Electronic Colloquium on Computational Complexity, Report No. 121 (2015)

Extractors for Affine Sources with Polylogarithmic Entropy

Xin Li
Department of Computer Science
Johns Hopkins University
Baltimore, MD 21218, U.S.A.
lixints@cs.jhu.edu

July 25, 2015

Abstract

We give the first explicit construction of deterministic extractors for affine sources over $\mathbb{F}_2$, with entropy $k \geq \log^C n$ for some large enough constant C, where n is the length of the source. Previously the best known results are by Bourgain [Bou07], Yehudayoff [Yeh11] and Li [Li11b], which require the affine source to have entropy at least $\Omega(n/\sqrt{\log \log n})$. Our extractor outputs one bit with error $n^{-\Omega(1)}$.

Our construction is obtained by reducing an affine source to a non-oblivious bit-fixing source, and then applying a deterministic extractor for such sources in the recent breakthrough result of two-source extractors by Chattopadhyay and Zuckerman [CZ15]. To reduce an affine source to a non-oblivious bit-fixing source, we adapt the alternating extraction based approach in previous work on independent source extractors [Li13a] to the affine setting.

ISSN 1433-8092

1 Introduction

Randomness extraction is a broad area that studies the problem of converting biased random sources into nearly uniform random bits. The natural motivation comes from the wide application of randomness in computation, such as in algorithms, distributed computing and cryptography, and the requirement that the random bits used should be uniformly distributed. In reality, however, natural random sources almost always have serious bias, and these random sources are known as weak random sources. Therefore, intuitively, a randomness extractor takes as input one or more weak random sources, and outputs a distribution that is statistically close to uniform.

Formally, a weak random source is modeled as a probability distribution over n bit strings with some entropy k. In the context of randomness extraction, the standard measure of entropy is the so called *min-entropy*, which is defined as follows.

Definition 1.1. The *min-entropy* of a random variable X is

$$H_\infty(X) = \min_{x \in \mathsf{supp}(X)} \log_2(1/\Pr[X = x]).$$

For $X \in \{0,1\}^n$, we call X an $(n, H_\infty(X))$-source, and we say X has *entropy rate* $H_\infty(X)/n$.

However, one can easily show that it is impossible to construct deterministic randomness extractors for one (n,k) source, even if k is as large as $n-1$. Thus, the study of randomness extractors has been pursued in two different directions. The first one is to allow the extractor itself to be randomized. In this case one ends up with the notion of *seeded extractors* [NZ96], where the extractor is given a short uniform random seed (typically of length say $O(\log n)$). It is now possible to construct such extractors for all possible weak random sources. Seeded extractors have a lot of applications in theoretical computer science and have been studied extensively, resulting in almost optimal constructions [LRVW03, GUV09, DKSS09].

Another direction is to impose some special structure on the weak source, and thereby allows the construction of deterministic randomness extractors. For example, there has been a long line of research focusing on constructing extractors for independent weak random sources [CG88, BIW04, Raz05, Bou05, Rao06, BRSW06, Li11a, Li13b, Li13a, Li15, Coh15, CZ15]. In this paper, we focus on another well studied model, where the weak random source is called an *affine source* and is the uniform distribution over some unknown affine subspace.

Definition 1.2. (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

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

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 1.3. (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 $q = 2$. 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 $m < k - O(1)$. The problem is to given an explicit construction of such a function.

A weaker version of the extractor, called an affine disperser, only requires the output to have a large support size.

Definition 1.4. (affine disperser) A function $\mathsf{ADisp} : \mathbb{F}_q^n \to \{0,1\}^m$ is a deterministic (k,ϵ)-affine disperser if for every $(n,k)_q$ affine source X,

$$|\mathsf{Supp}(\mathsf{ADisp}(X))| \geq (1-\epsilon)2^m.$$

The function is called a zero-error disperser if $\epsilon = 0$.

There has been a lot of work studying affine extractors and dispersers. For example, Gabizon and Raz [GR05] constructed explicit extractors for affine sources even with entropy 1. However, their constructions require the field size to be much larger than n, i.e., $q > n^{\Omega(1)}$, in order to use Weil's theorem. DeVos and Gabizon [DG10] constructed explicit extractors for $(n,k)_q$ affine sources when $q = \Omega((n/k)^2)$ and the characteristic of the field $\mathbb{F}_q$ is $\Omega(n/k)$. As the field size gets smaller, constructing explicit affine extractors becomes significantly harder.

The extreme and hardest case where the field is $\mathbb{F} = \mathrm{GF}(2)$, is the focus of the rest of the paper. Note that in this case the min-entropy $H_{\infty(X)}$ is the same as the standard Shannon entropy $H(X)$. Here, it is well known how to construct extractors for affine sources with entropy rate greater than $1/2$. However the problem becomes much harder as the entropy rate drops to $1/2$ and below $1/2$. Bourgain [Bou07] used sophisticated character sum estimates to give an extractor for affine sources with entropy $k = \delta n$ for any constant $\delta > 0$. This was later slightly improved to $k = \Omega(n/\sqrt{\log\log n})$ by Yehudayoff [Yeh11] and the author [Li11b], which is the state of the art. Rao [Rao09] constructed extractors for affine sources with entropy as small as $\mathrm{polylog}(n)$, as long as the subspace of X has a basis of low-weight vectors.

In the case of constructing dispersers for affine sources over $\mathrm{GF}(2)$, Ben-Sasson and Kopparty [BSK09] constructed dispersers for affine sources with entropy $\Omega(n^{4/5})$. Shaltiel [Sha11] gave a construction that works for entropy $2^{\log^{0.9} n}$, which remains the best known result.

1.1 Our Result

In this paper we give an affine extractor over $\mathbb{F}_2$ that works for entropy $k \geq \mathrm{polylog}(n)$, thus improving all previous results in terms of the entropy requirement. Our extractor outputs one bit and has error $n^{-\Omega(1)}$. Specifically, we have

Theorem 1.5. *There exists a constant $C > 1$ and an efficiently computable function $\mathsf{AExt} : \{0,1\}^n \to \{0,1\}$ such that for any (n,k) affine source X with $k \geq \log^C n$, we have that*

$$|\mathsf{AExt}(X) - U_1| \leq \epsilon,$$

where $\epsilon = n^{-\Omega(1)}$.

1.2 Overview of the construction

Our construction is actually quite intuitive, although the analysis is non-trivial. On the high level, our construction follows the recent breakthrough result of the two-source extractor construction by Chattopadhyay and Zuckerman [CZ15]. Specifically, we will first reduce an affine source to a (q, t, γ)-non-oblivious bit-fixing source as defined in [CZ15]. Intuitively, this means that the new source has q "bad" bits which can depend arbitrarily on the other bits. However, if we consider the rest "good" bits, then any t such bits are γ-close to uniform. At the heart of [CZ15] is an explicit deterministic extractor for such sources (with appropriate parameters q, t, γ), which is a derandomized monotone version of the Ajtai-Linial resilient function (the function itself is in AC0, and thus fooled by polylog-wise independence). Thus, once we reduce an affine source to such a non-oblivious bit-fixing source, we can apply this deterministic extractor and output one bit that is $n^{-\Omega(1)}$-close to uniform.

We now describe how to reduce an affine extractor to a non-oblivious bit-fixing source. We will mainly adapt techniques from previous work on extractors for independent sources. Specifically, by using ideas from alternating extraction (Figure 1), one of the author's previous work [Li15] obtained a somewhere random source with $N = \text{poly}(n)$ rows from two independent (n, k) sources with $k \geq \text{polylog}(n)$. The somewhere random source has the property that except for a small fraction of "bad" rows, the rest of the rows are almost t-wise independent for $t = k^{\Omega(1)}$ in the sense that any t of these rows are $\gamma = 2^{-k^{\Omega(1)}}$-close to uniform. Thus, these rows (or, say, taking one bit each row) form exactly a (q, t, γ)-non-oblivious bit-fixing source.

Now we need to adapt that construction to affine sources. Of course we now only have one affine source and not two independent sources. However, due to the special structure of affine sources we can still apply similar ideas as in [Li13a, Li15]. Specifically, we will use a special kind of strong seeded extractors called *linear seeded extractors*. These extractors have the property that for any fixed seed, the output is a linear function of the source. We take such a seeded extractor with seed length $O(\log n)$ and error ϵ, and use every possible seed to extract from the affine source X. This gives us a matrix (or somewhere random source) of $N = \text{poly}(n)$ rows, where each row corresponds to the output of the extractor on a particular seed. A standard argument shows that if X is affine, then at least $1 - 2\epsilon$ fraction of the rows are truly uniform, although they may depend on each other in arbitrary ways. We further restrict the size of each row, so that the length is much smaller than the entropy of X.

We can now use these rows and the source X itself to do the same alternating extraction protocol as in [Li13a, Li15] to make the "good" rows almost t-wise independent for $t = k^{\Omega(1)}$, with error $\gamma = 2^{-k^{\Omega(1)}}$. To see why alternating extraction works in this case, consider one particular uniform row Y. Note that Y is a linear function of X, so Y is also an affine source. Recall that the length of Y is much smaller than the entropy of X. A standard argument shows that X can be decomposed into $X = A + B$ where both A, B are affine sources, $A = L(Y)$ for some linear bijection L, and B is independent of Y. Thus, to do the alternating extraction, we can first take a small slice of Y to be S_1, and use a linear seeded extractor Ext to compute $R_1 = \mathsf{Ext}(X, S_1)$. Note that $R_1 = \mathsf{Ext}(X, S_1) = \mathsf{Ext}(A, S_1) + \mathsf{Ext}(B, S_1)$. By the property of a strong extractor we know that with high probability over the fixing of S_1, $\mathsf{Ext}(B, S_1)$ is close to uniform (since S_1 is independent of B). Note that S_1 is a deterministic function of A and A is independent of B, thus $R_1 = \mathsf{Ext}(A, S_1) + \mathsf{Ext}(B, S_1)$ is also uniform conditioned on the fixing of S_1.

Next, suppose the length of R_1 is much smaller than the length of Y ,we can then use R_1 and apply Ext back to Y to extract $S_2 = \mathsf{Ext}(Y, R_1)$. The reason is that we can first fix $\mathsf{Ext}(A, S_1)$.

Note that we have already fixed S_1 so this is a deterministic function of A (or Y). Therefore after fixing it, $\mathsf{Ext}(B, S_1)$ is still uniform and independent of Y, and now $R_1 = \mathsf{Ext}(A, S_1) + \mathsf{Ext}(B, S_1)$ is independent of Y. Since the length of R_1 is small, conditioned on this fixing Y still has a lot of entropy left. Therefore we can now extract $S_2 = \mathsf{Ext}(Y, R_1)$. Continue doing this, we can see that alternating extraction works as long as we always use a strong linear seeded extractor. Intuitively, it's like alternating extraction between the two independent affine sources Y and B. Now we can use similar arguments as in [Li13a] to convert the somewhere random source into almost t-wise independent.[1]

However, there are a few subtle technical problems we need to deal with. First, when we generalize the above alternating extraction to run for t rows $Y^1, Y^2, \cdots, Y^t$ simultaneously, we will need to consider the concatenation $Y = Y^1 \circ Y^2 \circ \cdots \circ Y^t$ and decompose X into $X = A + B = L(Y) + B$. This ensures that we can condition on the fixing of all the intermediate random variables obtained from $Y^1, Y^2, \cdots, Y^t$ without affecting B. Another subtlety arises in the analysis as follows. The alternating extraction will take some $b < \log n$ rounds, with each round consisting of some $k^{\Omega(1)}$ steps. At the end of round j, for each Y^i we need to use the R^{ij} variable extracted from X to extract another $Y^{i(j+1)}$ from Y^i to start the next round of alternating extraction. Here we would like to argue that for those $\{R^{\ell j}\}$ that have already become independent of R^{ij}, we can first fix all $\{Y^{\ell(j+1)}\}$ and all the R variables produced in round $j+1$, and $Y^{i(j+1)}$ is still uniform. This ensures that whatever is already independent will remain independent. While this is true in the case of two independent sources, it is no longer true in the case of an affine source. The reason is again, as explained above, when we fix $R = \mathsf{Ext}(A, S) + \mathsf{Ext}(B, S)$, the part of $\mathsf{Ext}(A, S)$ is a function of A (and Y). Thus this fixing may cause $Y^{i(j+1)}$ to lose entropy (note that fixing $\mathsf{Ext}(B, S)$ will not since B is independent of Y). Fortunately, we can get around this by restricting the length of the R variables to be much smaller than the length of $Y^{i(j+1)}$. We note that if we take a seeded extractor with error ϵ, and use a seed that loses ℓ bits of entropy, then the extractor still works with error increased to $2^{\ell}\epsilon$. Thus by appropriately choosing the parameters (making ℓ small enough) we can ensure that the new round of alternating extraction still goes through.

One final point is that the extractor for non-oblivious bit-fixing source in [CZ15] can only handle the case where $q = N^{1-\delta}$ for any constant $\delta > 0$. This means that to convert the affine source X into a somewhere random source in the first step, we need to take a strong linear seeded extractor with seed length $O(\log n)$ and error $\epsilon = 1/\mathrm{poly}(n)$, i.e., an extractor with optimal seed length. We construct such a strong linear seeded extractor by combining the lossless condenser in [GUV09] and another strong linear seeded extractor in [SU05]. We note that the condenser in [GUV09] itself may not be linear, but can be made linear with the same parameters by a careful instantiation, following a result in [CI15]. Thus in this step we can use $O(\log n)$ bits to condense the source into a $(n' = O(k), k)$ source with error $1/\mathrm{poly}(n)$. We then use the linear seeded extractor in [SU05], which has seed length $d = O\left(\log n' + \frac{\log n'}{\log k} \log\left(\frac{1}{\epsilon}\right)\right)$. Note that $n' = O(k)$. Thus if we take $\epsilon = 1/\mathrm{poly}(n)$ we get $d = O(\log n)$. Altogether we get a strong seeded extractor with seed length $O(\log n)$ and error $\epsilon = 1/\mathrm{poly}(n)$. Since both the condenser and the extractor are linear, the combined extractor is also linear.

[1] We remark that we can also use the flip-flop alternating extraction developed in [Coh15], which may result in an improvement in the constants. However in this paper we do not try to optimize the constant C in our final result where $k \geq \log^C n$.

Organization. The rest of the paper is organized as follows. We give some preliminaries in Section 2. In Section 3 we define alternating extraction, an important ingredient in our construction. We present our main construction of affine extractors in Section 4. Finally we conclude with some open problems in Section 5.

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

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

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

2.2 Somewhere Random Sources, Mergers and Condensers

Definition 2.2 (Somewhere Random sources)**.** A source $X = (X_1, \cdots, X_t)$ is (r, t) *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 2.3. 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 2.4. 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.

2.3 Strong Linear Seeded Extractors

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

Definition 2.5. A function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k, ϵ) *strong seeded extractor* if for every min-entropy k source X,

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

where U_m is the uniform distribution on m bits and R is the uniform distribution on d bits independent of X. 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 $u \in \{0,1\}^d$.

We have the following simple fact.

Lemma 2.6. *If* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a* (k, ϵ) *strong seeded extractor, then for every* (n, k) *source* X *and every independent* (d, k') *source* R*,*

$$|\mathsf{Ext}(X, R) - (U_m, R)| \leq 2^{d-k'}\epsilon.$$

Proof. Without loss of generality we can assume that R is the uniform distribution over some subset S of size $2^{k'}$. Then for any $r \in S$, we have $\Pr[R = r] = 2^{-k'}$. Thus

$$\begin{aligned}
|\mathsf{Ext}(X, R) - (U_m, R)| &= \sum_{r \in S} 2^{-k'} |\mathsf{Ext}(X, r) - U_m| = \sum_{r \in S} 2^{d-k'} \cdot 2^{-d} |\mathsf{Ext}(X, r) - U_m| \\
&\leq \sum_{r \in \{0,1\}^d} 2^{d-k'} |2^{-d}\mathsf{Ext}(X, r) - 2^{-d}U_m| = 2^{d-k'} |\mathsf{Ext}(X, R) - (U_m, R)|_{R \leftarrow U_d} \\
&\leq 2^{d-k'}\epsilon.
\end{aligned}$$

□

Lemma 2.7 ([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,*

$$\Pr_{u \leftarrow_R U_d}[|\mathsf{Ext}(X, u) - U_m| = 0] \geq 1 - 2\epsilon$$

2.4 The Structure of Affine Sources

The following lemma is proved in [Li11b].

Lemma 2.8. *(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* $A = L^{-1}(L(A))$.

2.5 Non-oblivious bit-fixing source

Definition 2.9. A distribution D on n bits is t-wise independent if the restriction of D to any t bits is uniform. Further D is a (t, ϵ)-wise independent distribution if the distribution obtained by restricting D to any t coordinates is ϵ-close to uniform.

Definition 2.10. A source X on $\{0,1\}^n$ is called a (q, t)-non-oblivious bit-fixing source if there exists a subset of coordinates $Q \subseteq [n]$ of size at most q such that the joint distribution of the bits indexed by $\overline{Q} = [n] \setminus Q$ is t-wise independent. The bits in the coordinates indexed by Q are allowed to arbitrarily depend on the bits in the coordinates indexed by $\overline{Q}$.

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

2.6 Previous Work that We Use

We are going to use two constructions of linear seeded extractors in this paper. The first one is for the purpose of obtaining small error. For this we use Trevisan's extractor:

Theorem 2.11 ([Tre01, RRV02]). *For every $n, k, m \in \mathbb{N}$ and $\epsilon > 0$ such that $m \leq k \leq n$, there is an explicit (k, ϵ) strong seeded extractor $\mathsf{TrExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d = O\left(\frac{\log^2(n/\epsilon)}{\log(k/m)}\right)$.*

This extractor is actually a linear seeded extractor. By setting the parameters appropriately, we get the following corollary.

Corollary 2.12 ([Tre01, RRV02]). *For every $n, k \in \mathbb{N}$ and $\epsilon > 0$ such that $k \leq n$, there is an explicit (k, ϵ) strong linear seeded extractor $\mathsf{TrExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{\Omega(k)}$ with $d = O(\log^2(n/\epsilon))$.*

The next one is for the purpose of obtaining a short seed (i.e., $O(\log n)$). For this we need the following extractor.

Theorem 2.13 ([SU05]). *For every $n \in \mathbb{N}$, constant $\delta > 0$, $\epsilon \geq 2^{-k^{\delta/4}}$, and $k \geq \log^{4/\delta} n$ there is an explicit (k, ϵ) strong linear seeded extractor $\mathsf{SUExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d = O\left(\log n + \frac{\log n}{\log k} \log\left(\frac{1}{\epsilon}\right)\right)$ and $m = k^{1-\delta}$.*

We also note that the lossless condenser in [GUV09] can be made linear.

Theorem 2.14 ([CI15]). *For any constant $\alpha > 0$ and any $n \in \mathbb{N}, k \leq n, \epsilon > 0$ there is an explicit strong (k, ϵ)-lossless condenser $\mathsf{Cond} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d \leq (1 + 1/\alpha)(\log(nk/\epsilon) + O(1))$ and $m \leq (1 + \alpha)k$. Moreover, Cond is a linear function for every fixed choice of the seed.*

We now have the following theorem.

Theorem 2.15. *There exists a constant $c > 1$ such that for every $n, k \in \mathbb{N}$ with $c \log^8 n \leq k \leq n$, and $\epsilon \geq n^{-2}$, there is an explicit (k, ϵ) strong linear seeded extractor $\mathsf{LExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d = O(\log n)$ and $m = \sqrt{k}$.*

Proof. Given any (n, k) source X, we first take $O(\log n)$ bits and use Theorem 2.14 to condense X into an (n', k) source Y with length $n' = O(k)$, and error $\epsilon/2$. We then use Theorem 2.13 to extract $m = \sqrt{k}$ bits from Y with error $\epsilon/2$ (i.e., take $\delta = 1/2$ in Theorem 2.13). One can check that the conditions of that theorem are satisfied. This will use another $O\left(\log n' + \frac{\log n'}{\log k} \log\left(\frac{2}{\epsilon}\right)\right) = O(\log n)$ bits. Since both the condenser and the extractor are linear and strong, the composed extractor is also a strong linear seeded extractor. □

A key ingredient in our affine extractor is the following extractor for non-oblivious bit-fixing source developed recently by Chattopadhyay and Zuckerman [CZ15].

Theorem 2.16 ([CZ15]). *There exists a constant c such that for any constant $\delta > 0$, and for all $n \in \mathbb{N}$, there exists an explicit extractor $\mathsf{bitExt} : \{0,1\}^n \to \{0,1\}$ for the class of (q, t, γ)-non-oblivious bit-fixing sources with error $n^{-\Omega(1)}$, where $q \leq n^{1-\delta}$, $t \geq c \log^{18}(n)$ and $\gamma \leq 1/n^{t+1}$.*

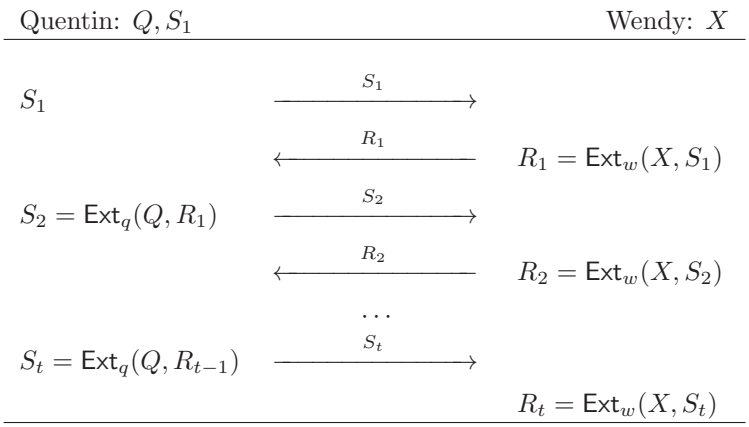

Figure 1: Alternating Extraction.

3 Alternating Extraction

An important ingredient in our construction is the following alternating extraction protocol, which has been used a lot in recent constructions of independent source extractors [Li13b, Li13a]. Here we will use it in the context of affine sources.

Alternating Extraction. Assume that we have two parties, Quentin and Wendy. Quentin has a source Q, Wendy has a source X. Also assume that Quentin has a uniform random seed S_1 (which may be correlated with Q). Let Ext_q and Ext_w be the strong linear seeded extractors in Corollary 2.12. Let ℓ be an integer parameter for the protocol. For some integer parameter $t > 0$, the *alternating extraction protocol* is an interactive process between Quentin and Wendy that runs in t steps.

In the first step, Quentin sends S_1 to Wendy, Wendy computes $R_1 = \mathsf{Ext}_w(X, S_1)$. She sends R_1 to Quentin and Quentin computes $S_2 = \mathsf{Ext}_q(Q, R_1)$. In this step R_1, S_2 each outputs ℓ bits. In each subsequent step i, Quentin sends S_i to Wendy, Wendy computes $R_i = \mathsf{Ext}_w(X, S_i)$. She replies R_i to Quentin and Quentin computes $S_{i+1} = \mathsf{Ext}_q(Q, R_i)$. In step i, R_i, S_{i+1} each outputs ℓ bits. Therefore, this process produces the following sequence:

$$S_1, R_1 = \mathsf{Ext}_w(X, S_1), S_2 = \mathsf{Ext}_q(Q, R_1), \cdots, S_t = \mathsf{Ext}_q(Q, R_{t-1}), R_t = \mathsf{Ext}_w(X, S_t).$$

Look-Ahead Extractor. Now we can define our look-ahead extractor. Let $Y = (Q, S_1)$ be a seed, the look-ahead extractor is defined as

$$\mathsf{laExt}(X, Y) = \mathsf{laExt}(X, (Q, S_1)) \stackrel{def}{=} R_1, \cdots, R_t.$$

We first prove the following lemma.

Lemma 3.1. *Let X be an affine source on n bits, Z be a linear function of X, $Y = (Y_1 = (Q_1, S_1), Y_2 = (Q_2, S_2), \cdots, Y_h = (Q_h, S_h))$ and Y' be linear functions of Z, such that $H(Y'|Y) \geq k_1$, $H(X|Z) \geq k_2$. Assume the following hold: $\forall i$, Q_i has m bits with $m < n$, and S_i has ℓ bits; $H(Q_1) = k_q$ and S_1 is uniform; $k_q \geq 2ht\ell + 10\ell$, $k_1 \geq ht\ell + 10\ell$ and $k_2 \geq ht\ell + 10\ell$. Let Ext_q and Ext_w be strong linear seeded extractors as in Corollary 2.12, set up to use ℓ bits to extract from $(m, 10\ell)$*

sources and $(n, 10\ell)$ sources respectively, with error ϵ and $\ell = O(\log^2(n/\epsilon))$. For any $i \in [h]$, let $(R_{i1}, \cdots, R_{it}) = \mathsf{laExt}(X, Y_i)$ and $\{S_{ij}, j = 1, \cdots, t\}$ denote the random variables corresponding to $\{S_j\}$ that are produced when computing $\mathsf{laExt}(X, Y_i)$. For any $j \in [t]$, let $\overline{S_{ij}} = (S_{i1}, \cdots, S_{ij})$ for $i \in [h]$ and $\overline{R_{ij}} = (R_{i1}, \cdots, R_{ij})$ for $i \in [h]$. Then for any $0 \le j \le t$, we have that

$$\begin{aligned}&(R_{1j}, \{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{i(j-1)}}, i \in [h]\}, Y)\\ \approx_{(2j-1)\epsilon} &(U_\ell, \{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{i(j-1)}}, i \in [h]\}, Y).\end{aligned}$$

and

$$\begin{aligned}&(S_{1(j+1)}, \{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\})\\ \approx_{(2j)\epsilon} &(U_\ell, \{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\}).\end{aligned}$$

Moreover, conditioned on $(\{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{i(j-1)}}, i \in [h]\})$, we have that X is still an affine source, $(\{R_{ij}, i \in [h]\})$ are deterministic linear functions of X, $H(Q_1) \ge k_q - (2j-1)h\ell$, $H(Y'|Y) \ge k_1 - (j-1)h\ell$ and $H(X|Z) \ge k_2 - (j-1)h\ell$; conditioned on $(\{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\})$, we have that X is still an affine source, $(\{S_{i(j+1)}, i \in [h]\})$ are deterministic linear functions of $\{Y_1, \cdots, Y_h\}$ respectively, $H(Q_1) \ge k_q - 2jh\ell$, $H(Y'|Y) \ge k_1 - jh\ell$ and $H(X|Z) \ge k_2 - jh\ell$.

Proof. We prove the lemma by induction on j. When $j = 0$, the statement is trivially true. Now we assume that the statement holds for some j and we prove it for $j + 1$.

We first fix $(\{\overline{S_{ij}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\})$. Note that after this fixing, X is still an affine source. Since Y, Y' and Z are linear functions of X, they are still all affine sources as well. Thus by Lemma 2.8, there exist independent affine sources A, B such that $X = A + B$ and there exists a linear bijection L between A and Z. Thus B is also independent of Z. Note that we have $H(X|Z) \ge k_2 - jh\ell \ge 10\ell$, thus $H(B) \ge 10\ell$.

Since $(\{S_{i(j+1)}, i \in [h]\})$ are linear function of Y and Y is a linear function of Z, we have that $(\{S_{i(j+1)}, i \in [h]\})$ are also linear functions of Z; thus B is independent of $(A, \{S_{i(j+1)}, i \in [h]\}, Y)$. If $S_{1(j+1)}$ is uniform, then by Corollary 2.12 we have

$$(\mathsf{Ext}_w(B, S_{1(j+1)}), S_{1(j+1)}) \approx_\epsilon (U_\ell, S_{1(j+1)}).$$

Note that $R_{1(j+1)} = \mathsf{Ext}_w(X, S_{1(j+1)}) = \mathsf{Ext}_w(A, S_{1(j+1)}) + \mathsf{Ext}_w(B, S_{1(j+1)})$ since Ext_w is a linear seeded extractor. Thus for any fixing of $S_{1(j+1)}$, we have that $\mathsf{Ext}_w(B, S_{1(j+1)})$ is a deterministic linear function of B, and is thus independent of $(\mathsf{Ext}_w(A, S_{1(j+1)}), \{S_{i(j+1)}, i \in [h]\}, Y)$. Therefore, we also have that

$$(R_{1(j+1)}, \{S_{i(j+1)}, i \in [h]\}, Y) \approx_\epsilon (U_\ell, \{S_{i(j+1)}, i \in [h]\}, Y).$$

Adding back the error, we have

$$\begin{aligned}&(R_{1(j+1)}, \{\overline{S_{i(j+1)}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\}, Y)\\ \approx_{(2j+1)\epsilon} &(U_\ell, \{\overline{S_{i(j+1)}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\}, Y). \qquad (1)\end{aligned}$$

Moreover, note that initially $(\{S_{i(j+1)}, i \in [h]\})$ are deterministic linear functions of $\{Y_1, \cdots, Y_h\}$ respectively. Thus if we further condition on the fixing of $(\{S_{i(j+1)}, i \in [h]\})$ (i.e, conditioned on $(\{\overline{S_{i(j+1)}}, i \in [h]\}, \{\overline{R_{ij}}, i \in [h]\})$), we have that X is still an affine source, and $(\{R_{i(j+1)}, i \in [h]\})$ are deterministic linear functions of X. Furthermore $H(Q_1) \geq k_q - 2jh\ell - h\ell = k_q - (2(j+1)-1)h\ell$. On the other hand $H(Y'|Y)$ and $H(X|Z)$ will remain the same since $(\{S_{i(j+1)}, i \in [h]\})$ are deterministic linear functions of Y. So $H(Y'|Y) \geq k_1 - (j+1-1)h\ell$ and $H(X|Z) \geq k_2 - (j+1-1)h\ell$.

Now, recall that $\forall i$, we have $R_{i(j+1)} = \mathsf{Ext}_w(X, S_{i(j+1)}) = \mathsf{Ext}_w(A, S_{i(j+1)}) + \mathsf{Ext}_w(B, S_{i(j+1)})$. Let $R^A_{i(j+1)} = \mathsf{Ext}_w(A, S_{i(j+1)})$ and $R^B_{i(j+1)} = \mathsf{Ext}_w(B, S_{i(j+1)})$, thus $R_{i(j+1)} = R^A_{i(j+1)} + R^B_{i(j+1)}$. We now fix $(\{S_{i(j+1)}, i \in [h]\})$. Note that we have just shown that conditioned on this further fixing, X is still an affine source; thus Y, Y' and Z are all still affine sources as well. Note that now $R^A_{i(j+1)}$ is a deterministic linear function of A, and $R^B_{i(j+1)}$ is a deterministic linear function of B. Thus $(R^A_{i(j+1)}, i \in [h])$ is independent of $(R^B_{i(j+1)}, i \in [h])$.

We now further fix all $R^A_{i(j+1)}$. Note that these are all linear functions of A with size ℓ; thus conditioned on these fixings, we have that X is still an affine source. Since there is a bijection between A and Z, we have that now $H(Q_1) \geq k_q - (2j+1)h\ell - h\ell = k_q - 2(j+1)h\ell \geq 10\ell$. Moreover $H(Y'|Y) \geq k_1 - jh\ell - h\ell = k_1 - (j+1)h\ell$. On the other hand $H(X|Z)$ remains the same since A is a linear function of Z.

Now note that $\forall i$, $R_{i(j+1)} = R^A_{i(j+1)} + R^B_{i(j+1)}$ is a linear function of B, and is thus independent of (A, Z, Y, Y'). If we ignore the error in Equation 1, we know that conditioned on these fixings, $R_{1(j+1)} = R^A_{1(j+1)} + R^B_{1(j+1)}$ is uniform. Therefore by Corollary 2.12 we have

$$(S_{1(j+2)}, R_{1(j+1)}) \approx_\epsilon (U_\ell, R_{1(j+1)}).$$

Note that conditioned on $R_{1(j+1)}$, we have that $S_{1(j+2)}$ is a deterministic linear function of Y_1, and is thus independent of $(B, \{R_{i(j+1)}, i \in [h]\})$. Therefore we also have

$$(S_{1(j+2)}, \{R_{i(j+1)}, i \in [h]\}) \approx_\epsilon (U_\ell, \{R_{i(j+1)}, i \in [h]\}).$$

Adding back the error from Equation 1, we have

$$\begin{aligned}&(S_{1(j+2)}, \{S_{i(j+1)}, i \in [h]\}, \{R_{i(j+1)}, i \in [h]\})\\ \approx_{2(j+1)\epsilon} &(U_\ell, \{S_{i(j+1)}, i \in [h]\}, \{R_{i(j+1)}, i \in [h]\}).\end{aligned}$$

We can now further fix $(R^B_{i(j+1)}, i \in [h])$. Since $(R^A_{i(j+1)}, i \in [h])$ have already been fixed, this will fix $(R_{i(j+1)}, i \in [h])$ and thus we have fixed $(\{\overline{S_{i(j+1)}}, i \in [h]\}, \{\overline{R_{i(j+1)}}, i \in [h]\})$. Since $(R^B_{i(j+1)}, i \in [h])$ are linear functions of B, conditioned on these fixings X is still an affine source. Moreover, this fixing will not affect $H(Q_1)$ or $H(Y'|Y)$ since B is independent of (A, Z, Y, Y'). Thus we have that $H(Q_1) \geq k_q - 2(j+1)h\ell$, $H(Y'|Y) \geq k_1 - (j+1)h\ell$ and $H(X|Z) \geq k_2 - jh\ell - h\ell = k_2 - (j+1)h\ell$.

Note that $j \leq t$, thus the lemma is proved. □

4 The Affine Extractor

In this section we describe our construction. First we have the following algorithm that obtains a somewhere random source.

Algorithm 4.1 ($\mathsf{SR}(X)$)**.**

Input: X— an (n,k)-affine source with $k \geq \text{polylog}(n)$.
Output: W — a source that is close to an SR-source.

Sub-Routines and Parameters:
Let $0 < \alpha < \beta < 1$ be two constants to be chosen later. Let $\ell = k^{\beta}$. Pick an integer h such that $k^{\alpha} \leq h < 2k^{\alpha}$ and $h = 2^l$ for some integer $l > 0$. Let $\mathsf{Ext}_q, \mathsf{Ext}_w$ be strong linear extractors from Corollary 2.12, set up to extract from $((h^2+12)\ell, 10\ell)$ sources and $(n, 10\ell)$ sources respectively, with seed length $\ell > \log^2 n$, error $\epsilon = 2^{-\Omega(\sqrt{\ell})}$ and output length ℓ. These will be used in IaExt. Let $\mathsf{Ext}_1, \mathsf{Ext}_2, \mathsf{Ext}_3$ be strong linear extractors from Corollary 2.12, with parameters as follows.

- Let $d > \log^2 n$ be an integer such that when we use d uniform bits to extract from an (n,k) source as in Corollary 2.12, the error $\epsilon' = 2^{-\Omega(\sqrt{d})}$ satisfies that $2^{(2h^3+h^2+11h)\ell}\epsilon' \leq \epsilon = 2^{-\Omega(\sqrt{\ell})}$. Note that it suffices to take $d = ch^6\ell^2$ for some constant $c > 1$.
- Ext_1 uses d bits to extract from $(n, 10\ell)$ sources, with error ϵ' and output length ℓ.
- Ext_2 uses ℓ bits to extract from $(\sqrt{k}, (4h^2+20)\ell)$ sources, with error $\epsilon = 2^{-\Omega(\sqrt{\ell})}$ and output length $(2h^2+10)\ell$.
- Ext_3 uses ℓ bits to extract from from $(\sqrt{k}, 2d)$ sources, with error $\epsilon = 2^{-\Omega(\sqrt{\ell})}$ and output length d.

1. Let LExt be the linear seeded extractor in Theorem 2.15, which uses $d' = O(\log n)$ bits to extract from an (n,k) source and output $m = \sqrt{k}$ bits with error n^{-2}. Let $N = 2^{d'} = \text{poly}(n)$ and enumerate all possible choices of the seed $r_1, \cdots, r_N$. For every $i \in [N]$ compute $Y^i = \mathsf{LExt}(X, r_i)$.
2. For every $i = 1, \cdots, N$, use X and Y^i to compute W^i as follows.
   (a) Compute the binary expression of $i-1$, which consists of $d' = \log N = O(\log n)$ bits. Divide these bits sequentially from left to right into $b = \lceil \frac{d'}{l} \rceil$ blocks of size l (the last block may have less than l bits, then we add 0s at the end to make it l bits). Now from left to right, for each block $j = 1, \cdots, b$, we obtain an integer $\mathsf{Ind}_{ij} \leq 2^l$ such that the binary expression of $\mathsf{Ind}_{ij} - 1$ is the same as the bits in block j.
   (b) Let Y^{i1} be the first d bits of Y^i. Set $j = 1$. While $j < b$ do the following.
      i. Compute $R_0^{ij} = \mathsf{Ext}_1(X, Y^{ij})$ and $Y'^{ij} = \mathsf{Ext}_2(Y^i, R_0^{ij})$.
      ii. Compute $(R_1^{ij}, \cdots, R_h^{ij}) = \mathsf{IaExt}(X, Y'^{ij})$, where $Q = Y'^{ij}$ and S_1 is the first ℓ bits of Y'^{ij}.
      iii. Compute $Y^{i(j+1)} = \mathsf{Ext}_3(Y^i, R^{ij}_{\mathsf{Ind}_{ij}})$.
      iv. Set $j = j+1$.
   (c) Finally, compute $(R_1^{ib}, \cdots, R_h^{ib}) = \mathsf{IaExt}(X, Y^{ib})$ and set $W^i = R^{ib}_{\mathsf{Ind}_{ib}}$.
3. Let $W = W^1 \circ \cdots \circ W^N$.

We now introduce some notation. For any $i \in [N]$ and $j \in [b]$, we let $Y^{i(\leq j)}$ denote $(Y^{i1}, \cdots, Y^{ij})$ and similarly $Y'^{i(\leq j)}$ denote $(Y'^{i1}, \cdots, Y'^{ij})$; let $R^{i(\leq j)}_{\mathsf{Ind}_{i(\leq j)}}$ denote $(R^{i1}_{\mathsf{Ind}_{i1}}, \cdots, R^{ij}_{\mathsf{Ind}_{ij}})$ and let $f^j(i)$ denote the integer whose binary expression is the concatenation of the binary expression of $i-1$ from block 1 to block j. Recall that for any i, j, when computing $\mathsf{IaExt}(X, Y^{ij})$ we will compute $S^{ij}_1, \cdots, S^{ij}_h$ and $R^{ij}_1, \cdots, R^{ij}_h$. Let $\overline{S^{ij}} = (S^{ij}_1, \cdots, S^{ij}_{\max(\mathsf{Ind}_{vj}-1, \mathsf{Ind}_{ij})})$ and similarly $\overline{R^{ij}} = (R^{ij}_1, \cdots, R^{ij}_{\max(\mathsf{Ind}_{vj}-1, \mathsf{Ind}_{ij})})$; let $\overline{S^{i(\leq j)}} = (\overline{S^{i1}}, \cdots, \overline{S^{ij}})$ and similarly $\overline{R^{i(\leq j)}} = (\overline{R^{i1}}, \cdots, \overline{R^{ij}})$. We have the following lemma.

Lemma 4.2. *Assume that $k \geq 9b^2d^2h^2$. Fix any $v \in [N]$ such that Y^v is uniform. Let $T \subset [N]$ be any subset with $|T| = h$ and $v \in T$, and let Z_T be the concatenation of all Y^i where $i \in T$. For any $j \in [b]$, define $T^j_v = \{i \in T : f^j(i) < f^j(v)\}$ and let $T_v = T^b_v$. Let $\tilde{T}^j_v = T_v \setminus T^j_v$. Then for any $j \in [b]$, we have that*

- *At the beginning of iteration j, conditioned on $(\{Y'^{i(\leq j-1)}, Y^{i(\leq j-1)}, \overline{S^{i(\leq j-1)}}, \overline{R^{i(\leq j-1)}}, i \in T_v\})$, we have*
  1. *X is still an affine source.*
  2. *$\{Y^{ij}, i \in T_v\}$ are linear functions of Z_T.*
  3. *$H(Y^v) \geq \sqrt{k} - 2(j-1)dh$, $H(X|Z_T) \geq k - h\sqrt{k} - 2(j-1)h^2\ell$.*
  4. *With probability $1 - \epsilon_{j1}$ over the fixing of $\{Y'^{i(\leq j-1)}, Y^{i(\leq j-1)}, \overline{S^{i(\leq j-1)}}, \overline{R^{i(\leq j-1)}}, i \in T_v\}, \{Y^{ij}, i \in T^{j-1}_v\}$, we have $Y^{vj} = U_d$. Here $\epsilon_{j1} = 4j(h+1)\epsilon$.*
- *At the end of iteration j, we have*

$$\begin{aligned}&(R^{vj}_{\mathsf{Ind}_{vj}}, \{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, i \in T_v\}, \{\overline{R^{i(\leq j)}}, i \in T^j_v\})\\ \approx_{\epsilon_{j2}} &(U_\ell, \{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, i \in T_v\}, \{\overline{R^{i(\leq j)}}, i \in T^j_v\}),\end{aligned}$$

  where $\epsilon_{j2} = 4j(h+1)\epsilon + (2h+1)\epsilon$.

Proof. We prove the lemma by induction on j. Note that $T_v = \{i \in T : i < v\}$ and $\tilde{T}^j_v = T_v \setminus T^j_v$ contains all the numbers in T that are less than v but have the same binary expression in the first j blocks.

We first show that properties 1, 2 and 3 in the first part of the statement hold. When $j = 1$ these are trivially true. Now suppose they hold for some j and we'll show that they hold for $j+1$. We first fix $(\{Y'^{i(\leq j-1)}, Y^{i(\leq j-1)}, \overline{S^{i(\leq j-1)}}, \overline{R^{i(\leq j-1)}}, i \in T_v\})$ and we know that conditioned on this fixing, properties 1, 2 and 3 hold. We now further fix $\{Y^{ij}, i \in T_v\}$. Note that conditioned on this fixing, X is still an affine source, and $\{R^{ij}_0, i \in T_v\}$ are deterministic linear functions of X. We then further fix $\{R^{ij}_0, i \in T_v\}$. Note that conditioned on this fixing, X is still an affine source, and $\{Y'^{ij}, i \in T_v\}$ are deterministic linear functions of $\{Y^i, i \in T_v\}$ respectively. We thus further fix $\{Y'^{ij}, i \in T_v\}$. Note that conditioned on this fixing, X is still an affine source. Now for any $i \in T_v$, in the computation of $(R^{ij}_1, \cdots, R^{ij}_h) = \mathsf{IaExt}(X, Y'^{ij})$ we can fix $R^{ij}_1, R^{ij}_2, \cdots$ one by one, and we note that conditioned on the fixing of the previous one, the next one is a deterministic linear function of X. Thus we can fix $\{\overline{R^{ij}}, i \in T_v\}$ and after this fixing, X is still an affine source. Note that once $\{\overline{R^{ij}}, i \in T_v\}$ are fixed, $\{\overline{S^{ij}}, i \in T_v\}$ are also fixed since they are functions of $\{\overline{R^{ij}}, i \in T_v\}$ and $\{Y'^{ij}, i \in T_v\}$. Thus we have fixed $(\{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, \overline{R^{i(\leq j)}}, i \in T_v\})$ and conditioned on

this fixing, X is still an affine source. Furthermore now $\{Y^{i(j+1)}, i \in T_v\}$ are linear functions of $\{Y^i, i \in T_v\} = Z_T$.

Next we look at the $H(Y^v)$ and $H(X|Z_T)$. We note that since Y^v and Z_T are linear functions of X, whenever X is an affine source, they are also both affine sources. We can now repeat the argument above, and since each time we are conditioning on some linear functions of X, the conditional entropy will decrease by at most the size of the random variables being conditioned on. We further note that when we condition on $R_t^{ij}, t = 0, \cdots, h$, we may lose entropy in both $H(Y^v)$ and $H(X|Z_T)$; while when we condition on Y^{ij} and $Y'ij$, we only lose entropy in $H(Y^v)$ since they are deterministic functions of Z_T. Note that the total size of $\{R_t^{ij}, t = 0, \cdots, h, i \in T_v\}$ is at most $h(h+1)\ell < 2h^2\ell$, while the total size of $\{Y^{ij}, Y'^{ij}, R_t^{ij}, t = 0, \cdots, h, i \in T_v\}$ is at most $h(d + (2h^2+10)\ell) + h(h+1)\ell < 2dh$. Thus we know that at the beginning of iteration $j+1$, we have $H(Y^v) \geq \sqrt{k} - 2(j-1)dh - 2dh = \sqrt{k} - 2jdh$ and $H(X|Z_T) \geq k - h\sqrt{k} - 2(j-1)h^2\ell - 2h^2\ell = k - h\sqrt{k} - 2jh^2\ell$.

Now we show that property 4 in the first part and the second part hold. Again we use induction. When $j = 1$, we note that $Y^{v1} = U_\ell$. Thus property 4 holds. Now suppose property 4 holds for some j; we will show that the second part of the statement is true for iteration j, and that property 4 holds for iteration $j+1$. This will establish the lemma.

We first note that by our choice of the parameters, even if conditioned on all the $(\{Y'^{i(\leq b)}, Y^{i(\leq b)}, \overline{S^{i(\leq b)}}, \overline{R^{i(\leq b)}}, i \in T_v\})$, we have that $H(Y^v) \geq \sqrt{k} - 2bdh \geq bdh$ and $H(X|Z_T) \geq k - h\sqrt{k} - 2bh^2\ell > 0.9k$. Thus no matter when we apply Ext_1, Ext_2 or Ext_3 in the case of $i = v$, the source always has enough entropy for extraction.

We now first fix $(\{Y'^{i(\leq j-1)}, Y^{i(\leq j-1)}, \overline{S^{i(\leq j-1)}}, \overline{R^{i(\leq j-1)}}, i \in T_v\})$. Note that conditioned on this fixing, X is still an affine source. Note that Z_T is a linear function of X and $\{Y^{ij}, i \in T_v\}$ are linear functions of Z_T, thus they are all affine sources. We will now further fix $\{Y^{ij}, i \in T_v^{j-1}\}$. Note that since they are all linear functions of Z_T, conditioned on this fixing X is still an affine source. By induction hypothesis, with probability $1 - \epsilon_{j1}$ over the fixing of all these random variables, Y^{vj} is uniform.

Note that now for any $i \in T_v^{j-1}$, we have $R_0^{ij} = \mathsf{Ext}_1(X, Y^{ij})$ is a deterministic linear function of X. We can now further fix all $\{R_0^{ij}, i \in T_v^{j-1}\}$ and conditioned on this fixing, X is still an affine source. After this fixing, for any $i \in T_v^{j-1}$, we have $Y'^{ij} = \mathsf{Ext}_2(Y^i, R_0^{ij})$ is a deterministic function of Y^i. We can now further fix all $\{Y'^{ij}, i \in T_v^{j-1}\}$. Conditioned on this fixing X is still an affine source, and now we have that all the $\{R_t^{ij}, i \in T_v^{j-1}\}$ are deterministic functions of X. Moreover, for any $i \in T_v^{j-1}$, if we fix R_t^{ij}, then R_{t+1}^{ij} is a deterministic linear function of X. Thus for any $i \in T_v^{j-1}$, we can fix all $\{R_t^{ij}, t = 1, \cdots, \max(\mathsf{Ind}_{vj} - 1, \mathsf{Ind}_{ij})\}$ one by one, and conditioned on all these fixings, X is still an affine source. Note that this also fixes all $\{S_t^{ij}, t = 1, \cdots, \max(\mathsf{Ind}_{vj} - 1, \mathsf{Ind}_{ij})\}$ since they are deterministic functions of $\{R_t^{ij}\}$ and $\{Y'^{ij}\}$. Thus we have fixed all $\{Y^{ij}, Y'^{ij}, \overline{S^{ij}}, \overline{R^{ij}}, i \in T_v^{j-1}\}$.

Note that in the above process, we may lose entropy in Y^{vj} when we fix $\{R_t^{ij}, t = 0, \cdots, \max(\mathsf{Ind}_{vj} - 1, \mathsf{Ind}_{ij}), i \in T_v^{j-1}\}$ and $\{Y'^{ij}, i \in T_v^{j-1}\}$. However, note that the size of all these random variables is at most $|T_v^{j-1}|((h+1)\ell + (2h^2+10)\ell) \leq h((h+1)\ell + (2h^2+10)\ell) = (2h^3 + h^2 + 11h)\ell$, thus $H(Y^{v1}) \geq d - (2h^3 + h^2 + 11h)\ell$.

Now by Lemma 2.8, there exist independent affine sources A, B such that $X = A + B$ and there exists a linear bijection L between A and Z_T. Thus B is also independent of $(Z_T, \{Y_i, i \in T_v\})$. Note that $H(B) = H(X|Z_T) \geq 0.9k$ and $H(Y_v) \geq d - (2h^3 + h^2 + 11h)\ell$. Since Y^{vj} is a deterministic function of Y_v, by Lemma 2.6 we have

$$(\mathsf{Ext}_2(B, Y^{vj}), Y^{vj}) \approx_\epsilon (U_\ell, Y^{vj}).$$

Note that $R_0^{vj} = \mathsf{Ext}_2(A, Y^{vj}) + \mathsf{Ext}_2(B, Y^{vj})$. Let $R^A = \mathsf{Ext}_2(A, Y^{vj})$ and $R^B = \mathsf{Ext}_2(B, Y^{vj})$, thus $R_0^{vj} = R^A + R^B$. We now fix Y^{vj}. Note that after this fixing, R^B is a deterministic linear function of B, and is thus independent of $(A, Y^i, i \in T_v)$. If we ignore the error, then R^B is still uniform. Thus we can further fix all $\{Y^{ij}, i \in \tilde{T}_v^{j-1}\}$ (since they are deterministic linear functions of Y^i) and R^B is still uniform. Note that after this fixing X is still an affine source. Now, all the $\{\mathsf{Ext}_2(A, Y^{ij}), i \in \tilde{T}_v^{j-1}\}$ become deterministic linear functions of A, and are thus independent of R^B. So we can now further fix all $\{\mathsf{Ext}_2(A, Y^{ij}), i \in \tilde{T}_v^{j-1}\}$ and R^B is still uniform and independent of $\{Y^i, i \in T_v\}$. Note that conditioned on this fixing we have $R_0^{vj} = R^A + R^B$ is uniform and independent of all $\{Y^i, i \in \tilde{T}_v^{j-1}\}$. Thus by Corollary 2.12 we have

$$(Y'^{vj}, R_0^{vj}) \approx_\epsilon (U_{(2h^2+10)\ell}, R_0^{vj}).$$

We can now further fix R^B, and conditioned on this fixing Y'^{vj} is a deterministic function of Y^v, and is thus independent of all $\{\mathsf{Ext}(B, Y^{ij}), i \in \tilde{T}_v^{j-1}\}$ since they are deterministic linear functions of B. We can therefore fix all $\{\mathsf{Ext}(B, Y^{ij}), i \in \tilde{T}_v^{j-1}\}$ and Y'^{vj} is still close to uniform. Note since $\{\mathsf{Ext}(A, Y^{ij}), i \in \tilde{T}_v^{j-1}\}$ have been fixed before, now we have fixed all $\{R_0^{ij}, i \in \tilde{T}_v^{j-1}\}$. Now adding back all the error, we get that after all these fixings,

$$Y'^{vj} \approx_{2\epsilon} U_{(2h^2+10)\ell}.$$

Ignoring the error, we can now apply Lemma 3.1 (where $Y = (Y'^{ij}, i \in T_v)$, $Y' = Y^v$ and $Z = Z_T$). Thus conditioned on the further fixing of $\{S_1^{ij}, \cdots, S_{\mathsf{Ind}_{vj}-1}^{ij}, i \in \tilde{T}_v^{j-1}\}$ and $\{R_1^{ij}, \cdots, R_{\mathsf{Ind}_{vj}-1}^{ij}, i \in \tilde{T}_v^{j-1}\}$, we have that X is still an affine source, and $\{S_{\mathsf{Ind}_{vj}}^{ij}, i \in \tilde{T}_v^{j-1}\}$ are deterministic linear functions of $\{Y'^{ij}, i \in \tilde{T}_v^{j-1}\}$ respectively. Moreover $H(X|Z_T) \geq 0.9k > 10\ell$. Therefore again by Lemma 2.8, there exist independent affine sources A, B such that $X = A + B$ and there exists a linear bijection L between A and Z_T. Thus B is also independent of Z_T and $H(B) = H(X|Z_T) > 10\ell$.

Lemma 3.1 also tells us that

$$\begin{aligned}&(S_{\mathsf{Ind}_{vj}}^{vj}, \{S_1^{ij}, \cdots, S_{\mathsf{Ind}_{vj}-1}^{ij}, R_1^{ij}, \cdots, R_{\mathsf{Ind}_{vj}-1}^{ij}, i \in \tilde{T}_v^{j-1}\})\\ \approx_{(2(\mathsf{Ind}_{vj}-1))\epsilon}&(U_\ell, \{S_1^{ij}, \cdots, S_{\mathsf{Ind}_{vj}-1}^{ij}, R_1^{ij}, \cdots, R_{\mathsf{Ind}_{vj}-1}^{ij}, i \in \tilde{T}_v^{j-1}\}).\end{aligned}$$

Ignoring the error, conditioned on the further fixing of $\{S_1^{ij}, \cdots, S_{\mathsf{Ind}_{vj}-1}^{ij}, i \in \tilde{T}_v^{j-1}\}$ and $\{R_1^{ij}, \cdots, R_{\mathsf{Ind}_{vj}-1}^{ij}, i \in \tilde{T}_v^{j-1}\}$, we have that $S_{\mathsf{Ind}_{vj}}^{vj}$ is uniform. Since $S_{\mathsf{Ind}_{vj}}^{vj}$ is a deterministic linear function of Y^v, it is independent of B. Thus by Corollary 2.12 we have

$$(\mathsf{Ext}_w(B, S_{\mathsf{Ind}_{vj}}^{vj}), S_{\mathsf{Ind}_{vj}}^{vj}) \approx_\epsilon (U_\ell, S_{\mathsf{Ind}_{vj}}^{vj}).$$

Note that for any $i \in \tilde{T}_v^{j-1}$, we have $R_{\mathsf{Ind}_{vj}}^{ij} = \mathsf{Ext}_w(X, S_{\mathsf{Ind}_{vj}}^{ij}) = \mathsf{Ext}_w(A, S_{\mathsf{Ind}_{vj}}^{ij}) + \mathsf{Ext}_w(B, S_{\mathsf{Ind}_{vj}}^{ij})$. Thus for any fixing of $S_{\mathsf{Ind}_{vj}}^{vj}$, we have $\mathsf{Ext}_w(B, S_{\mathsf{Ind}_{vj}}^{vj})$ is a deterministic linear function of B, and is thus independent of $(A, Z_T = \{Y^i, i \in T_v\})$. Therefore it is also true that

$$(R^{vj}_{\mathsf{Ind}_{vj}}, \{S^{ij}_{\mathsf{Ind}_{vj}}, i \in \tilde{T}^{j-1}_v\}, \{Y'^{ij}, i \in \tilde{T}^{j-1}_v\}) \approx_\epsilon (U_\ell, \{S^{ij}_{\mathsf{Ind}_{vj}}, i \in \tilde{T}^{j-1}_v\}, \{Y'^{ij}, i \in \tilde{T}^{j-1}_v\}).$$

Now we add back all the error, and notice that we have already fixed all $\{Y'^{i(\leq j-1)}, Y^{i(\leq j-1)}, \overline{S^{i(\leq j-1)}}, \overline{R^{i(\leq j-1)}}, i \in T_v\}$, $\{Y^{ij}, i \in T_v\}$, $\{Y'^{ij}, i \in T^{j-1}_v\}$, $\{\overline{S^{ij}}, \overline{R^{ij}}, i \in T^{j-1}_v\}$. Furthermore notice that for any $i \in T^j_v \setminus T^{j-1}_v$, we must have $\mathsf{Ind}_{ij} < \mathsf{Ind}_{vj}$, thus $\max(\mathsf{Ind}_{vj} - 1, \mathsf{Ind}_{ij}) = \mathsf{Ind}_{vj} - 1$. Therefore for these i when we fix $\{R^{ij}_1, \cdots, R^{ij}_{\mathsf{Ind}_{vj}-1}\}$ we have fixed $\overline{R^{ij}}$. On the other hand for any $i \in T_v$ we have that $\mathsf{Ind}_{ij} \leq \mathsf{Ind}_{vj}$ so if we fix all $S^{ij}_1, \cdots, S^{ij}_{\mathsf{Ind}_{vj}}$ we have fixed $\overline{S^{ij}}$. Thus we have

$$\begin{aligned}&(R^{vj}_{\mathsf{Ind}_{vj}}, \{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, i \in T_v\}, \{\overline{R^{i(\leq j)}}, i \in T^j_v\})\\ \approx_{\epsilon_{j2}} &(U_\ell, \{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, i \in T_v\}, \{\overline{R^{i(\leq j)}}, i \in T^j_v\}),\end{aligned}$$

where $\epsilon_{j2} = \epsilon_{j1} + 2\epsilon + (2(\mathsf{Ind}_{vj} - 1))\epsilon + \epsilon \leq \epsilon_{j1} + (2h+1)\epsilon = 4j(h+1)\epsilon + (2h+1)\epsilon$. Thus the second part of the statement for iteration j is true.

Now conditioned on the fixing of $\{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, i \in T_v\}, \{\overline{R^{i(\leq j)}}, i \in T^j_v\}$, we have that $\mathsf{Ext}_w(B, S^{vj}_{\mathsf{Ind}_{vj}})$ is still uniform (ignoring the error) and is a deterministic linear function of B. We will now further fix all $\{\mathsf{Ext}_w(A, S^{ij}_{\mathsf{Ind}_{vj}}), i \in \tilde{T}^{j-1}_v\}$. Since these are all deterministic linear functions of A, conditioned on these fixings we have X is still an affine source, and $\mathsf{Ext}_w(B, S^{vj}_{\mathsf{Ind}_{vj}})$ is still uniform. Now $R^{vj}_{\mathsf{Ind}_{vj}} = \mathsf{Ext}_w(A, S^{vj}_{\mathsf{Ind}_{vj}}) + \mathsf{Ext}_w(B, S^{vj}_{\mathsf{Ind}_{vj}})$ is still uniform and is a deterministic linear function of B, and is thus independent of (Z_T, Y^v). Moreover, all $\{R^{ij}_{\mathsf{Ind}_{ij}}, i \in T^j_v\}$ have been fixed and all $\{R^{ij}_{\mathsf{Ind}_{vj}}, i \in \tilde{T}^j_v\}$ are deterministic linear functions of B. Therefore now all $\{Y^{i(j+1)} = \mathsf{Ext}_3(Y^i, R^{ij}_{\mathsf{Ind}_{ij}}), i \in T^j_v\}$ are deterministic linear functions of $\{Y^i, i \in T^j_v\}$ respectively. We can thus now further fix all these $\{Y^{i(j+1)}, i \in T^j_v\}$ and conditioned on this fixing, X is still an affine source and Y^v still has enough entropy. Now by Corollay 2.12 we have

$$(Y^{v(j+1)}, R^{vj}_{\mathsf{Ind}_{vj}}) \approx_\epsilon (U_d, R^{vj}_{\mathsf{Ind}_{vj}}).$$

Note that conditioned on $R^{vj}_{\mathsf{Ind}_{vj}}$, we have that $Y^{v(j+1)}$ is a deterministic function of Y^v, and is thus independent of all $\{R^{ij}_{\mathsf{Ind}_{vj}}, i \in \tilde{T}^j_v\}$ since they are deterministic functions of B. Note that for any $i \in \tilde{T}^j_v$, we must have $\mathsf{Ind}_{ij} = \mathsf{Ind}_{vj}$ and thus $\max(\mathsf{Ind}_{vj} - 1, \mathsf{Ind}_{ij}) = \mathsf{Ind}_{ij}$. Therefore it is also true that

$$(Y^{v(j+1)}, \{R^{ij}_{\mathsf{Ind}_{ij}}, i \in \tilde{T}^j_v\}) \approx_\epsilon (U_d, \{R^{ij}_{\mathsf{Ind}_{ij}}, i \in \tilde{T}^j_v\}).$$

Therefore we have that

$$\begin{aligned}&(Y^{v(j+1)}, \{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, \overline{R^{i(\leq j)}}, i \in T_v\}, \{Y^{i(j+1)}, i \in T^j_v\})\\ \approx_{\epsilon'} &(U_\ell, \{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, \overline{R^{i(\leq j)}}, i \in T_v\}, \{Y^{i(j+1)}, i \in T^j_v\}),\end{aligned}$$

where $\epsilon' = 2\epsilon + (2(\mathsf{Ind}_{vj} - 1))\epsilon + \epsilon + \epsilon \leq 2(h+1)\epsilon$. This is conditioned on the event that Y^{vj} is uniform at the beginning of iteration j, which happens with probability $1 - \epsilon_{j1}$. By Lemma 2.7, now

with all but another $2\epsilon' \leq 4(h+1)\epsilon$ probability, conditioned on $\{Y'^{i(\leq j)}, Y^{i(\leq j)}, \overline{S^{i(\leq j)}}, \overline{R^{i(\leq j)}}, i \in T_v\}, \{Y^{i(j+1)}, i \in T_v^j\}$ we have that $Y^{v(j+1)}$ is uniform. Thus property 4 in the first part holds for iteration $j+1$ with $\epsilon_{(j+1)1} = \epsilon_{j1} + 4(h+1)\epsilon = 4(j+1)(h+1)\epsilon$. □

We now have the following lemma.

Lemma 4.3. *Assume that $k \geq 9b^2d^2h^2$ and X is an (n,k)-affine source. Let $N = 2^{d'} = \text{poly}(n)$ and $W = W^1 \circ \cdots \circ W^N = \mathsf{SR}(X)$. Then there exists a subset $S \subset [N]$ with $|S| \geq (1 - \frac{2}{n^2})N$ such that for any subset $S' \subset S$ with $|S'| = h$, we have that*

$$(W^i, i \in S') \approx_\epsilon U_{h\ell},$$

where $\epsilon = 2^{-\Omega(\sqrt{\ell})}$.

Proof. First note that LExt is a strong linear seeded extractor with seed length $d' = O(\log n)$ and error n^{-2}. Thus by Lemma 2.7 there exists a subset $S \subset [N]$ with $|S| \geq (1 - \frac{2}{n^2})N$ such that $\forall i \in S$, we have that Y^i is uniform.

Now consider any subset $S' \subset S$ with $|S'| = h$. We order the elements in S' to be $i_1 < i_2 < \cdots < i_h$. Since $S' \subset S$, for any $j \in [h]$ we have that Y^{i_j} is uniform. We now apply Lemma 4.2 to the set S'. Note that $f^b(i) = i - 1$, thus for any $v \in S'$ we have $S_v'^b = \{i \in S' : i < v\}$. Also note that $W^i = R^{ib}_{\mathsf{Ind}_{ib}}$ for any $i \in [N]$. Thus by Lemma 4.2, for any $j \in [h]$ we have that

$$(W^{i_j}, W^{i_1}, \cdots, W^{i_{j-1}}) \approx_{O(bh2^{-\Omega(\sqrt{\ell})})} (U_\ell, W^{i_1}, \cdots, W^{i_{j-1}}).$$

Thus we have that

$$(W^{i_1}, \cdots, W^{i_h}) \approx_\epsilon U_{h\ell},$$

where $\epsilon = O(bh^2 2^{-\Omega(\sqrt{\ell})}) = 2^{-\Omega(\sqrt{\ell})}$ since $\ell = k^\beta > k^\alpha$, $h < 2k^\alpha$ and $b < \log n = k^{O(1)}$. □

We can now state our affine extractor.

Algorithm 4.4 ($\mathsf{AExt}(X)$)**.**

Input: X— an (n,k)-affine source with $k \geq \text{polylog}(n)$.
Output: Z — a bit that is $n^{-\Omega(1)}$-close to uniform.

Sub-Routines and Parameters:
Let SR be the function in Algorithm 4.1. Let bitExt be the extractor for non-oblivious bit-fixing sources in Theorem 2.16.

1. Let $W = W^1 \circ \cdots \circ W^N = \mathsf{SR}(X)$ where $N = \text{poly}(n)$. Take the first bit of each W^i and let V be the concatenation.
2. Compute $Z = \mathsf{bitExt}(V)$.

We have the following theorem.

Theorem 4.5. *There exists a constant $C > 1$ such that for any (n, k) affine source X with $k \geq \log^C n$, we have that*

$$|\mathsf{AExt}(X) - U_1| \leq \epsilon,$$

where $\epsilon = n^{-\Omega(1)}$.

Proof. By Lemma 4.3, if $k \geq 9b^2d^2h^2$ then there exists a subset $S \subset [N]$ with $|S| \geq (1 - \frac{2}{n^2})N$ such that for any subset $S' \subset S$ with $|S'| = h$, we have that

$$(W^i, i \in S') \approx_{\epsilon'} U_{h\ell},$$

where $\epsilon' = 2^{-\Omega(\sqrt{\ell})}$.

Therefore by definition V is a (q, t, γ)-non-oblivious bit-fixing source with $q = 2N/n^2$, $t = h$ and $\gamma = \epsilon' = 2^{-\Omega(\sqrt{\ell})}$. We now apply Theorem 2.16. Note that $q = 2N/n^2 \leq N^{1-\delta}$ for some constant $\delta > 0$ since $N = \text{poly}(n)$. We also need that $t = h \geq O(\log^{18}(N)) = O(\log^{18} n)$and $\gamma \leq 1/N^{t+1} = 1/n^{O(t)}$.

Note that $b < \log n$, $d = O(h^6\ell^2)$, $\ell = k^\beta$, and $k^\alpha \leq h < 2k^\alpha$. Thus altogether all conditions are satisfied if

$$k \geq ck^{14\alpha+4\beta} \log^2 n, k^\alpha \geq c_1 \log^{18} n, \text{ and } \sqrt{\ell} = k^{\beta/2} \geq c_2 k^\alpha \log n,$$

for some constants c, c_1, c_2.

It is now easy to check that if we take α, β to be small enough with $\alpha < \beta/2$ and $k \geq \log^C n$ for a big enough constant $C > 1$, then all the above conditions are satisfied. Thus by Theorem 2.16 the output of AExt is ϵ-close to uniform with $\epsilon = N^{-\Omega(1)} = n^{-\Omega(1)}$. Note that $N = \text{poly}(n)$ so the extractor can be computed in polynomial time. ■

5 Open Problems

The most obvious open problem left here is to increase the output length of our extractor and improve the error. Currently our extractor only outputs one bit with error $n^{-\Omega(1)}$, while by the probabilistic method one can hope to extract $\Omega(k)$ bits with error $2^{-\Omega(k)}$. Note that in the case of two-source extractors, if one can improve the output length of the extractor in [CZ15] to $O(\log n)$, then one can immediately obtain output length close to k by applying a seeded extractor to one of the sources. However, in the affine case, it is not clear if one can apply this trick.

References

[BIW04] Boaz Barak, R. Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 384–393, 2004.

[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.

[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 *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, 2006.

[BSK09] Eli Ben-Sasson and Swastik Kopparty. Affine dispersers from subspace polynomials. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, 2009.

[CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[CI15] Mahdi Cheraghchi and Piotr Indyk. Nearly optimal deterministic algorithm for sparse walsh-hadamard transforms. Technical Report TR15-076, Electronic Colloquium on Computational Complexity, 2015.

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

[CZ15] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functionss. Technical Report TR15-119, Electronic Colloquium on Computational Complexity, 2015.

[DG10] Matt DeVos and Ariel Gabizon. Simple affine extractors using dimension expansion. In *Proc. of the 25th CCC*, 2010.

[DKSS09] Z. Dvir, S. Kopparty, S. Saraf, and M. 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.

[GR05] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, 2005.

[GUV09] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *Journal of the ACM*, 56:1–34, 2009.

[Li11a] Xin Li. Improved constructions of three source extractors. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 126–136, 2011.

[Li11b] Xin Li. A new approach to affine extractors and dispersers. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 137–147, 2011.

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

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

[Li15] Xin Li. Three source extractors for polylogarithmic min-entropy. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[LRVW03] C. J. Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: Optimal up to constant factors. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 602–611, 2003.

[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 *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, 2006.

[Rao09] Anup Rao. Extractors for low-weight affine sources. In *Proc. of the 24th CCC*, 2009.

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

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

[Sha11] Ronen Shaltiel. Dispersers for affine sources with sub-polynomial entropy. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, 2011.

[SU05] Ronen Shaltiel and Chris Umans. Simple extractors for all min-entropies and a new pseudorandom generator. *Journal of the ACM*, 52:172–216, 2005.

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

[Yeh11] Amir Yehudayoff. Affine extractors over prime fields. *Combinatorica*, 2011.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de