delta)}.$$

Since R_1 is a deterministic function of X this also implies that

$$\Pr_{x \leftarrow_R X, r = r_1(x)}[|\mathsf{LExt}(Y, r) - U_{m_3}| = 0] \geq 1 - n^{-\Omega(\delta)}.$$

Note that conditioned on $X = x$, H_{xy} is a linear function of Y, thus it is an affine source. Therefore with probability $1 - n^{-\Omega(\delta)}$ over the fixing of $X = x$, H_{xy} is an affine SR-source. Note that it has $n^{1/2}$ rows and each row has length $m_3 = \Omega(k) = \Omega(n^{1/2+\delta})$. Therefore by Theorem 2.24,

$$|\mathsf{TAExt}(X, Y) - U_m| < n^{-\Omega(\delta)} + 2^{-n^{\Omega(1)}} = n^{-\Omega(\delta)},$$

and $m = \Omega(k)$. $\blacksquare$

Remark 5.4. Note that to compute H_{xy} we apply a strong linear seeded extractor to Y and each R_i, and R_i is a deterministic of X. Thus we can use the same argument before (the property of strong linear seeded extractors and the structure of affine sources) to show that our construction works even if (X, Y) is an affine block source, instead of independent sources.

6 Conclusions and Open Problems

In this paper we study the problem of constructing extractors for independent weak random sources and affine sources. In the case of independent sources, we give an extractor for three independent (n, k) sources with $k = n^{1/2+\delta}$ for any constant $0 < \delta < 1/2$. This improves the previous best result of [Rao06], where the min-entropy is required to be at least $n^{0.9}$. We also give extractors for three independent sources with uneven lengths, where two of them can have any polynomially small min-entropy, or even polylogarithmic min-entropy, while the length of the third source is significantly smaller than the min-entropy of the other two. This improves the result of [RZ08].

In the case of affine extractors, we give an extractor for two independent affine (n, k) sources with $k = n^{1/2+\delta}$ for any constant $0 < \delta < 1/2$. In fact, our extractor works even if it is an affine block source, with the first block being an (n, k) affine source, and the second block being an (n, k) affine source conditioned on the fixing of the first one. We hope that this result can help us understand the nature of affine sources and build better deterministic extractors for affine sources.

The obvious open problem here is to build extractors for sources with smaller min-entropy. For example, it would be very interesting if we can construct extractors for three independent sources with any polynomially small min-entropy. In the case of affine sources, an extractor for two independent affine sources with any polynomially small entropy would also be interesting.

Another open problem is to reduce the error in our three source extractor and affine two source extractor. We only achieve an error of $1/\mathrm{poly}(n)$ in both of these cases, and it would be interesting to find a way to decrease the error to be exponentially small.

Acknowledgements

We thank David Zuckerman for useful discussions.

References

[BIW04] Boaz Barak, R. Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. In *Proc. of 45th FOCS*, pages 384–393, 2004.

[BKS+05] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 1–10, 2005.

[BRSW06] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson. 2 source dispersers for $n^{o(1)}$ entropy and Ramsey graphs beating the Frankl-Wilson construction. In *Proc. of 38th STOC*, 2006.

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

[Bou07] Jean Bourgain. On the construction of affine-source extractors. *Geometric and Functional Analysis*, 1:33–57, 2007.

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

[DW08] Zeev Dvir and Avi Wigderson. Kakeya sets, new mergers and old extractors. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, 2008.

[FS02] Lance Fortnow and Ronen Shaltiel. Recent developments in explicit constructions of extractors, 2002.

[GR05] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. In *Proc. of 46th FOCS*, 2005.

[GRS04] Ariel Gabizon, Ran Raz, and Ronen Shaltiel. Deterministic extractors for bit-fixing sources by obtaining an independent seed. In *Proc. of 45th FOCS*, 2004.

[GUV07] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from parvaresh-vardy codes. In *Proceedings of the 22nd Annual IEEE Conference on Computational Complexity*, 2007.

[KRVZ06] Jesse Kamp, Anup Rao, Salil Vadhan, and David Zuckerman. Deterministic extractors for small space sources. In *Proc. of 38th STOC*, 2006.

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

[Li10] Xin Li. A new approach to affine extractors and dispersers. Technical Report TR10-064, ECCC: Electronic Colloquium on Computational Complexity, 2010.

[LRVW03] C. J. Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: Optimal up to constant factors. In *Proc. of 35th STOC*, pages 602–611, 2003.

[MW97] Ueli M. Maurer and Stefan Wolf. Privacy amplification secure against active adversaries. In *Advances in Cryptology — CRYPTO '97, 17th Annual International Cryptology Conference, Proceedings*, 1997.

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

[Rao06] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. In *Proc. of 38th STOC*, 2006.

[Rao09] Anup Rao. Extractors for low-weight affine sources. In *Proceedings of the 24nd Annual IEEE Conference on Computational Complexity*, 2009.

[RZ08] Anup Rao and David Zuckerman. Extractors for 3 uneven length sources. In *Random 2008*, 2008.

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

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

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

[TV00] Luca Trevisan and Salil Vadhan. Extracting randomness from samplable distributions. In *Proc. of 41st FOCS*, pages 32–42, 2000.

[Yeh10] Amir Yehudayoff. Affine extractors over prime fields. *Manuscript*, 2010.

[Zuc07] David Zuckerman. Linear degree extractors and the inapproximability of max clique and chromatic number. In *Theory of Computing*, pages 103–128, 2007.