Electronic Colloquium on Computational Complexity, Report No. 37 (2011)

Extractors and Lower Bounds for Locally Samplable Sources

Anindya De* Thomas Watson†

March 17, 2011

Abstract

We consider the problem of extracting randomness from sources that are efficiently samplable, in the sense that each output bit of the sampler only depends on some small number d of the random input bits. As our main result, we construct a deterministic extractor that, given any d-local source with min-entropy k on n bits, extracts $\Omega(k^2/nd)$ bits that are $2^{-n^{\Omega(1)}}$-close to uniform, provided $d \leq o(\log n)$ and $k \geq n^{2/3+\gamma}$ (for arbitrarily small constants $\gamma > 0$).

Using our result, we also improve a result of Viola (FOCS 2010), who proved a $1/2 - O(1/\log n)$ statistical distance lower bound for $o(\log n)$-local samplers trying to sample input-output pairs of an explicit boolean function, assuming the samplers use at most $n+n^{1-\delta}$ random bits for some constant $\delta > 0$. Using a different function, we simultaneously improve the lower bound to $1/2 - 2^{-n^{\Omega(1)}}$ and eliminate the restriction on the number of random bits.

1 Introduction

Randomness extraction is the following general problem. Given a sample from an imperfect physical source of randomness, which is modeled as a probability distribution on bit strings of length n, we wish to apply an efficient deterministic algorithm to the sample to produce an output which is almost uniformly distributed (and is thus suitable for use by a randomized algorithm). Of course, to extract randomness from a source, the source needs to "contain" a certain amount of randomness to begin with. It is well established that the most suitable measure of the amount of randomness in a source is its *min-entropy* (defined below). However, even if the source is known to have at least $n - 1$ bits of min-entropy, no algorithm can extract even a single bit that is guaranteed to be close to uniformly distributed. To deal with this problem, researchers have constructed *seeded extractors*, which have access to a short uniformly random seed that is statistically independent of the source and which acts as a catalyst for the extraction process (see [Sha02] for a survey).

However, there is a sense in which seeded extractors are overkill: They are guaranteed to work for completely arbitrary sources that have high enough min-entropy. It is reasonable to assume the physical source of randomness has some limited structure, in which case deterministic (that is, seedless) extraction may become viable. There are several classes of sources for which researchers have constructed good deterministic extractors. One such class is independent sources, where the n bits are partitioned into blocks which are assumed to be statistically independent of each other [CG88, DEOR04, BIW06, Bou05, BKS+10, Raz05, Sha08, Rao09a, BRSW06, Rao08, RZ08, RY11,

*Computer Science Division, University of California, Berkeley. Supported by NSF grant CCF-0917417.

†Computer Science Division, University of California, Berkeley. Supported by a National Science Foundation Graduate Research Fellowship and NSF grant CCF-0917417.

ISSN 1433-8092

Li11a]. Other such classes include so-called bit-fixing sources [CFG+85, KZ07, GRS06, Rao09b], affine sources [GR08, Bou07, Rao09b, DG10, Yeh10, Li11b], polynomial sources [DGW09], and algebraic varieties [Dvi09].

Trevisan and Vadhan [TV00] considered deterministic extractors for the class of sources that are samplable by efficient algorithms given uniform random bits. One may initially be concerned that extracting randomness from such sources is somehow circular or vacuous: We are assuming uniform random bits are used to sample the source, and our goal then is to "undo" the sampling and get uniform random bits back. The point is that this class of sources is just a model for physical sources. This is motivated by the following postulate about the universe: A physical source of randomness is generated by an efficient process in nature, so it is reasonable to model the source as being sampled by an efficient algorithm.

Trevisan and Vadhan constructed extractors for the class of sources samplable by general *time-bounded* algorithms, but their constructions are conditional on standard complexity-theoretic conjectures. It is common in other areas of research, such as proving lower bounds and constructing pseudorandom generators, that proving unconditional limits on the power of time-bounded algorithms is beyond the reach of current techniques. Thus we consider more restricted types of algorithms, such as small-space algorithms and bounded-depth circuits, which are combinatorially simple enough for us to prove unconditional results. Hence it is natural to try to construct unconditional deterministic extractors for sources samplable by such restricted algorithms. Kamp et al. [KRVZ11] succeeded in doing so for small-space samplers.

However, it is an open problem to construct an unconditional deterministic extractor for sources samplable by polynomial-size constant-depth circuits with unbounded fan-in gates (even for depth two circuits). A basic obstacle is that this requires that input-output pairs of the extractor cannot be sampled by such circuits, and it is not even known how to construct an explicit function with the latter property. For example, although the parity function is known not to have subexponential-size constant-depth circuits [Yao85, Hås86], input-output pairs can be sampled very efficiently: Just take uniformly random bits $x_1, \ldots, x_n$ and output $x_1, x_1 \oplus x_2, x_2 \oplus x_3, \ldots, x_{n-1} \oplus x_n, x_n$.

Our goal in this paper is to expand the frontier of unconditional deterministic randomness extraction for sources with low-complexity samplers. We succeed in constructing extractors for sources samplable by small-depth circuits with *bounded* fan-in gates, which corresponds to the class NC^0. This is equivalent to requiring that each output bit of the sampler only depends on a small number of input bits. We call such sources *locally samplable*.

1.1 Results

We first give the formal definitions of extractors and locally samplable sources.

A distribution on a finite set S is said to have *min-entropy* at least k if each element of S occurs with probability at most 2^{-k}. The *statistical distance* between two distributions D_1 and D_2 on a finite set S is defined to be $\|D_1 - D_2\| = \max_{T \subseteq S} \left| \Pr_{D_1}[T] - \Pr_{D_2}[T] \right|$. If $\|D_1 - D_2\| \leq \epsilon$ then we also say D_1 and D_2 are ϵ-close. If $f : S \to S'$ and D is a distribution on S, then we let $f(D)$ denote the distribution on S' obtained by drawing a sample from D and applying f to it. When we mention a distribution multiple times in an expression, all instantiations refer to a single sample from the distribution; for example, $\big(D, f(D)\big)$ denotes the distribution obtained by sampling $w \sim D$ and outputting the pair $\big(w, f(w)\big)$. We use U_n to denote the uniform distribution on $\{0,1\}^n$. If $\mathcal{C}$ is a class of distributions on $\{0,1\}^n$, then a function $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ is called a (k, ϵ)-*extractor for* $\mathcal{C}$ if for every distribution $D \in \mathcal{C}$ with min-entropy at least k, $\big\|\mathrm{Ext}(D) - U_m\big\| \leq$

ϵ. Informally, when we say an extractor is *explicit* we mean that a uniform polynomial-time deterministic algorithm with the desired behavior is exhibited.

We define a *d-local sampler* to be a function $f : \{0,1\}^r \to \{0,1\}^n$ such that each output bit depends on at most d input bits. In other words, for every $j \in \{1,\ldots,n\}$ there exists a subset $I_j \subseteq \{1,\ldots,r\}$ with $|I_j| \le d$ and a function $f_j : \{0,1\}^{|I_j|} \to \{0,1\}$ such that the j^{th} output bit of f is obtained by evaluating f_j on the input bits indexed by I_j. The output distribution of the sampler is $f(U_r)$. We say a distribution D on $\{0,1\}^n$ is a *d-local source* if there exists a d-local sampler (with any input length r) whose output distribution is D.

Our three main theorems are as follows.

Theorem 1. *For every constant $\gamma > 0$ there exists a constant $\beta > 0$ such that there exists an explicit (k,ϵ)-extractor for the class of d-local sources with output length $m = k^2/8nd$ and error $\epsilon = 2^{-n^\beta}$, provided $k \ge n^{2/3+\gamma}$ and $d \le \beta \log n$.*

Theorem 2. *For every constant $\gamma > 0$ there exists a constant $\beta > 0$ such that there exists an explicit (k,ϵ)-extractor for the class of 1-local sources with output length $m = k - o(k)$ and error $\epsilon = 2^{-n^\beta}$, provided $k \ge n^{1/2+\gamma}$.*

Theorem 3. *There exists a universal constant $\beta > 0$ and an explicit function $F : \{0,1\}^n \to \{0,1\}$ such that for every d-local source D on $\{0,1\}^{n+1}$ with $d \le \beta \log n$, $\big\|D - \big(U_n, F(U_n)\big)\big\| \ge 1/2 - 2^{-n^\beta}$.*

1.2 Techniques

We now discuss the techniques we use to prove these three theorems. The proof of Theorem 1 has three steps.

The first step is to construct a certain extractor for 1-local sources (which in particular yields Theorem 2). To do this, we observe that extractors for so-called low-weight affine sources also work for 1-local sources. Then we construct an extractor for low-weight affine sources, building on and improving Rao's extractor from [Rao09b]. While Rao's extractor handles affine sources of min-entropy at least k and weight at most k^γ for some constant $\gamma > 0$, our improvement handles sources with weight at most $k^{1-\gamma}$ for *any* constant $\gamma > 0$. The key ingredient in our improvement is the strong condenser of Guruswami, Umans, and Vadhan [GUV09]. We present this step in Section 3.

The second step is to show that extractors for 1-local sources also work for $o(\log n)$-local sources. To do this, we relate the problem to a concept we call *superindependent matchings* in bipartite graphs, and we prove a combinatorial lemma about the existence of such matchings. We present this step in Section 4.

The third step is to increase the output length of the extractor using the technique of "obtaining an independent seed" introduced by Gabizon et al. [GRS06] (see also [Sha08]). Combining step 1 and step 2 yields an extractor with output length $\Omega(k^2/nd^3 2^d)$. To increase the output length to $\Omega(k^2/nd)$, we adapt the technique from [GRS06]. A key ingredient in our argument is a lemma due to Vadhan [Vad04], which is a strengthened version of a classic lemma due to Nisan and Zuckerman [NZ96]. While the result of [GRS06] achieves output length $k - o(k)$ for bit-fixing sources, we lose a factor of $\Omega(k/n)$ in the output length due to the use of Vadhan's lemma, and we lose another factor of $\Omega(1/d)$ since conditioning on p bits of the output of a d-local sampler could cause a loss of pd bits of min-entropy. We present this step in Section 5.

Viola [Vio10] proved a version of Theorem 3 where the statistical distance lower bound is only $1/2 - O(1/\log n)$, and the d-local sampler is restricted to use at most $n + n^{1-\delta}$ random bits for any constant $\delta > 0$. His function F is what he calls "majority mod p". Using a different function F (namely, any bit of the extractor underlying Theorem 1), we simultaneously improve the lower bound to $1/2 - 2^{-n^{\Omega(1)}}$ and eliminate the restriction on the number of random bits. Our proof of Theorem 3 uses ideas similar to Viola's, but is actually somewhat simpler given the extraction property of F. In [Vio10], Viola also showed that for symmetric functions F, one cannot hope to get such a strong lower bound for samplers that are polynomial-size constant-depth circuits. Our extractor function F is not symmetric, so in a sense we break this barrier. We present the proof of Theorem 3 in Section 6.

We also mention in passing that Lovett and Viola [LV11] exhibited an explicit distribution on $\{0,1\}^n$ that cannot be sampled within statistical distance $1 - 1/n^{o(1)}$ by polynomial-size constant-depth circuits, namely the uniform distribution over the codewords of any asymptotically good error-correcting code. However, this distribution is not of the same form as sampling input-output pairs.

1.3 Previous Work on the Power of Locally Computable Functions

There has been a substantial amount of work on whether various cryptographic and complexity-theoretic objects can be computed locally. Several works [DM04, Lu04, Vad04, Zim10, DT09] have studied the problem of constructing locally computable seeded extractors (that is, the extractor itself is locally computable, as opposed to our setting where the sampler for the source is locally computable). A variety of works [CM01, MST06, AIK06, AIK08, IKOS08, App11] have given positive and negative results on the existence of locally computable pseudorandom generators. Several works [Hås87, Gol00, CEMT09, BQ09] have studied the possibility of locally computable one-way functions. Goldwasser et al. [GGH+07] gave positive and negative results on interactive proof systems with locally computable verifiers. Arora et al. [ASW09] show that the adjacency list of certain logarithmic-degree expander graphs can be computed with constant locality, and they ask whether the same holds for constant-degree expander graphs.

2 Preliminaries

In this paper we work with bipartite graphs $G = (L, R, E)$, where L, R are disjoint finite sets (the left and right nodes) and E is a set of unordered pairs where one element comes from L and the other from R. The distance between two nodes is the number of edges on a shortest path between them.

To every function $f : \{0,1\}^r \to \{0,1\}^n$ we associate a bipartite graph $G = (L, R, E)$ where $L = \{1, \ldots, r\} \times \{\text{in}\}$, $R = \{1, \ldots, n\} \times \{\text{out}\}$, and $\big\{(i, \text{in}), (j, \text{out})\big\} \in E$ if and only if the j^{th} output bit of f depends on the i^{th} input bit of f (that is, for some setting of all input bits except the i^{th}, the j^{th} output bit equals the i^{th} input bit or its complement). Note that we include no extraneous edges, and the graph is unique. We use $I_j \times \{\text{in}\}$ to denote the set of neighbors of (j, out) and $J_i \times \{\text{out}\}$ to denote the set of neighbors of (i, in). Observe that if $f(U_r)$ has min-entropy at least k, then there are at least k non-isolated nodes in L, and in particular $r \geq k$.

We say f is a *d-local sampler* each node in R has degree at most d, and we say a distribution on $\{0,1\}^n$ is a *d-local source* if it equals $f(U_r)$ for some d-local sampler f (with any input length

r). We say f is a (d,c)-*local sampler* if each node in R has degree at most d and each node in L has degree at most c, and we say a distribution on $\{0,1\}^n$ is a (d,c)-*local source* if it equals $f(U_r)$ for some (d,c)-local sampler f (with any input length r).

Suppose Y is a finite set of indices, $(p_y)_{y\in Y}$ is a distribution on Y, and for each $y \in Y$, D_y is a distribution on a finite set S. Then the *convex combination* $\sum_{y\in Y} p_y D_y$ is defined to be the distribution on S obtained by sampling y according to $(p_y)_{y\in Y}$ and then outputting a sample from D_y.

Lemma 1. *Suppose Ext* $: \{0,1\}^n \to \{0,1\}^m$ *is any function and* $D = \sum_{y\in Y} p_y D_y$ *is a distribution on* $\{0,1\}^n$*. Then for every* $\epsilon \geq 0$*,*

$$\big\|Ext(D) - U_m\big\| \;\leq\; \epsilon + \Pr_{y\sim(p_y)_{y\in Y}}\Big[\big\|Ext(D_y) - U_m\big\| > \epsilon\Big].$$

Proof. First, observe that $\text{Ext}(D) = \sum_{y\in Y} p_y \text{Ext}(D_y)$. Now for every $T \subseteq \{0,1\}^n$ we have

$$\begin{aligned}
&\big|\Pr_{\text{Ext}(D)}[T] - \Pr_{U_m}[T]\big| \\
=\;& \Big|\textstyle\sum_{y\in Y} p_y\big(\Pr_{\text{Ext}(D_y)}[T] - \Pr_{U_m}[T]\big)\Big| \\
\leq\;& \textstyle\sum_{y\in Y} p_y\big|\Pr_{\text{Ext}(D_y)}[T] - \Pr_{U_m}[T]\big| \\
\leq\;& \epsilon\cdot\Pr_{y\sim(p_y)_{y\in Y}}\Big[\big|\Pr_{\text{Ext}(D_y)}[T] - \Pr_{U_m}[T]\big| \leq \epsilon\Big] + 1\cdot\Pr_{y\sim(p_y)_{y\in Y}}\Big[\big\|\text{Ext}(D_y) - U_m\big\| > \epsilon\Big] \\
\leq\;& \epsilon + \Pr_{y\sim(p_y)_{y\in Y}}\Big[\big\|\text{Ext}(D_y) - U_m\big\| > \epsilon\Big]
\end{aligned}$$

which gives the desired bound on $\big\|\text{Ext}(D) - U_m\big\|$. □

Corollary 1. *Suppose every distribution in* $\mathcal{C}$ *with min-entropy at least* k *can be written as a convex combination* $\sum_{y\in Y} p_y D_y$ *where* $\Pr_{y\sim(p_y)_{y\in Y}}\big[D_y$ *is in* $\mathcal{C}'$ *and has min-entropy at least* $k'\big] \geq 1-\delta$*. Then every* (k',ϵ')*-extractor for* $\mathcal{C}'$ *is also a* (k,ϵ)*-extractor for* $\mathcal{C}$ *where* $\epsilon = \epsilon' + \delta$*.*

Corollary 2. *Suppose every distribution in* $\mathcal{C}$ *with min-entropy at least* k *is a convex combination of distributions in* $\mathcal{C}'$ *with min-entropy at least* k'*. Then every* (k',ϵ)*-extractor for* $\mathcal{C}'$ *is also a* (k,ϵ)*-extractor for* $\mathcal{C}$*.*

Lemma 2. *Every* d*-local source with min-entropy at least* k *is a convex combination of* (d,c)*-local sources with min-entropy at least* $k - nd/c$*.*

Proof. Consider an arbitrary d-local sampler $f : \{0,1\}^r \to \{0,1\}^n$ whose output distribution has min-entropy at least k, and let $G = (L,R,E)$ be the associated bipartite graph. Since $|E| \leq nd$, there are at most nd/c nodes in L with degree greater than c; without loss of generality these nodes are $\{r-\ell+1,\ldots,r\}\times\{\text{in}\}$ for some $\ell \leq nd/c$. For each string $y \in \{0,1\}^\ell$, define $f_y : \{0,1\}^{r-\ell} \to \{0,1\}^n$ as $f_y(x) = f(x,y)$ (hardwiring the last ℓ bits to y). Then $f(U_r) = \sum_{y\in\{0,1\}^\ell} \frac{1}{2^\ell} f_y(U_{r-\ell})$. Moreover, each $f_y(U_{r-\ell})$ is a (d,c)-local source with min-entropy at least $k - nd/c$, since if some $z \in \{0,1\}^n$ and $y^* \in \{0,1\}^\ell$ satisfied $\Pr_{x\sim U_{r-\ell}}\big[f_{y^*}(x) = z\big] > 1/2^{k-nd/c}$ then we would have

$$\Pr_{x\sim U_{r-\ell},y\sim U_\ell}\big[f(x,y)=z\big] \;\geq\; \Pr_{y\sim U_\ell}[y=y^*]\cdot\Pr_{x\sim U_{r-\ell}}\big[f(x,y^*)=z\big] \;>\; \tfrac{1}{2^\ell}\cdot\tfrac{1}{2^{k-nd/c}} \;\geq\; 1/2^k$$

contradicting that $f(U_r)$ has min-entropy at least k. □

In this paper we also make use of seeded extractors. A function $\mathrm{SExt} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ is called a *seeded* (k, ϵ)*-extractor* if for every distribution D on $\{0,1\}^n$ with min-entropy at least k, $\big\|\mathrm{SExt}(D, U_t) - U_m\big\| \leq \epsilon$ where U_t is independent of D. We say SExt is a *strong seeded* (k, ϵ)*-extractor* if for every distribution D on $\{0,1\}^n$ with min-entropy at least k, $\big\|\big(U_t, \mathrm{SExt}(D, U_t)\big) - U_{t+m}\big\| \leq \epsilon$. We say SExt is *linear* if for every seed $\tau \in \{0,1\}^t$, the function $\mathrm{SExt}(\cdot, \tau) : \{0,1\}^n \to \{0,1\}^m$ is linear over $\mathbb{F}_2$, where $\mathbb{F}_q$ denotes the finite field of size q.

If $z \in \{0,1\}^n$ and $J \subseteq \{1, \ldots, n\}$, then we let $z|_J \in \{0,1\}^{|J|}$ denote the substring of z indexed by the coordinates in J. If D is a distribution on $\{0,1\}^n$ and $J \subseteq \{1, \ldots, n\}$, then we let $D|_J$ denote the marginal distribution on the coordinates in J.

Finally, all logarithms in this paper are base 2.

3 1-Local Sources

An *affine source* is a distribution on $\{0,1\}^n$ which is uniform over an affine subspace (where $\{0,1\}^n$ is viewed as a vector space over $\mathbb{F}_2$). If the subspace has dimension k then it has size 2^k and hence the source has min-entropy k. The distribution can be sampled by picking $x_1, \ldots, x_k \in \{0,1\}$ uniformly at random and outputting $z_0 + x_1 z_1 + \cdots + x_k z_k$ where $z_0 \in \{0,1\}^n$ is a shift vector and $z_1, \ldots, z_k \in \{0,1\}^k$ are a basis of the associated linear subspace. The source is said to be a *weight-*c *affine source* if there are some basis vectors $z_1, \ldots, z_k$ each of which has Hamming weight at most c.

Observation 1. *Every* $(1, c)$*-local source is also a weight-*c *affine source.*

Proof. Consider an arbitrary $(1, c)$-local sampler $f : \{0,1\}^k \to \{0,1\}^n$ and assume without loss of generality that there are no isolated nodes on the left side of the associated bipartite graph. For each $i \in \{1, \ldots, k\}$, let $J_i \times \{\mathrm{out}\}$ be the set of neighbors of (i, in), and let $1_{J_i} \in \{0,1\}^n$ be the characteristic vector of this set. For each $i \in \{1, \ldots, k\}$ we have $|J_i| \leq c$ and hence 1_{J_i} has Hamming weight at most c (since f is a $(1, c)$-local sampler). It is straightforward to verify that the output distribution of f is sampled by picking $x_1, \ldots, x_k \in \{0,1\}$ uniformly at random and outputting $f(0^k) + x_1 1_{J_1} + \cdots + x_k 1_{J_k}$. Moreover, the vectors 1_{J_i} are linearly independent. ☐

Rao [Rao09b] (building on [Rao09a]) constructed extractors for low-weight affine sources.

Theorem 4 ([Rao09b]). *There exist universal constants* $C, \gamma > 0$ *such that for all* $k \geq \log^C n$ *there exists an explicit* $(k, 2^{-k^{\Omega(1)}})$*-extractor with output length* $m = k - o(k)$ *for the class of weight-*k^γ *affine (and in particular,* $(1, k^\gamma)$*-local) sources.*

We improve Rao's result to obtain the following theorem.

Theorem 5. *There exists a universal constant* $C > 0$ *such that for any constant* $\gamma > 0$ *and all* $k \geq \log^{C/\gamma} n$ *there exists an explicit* $(k, 2^{-k^{\Omega(1)}})$*-extractor with output length* $m = k - o(k)$ *for the class of weight-*$k^{1-\gamma}$ *affine (and in particular,* $(1, k^{1-\gamma})$*-local) sources.*

We now explain how Theorem 2 follows from Theorem 5, Lemma 2, and Corollary 2. We first note the following immediate corollary of Theorem 5.

Corollary 3. *For every constant* $\gamma > 0$ *there exists a constant* $\beta > 0$ *such that for all* $k \geq n^{1/2+\gamma}$ *there exists an explicit* $(k, 2^{-n^\beta})$*-extractor with output length* $m = k - o(k)$ *for the class of weight-*$n^{1/2}$ *affine (and in particular,* $(1, n^{1/2})$*-local) sources.*

Lemma 2 implies that every 1-local source with min-entropy at least $k \geq n^{1/2+\gamma}$ is a convex combination of $(1, n^{1/2})$-local sources with min-entropy at least $k - n^{1/2} \geq k - o(k)$. Theorem 2 then follows from Corollary 2 and Corollary 3.

Bourgain [Bou07], Yehudayoff [Yeh10], and Li [Li11b] constructed extractors for linear min-entropy affine sources (of arbitrary weight), achieving better error but worse output length than Theorem 5.

Theorem 6 ([Bou07]). *For every constant $\delta > 0$ there exists an explicit $(\delta n, 2^{-\Omega(n)})$-extractor with output length $m = \Omega(n)$ for the class of affine (and in particular, 1-local) sources.*

Theorem 6 can be used to improve the error in Theorem 1 and Theorem 2 when $k \geq \Omega(n)$ and $d \leq O(1)$. We omit the details, so as to avoid having a laundry list of results.

We now describe the proof of Theorem 5. To do this, we need a construction of linear strong seeded extractors with good seed length, which we present in Section 3.1. Then in Section 3.2 we derive Theorem 5.

3.1 A Strong Linear Extractor with Seed Length $\log n + O(\log(k/\epsilon))$

In this section we construct a linear strong seeded extractor $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with $m = k^{0.99}$ and seed length $t = \log n + O(\log(k/\epsilon))$. It is very important to us that the seed length here has $\log n$ and not $O(\log n)$. We also note that without the linearity property, these objects are explicitly constructed and stated in [GUV09, Theorem 4.19]. However, we construct such objects with the linearity property by using a construction from [GUV09] and then bootstrapping it with other known constructions. To do this, we first define and construct objects called strong linear condensers.

3.1.1 Construction of a Strong Linear Condenser

We first define strong condensers.

Definition 1. *A map $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ is a* strong $k \to_\epsilon k'$ condenser *if for every distribution X with min-entropy at least k,*

$$\Pr_{y \in U_t}\left[C(X,y) \text{ is } \epsilon\text{-close to a distribution with min-entropy at least } k'\right] \;\geq\; 1 - \epsilon.$$

Recall that we say C is *linear* if for every $y \in \{0,1\}^t$, the function $C(\cdot, y) : \{0,1\}^n \to \{0,1\}^m$ is linear over $\mathbb{F}_2$.

We now describe the construction of the strong linear condenser. The construction is the same as one of the constructions in [GUV09]. However, we need to argue about its linearity as well as the parameters. Hence, we state their construction and result here. To do this, consider a finite field $\mathbb{F}_q$ for some $q = 2^t$. Let ζ be a generator of the multiplicative group $\mathbb{F}_q^*$. Then the map $C : \mathbb{F}_q^{n'} \times \mathbb{F}_q \to \mathbb{F}_q^{m'}$ is as follows.

> Given $f = (f_0, \ldots, f_{n'-1}) \in \mathbb{F}_q^{n'}$, we interpret it as a polynomial $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $f : x \mapsto \sum_{0 \leq i < n'} f_i x^i$. We now describe C as $C : (f, y) \mapsto \big(f(y), f(\zeta y), \ldots, f(\zeta^{m'-1} y)\big)$.

Observation 2. *The map $C(\cdot, y) : f \mapsto C(f, y)$ is $\mathbb{F}_q$-linear.*

Observation 3. *For $q = 2^t$, there is an isomorphism ϕ between $(\mathbb{F}_q, +)$ and $(\mathbb{F}_2^t, \oplus)$. Further, this isomorphism is computable in time polynomial in t.*

The above two observations can be used to interpret C as a polynomial time computable map $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$. Here $n = n' \cdot t$ and $m = m' \cdot t$. Further, the map C is $\mathbb{F}_2$-linear, and it is polynomial time computable since a generator of $\mathbb{F}_q^*$ can be computed in time polynomial in $\log q$ [Sho88]. We now state the following theorem [GUV09, Theorem 6.2], which says that C is a strong condenser.

Theorem 7 ([GUV09]). *For every $n \in \mathbb{N}$, $\ell \leq n$ such that 2^ℓ is an integer, and for every $\alpha, \epsilon > 0$, the function $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ as defined above is a*

$$(1 + 1/\alpha)\ell d + \log(1/\epsilon) \to_{3\epsilon} \ell d + t - 2 \textit{ strong condenser}$$

with $t \leq (1 + (1/\alpha))d$ and $m \leq (1 + 1/\alpha)\ell d$ where $d = \lceil \alpha \log(4n\ell/\epsilon) \rceil$, provided $\ell d \geq \log(1/\epsilon)$.

The following important corollary follows by setting parameters correctly in the result. Let $k \geq C \log^2 n$ for some large $C > 0$, and set the parameters as follows.

- $\epsilon = 1/100$
- $\alpha = (\log k)/(100 \log n)$
- $\ell = k/(100 \log n)$

This implies the following.

- $d = \left\lceil \frac{(\log k)(\log n + \log k - \log\log n + O(1))}{100 \log n} \right\rceil = \frac{(\log k)(\log n + \log k - \log\log n)(1+o(1))}{(100 \log n)}$
- $t \leq (\log n + \log k - \log\log n)(1 + (2 \log k / \log n)) \leq \log n + 5 \log k$
- $M \leq \frac{k}{100 \log n} \cdot (\log n + 5 \log k) + t \leq k$
- $\ell d \geq (k \log k)/(10^4 \log n) \geq \sqrt{k}$

Hence, we now get the following corollary.

Corollary 4. *There exists an explicit linear $k \to_{3/100} \sqrt{k}$ strong condenser $C : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with $t \leq \log n + 5 \log k$ and $m \leq k$.*

3.1.2 Combination with Linear Extractors

We now recall that the extractors in [Tre01, RRV02] are also linear. More precisely, the following theorem was proven in [Tre01].

Theorem 8 ([Tre01]). *For every constant $\gamma > 0$ there exists an explicit linear strong seeded $(n^{1/2}, \epsilon)$-extractor $Ext : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with $m = n^{1/2-\gamma}$, $\epsilon = 1/100$, and $t = O(\log n)$.*

We can combine Theorem 8 and Corollary 4 to get the following theorem.

Theorem 9. *There exists a constant c such that for every constant $\gamma > 0$ and every $k \geq c \log^2 n$ there exists an explicit linear strong seeded (k, ϵ)-extractor $Ext : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with $m = k^{1/2-\gamma}$, $\epsilon = 1/50$, and $t = \log n + c \cdot \log k$.*

3.2 Improved Extractors for Low-Weight Affine Sources

In this section we prove Theorem 5. As we have said before, Rao [Rao09b] proves the same kind of theorem except it is weaker in the upper bound on the weight allowed for the affine sources. Our extractor construction uses exactly the same steps as [Rao09b], except the components used in our construction are tailor made for our purposes thus helping us achieve better parameters.

In order to describe the better extractors, we first recall the following linear error-correcting code construction (BCH code) [Sud].

Theorem 10. *For every $d \leq n$ there exists a polynomial time computable parity check function $P : \mathbb{F}_2^n \to \mathbb{F}_2^t$ for a linear code with distance at least d, such that $t = O(d \log n)$.*

We now recall the following claim from [Rao09b].

Claim 1. *Let $P : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be a parity check function for a linear code with distance d. Let X be any weight-w affine source with min-entropy at least d/w. Then $P(X)$ is an affine source with min-entropy at least d/w. Also, the min-entropy of $P(X)$ is at most t.*

By combining Theorem 10 and Claim 1, we get the following lemma.

Lemma 3. *For every constant $\gamma > 0$ and every k there exists a polynomial time computable linear function $P : \mathbb{F}_2^n \to \mathbb{F}_2^{m'}$ with $m' = O(k^{1-\gamma/2} \cdot \log n)$ such that if X is a weight-$k^{1-\gamma}$ affine source with min-entropy at least k, then the min-entropy of $P(X)$ is at least $k^{\gamma/2}$ and at most m'.*

Now let $\text{Ext}_1 : \{0,1\}^{m'} \times \{0,1\}^{t_1} \to \{0,1\}^{m''}$ be the seeded extractor from Theorem 9 with $m' = O(k^{1-\gamma/2} \cdot \log n)$ and $t_1 = \log m' + (\gamma/4) \log k + O(1)$ and $m'' = k^{\gamma/4c}$, where c is the constant from Theorem 9. In Figure 1 we present the routine LOW-CONVERT, which was defined and analyzed in [Rao09b, Lemma 4.3]. We note that the only properties of LOW-CONVERT used in the analysis in [Rao09b] are that P and Ext_1 are linear and that Ext is a strong seeded extractor with error $\leq 1/2$. To state the result, it is convenient to define the concept of an affine somewhere random source.

Definition 2. *A distribution X on $\{0,1\}^{\ell \times \ell'}$ is said to be an* affine somewhere random source *if X is an affine source and for some $1 \leq i \leq \ell$, the i^{th} row of X is uniformly random.*

Lemma 4. *For m', t_1, and m'' as specified above, if X is a weight-$k^{1-\gamma}$ affine source with min-entropy at least k, then $LC(X)$ is a $2^{t_1} \times m''$ affine somewhere random source.*

In order to define the next routine, we recall an extractor construction from [RRV02] for a particular setting of parameters.

Theorem 11 ([RRV02]). *There is an explicit linear strong seeded (k, ϵ)-extractor $Ext_2 : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with $t = O(\log^3(n/\epsilon))$ and $m = k - O(\log^3(n/\epsilon))$.*

In Figure 2 we present the routine AFFINE-CONVERT from [Rao09b]. The following lemma was proven in [Rao09b, Theorem 4.5]. Again, we note that the only thing that is used in the analysis of AFFINE-CONVERT is that Ext_2 is a linear strong seeded extractor.

Theorem 12. *Let c be the constant from from Theorem 9. For any constant $\gamma > 0$, if X is a weight-$k^{1-\gamma}$ affine source with min-entropy at least $k \geq \log^{10c/\gamma} n$, then $AC(x)$ is $2^{-k^{\Omega(1)}}$-close to a convex combination of somewhere random affine sources of size $2^{t_1} \times m_1$, where $m_1 = k - o(k)$.*

LOW-CONVERT(X)

Input: $x \in \{0,1\}^n$
Output: $z \in \{0,1\}^{2^{t_1} \times m''}$

Subroutines used: $P : \{0,1\}^n \to \{0,1\}^{m'}$ defined in Claim 1, and $\mathrm{Ext}_1 : \{0,1\}^{m'} \times \{0,1\}^{t_1} \to \{0,1\}^{m''}$ from Theorem 9. Here $m' = O(k^{1-\gamma/2} \cdot \log n)$, $t_1 = \log m' + (\gamma/4)\log k + O(1)$, and $m'' = k^{\gamma/4c}$.

For $1 \le i \le 2^{t_1}$, the i^{th} row of the output is defined by $LC(x,i) = \mathrm{Ext}_1(P(x), i)$.

Figure 1: LOW-CONVERT

AFFINE-CONVERT(X)

Input: $x \in \{0,1\}^n$
Output: $z \in \{0,1\}^{2^{t_1} \times m_1}$

Subroutines used: $LC : \{0,1\}^n \to \{0,1\}^{2^{t_1} \times m''}$ defined in Lemma 4, and $\mathrm{Ext}_2 : \{0,1\}^n \times \{0,1\}^{t_2} \to \{0,1\}^{m_1}$ from Theorem 11 with $t_2 = m''$.

For $1 \le i \le 2^{t_1}$, the i^{th} row of the output is defined by $AC(x,i) = \mathrm{Ext}_2(x, LC(X)_i)$.

Figure 2: AFFINE-CONVERT

The important thing about the above theorem is that the output of $AC(x)$ is a convex combination of somewhere random affine sources. More importantly, the number of rows is $2^{t_1} = O(m' \cdot k^{\gamma/4}) = O(k^{1-\gamma/4} \log n)$. Assuming $k \ge \log^{10c/\gamma} n$ (as in Theorem 12), we get that that the number of rows is $2^{t_1} \le k^{1-5\gamma/6} \ll k$. At this point, we can apply the routine AFFINE-SREXT from [Rao09b]. More precisely, we have the following [Rao09b, Theorem 3.1].

Theorem 13 ([Rao09b]). *For any constant $\gamma > 0$ there is an explicit function $A : \{0,1\}^{k^{1-\gamma} \times k} \to \{0,1\}^m$ such that if X is a somewhere random affine source of size $k^{1-\gamma} \times k$, then $A(X)$ is $2^{-k^{\Omega(1)}}$-close to U_m, where $m = k - o(k)$.*

Remark 1. *We note that Theorem 3.1 in [Rao09b] discusses somewhere random affine sources of size $k^{0.7} \times k$. However, it is straightforward to see that the result just requires the number of rows in the somewhere random affine source to be polynomially smaller than the length of each row.*

We can now combine Theorem 12 and Theorem 13 to get Theorem 5.

4 d-Local Sources

The following theorem shows that to get extractors for d-local sources, it suffices to construct extractors for 1-local sources.

Theorem 14. *Every (k', ϵ')-extractor for $(1, 2nd/k)$-local sources is also a (k, ϵ)-extractor for d-local sources, where $k' = k^2/4nd^3 2^d$ and $\epsilon = \epsilon' + e^{-k'/4}$.*

Assuming $k \geq n^{2/3+\gamma}$ (for constant $\gamma > 0$) and $d \leq \beta \log n$ (for small enough constant $\beta > 0$) in Theorem 14, we find that it suffices to have a (k', ϵ')-extractor for $(1, c)$-local sources where $k' \geq n^{1/3+\gamma}$ and $c = 2nd/k \leq n^{1/3} \leq (k')^{1-\gamma}$. Such an extractor is given by Theorem 5, with error $\epsilon' = 2^{-n^{\Omega(1)}}$ (and thus $\epsilon = \epsilon' + e^{-k'/4} \leq 2^{-n^{\Omega(1)}}$). This already yields a version of Theorem 1 with output length $k' - o(k') = \Omega(k^2/nd^3 2^d)$.

As a corollary to Theorem 14, we also find that if we could construct an explicit extractor for 1-local sources with min-entropy at least n^γ for arbitrarily small constants $\gamma > 0$ (with output length $m \geq 1$ and error $\epsilon \leq 1/2$, say) then we would get explicit extractors for $o(\log n)$-local sources with min-entropy at least $n^{1/2+\gamma}$ for arbitrarily small constants $\gamma > 0$. This $n^{1/2}$ min-entropy barrier is common in extractor constructions.

4.1 Superindependent Matchings

We first prove a combinatorial lemma that is needed for the proof of Theorem 14.

Definition 3. *Given a bipartite graph $G = (L, R, E)$, we say a set of edges $M \subseteq E$ is a* superindependent matching *if there is no path of length at most two in G from an endpoint of an edge in M to an endpoint of a different edge in M.*

Lemma 5. *Suppose $G = (L, R, E)$ is a bipartite graph with no isolated nodes and such that each node in L has degree at most c and each node in R has degree at most d. Then G has a superindependent matching of size at least $|L|/d^2c$.*

Proof. Let M be a largest superindependent matching in G, and suppose for contradiction that $|M| < |L|/d^2c$. Note that for each node in R, the number of nodes in L within distance three in G is at most $d(1 + c(d-1)) \leq d^2c$. Thus the number of nodes in L within distance three of the right endpoints of edges in M is at most $|M| \cdot d^2c < |L|$. Hence there exists a node $u \in L$ at distance greater than three from the right endpoint of every edge in M. Since G has no isolated nodes, there exists a node $v \in R$ such that $\{u, v\} \in E$. Note that there is no path of length at most two from either u or v to an endpoint of an edge in M, since otherwise a simple case analysis would show that u is within distance three of the right endpoint of an edge in M. Thus $M \cup \{\{u, v\}\}$ is a superindependent matching, contradicting the maximality of M. □

4.2 Proof of Theorem 14

Suppose $\text{Ext} : \{0,1\}^n \to \{0,1\}^m$ is a (k', ϵ')-extractor for $(1, 2nd/k)$-local sources. By Corollary 2 and Lemma 2 it suffices to show that Ext is a $(k/2, \epsilon)$-extractor for (d, c)-local sources where $c = 2nd/k$. The plan is to show that every (d, c)-local source with min-entropy at least $k/2$ is a convex combination of $(1, c)$-local sources most of which have min-entropy at least k', and then apply Corollary 1.

So consider an arbitrary (d, c)-local sampler $f : \{0,1\}^r \to \{0,1\}^n$ whose output distribution has min-entropy at least $k/2$, and let $G = (L, R, E)$ be the associated bipartite graph. If we obtain $\widetilde{G}$ from G by removing any isolated nodes, then $\widetilde{G}$ still has at least $k/2$ nodes on its left side. Applying Lemma 5 to $\widetilde{G}$ tells us that G has a superindependent matching M of size at least

$k/(2d^2c)$. Let $\ell = |M|$, and without loss of generality assume that the left endpoints of M are $L' = \{1, \ldots, \ell\} \times \{\text{in}\}$. We write inputs to f as (x, y) where $x \in \{0,1\}^\ell$ and $y \in \{0,1\}^{r-\ell}$. Since M is superindependent, each node in R is adjacent to at most one node in L'. Thus if we define $f_y : \{0,1\}^\ell \to \{0,1\}^n$ as $f_y(x) = f(x, y)$ (hardwiring the last $r - \ell$ input bits to y) then for each y, f_y is a $(1, c)$-local sampler. Observe that $f(U_r) = \sum_{y \in \{0,1\}^{r-\ell}} \frac{1}{2^{r-\ell}} f_y(U_\ell)$.

Let $G_y = (L', R, E_y)$ denote the bipartite graph associated with f_y. As noted in Observation 1, the min-entropy of $f_y(U_\ell)$ is the number of nodes in L' that are non-isolated in G_y. Although each node in L' is non-isolated in G (since $M \subseteq E$), edges incident to L' may disappear when we hardwire y. We claim that with high probability over y, plenty of nodes in L' are still non-isolated in G_y and hence $f_y(U_\ell)$ has high min-entropy. For $i \in \{1, \ldots, \ell\}$ let $(j_i, \text{out}) \in R$ be the neighbor of (i, in) in M, and let $I_{j_i} \times \{\text{in}\}$ be the set of neighbors of (j_i, out) in G. Since the j_i^{th} output bit of f depends on the i^{th} input bit, there exists a string $w_i \in \{0,1\}^{|I_{j_i}|-1}$ such that hardwiring the input bits corresponding to $I_{j_i} \backslash \{i\}$ to w_i leaves the edge $\big\{(i, \text{in}), (j_i, \text{out})\big\}$ in place, and in particular ensures that (i, in) is non-isolated. Since M is superindependent, the sets I_{j_i} for $i \in \{1, \ldots, \ell\}$ are pairwise disjoint and in particular, each $I_{j_i} \backslash \{i\} \subseteq \{\ell + 1, \ldots, r\}$. We assume the bits of y are indexed starting at $\ell + 1$, so for example $y|_{\{\ell+1\}}$ is the first bit of y. By the disjointness, we find that the events $y|_{I_{j_i} \backslash \{i\}} = w_i$ (for $i \in \{1, \ldots, \ell\}$) are fully independent over $y \sim U_{r-\ell}$. Moreover, each of these events occurs with probability at least $1/2^{d-1}$ since $|w_i| \le d - 1$. Thus we have

$$
\begin{aligned}
& \Pr_{y \sim U_{r-\ell}} \big[f_y(U_\ell) \text{ does not have min-entropy at least } k' \big] \\
= \; & \Pr_{y \sim U_{r-\ell}} \Big[\big| \big\{ i \in \{1, \ldots, \ell\} \;:\; (i, \text{in}) \text{ is non-isolated in } G_y \big\} \big| < k' \Big] \\
\le \; & \Pr_{y \sim U_{r-\ell}} \Big[\big| \big\{ i \in \{1, \ldots, \ell\} \;:\; y|_{I_{j_i} \backslash \{i\}} = w_i \big\} \big| < k' \Big] \\
\le \; & e^{-k/8d^2c2^d}
\end{aligned}
$$

by a standard Chernoff bound.

To summarize, we have shown that every (d, c)-local source with min-entropy at least $k/2$ is a uniform convex combination of $(1, c)$-local sources, at most $e^{-k/8d^2c2^d}$ fraction of which do not have min-entropy at least k'. It now follows from Corollary 1 that Ext is a $(k/2, \epsilon)$-extractor for (d, c)-local sources. This finishes the proof of Theorem 14.

5 Increasing the Output Length

Combining the results from Section 3 and Section 4 yields an extractor for d-local sources with output length $\Omega(k^2/nd^3 2^d)$, provided $d \le o(\log n)$ and the min-entropy k is at least $n^{2/3+\gamma}$. In this section we show how to improve the output length to $\Omega(k^2/nd)$, which is a significant improvement when $k \ge \Omega(n)$ and d is large. We present the general method in Section 5.1, and then we apply the general method to obtain Theorem 1 in Section 5.2.

5.1 The General Method

We now present our general theorem on increasing the output length of extractors for d-local sources (Theorem 15 below), which uses the technique of "obtaining an independent seed". As in [GRS06], the strategy is to take the output of a deterministic extractor and use part of it to sample a set of coordinates of the source, which are then plugged into a seeded extractor, using the other part of

Ingredients:

$\text{Ext}' : \{0,1\}^n \to \{0,1\}^{m'}$

$\text{Ext}'_1 : \{0,1\}^n \to \{0,1\}^s$ is the first s bits of Ext'

$\text{Ext}'_2 : \{0,1\}^n \to \{0,1\}^{m'-s}$ is the last $m'-s$ bits of Ext'

$\text{Samp} : \{0,1\}^s \to \binom{\{1,\dots,n\}}{p}$

$\text{SExt} : \{0,1\}^p \times \{0,1\}^{m'-s} \to \{0,1\}^m$

Result:

$\text{Ext} : \{0,1\}^n \to \{0,1\}^m$ defined as $\text{Ext}(z) = \text{SExt}\big(z|_{\text{Samp}(\text{Ext}'_1(z))}, \text{Ext}'_2(z)\big)$

Figure 3: Increasing the output length of an extractor for d-local sources

the deterministic extractor's output as the seed. A key ingredient (which was not used in [GRS06]) is a fundamental lemma of Nisan and Zuckerman [NZ96], which roughly says that if we sample the coordinates appropriately, then the min-entropy rate of the marginal distribution on those coordinates is almost as high as the min-entropy rate of the whole source.[1] However, the original Nisan-Zuckerman lemma loses a logarithmic factor in the min-entropy rate. We use a strengthened version of the lemma, due to Vadhan [Vad04], which only loses a constant factor.

We use $\binom{\{1,\dots,n\}}{p}$ to denote the set of subsets of $\{1,\dots,n\}$ of size p.

Definition 4. *We say Samp* $: \{0,1\}^s \to \binom{\{1,\dots,n\}}{p}$ *is a* (μ,η)*-sampler if for every* $g : \{1,\dots,n\} \to [0,1]$ *with* $\frac{1}{n}\sum_{j=1}^{n} g(j) \geq \mu$ *it holds that* $\Pr_{\sigma\sim U_s}\left[\frac{1}{p}\sum_{j\in \mathit{Samp}(\sigma)} g(j) < \mu/2\right] \leq \eta$.

Lemma 6 ([Vad04]). *There exists a universal constant* $\alpha > 0$ *such that the following holds. Suppose Samp* $: \{0,1\}^s \to \binom{\{1,\dots,n\}}{p}$ *is a* $\big(k/2n\log(4n/k),\eta\big)$*-sampler and* D *is a distribution on* $\{0,1\}^n$ *with min-entropy at least* k*. Then with probability at least* $1-\sqrt{\eta+2^{-\alpha k}}$ *over* $\sigma\sim U_s$ *it holds that* $D|_{\mathit{Samp}(\sigma)}$ *is* $\sqrt{\eta+2^{-\alpha k}}$*-close to a distribution with min-entropy at least* $pk/4n$*.*

We also need the following lemma from [GRS06], which we state in a slightly nonstandard way for convenience when we apply the lemma.

Lemma 7 ([GRS06]). *Consider any distribution on* $\{0,1\}^{s_1}\times\{0,1\}^{s_2}\times\{0,1\}^{s_3}$ *which is* ϵ'*-close to uniform, and suppose* σ *is in the support of the marginal distribution on the second coordinate. Then the marginal distribution on the first and third coordinates, conditioned on the second coordinate being* σ*, is* $(\epsilon' 2^{s_2+1})$*-close to uniform.*

We now present the general theorem on increasing the output length.

Theorem 15. *Consider the construction in Figure 3, and let* α *be as in Lemma 6. Suppose Ext′ is a* (k',ϵ')*-extractor for* d*-local sources, Samp is a* $\big(k/2n\log(4n/k),\eta\big)$*-sampler, and SExt is a seeded* $(pk/4n,\epsilon'')$*-extractor. Then Ext is a* (k,ϵ)*-extractor for* d*-local sources, where* $k = k'+pd$ *and* $\epsilon = \epsilon'(2^{s+1}+1) + 2\sqrt{\eta+2^{-\alpha k}}+\epsilon''$*.*

Proof. Consider an arbitrary d-local sampler $f : \{0,1\}^r \to \{0,1\}^n$ whose output distribution has min-entropy at least k, and let $G = (L,R,E)$ be the associated bipartite graph. Our goal is to show that $\big\|\text{Ext}\big(f(U_r)\big) - U_m\big\| \leq \epsilon$.

[1] Min-entropy rate just means the min-entropy divided by the length of the source.

Let us call $\sigma \in \{0,1\}^s$ *good* if $f(U_r)|_{\text{Samp}(\sigma)}$ is $\sqrt{\eta + 2^{-\alpha k}}$-close to a distribution with min-entropy at least $pk/4n$, and *bad* otherwise. For each σ we let $U_r^{(\sigma)}$ be the uniform distribution over $w \in \{0,1\}^r$ such that $\text{Ext}'_1\big(f(w)\big) = \sigma$.[2]

Claim 2. *For each good σ, $\big\|Ext\big(f(U_r^{(\sigma)})\big) - U_m\big\| \le \epsilon' 2^{s+1} + \sqrt{\eta + 2^{-\alpha k}} + \epsilon''$.*

Assuming Claim 2, we can prove the theorem as follows. Observe that

$$f(U_r) \;=\; \textstyle\sum_{\sigma \in \{0,1\}^s} \Pr_{w \sim U_r}\big[\text{Ext}'_1\big(f(w)\big) = \sigma\big] f(U_r^{(\sigma)}).$$

Then using the shorthand $\epsilon''' = \epsilon' 2^{s+1} + \sqrt{\eta + 2^{-\alpha k}} + \epsilon''$ we have

$$\begin{aligned}
\big\|\text{Ext}\big(f(U_r)\big) - U_m\big\| \;&\le\; \epsilon''' + \Pr_{w \sim U_r}\Big[\big\|\text{Ext}\big(f(U_r^{(\sigma)})\big) - U_m\big\| > \epsilon''' \text{ where } \sigma = \text{Ext}'_1\big(f(w)\big)\Big] \\
&\le\; \epsilon''' + \Pr_{w \sim U_r}\big[\text{Ext}'_1\big(f(w)\big) \text{ is bad}\big] \\
&\le\; \epsilon''' + \epsilon' + \Pr_{\sigma \sim U_s}[\sigma \text{ is bad}] \\
&\le\; \epsilon''' + \epsilon' + \sqrt{\eta + 2^{-\alpha k}} \\
&=\; \epsilon
\end{aligned}$$

where the first line follows by Lemma 1, the second line follows by Claim 2, the third line follows by $\big\|\text{Ext}'_1\big(f(U_r)\big) - U_s\big\| \le \epsilon'$ (since $f(U_r)$ is a d-local source with min-entropy at least $k \ge k'$), and the fourth line follows by Lemma 6.

It remains to prove Claim 2. Consider an arbitrary fixed good $\sigma \in \{0,1\}^s$, and without loss of generality assume the nodes in L adjacent to $\text{Samp}(\sigma) \times \{\text{out}\}$ are $\{r-\ell+1, \ldots, r\} \times \{\text{in}\}$ for some $\ell \le pd$. For each string $y \in \{0,1\}^\ell$, define $f_y : \{0,1\}^{r-\ell} \to \{0,1\}^n$ as $f_y(x) = f(x,y)$ (hardwiring the last ℓ bits to y). Then each $f_y(U_{r-\ell})$ is a d-local source with min-entropy at least $k - \ell \ge k'$ (see the proof of Lemma 2). Thus, $\big\|\text{Ext}'\big(f_y(U_{r-\ell})\big) - U_{m'}\big\| \le \epsilon'$. Now consider the joint distribution

$$\Big(U_r|_{\{r-\ell+1,\ldots,r\}}, \text{Ext}'_1\big(f(U_r)\big), \text{Ext}'_2\big(f(U_r)\big)\Big).$$

That is, sample $(x,y) \sim U_r$ and output y along with both parts of $\text{Ext}'\big(f(x,y)\big)$. We have just argued that conditioned on the first coordinate of this distribution being any particular $y \in \{0,1\}^\ell$, the marginal distribution of the other two coordinates is ϵ'-close to uniform. Thus the entire distribution is ϵ'-close to uniform. By Lemma 7 (with $s_1 = \ell$, $s_2 = s$, and $s_3 = m' - s$), the joint distribution

$$\Big(U_r^{(\sigma)}|_{\{r-\ell+1,\ldots,r\}}, \text{Ext}'_2\big(f(U_r^{(\sigma)})\big)\Big)$$

is $(\epsilon' 2^{s+1})$-close to the uniform distribution $\big(U_\ell, U_{m'-s}\big)$ where U_ℓ and $U_{m'-s}$ are independent. Let us define $f^{(\sigma)} : \{0,1\}^\ell \to \{0,1\}^p$ by $f^{(\sigma)}(y) = f(x,y)|_{\text{Samp}(\sigma)}$ for any $x \in \{0,1\}^{r-\ell}$ (this value does not depend on x since nodes in $\text{Samp}(\sigma) \times \{\text{out}\}$ are only adjacent to nodes in $\{r-\ell+1, \ldots, r\} \times \{\text{in}\}$). Then we have

$$\text{Ext}\big(f(U_r^{(\sigma)})\big) \;=\; \text{SExt}\Big(f^{(\sigma)}\big(U_r^{(\sigma)}|_{\{r-\ell+1,\ldots,r\}}\big), \text{Ext}'_2\big(f(U_r^{(\sigma)})\big)\Big)$$

and thus

$$\big\|\text{Ext}\big(f(U_r^{(\sigma)})\big) - \text{SExt}\big(f^{(\sigma)}(U_\ell), U_{m'-s}\big)\big\| \;\le\; \epsilon' 2^{s+1}. \tag{1}$$

[2] Formally, we only consider σ's in the support of $\text{Ext}'_1\big(f(U_r)\big)$.

Letting D denote a distribution on $\{0,1\}^p$ with min-entropy at least $pk/4n$ that $f(U_r)|_{\mathrm{Samp}(\sigma)} = f^{(\sigma)}(U_\ell)$ is $\sqrt{\eta + 2^{-\alpha k}}$-close to (such a D exists since σ is good), we have

$$\left\|\mathrm{SExt}\big(f^{(\sigma)}(U_\ell), U_{m'-s}\big) - \mathrm{SExt}\big(D, U_{m'-s}\big)\right\| \;\le\; \sqrt{\eta + 2^{-\alpha k}}. \tag{2}$$

Since SExt is a seeded $(pk/4n, \epsilon'')$-extractor, we have

$$\left\|\mathrm{SExt}\big(D, U_{m'-s}\big) - U_m\right\| \;\le\; \epsilon''. \tag{3}$$

Combining Inequality 1, Inequality 2, and Inequality 3 yields Claim 2. This finishes the proof of Theorem 15. □

5.2 Applying Theorem 15

In order to apply Theorem 15, we need explicit constructions of Ext′, Samp, and SExt. An appropriate construction of Samp is given by the following lemma.

Lemma 8 ([NZ96]). *There exists an explicit (μ,η)-sampler Samp : $\{0,1\}^s \to \binom{\{1,\ldots,n\}}{p}$ with $s = 4\log n \cdot \log\frac{1}{\eta}$, provided $\mu p \ge 64\log\frac{1}{\eta}$ and $\eta < 1/16$.*

The interesting thing about samplers as defined in Definition 4 is that they produce a set of fixed size. (Typically, samplers either produce a multiset of fixed size or a set of random size, and the latter is sufficient for the argument in [GRS06].) Nisan and Zuckerman [NZ96] proved Lemma 8 by partitioning the n coordinates into p blocks, picking one coordinate from each block in an $O(\log\frac{1}{\eta})$-wise independent way, and using the concentration bounds of [SSS95, BR94].[3] Vadhan [Vad04] also constructed a sampler that produces a set of fixed size, and with better seed length for a certain range of parameters. However, his seed length is actually not good enough for our range of parameters.

As for the seeded extractor SExt, plenty of known constructions are good enough for our purpose. For example, we can use the following construction, due to Raz, Reingold, and Vadhan.

Theorem 16 ([RRV99]). *For every $\omega(1) \le k \le n$ and $\epsilon > 0$ there exists an explicit seeded (k,ϵ)-extractor SExt : $\{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with $m = k$ and $t = O\big((\log^2 n + \log\frac{1}{\epsilon})\cdot\log k\big)$.*

At last, we can prove Theorem 1.

Proof of Theorem 1. Assume $k \ge n^{2/3+\gamma}$ and $d \le \beta\log n$ for small enough constant $\beta > 0$. Then for some constant $\beta' > 0$ to be specified shortly, define

- $\epsilon' = 2^{-n^{\beta'}}$
- $k' = k/2$
- $m' = (k')^2/8nd^3 2^d$
- $p = k/2d$

[3] Actually, Nisan and Zuckerman proved a version with slightly different constants and where the sampler only needs to work for boolean functions g, but the proof goes through to yield Lemma 8.

- $\mu = k/2n \log(4n/k)$
- $\eta = 2^{-n^{\beta'/2}}$
- $s = 4 \log n \cdot \log \frac{1}{\eta}$
- $\epsilon'' = 2^{-n^{1/4}}$
- $m = pk/4n$
- $t = m' - s$.

As shown in Section 4 (by combining Theorem 14 with Theorem 5), there exists an explicit (k', ϵ')-extractor $\mathrm{Ext}' : \{0,1\}^n \to \{0,1\}^{m'}$ for d-local sources, provided β' is small enough. By Lemma 8 there exists an explicit (μ, η)-sampler $\mathrm{Samp} : \{0,1\}^s \to \binom{\{1,\ldots,n\}}{p}$. Since $t \geq \omega\big((\log^2 p + \log \frac{1}{\epsilon''}) \cdot \log m\big)$, by Theorem 16 there exists an explicit seeded (m, ϵ'')-extractor $\mathrm{SExt} : \{0,1\}^p \times \{0,1\}^t \to \{0,1\}^m$. Thus by Theorem 15, Ext is a (k, ϵ)-extractor for d-local sources, where $\epsilon = \epsilon'(2^{s+1} + 1) + 2\sqrt{\eta + 2^{-\alpha k}} + \epsilon'' \leq 2^{-n^{\beta}}$ provided β is small enough. □

6 Improved Lower Bounds for Sampling Input-Output Pairs

For this section, we define a (d, c, k)-*local sampler* to be a (d, c)-local sampler with at least k non-isolated nodes on the left side of its associated bipartite graph (that is, it makes nontrivial use of at least k random bits). We say a distribution on $\{0,1\}^n$ is a (d, c, k)-*local source* if it equals $f(U_r)$ for some (d, c, k)-local sampler f (with any input length r). Note that a (d, c, k)-local source might not have min-entropy at least k.

Theorem 17. *Suppose Ext* $: \{0,1\}^n \to \{0,1\}$ *is a* $(0, \epsilon)$*-extractor for* $(d, 8d, n/4)$*-local sources, where* $d < n/8$*. Then for every* d*-local source* D *on* $\{0,1\}^{n+1}$ *we have* $\big\|D - \big(U_n, \mathit{Ext}(U_n)\big)\big\| \geq 1/2 - \epsilon - 2^{-n/2}$.

It might seem suspicious that we are assuming Ext is a $(0, \epsilon)$-extractor. We are not, in fact, extracting from sources with 0 min-entropy — it is possible to derive a lower bound on the min-entropy of any $(d, 8d, n/4)$-local source. The point is that for Theorem 17, we do not care about the min-entropy, only the number of non-isolated input nodes.

In the proof of Theorem 14, we implicitly showed that any particular bit of the extractor from Theorem 5 (for min-entropy $n^{0.9}$ and weight $\log n$) is a $(0, \epsilon)$-extractor for $(d, 8d, n/4)$-local sources, with error $\epsilon = 2^{-n^{\Omega(1)}}$. Theorem 3 follows immediately from this and Theorem 17.

Proof of Theorem 17. Consider an arbitrary d-local sampler $f : \{0,1\}^r \to \{0,1\}^{n+1}$, and let $G = (L, R, E)$ be the associated bipartite graph. Since $|E| \leq (n+1)d$, there are at most $(n+1)/8$ nodes in L with degree greater than $8d$. Also, at most $d \leq (n-1)/8$ nodes in L are adjacent to $(n+1, \mathrm{out})$. Without loss of generality, the nodes in L that either have degree greater than $8d$ or are adjacent to $(n+1, \mathrm{out})$ are $\{r - \ell + 1, \ldots, r\} \times \{\mathrm{in}\}$ for some $\ell \leq (n+1)/8 + (n-1)/8 = n/4$. For each string $y \in \{0,1\}^{\ell}$, define $f_y : \{0,1\}^{r-\ell} \to \{0,1\}^{n+1}$ as $f_y(x) = f(x, y)$ (hardwiring the last ℓ bits to y) and let $G_y = (L', R, E_y)$ be the associated bipartite graph, where $L' = \{1, \ldots, r-\ell\} \times \{\text{in}\}$. Observe that $f(U_r) = \sum_{y \in \{0,1\}^\ell} \frac{1}{2^\ell} f_y(U_{r-\ell})$. We define the tests

$$T_1 = \big\{z \in \{0,1\}^{n+1} : \exists x \in \{0,1\}^{r-\ell}, y \in \{0,1\}^\ell \text{ such that } f(x,y) = z \text{ and } \big|\{i \in \{1,\ldots,r-\ell\} : (i,\text{in}) \text{ is non-isolated in } G_y\}\big| < n/4\big\}$$

and

$$T_2 = \big\{z \in \{0,1\}^{n+1} : \text{Ext}(z|_{\{1,\ldots,n\}}) \neq z|_{\{n+1\}}\big\}$$

(in other words, the support of $\big(U_n, \text{Ext}(U_n)\big)$ is the complement of T_2). Finally, we define the test $T = T_1 \cup T_2$.

Claim 3. $\Pr_{f(U_r)}[T] \geq 1/2 - \epsilon$.

Claim 4. $\Pr_{(U_n, Ext(U_n))}[T] \leq 2^{-n/2}$.

Combining the two claims, we have $\big|\Pr_{f(U_r)}[T] - \Pr_{(U_n,\text{Ext}(U_n))}[T]\big| \geq 1/2 - \epsilon - 2^{-n/2}$, thus witnessing that $\big\|f(U_r) - \big(U_n, \text{Ext}(U_n)\big)\big\| \geq 1/2 - \epsilon - 2^{-n/2}$.

Proof of Claim 3. It suffices to show that for each $y \in \{0,1\}^\ell$, $\Pr_{f_y(U_{r-\ell})}[T] \geq 1/2 - \epsilon$. If y is such that $\big|\{i \in \{1,\ldots,r-\ell\} : (i,\text{in}) \text{ is non-isolated in } G_y\}\big| < n/4$ then of course $\Pr_{f_y(U_{r-\ell})}[T_1] = 1$. Otherwise, $f_y(U_{r-\ell})$ is a $(d, 8d, n/4)$-source on $\{0,1\}^{n+1}$. Note that $(n+1, \text{out})$ is isolated in G_y; we define $b_y \in \{0,1\}$ to be the fixed value of the $(n+1)$st output bit of f_y, and we define $f'_y : \{0,1\}^{r-\ell} \to \{0,1\}^n$ to be the first n output bits of f_y. Since $f'_y(U_{r-\ell})$ is a $(d, 8d, n/4)$-source on $\{0,1\}^n$, we have $\big\|\text{Ext}\big(f'_y(U_{r-\ell})\big) - U_1\big\| \leq \epsilon$ and thus $\Pr_{b \sim \text{Ext}(f'_y(U_{r-\ell}))}[b \neq b_y] \geq 1/2 - \epsilon$. In other words, $\Pr_{f_y(U_{r-\ell})}[T_2] \geq 1/2 - \epsilon$. This finishes the proof of Claim 3. □

Proof of Claim 4. By definition, $\Pr_{(U_n,\text{Ext}(U_n))}[T_2] = 0$. Note that $|T_1| \leq 2^{n/2}$ since each string in T_1 can be described by a string of length at most $\ell + n/4 \leq n/2$, namely an appropriate value of y along with the bits of x such that the corresponding nodes in L' are non-isolated in G_y. Since $\big(U_n, \text{Ext}(U_n)\big)$ is uniform over a set of size 2^n, we get $\Pr_{(U_n,\text{Ext}(U_n))}[T_1] \leq 2^{n/2}/2^n = 2^{-n/2}$. This finishes the proof of Claim 4. □

This finishes the proof of Theorem 17. □

7 Open Problems

One open problem is to improve our results quantitatively. This may require more sophisticated tools for understanding the min-entropy of the output distribution of a local sampler.

A major problem that remains open is to exhibit an explicit boolean function for which input-output pairs cannot be sampled exactly by polynomial-size constant-depth circuits. Solving this problem might pave the way for constructions of extractors for sources samplable by polynomial-size constant-depth circuits.

In this paper, we have considered samplers where each output bit only depends on a small number of input bits. What about samplers where each input bit only influences a small number of output bits?

Acknowledgments

We thank Zeev Dvir, Omer Reingold, Salil Vadhan, and Avi Wigderson for helpful email exchanges. In particular, A.D. would like to thank Omer and Salil for answering his innumerable queries about extractors and Salil for suggesting the use of GUV condensers. We had helpful conversations about this work with Urmila Mahadev, Luca Trevisan, and Gregory Valiant.

References

[AIK06] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. *SIAM Journal on Computing*, 36(4):845–888, 2006.

[AIK08] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. On pseudorandom generators with linear stretch in NC^0. *Computational Complexity*, 17(1):38–69, 2008.

[App11] Benny Applebaum. Pseudorandom generators with long stretch and low locality from random local one-way functions. Technical Report TR11-007, Electronic Colloquium on Computational Complexity, 2011.

[ASW09] Sanjeev Arora, David Steurer, and Avi Wigderson. Towards a study of low-complexity graphs. In *Proceedings of the 36th International Colloquium on Automata, Languages and Programming*, pages 119–131, 2009.

[BIW06] Boaz Barak, Russell Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. *SIAM Journal on Computing*, 36(4):1095–1118, 2006.

[BKS+10] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. *Journal of the ACM*, 57(4), 2010.

[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.

[BQ09] Andrej Bogdanov and Youming Qiao. On the security of Goldreich's one-way function. In *Proceedings of the 13th International Workshop on Randomization and Computation*, pages 392–405, 2009.

[BR94] Mihir Bellare and John Rompel. Randomness-efficient oblivious sampling. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, pages 276–287, 1994.

[BRSW06] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson. 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction. In *Proceedings of the 38th ACM Symposium on Theory of Computing*, pages 671–680, 2006.

[CEMT09] James Cook, Omid Etesami, Rachel Miller, and Luca Trevisan. Goldreich's one-way function candidate and myopic backtracking algorithms. In *Proceedings of the 6th Theory of Cryptography Conference*, pages 521–538, 2009.

[CFG+85] Benny Chor, Joel Friedman, Oded Goldreich, Johan Håstad, Steven Rudich, and Roman Smolensky. The bit extraction problem or t-resilient functions. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 396–407, 1985.

[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.

[CM01] Mary Cryan and Peter Bro Miltersen. On pseudorandom generators in NC^0. In *Proceedings of the 26th International Symposium on Mathematical Foundations of Computer Science*, pages 272–284, 2001.

[DEOR04] Yevgeniy Dodis, Ariel Elbaz, Roberto Oliveira, and Ran Raz. Improved randomness extraction from two independent sources. In *Proceedings of the 8th International Workshop on Randomization and Computation*, pages 334–344, 2004.

[DG10] Matt DeVos and Ariel Gabizon. Simple affine extractors using dimension expansion. In *Proceedings of the 25th IEEE Conference on Computational Complexity*, pages 50–57, 2010.

[DGW09] Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009.

[DM04] Stefan Dziembowski and Ueli Maurer. Optimal randomizer efficiency in the bounded-storage model. *Journal of Cryptology*, 17(1):5–26, 2004.

[DT09] Anindya De and Luca Trevisan. Extractors using hardness amplification. In *Proceedings of the 13th International Workshop on Randomization and Computation*, pages 462–475, 2009.

[Dvi09] Zeev Dvir. Extractors for varieties. In *Proceedings of the 24th IEEE Conference on Computational Complexity*, pages 102–113, 2009.

[GGH+07] Shafi Goldwasser, Dan Gutfreund, Alexander Healy, Tali Kaufman, and Guy Rothblum. Verifying and decoding in constant depth. In *Proceedings of the 39th ACM Symposium on Theory of Computing*, pages 440–449, 2007.

[Gol00] Oded Goldreich. Candidate one-way functions based on expander graphs. Technical Report TR00-090, Electronic Colloquium on Computational Complexity, 2000.

[GR08] Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Combinatorica*, 28(4):415–440, 2008.

[GRS06] Ariel Gabizon, Ran Raz, and Ronen Shaltiel. Deterministic extractors for bit-fixing sources by obtaining an independent seed. *SIAM Journal on Computing*, 36(4):1072–1094, 2006.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *Journal of the ACM*, 56(4), 2009.

[Hås86] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th ACM Symposium on Theory of Computing*, pages 6–20, 1986.

[Hås87] Johan Håstad. One-way permutations in NC^0. *Information Processing Letters*, 26(3):153–155, 1987.

[IKOS08] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In *Proceedings of the 40th ACM Symposium on Theory of Computing*, pages 433–442, 2008.

[KRVZ11] Jesse Kamp, Anup Rao, Salil Vadhan, and David Zuckerman. Deterministic extractors for small-space sources. *Journal of Computer and System Sciences*, 77(1):191–220, 2011.

[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.

[Li11a] Xin Li. Improved constructions of three source extractors. In *Proceedings of the 26th IEEE Conference on Computational Complexity (to appear)*, 2011.

[Li11b] Xin Li. A new approach to affine extractors and dispersers. In *Proceedings of the 26th IEEE Conference on Computational Complexity (to appear)*, 2011.

[Lu04] Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1):27–42, 2004.

[LV11] Shachar Lovett and Emanuele Viola. Bounded-depth circuits cannot sample good codes. In *Proceedings of the 26th IEEE Conference on Computational Complexity (to appear)*, 2011.

[MST06] Elchanan Mossel, Amir Shpilka, and Luca Trevisan. On epsilon-biased generators in NC^0. *Random Structures and Algorithms*, 29(1):56–81, 2006.

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

[Rao08] Anup Rao. A 2-source almost-extractor for linear entropy. In *Proceedings of the 12th International Workshop on Randomization and Computation*, pages 549–556, 2008.

[Rao09a] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. *SIAM Journal on Computing*, 39(1):168–194, 2009.

[Rao09b] Anup Rao. Extractors for low-weight affine sources. In *Proceedings of the 24th IEEE Conference on Computational Complexity*, pages 95–101, 2009.

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

[RRV99] Ran Raz, Omer Reingold, and Salil Vadhan. Error reduction for extractors. In *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*, pages 191–201, 1999.

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

[RY11] Ran Raz and Amir Yehudayoff. Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors. *Journal of Computer and System Sciences*, 77(1):167–190, 2011.

[RZ08] Anup Rao and David Zuckerman. Extractors for three uneven-length sources. In *Proceedings of the 12th International Workshop on Randomization and Computation*, pages 557–570, 2008.

[Sha02] Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the European Association for Theoretical Computer Science*, 77:67–95, 2002.

[Sha08] Ronen Shaltiel. How to get more mileage from randomness extractors. *Random Structures and Algorithms*, 33(2):157–186, 2008.

[Sho88] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. In *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, pages 283–290, 1988.

[SSS95] Jeanette Schmidt, Alan Siegel, and Aravind Srinivasan. Chernoff-Hoeffding bounds for applications with limited independence. *SIAM Journal on Discrete Mathematics*, 8(2):223–250, 1995.

[Sud] Madhu Sudan. Essential coding theory – course notes. Available on the web at `http://theory.lcs.mit.edu/~madhu/coding/`.

[Tre01] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

[TV00] Luca Trevisan and Salil Vadhan. Extracting randomness from samplable distributions. In *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, pages 32–42, 2000.

[Vad04] Salil Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2004.

[Vio10] Emanuele Viola. The complexity of distributions. In *Proceedings of the 51st IEEE Symposium on Foundations of Computer Science*, pages 202–211, 2010.

[Yao85] Andrew Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 1–10, 1985.

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

[Zim10] Marius Zimand. Simple extractors via constructions of cryptographic pseudo-random generators. *Theoretical Computer Science*, 411(10):1236–1250, 2010.

ECCC ISSN 1433-8092
http://eccc.hpi-web.de