*Electronic Colloquium on Computational Complexity*
ECCC TECHNICAL REPORTS SERIES 1994 REPORT NR: TR94–002

# Tiny Families of Functions with Random Properties: A Quality–Size Trade–off for Hashing

Oded Goldreich[†] Avi Wigderson[‡]

*Received November 6 1994*

**Abstract.** We present three explicit constructions of hash functions, which exhibit a trade-off between the size of the family (and hence the number of random bits needed to generate a member of the family), and the quality (or error parameter) of the pseudo-random property it achieves. Unlike previous constructions, most notably universal hashing, the size of our families is essentially independent of the size of the domain on which the functions operate.

The first construction is for the *mixing* property – mapping a proportional part of any subset of the domain to any other subset. The other two are for the *extraction* property – mapping any subset of the domain almost uniformly into a range smaller than it. The second and third constructions handle (respectively) the extreme situations when the range is very large or very small.

We provide lower bounds showing our constructions are nearly optimal, and mention some applications of the new constructions.

**Keywords:** Randomness, small sample spaces, hashing functions.

[†] Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel. Email: oded@wisdom.weizmsnn.ac.il. Research was supported in part by grant No. 92-00226 from the United States – Israel Binational Science Foundation (BSF), Jerusalem, Israel.

[‡] Institute for Computer Science, Hebrew University, Jerusalem, Israel. Email: avi@cs.huji.ac.il. Research was supported in part by the Wolfson Research Awards, administered by the Israel Academy of Sciences and Humanities.

# 1 Introduction

In 1979, Carter and Wegman introduced the notion of universal hashing functions [7]. Though these functions were introduced with data storage application in mind, they found many applications to complexity theory [29, 31, 34, 17, 16, 20, 21, 18, 19, 26, 27, 36]. This wide range of applications owns its existence to two related 'random' properties of these succinct and efficiently computable functions: the *extraction* and the *mixing* properties.

For a family $F$ of functions, each mapping $n$-bit strings to $m$-bit strings, the *extraction* property asserts the following. Every subset of $K \cdot 2^m$ strings in the domain $\{0,1\}^n$, is mapped almost uniformly to the range $\{0,1\}^m$, by all but a small fraction of the functions in the family. The parameter $K > 1$ determines the quality of the approximation to the uniform distribution and the fraction of bad functions in $F$ (i.e. those that don't achieve this approximation). The extraction property is the heart of the Leftover Hash Lemma [20] and its precurors, which were key to numerous results, e.g. in saving randomness [21], weak random sources [36], pseudorandom generators [16, 20] and interactive proofs [17].

The *mixing* property is meaningful also in case $m = n$, and in fact it is usually used with this choice. Hence, we assume for simplicity that $m = n$. Loosely speaking, the mixing property asserts that, for all but a small fraction of the functions $f$ in the family $F$, the membership in $A \times B$ of a pair $(a, f(a))$ with $a$ being a random element from the domain, is essentially the same as that of a random pair $(a, b)$ of elements. The prime use of the mixing property is in the logspace pseudorandom generators [26, 27].

In the definitions above, there is an error parameter $\epsilon$ (e.g. the fraction of bad functions, the distance from the uniform distribution etc.), which determines the quality of the mixing or extraction achieved by the family $F$. All the applications mentioned above take $F$ to be a universal family of hash functions. This family achieves the best possible quality parameter: $\epsilon$ is exponentially small in $m$. However, while small enough for these applications, a universal family has to be large: exponential in $n$.

But in some applications we may be content with a larger $\epsilon$ (i.e. lower quality), say constant or $1/poly(n)$. Can we use much smaller families $F$ in this case and achieve similar random properties? A straightforward counting argument shows (nonconstructively, of course) that there exist families $F$ of size $poly(1/\epsilon)$ (resp. $poly(n/\epsilon)$) achieving the mixing (resp. extraction) properties with quality $\epsilon$. Note that these bounds depend essentially only on the quality required, and not on the size of the domain.

The main contribution of this paper is in presenting explicit constructions of such families, thus yielding a trade-off between the size of the family and the desired quality. The first construction is for mixing, where we obtain a complete trade-off. The second and third constructions are for extraction, where we (respectively) handle two extreme cases: when $n - m \ll n$ and $m \ll n$. Our constructions are relatively simple. The first two of them combine universal hashing and expander graphs. (It is interesting to note that despite the similarity in these two constructions, the proofs are completely different). An alternative to the second construction, which is often

more efficient, uses the extractors of [28] instead of universal hashing. The third construction uses small-bias probability spaces of small size. We provide lower bounds to show that the first construction is nearly optimal, and the third is nearly optimal for sufficiently small $m$. By nearly optimal here we mean that the number of bits needed to describe a member of the family in our constructions is within a constant factor of the lower bound. The second construction uses a number of random bits which is at most quadratic in the lower bound.

It is not surprising that these constructions already found some interesting applications. Using the first construction we reduce the randomness complexity of two generic procedures as follows:

1. For sampling procedures, which use an asymptoticaly optimal number of sample points, the amount of randomness required to generate the sample points is reduced by a factor of 2; and

2. The randomess complexity of Nisan's "generalized logspace" generator [26], is reduced by a logarithmic factor.

The second construction implies a randomness–efficient leftover hash lemma. The third construction turned out to be the main technical tool in the recent result of [33] (who independently discovered a similar construction). They completely resolve the simulation problem of $BPP$ algorithms by Santha-Vazirani [32] sources. Recall that such a source is required to give the each successive output bit a nontrivial probability $\delta$ for both HEADS and TAILS. While the best previous result [35] required a constant $\delta > 0$, the new result requires only that on $n$-bit output, $\delta > n^{-\Omega(1)}$. A simple information theoretic argument [11] shows that this bound is best possible.

Despite the general interest in reducing the size of sample spaces achieving various random properties, very little was done for the proerties provided by universal hashing. The only previous result achieving such a quality-size trade-off is the paper [28]. They deal with extraction in the difficult range $m = \Theta(n)$ (which we cannot handle), via an ingenious construction. Moreover, they applied it to show that poly($S$) random bits add no power at all to space($S$) Turing machines! As mentioned above, [33] independently discovered a construction similar to our third one. They obtain the same bounds, but with a somewhat different proof.

## Organization

The following three sections are devoted to the corresponding three constructions mentioned above. Each section starts with a brief intuitive summary of the results obtained. Next, comes a formal statement of the result and a description of the construction which achieves it. We briefly touch on the technical tools used in the proof that the construction works, and present the relevant lower bound. In addition, for the first construction, we describe two applications.

The appendix contains four sections. In Section A we detail the technical tools used in the proofs. In Section B we give full proofs of the upper bounds for all constructions, and in section C the proofs of the lower bounds. Details for the sampling application (of the first construction) are given in section D.

## 2 Tiny Families of Functions with Mixing Properties

Recall that a function $f$ is mixing for sets $A, B$ of the domain, if membership in $A \times B$ of a pair $(a, f(a))$, with $a$ being a random element in the domain, occurs roghly as often as it would for a random pair $(a, b)$ of elements. The main result of this section is the explicit construction of an $\epsilon$-mixing family of size poly$(1/\epsilon)$. Here $\epsilon$ stands both for distance from truely random behaviour, as well as the fraction of bad functions which do not achieve this distance. We state the precise theorem, then describe the construction. We prove that our family has optimal size up to a polynomial, and present an application to saving randomaness in the generalized logspace model of [26]. We conclude with a different perspective of this result, advocated by Linial.

### Main result

**Theorem 1** *For every $\epsilon > 2^{-\Omega(n)}$, there exists a family of functions, each mapping $\{0,1\}^n$ to itself, satisfying the following properties.*

- succinctness: *the family contains a polynomial in $\frac{1}{\epsilon}$ number of functions, and each function is represented by a unique string of length $l(\epsilon) = O(\log \frac{1}{\epsilon})$.*
- efficient evaluation: *There exists a logspace algorithm that, on input a description of a function $f$ and a string $x$, returns $f(x)$.*
- mixing property: *For every two subsets $A, B \subseteq \{0,1\}^n$, all but an $\epsilon$ fraction of the functions $f$ in the family satisfy*

$$|\text{Prob}(X_n \in A \wedge f(X_n) \in B) - \rho(A)\rho(B)| \leq 2\epsilon$$

*where $\rho(S) \stackrel{\text{def}}{=} \frac{|S|}{2^n}$ denotes the density of the set $S$ and $X_n$ is a random variable uniformly distributed over $\{0,1\}^n$.*

### The Construction

The construction makes used of two basic tools which are frequently used for saving randomness: universal hashing functions and expander graphs.

We start by setting the parameters for the expander graph and the universal hashing family to be used. First, let $G$ be an expander graph of degree $d$, second eigenvalue $\lambda$, and vertex set $\{0,1\}^n$, so that $\frac{\lambda}{d} \leq \epsilon^2$. Such expander graphs are easily constructible for $d = \frac{1}{\epsilon^{O(1)}}$ (cf., [15]) [1] Assume, without loss of generality, that $d$ is a power of 2. For every $i \in [d] \stackrel{\text{def}}{=} \{1, 2..., d\}$ and $v \in \{0,1\}^n$, denote by $g_i(v)$ the vertex reached by moving along the $i^{\text{th}}$ edge of the vertex $v$.

[1] Actually, using Ramanujan Graphs, it suffices to have $d = \frac{4}{\epsilon^4}$ (cf., [23]). One may prefer the Gaber-Galil expander since it allows to avoid problems such as generating large primes and embedding $\{0,1\}^n$ in $GF(p)$, for a suitably large prime $p$.

We next consider a universal family, denoted $H$, of hash functions, each mapping $l \stackrel{\text{def}}{=} 4\log_2(1/\epsilon)$-bit long strings to $[d]$ (where $[d] = \{0,1\}^m$, for some $m$). Namely, a *uniformly chosen function* $h \in H$ maps each string $\alpha \in \{0,1\}^l$ uniformly into $[d]$ so that every two strings are mapped in an independent manner.

We now define the functions in our family, denoted $F$. For each hashing function $h \in H$, we introduce a function $f \in F$ defined by

$$f(v) \stackrel{\text{def}}{=} g_{h(\text{lsb}(v))}(v)$$

where $\text{lsb}(v)$ returns the $l$ least significant bits of $v \in \{0,1\}^n$. Namely, $f(v)$ is the vertex reached from $v$ by following the $i^{\text{th}}$ edge of $v$, where $i$ is the image of the $l$ least significant bits of $v$ under the function $h$. (We remark that our choice of using the $l$ least significant bits is arbitrary and any other efficient partition of $\{0,1\}^n$ into $2^l$ parts, of approximately the same size, will do.)

The full proof is given in the appendix. The two main technical tools it uses (see section A) are the Expander Mixing Lemma, and the pairwise independence of the universal hash function family.

## Lower Bound

**Theorem 2** *A family with mixing property of accuracy $\epsilon$, must have size at least $\sqrt{\frac{4}{\epsilon}}$.*

## Applications

We present two applications of the new construction. The first application is to reducing the randomness complexity of sampling techniques (specifically, by a factor of 2); and the second is to reducing the cost of the deterministic simulation of a generalization, due to Nisan [26], of random-logspace computations.

### Sampling

In many settings repeated sampling is used to estimate the average value of a huge set of values. Namely, there is a value function $\nu$ defined over a huge space, say $\nu : \{0,1\}^n \mapsto [0,1]$, and one wishes to approximate $\bar{\nu} \stackrel{\text{def}}{=} \frac{1}{2^n}\sum_{x\in\{0,1\}^n}\nu(x)$. To this end, one may randomly select a small sample set $S$ and compute $\frac{1}{|S|}\sum_{x\in S}\nu(x)$. Using a sample of $O(1/\epsilon^2)$ uniformly and independently selected points, one gets, with constant probability, an approximation that it within an additive factor of $\epsilon$ from the correct average. In fact, a set of $O(1/\epsilon^2)$ points selected in a pairwise-independent and uniform manner yields the same quality of approximation. Whereas generating $t$ totally independent random points in $\{0,1\}^n$ requires $t \cdot n$ unbiased coin flips, one can generate $t$ pairwise-independent random points using only $2 \cdot n$ unbiased coin flips [10]. Using the new family of functions, we further reduce the randomness complexity of the approximation problem to $n + O(\log(1/\epsilon))$, while almost maintaining the number of sample points.

**Definition 1** (sampler): *A* sampler *is a randomized algorithm that on input parameters* $n$ (length), $\epsilon$ (accuracy) *and* $\delta$ (error), *and oracle access to any function* $\nu : \{0,1\}^n \mapsto [0,1]$, *outputs, with probability at least* $1-\delta$, *a value that is at most* $\epsilon$ *away from* $\bar{\nu}$. *Namely,*

$$\text{Prob}(|\text{sampler}^{\nu}(n,\epsilon,\delta) - \bar{\nu}| > \epsilon) \ < \ \delta$$

**Theorem 3** *There exists a* poly$(n,\epsilon,\delta)$*-time sampler which*

- *makes* $O(\frac{1}{\delta\epsilon^2})$ *oracle queries; and*
- *tosses* $n + O(\log(1/\epsilon)) + O(\log(1/\delta))$ *coins.*

We remark that samplers for Boolean functions can be obtained in a more direct way; and furthermore, these samplers use only $n$ coin tosses (see appendix D). Using the result of Bellare et al [5], we get the same reduction in the randomness complexity, while reducing the number of sample points.

**Corollary 4** *There exists a* poly$(n,\epsilon,\log(1/\delta))$*-time sampler which*

- *makes* $O(\frac{\log(1/\delta)}{\epsilon^2})$ *oracle queries; and*
- *tosses* $n + O(\log(1/\epsilon)) + O(\log(1/\delta))$ *coins.*

The last sampler is optimal (up to a multiplicative factor) in its sample-complexity, and among the samplers with nearly optimal sample complexity the above is optimal (up to the additive logarithmic factors) in its randomness-complexity [6]. Previously, efficient samplers with optimal sample-complexity were known only for twice the randomness-complexity [5] (yet, [6] have proved, via an non-constructive argument, that samplers with sample and randomness complexities as in the corollary do exist).

### Generalized Random Logspace

In [26], Nisan considered the problem of saving randomness in a context in which $m$ randomized algorithms are executed and their output is fed to an $s$-space machine which then produces a final Boolean output. (Actually, the problem is not affected if the $s$-space machine is allowed to have output of length bounded by $O(s)$.) For simplicity, assume that each of the algorithms uses $n$ coin flips. The obvious way of running the entire procedure requires $m \cdot n$ coin flips. In case we are willing to tolerate an $\epsilon$ additive error (respectively, deviation) in the final output, more randomness-efficient solutions are possible. In particular, Nisan showed [26] that the randomness complexity can be decreased to

$$O(\max\{n, s + \log(m/\epsilon)\} \cdot \log m)$$

Replacing the universal hash functions used in [26] by our family of mixing functions, we show

**Theorem 5** *The above problem can be solved with randomness complexity*

$$n + O((s + \log(m/\epsilon)) \cdot \log m)$$

We remark that in many applications $n \gg s + \log(m/\epsilon)$. Specifically, it is reasonable to consider the case where $m$, $1/\epsilon$ and $n$ are all polynomially related, and furthermore $s = O(\log m)$. For these cases, our improvement yields a logarithmic reduction in the randomness complexity.

### A Different Perspective

The mixing property of families of functions should not be confused with the mixing property of graphs. Yet, the two are related as we shall see below. We say that a graph has a good mixing property if for every two subsets of vertices the fraction of edges connecting these subsets is approximately equal the product of the densities of these subsets. Clearly, a family of functions over $\{0,1\}^n$, with good mixing, induces a regular multi-graph[2] with good mixing. The converse is not obvious. Specifically, it was not even known whether the edges of some small degree graph with good mixing property (e.g., an expander) can be so colored that they induce a family of functions with a good mixing property. In fact, this problem has been advocated by Nati Linial.

Let us try to clarify the nature of this problem. Consider a $d$-degree expander with vertex-set $V \stackrel{\text{def}}{=} \{0,1\}^n$, and some $d$-coloring of its edges. For every two sets of vertices, $A$ and $B$, denote by $E_i(A,B)$ the set of edges of color $i$ that connect a vertex in $A$ to a vertex in $B$. By the Expander Mixing Lemma (see following section), it follows that the *average* of $\frac{|E_i(A,B)|}{|V|}$, taken over all $1 \leq i \leq d$, is approximately $\frac{|A|}{|V|} \cdot \frac{|B|}{|V|}$. The question is whether $\frac{|E_i(A,B)|}{|V|}$ is approximately $\frac{|A|}{|V|} \cdot \frac{|B|}{|V|}$, *for almost all* $1 \leq i \leq d$. One can easily verify that, in general, the answer is negative. Specifically, for Cayley Graph expanders (e.g., [24, 4, 23]), there are sets $A$ and $B$ for which *there exist no* $i$ such that $\frac{|E_i(A,B)|}{|V|}$ approximates $\frac{|A|}{|V|} \cdot \frac{|B|}{|V|}$. The problem raised by Nati Linial was to construct an expander for which the mixing property holds for most colors (and not only on the average).

We resolve this problem by presenting a transformation of edge-colored expanders to edge-colored expanders for which the mixing property holds for most colors (as required above). Our transformation preserves the vertex set and the expansion properties of the original expander, but increases the degree by a polynomial factor (i.e., from $d$ to $\text{poly}(d)$). Although the transformation is not explicitly presented in this extended abstract, it can be easily derived from the description.

## 3 Tiny Families Extracting High Min-entropy

Recall that the *extraction* property, for a family of functions each mapping $n$-bit strings to $m$-bit strings, means that each subset of $K \cdot 2^m$ strings in $\{0,1\}^n$ is mapped almost uniformly to $\{0,1\}^m$, by all but a small fraction of the functions in the family. We consider the extraction problem in

[2] A multi-graph is a graph in which parallel edges are allowed.

two special cases: the case where $m$ is very small (in the next section) and the case $m$ is very close to $n$ (in this section). Actually, we consider a generalization of the extraction problem to random variables with an upper bound, of $\frac{1}{K \cdot 2^m}$, on the probability function. Such a bound is called *min-entropy* (cf., Chor and Goldreich [9]).

**Definition 2** (min-entropy): *Let $X$ be a random variable. We say that $X$ has* min-entropy *$k$ if* $\mathrm{Prob}(X=x) \leq 2^{-k}$, *for each $x$.*

Here we treat the case of random variables with min-entropy $n-k$ with $k \ll n$. We construct a family of $\mathrm{poly}(2^k/\epsilon)$ functions mapping $\{0,1\}^n$ to $\{0,1\}^m$, where $m = n - O(k)$. For each such random variable, all but a $\epsilon$ fraction of the functions, when applied to it, yield a random variable which is $\epsilon$-close to uniform (in norm-1). Loosely speaking, this means that these functions are able to "smooth" almost the entire min-entropy; specifically, min-entropy $n-k$ is mapped to almost uniform distribution over the strings of length $n - O(k)$.

In a typical use of this extraction, most notably the applications of the leftover hash lemma, $\epsilon = 2^{-\Omega(k)}$. In these cases the size of our family is $\mathrm{poly}(1/\epsilon)$ which is optimal by the lower bound we give. There may be cases, however, where $\epsilon$ may be allowed to be much larger. Here we have an alternative constcruction with size $k^{O(\log(1/\epsilon))}$, which will be much smaller than $2^k/\epsilon$ in this case. We mention both in the precise theorem.

## Main Result

**Theorem 6** *Let $k < n$, $m < n-k$ and $\epsilon > 2^{-(n-m-O(k))/O(1)}$.* (Typically, $m = n - O(k)$ and $\epsilon = 2^{-\Theta(n-m)}$.) *There exists a family of functions, each mapping $\{0,1\}^n$ to $\{0,1\}^m$, satisfying the following properties.*

- succinctness: *the family contains a polynomial in $\frac{2^k}{\epsilon}$ number of functions, and each function is represented by a unique string of length $l(k,\epsilon) = O(k + \log\frac{1}{\epsilon})$. Alternatively, we can achieve size $k^{O(\log(1/\epsilon))}$, with the description length of each function being $l(k,\epsilon) = O((\log k)(\log(1/\epsilon))$.*
- efficient evaluation: *There exists a logspace algorithm that, on input a description of a function $f$ and a string $x$, returns $f(x)$.*
- extraction property: *For every random variable $X \in \{0,1\}^n$ of min-entropy $n-k$, all but an $\epsilon$ fraction of the functions $f$ in the family satisfy*

$$\sum_{\alpha \in \{0,1\}^m} |\mathrm{Prob}(f(X)=\alpha) - \frac{1}{2^m}| \leq \epsilon$$

## The construction

We start with the main construction. At the end, of this subsection, we explain how to modify it and get the alternative construction. Again, we use universal hashing functions and expander

graphs. This time we use an expander graph, $G$, degree $d$ (power of two), second eigenvalue $\lambda$, and vertex set $\{0,1\}^m$, so that $\frac{\lambda}{d} \leq \frac{\epsilon}{2^{k/2}}$. (Recall that such an expander can be constructed for $d = \text{poly}(\frac{2^k}{\epsilon})$.) As before, for every $i \in [d] \stackrel{\text{def}}{=} \{1, 2..., d\}$ and $v \in \{0,1\}^m$, denote by $g_i(v)$ the vertex reached by moving along the $i^{\text{th}}$ edge of the vertex $v$. The universal family, denoted $H$, contains hash functions each mapping $(n-m)$-bit long strings to $[d]$.

We now define the functions in our family, denoted $F$. For each hashing function $h \in H$, we introduce a function $f \in F$ defined by

$$f(x) \stackrel{\text{def}}{=} g_{h(\text{lsb}(x))}(\text{msb}(x))$$

where $\text{lsb}(x)$ returns the $n-m$ least significant bits of $x \in \{0,1\}^n$, and $\text{msb}(x)$ returns the $m$ most significant bits of $x$. Namely, $f(x)$ is the vertex reached from the vertex $v \stackrel{\text{def}}{=} \text{msb}(x)$ by following the $i^{\text{th}}$ edge of $v$, where $i$ is the image of the $n-m$ least significant bits of $x$ under the function $h$. (We remark that our choice of using the $n-m$ least significant bits is arbitrary and any other efficient partition of $\{0,1\}^n$ into $2^{n-m}$ parts, of approximately the same size, will do.)

Again, the full proof is provided in the appendix. Despite the apperant similarity to the construction for mixing, the proof here is completely different. It is based on "stronger" technical tools (see section A): the Expander Smoothing Lemma and the Leftover Hash Lemma.

Finally, to obtain the alternative construction mentioned in the main theorem of this section, simply replace the hash function family $H$ by a family of $(\delta, \epsilon)$-extractors from [28], with $\delta = \log k / \log(n-m)$, on the same domain and range used above. The proof for this construction is identical, since the extraction property of this family (see section A) guarantees the same as the Leftover Hash Lemma for these parameters.

### Lower Bound

We conclude with the lower bound. It shows, that for $\epsilon = 2^{-\Omega(k)}$, our first construction is optimal. It also shows that in the general, the number of bits used in the alternative construction is at most quadratic away from optimum.

**Theorem 7** *A family of functions from $\{0,1\}^n$ to $\{0,1\}$, with extraction property of accuracy $\epsilon < 1$ with respect to random variables of min-entropy $n - k \leq n - 1$, must have size at least* $\max\{k+1, (1/\epsilon) - 1\}$.

## 4 Tiny Families Extracting Low Min-Entropy

Here we treat the case of random variables with min-entropy $k$, with $k \ll n$. we construct a family of $\text{poly}(2^k n/\epsilon)$ functions mapping $\{0,1\}^n$ to $\{0,1\}^m$, where $m = \Omega(k)$. (Again, $\epsilon$ is the accuracy parameter.) Loosely speaking, this means that these functions are able to "smoothen" a constant fraction of the min-entropy; specifically, min-entropy $k$ is mapped to almost uniform distribution over the strings of length $\Omega(k)$.

## Main Result

**Theorem 8** *Let $5m < k < n$ and $\epsilon > 2^{-(k-5m)/3}$.* (Typically, $m = \frac{k}{8}$ and $\epsilon = 2^{-m}$.) *There exists a family of functions, each mapping $\{0,1\}^n$ to $\{0,1\}^m$, satisfying the following properties.*

- succinctness: *the family contains a polynomial in $\frac{2^m n}{\epsilon}$ number of functions, and each function is represented by a unique string of length $l(\frac{2^m n}{\epsilon}) = O(m + \log \frac{n}{\epsilon})$.*
- efficient evaluation: *There exists a logspace algorithm that, on input a description of a function $f$ and a string $x$, returns $f(x)$.*
- extraction property: *For every random variable $X \in \{0,1\}^n$ of min-entropy $k$, all but an $\epsilon$ fraction of the functions $f$ in the family satisfy*

$$\sum_{\alpha \in \{0,1\}^m} |\mathrm{Prob}(f(X) = \alpha) - \frac{1}{2^m}| \leq \epsilon$$

## The Construction

We use a construction of small probability spaces with small bias. In particular, we consider a prime $p \approx 2^m$ and a construction of $t \stackrel{\text{def}}{=} \frac{n}{m}$ random variables, $(\xi_1, ..., \xi_t)$, each distributed over $GF(p)$ with the following *small bias* property:

> for every $t$-long sequence $(a_1, ..., a_t)$ of elements in $GF(p)$, so that not all $a_i$'s are zero, the random variable $\sum_{i=1}^{t} a_i \xi_i$ is almost uniformly distributed over $GF(p)$ (i.e., its statistical distance from uniform is small).

Typically, such random variables are defined by the uniform distribution over some sample space $S \subseteq GF(p)^t$, and they can be show to satisfy also a related technical condition (see section A). We will use such a sample space, $S$, for bias $\epsilon' \stackrel{\text{def}}{=} \frac{\epsilon^3}{p^5}$. (Hence, using the sample space of [3, 14, 13], $|S| = \mathrm{poly}(\frac{n 2^k}{\epsilon})$.)

The functions in our family, denoted $F$, correspond to the samples in the small-bias space. Namely, for each $(s_1, ..., s_t) \in S$, we introduce the function $f \in F$ defined by

$$f(x) \stackrel{\text{def}}{=} \sum_{i=1}^{t} s_i x_i$$

where $x_i$ is the $i^{\text{th}}$ coordinate in $x \in GF(p)^t$ and the arithmetic is in $GF(p)$. The functions, so defined, map $GF(p)^t$ to $GF(p)$. Standard modifications can be applied to derive functions mapping $\{0,1\}^n$ to $\{0,1\}^m$ (recall $p \approx 2^m$).

The proof of this theorem is also given in the appendix. Despite the need for a norm-1 bound, it uses the fact that the construction of small–bias spaces of [3, 13] give a bound in norm-2 on the realted exponential sum (see section A). We then prove a Lindsey–like lemma on near-othogonal vectors and combine it with the bound above to give the result.

### Lower Bound

To illustrate that this construction is near optimal when $k = O(\log n)$ we restate Theorem 7 with the necessary change of parameters. We note that the $BPP$ simulation of [33] mentioned in the introduction indeed uses this construction for this value of the parameter $k$.

**Theorem 9** *A family of functions from* $\{0,1\}^n$ *to* $\{0,1\}$, *with extraction property of accuracy* $\epsilon < 1$ *with respect to random variables of min-entropy* $k \leq n-1$, *must have size at least* $\max\{n - k + 1, (1/\epsilon) - 1\}$.

## References


[1] M. Ajtai, J. Komlos, E. Szemerédi, "Deterministic Simulation in LOGSPACE", *Proc. 19th STOC*, 1987, pp. 132–140.

[2] N. Alon, "Eigenvalues, Geometric Expanders, Sorting in Rounds and Ramsey Theory", *Combinatorica*, 6 (1986), pp. 231–243.

[3] N. Alon, O. Goldreich, J. Hastad, R. Peralta, "Simple Constructions of Almost $k$-wise Independent Random Variables", *Journal of Random structures and Algorithms*, Vol. 3, No. 3, (1992), pp. 289–304.

[4] N. Alon and V.D. Milman, "Eigenvalues, Expanders and Superconcentrators", *25th FOCS*, 1984, pp. 320–322.

[5] M. Bellare, O. Goldreich, and S. Goldwasser "Randomness in Interactive Proofs", *31st FOCS*, 1990, pp. 318–326.

[6] R. Canetti, G. Even and O. Goldreich, "Lower Bounds for Sampling Algorithms", submitted to *IPL*, 1993.

[7] L. Carter and M. Wegman, "Universal Classes of Hash Functions", *J. Computer and System Sciences*, Vol. 18, pp. 143–154 (1979).

[8] A. Cohen, A. Wigderson, " Dispersers, Deterministic Amplification and Weak random Sources", *Proc. of the 30th FOCS*, pp. 14–19, 1989.

[9] B. Chor and O. Goldreich, "Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity", *SIAM J. Comput.*, Vol. 17, No. 2, April 1988, pp. 230–261.

[10] B. Chor and O. Goldreich, "On the Power of Two–Point Based Sampling," *Jour. of Complexity*, Vol 5, 1989, pp. 96–106.

[11] A. Cohen and A. Wigderson, "Dispensers, Deterministic Amplification, and Weak Random Sources", *30th FOCS*, 1989, pp. 14–19.

[12] P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, 1974.

[13] G. Even, "Construction of Small Probability Spaces for Deterministic Simulation", M.Sc. thesis, Computer Science Department, Technion, Haifa, Israel, 1991. (In Hebrew, abstract in English)

[14] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Veličković, "Approximations of General Independent Distributions", *24th STOC*, pp. 10–16, 1992.

[15] O. Gaber and Z. Galil, "Explicit Constructions of Linear Size Superconcentrators", *JCSS*, **22** (1981), pp. 407-420.

[16] O. Goldreich, H. Krawcyzk and M. Luby, "On the Existence of Pseudorandom Generators", *29th FOCS*, pp. 12–24, 1988.

[17] S. Goldwasser and M. Sipser, "Private Coins versus Public Coins in Interactive Proof Systems", *18th STOC*, pp. 59–68, 1986.

[18] R. Impagliazzo and M. Luby, "One-Way Functions are Essential for Complexity Based Cryptography", *30th FOCS*, pp. 230–235, 1989.

[19] R. Impagliazzo and L.A. Levin, "No Better Ways to Generate Hard NP Instances than Picking Uniformly at Random ", *31st FOCS*, pp. 812-821, 1990.

[20] R. Impagliazzo, L.A. Levin, and M.G. Luby, "Pseudorandom Generators from any One-Way Functions", *21st STOC*, pp. 12–24, 1989.

[21] R. Impagliazzo and D. Zuckerman, "How to Recycle Random Bits", *30th FOCS*, 1989, pp. 248-253.

[22] R.M. Karp, N. Pippinger and M. Sipser, "A Time-Randomness Tradeoff", *AMS Conference on Probabilistic Computational Complexity*, Durham, New Hampshire (1985).

[23] A. Lubotzky, R. Phillips, P. Sarnak, "Explicit Expanders and the Ramanujan Conjectures", *Proc. 18th STOC*, 1986, pp. 240-246.

[24] G.A. Margulis, "Explicit Construction of Concentrators", *Prob. Per. Infor.* 9 (4) (1973), 71–80. (English translation in *Problems of Infor. Trans.* (1975), 325–332.)

[25] J. Naor and M. Naor, "Small-bias Probability Spaces: Efficient Constructions and Applications", *22nd STOC*, 1990, pp. 213–223.

[26] N. Nisan, "Pseudorandom Generators for Space Bounded Machines", *22nd STOC*, pp. 204–212, 1990.

[27] N. Nisan, "$\mathcal{RL} \subseteq \mathcal{SC}$", *24th STOC*, pp. 619–623, 1992.

[28] N. Nisan and D. Zuckerman, "More Deterministic Simulation in LOGSPACE", *25th STOC*, pp. 235–244, 1993.

[29] M. Sipser, "A Complexity Theoretic Approach to Randomness", *15th STOC*, 1983, pp. 330–335.

[30] M. Sipser, "Expanders Randomness or Time vs Space", *Structure in Complexity Theory* (proceedings), 1986.

[31] L. Stockmeyer, "The Complexity of Approximate Counting", *15th STOC*, 1983, pp. 118–126.

[32] M. Santha and U. Vazirani, "Generating Quasi-Random Sequences from Slightly Random Sources", *JCSS*, Vol. 33, No. 1, pp. 75–87, 1986.

[33] A. Srinivasan and D. Zuckerman, "Computing with Very Weak Random Sources", manuscript, 1993.

[34] L. Valiant and V.V. Vazirani, "NP is as Easy as Detecting Unique Solutions", *Theoretical Computer Science*, Vol. 47, 1986, pp. 85–93.

[35] U. Vazirani and V. Vazirani, "Random Polynomial Time Equal to Semi-Random Polynomial Time", *Proc. 26th FOCS*, pp. 417–428, 1985.

[36] D. Zuckerman, "Simulating BPP Using a General Weak Random Source," *32nd FOCS*, 1991, pp. 79–89.

# A Technical Tools

## A.1 Universal Hashing

Loosely speaking, universal families of hashing functions consist of functions operating on the same domain-range pair so that a function uniformly selected in the family maps each pair of points in a pairwise independent and uniform manner. Specifically, a family, $H_{n,m}$, of functions from $\{0,1\}^n$ to $\{0,1\}^m$, is called *universal* if for every $x \neq y \in \{0,1\}^n$ and $\alpha, \beta \in \{0,1\}^m$ it holds

$$\text{Prob}(h(x)=\alpha \wedge h(y)=\beta) = 2^{-2m}$$

where the probability is taken over all choices of $h \in H_{n,m}$ with uniform probability distribution.

Several efficient families of universal hashing functions are known [7]. The functions in these families can be described using $O(n+m)$ bits and posses an efficient (e.g., polynomial-time and even logspace) evaluating algorithms.

The two main facts we will use about universal hash families are:

### Pairwise Independence

**Lemma 1** *The set of random variables $\{h(x)|x \in \{0,1\}^n\}$ defined by a random $h \in H$ are pairwise independent.*

### Leftover Hash Lemma

This fundamental lemma of [20] asserts that a random hash function from a universal family will smooth min-entropy $k$ (recall definition in the previous section) whenever the range $M$ is smaller than $k$. More precisely

**Lemma 2** (Leftover Hash Lemma [20]): *Let $X$ be any random variable on $\{0,1\}^n$ with min-entropy $k$. Then the distribution $(h, h(X))$, with $h$ chosen at random from $H_{n,m}$, has (norm-1) distance $2^{(m-k)/2}$ from the uniform distribution.*

## A.2 Expanders

### The Expander Mixing Lemma

The following lemma is folklore and has appeared in many papers. Loosely speaking, the lemma asserts that expander graphs (for which $d \gg \lambda$) have the property that the fraction of edges between two large sets of vertices approximately equals the product of the densities of these sets. This property is called *mixing*.

**Lemma 3** (Expander Mixing Lemma): *Let $G = (V, E)$ be an expander graph of degree $d$ and $\lambda$ be an upper bound on the absolute value of all eigenvalues, save the biggest one, of the adjacency*

*matrix of the graph. Then for every two subsets, $A, B \subseteq V$, it holds*

$$\left| \frac{|(A \times B) \cap E|}{|E|} - \frac{|A|}{|V|} \cdot \frac{|B|}{|V|} \right| \leq \frac{\lambda \sqrt{|A| \cdot |B|}}{d \cdot |V|} < \frac{\lambda}{d}$$

**The Expander Smoothing Lemma**

The following lemma follows easily by the standard techniques of dealing with random walks on expander graphs.

**Lemma 4** (Expander Smoothing Lemma): *Let $G = (V, E)$, $d$ and $\lambda$ be as in the previous lemma. Let $X$ be a random variable, distributed over $V$, so that $\mathrm{Prob}(X = v) \leq \frac{K}{|V|}$, for every $v \in V$, and $Y$ denote the vertex reached from $X$ by following a uniformly chosen edge. Then*

$$\sum_{v \in V} |\mathrm{Prob}(Y = v) - \frac{1}{|V|}| < \frac{\lambda}{d} \cdot \sqrt{K - 1}$$

## A.3 Small Probability Spaces with the Small Bias Property

The following definition of small-bias sample spaces implies the definition presented in section 4.

**Definition 3** *Let $k$ be an integer, $p$ be a prime and $\omega$ be a $p^{\text{th}}$ root of unity (in the complex field). A set $S \subseteq GF(p)^t$ is said to have $\epsilon$* bias (sample space for $GF(p)^t$) *if, for every $t$-long sequence $(a_1, ..., a_t)$ of elements in $GF(p)$, so that not all $a_i$'s are zero, the expectation of (the norm-2 of) $\omega^{\sum_{i=1}^{t} a_i s_i}$, taken over all $(s_1, ..., s_t) \in S$ with uniform distribution, is bounded above by $\epsilon$.*

By Alon et. al. [3] (see also Even et. al. [14])

**Theorem 10** *For every integer $t$, prime $p$ and $\epsilon > 0$, there exists an efficiently constructible $\epsilon$-bias sample space of size $(t/\epsilon)^2$ for $GF(p)^t$.*

## A.4 Nisan-Zuckerman Extractors

The following version (which is not completely general) of the results in [28] is sufficient for our purposes. A family of functions $H$ mapping $n$-bit strings to $m$-bit strings is $(\delta, \epsilon)$–extracting, if for every random variable $X$ of min-entropy $\delta n$, the distribution $(h, h(X))$ has distance $\epsilon$ from the uniform distribution, when $h$ is chosen uniformly from $H$. Then [28] prove:

**Theorem 11** [28]: *For every $\delta > 0$ and $\epsilon = \epsilon(n)$ there is an explicit construction of a $(\delta, \epsilon)$-extracting family with $m = \delta^2 n$ of size $n^{O(\log(1/\epsilon))}$.*

# B Proofs of Upper Bounds

## B.1 Mixing Families – Proof of Theorem 1

Clearly, the family $F$ satisfies the succinctness and efficiency requirements. We now turn to prove that it satisfies the mixing property. It suffices to consider sets $A$ of density $\geq \epsilon$ (otherwise the claim holds trivially).

We first observe that by the Expander Mixing Lemma, it holds that

$$|\mathrm{Prob}(X_n \in A \wedge g_D(X_n) \in B) - \rho(A)\rho(B)| < \frac{\lambda}{d} \leq \epsilon^2$$

where $D$ is a random variable uniformly distributed over $[d]$, and $A, B$ and $X_n$ are as in the statement of the theorem. Rewriting the above we get

$$\left| \sum_{a \in A} \mathrm{Prob}(g_D(a) \in B) - \rho(B) \cdot |A| \right| < \epsilon^2 \cdot 2^n \leq \epsilon |A| \tag{1}$$

Before continuing with the proof let us provide an overview. As just stated, the Expander Mixing Lemma states that $\sum_i \frac{1}{d} p_i(A,B)$ is a good approximation of $\rho(A)\rho(B)$, where $p_i(A,B) \stackrel{\mathrm{def}}{=} \mathrm{Prob}(X_n \in A \wedge g_i(X_n) \in B)$. If, for most $i \in [d]$, each $p_i(A,B)$ were a good approximation to $\rho(A)\rho(B)$ then we would be done. But, we don't know whether this property hold. Instead, we partition $A$ into a small number of subsets, $A_\alpha$, associate a random $i_\alpha \in [d]$ for each such $A_\alpha$ and consider how well $\sum_\alpha p_{i_\alpha}(A_\alpha, B)$ approximates $\sum_\alpha \rho(A_\alpha)\rho(B) = \rho(A)\rho(B)$. Specifically, the partition is to $\mathrm{poly}(1/\epsilon)$ many subsets and none of them is larger than $\mathrm{poly}(\epsilon) \cdot 2^n$. We show that when the $i_\alpha$'s are chosen in a pairwise independent manner the approximation is good with high probability. We conclude by noting that for a randomly chosen $h \in H$, setting $i_\alpha = h(\alpha)$, yields a sequence of pairwise independent $i_\alpha$'s.

Returning to the formal proof, we consider a partition of $A$ into $L \stackrel{\mathrm{def}}{=} 2^l$ subsets so that $A = \cup_{\alpha \in \{0,1\}^l} A_\alpha$ and $A_\alpha$ is the set of strings in $A$ containing only those strings $v$ with $\mathrm{lsb}(v) = \alpha$. Namely,

We now make the following mental experiment. We consider $L$ pairwise independent random variables uniformly distributed in $[d]$. These random variables are indexed by strings in $I \stackrel{\mathrm{def}}{=} \{0,1\}^l$ and are denoted by $\delta_{0^l}, ..., \delta_{1^l}$. We now define $L$ additional random variables, $Y_{0^l}, ..., Y_{1^l}$, so that $Y_\alpha$ represents the cardinality of the set of $a \in A_\alpha$ for which $g_{\delta_\alpha}(a) \in B$. Since both $D$ and $\delta_\alpha$ are uniformly distributed over $[d]$, we get

$$\begin{aligned} \mathrm{Exp}(Y_\alpha) &= \mathrm{Exp}(|\{a \in A_\alpha : g_D(a) \in B\}|) \\ &= \sum_{a \in A_\alpha} \mathrm{Prob}(g_D(a) \in B) \end{aligned}$$

and rewriting Eq 1, we get

**Fact 1:**

$$\left| \sum_{\alpha \in I} \mathrm{Exp}(Y_\alpha) - \rho(B) \cdot |A| \right| < \epsilon |A|$$

However, we are not interested in the expectation of the $Y_\alpha$'s, but rather in the probability that their sum deviates significantly from $\rho(B)\cdot|A|$. To this end we bound the probability that the sum of the $Y_\alpha$'s deviates significantly from their expectation. This is done below, using the Chebyshev Inequality

$$\begin{aligned} p &\stackrel{\text{def}}{=} \text{Prob}\left(\left|\sum_{\alpha\in I} Y_\alpha - \sum_{\alpha\in I}\text{Exp}(Y_\alpha)\right| > \epsilon|A|\right) \\ &< \frac{\text{Var}(\sum_\alpha Y_\alpha)}{(\epsilon|A|)^2} \\ &\leq \frac{\sum_\alpha \text{Exp}(Y_\alpha^2)}{(\epsilon|A|)^2} \\ &\leq \frac{\sum_\alpha |A_\alpha|^2}{\epsilon^2|A|^2} \end{aligned}$$

The sum of squares, $\sum_\alpha |A_\alpha|^2$, is maximized at the boundaries and is thus bounded by $\frac{2^n|A|}{L}$. Using the assumption $|A| > \epsilon 2^n$ and the definition of $L$, we get

$$p < \frac{2^n|A|}{L}\cdot\frac{1}{\epsilon^2|A|^2} < \frac{1}{L\epsilon^3} = \epsilon$$

Combining the bound for $p$ with Fact 1, we get

**Fact 2:**

$$\text{Prob}\left(\left|\sum_{\alpha\in I} Y_\alpha - \rho(B)\cdot|A|\right| > 2\epsilon|A|\right) < \epsilon$$

Since $H$ is a family of universal hashing function, it follows that the sequence of $h(\alpha)$'s is pairwise independent and uniformly distributed in $[d]$. Consequently, the $Y_\alpha$'s considered in the mental experiment actually represent the cardinality of the set $\{a\in A_\alpha : g_{h(\alpha)}(a)\in B\}$, when $h$ is uniformly chosen in $H$. Using Fact 2, we get

$$\text{Prob}\left(\left|\sum_{\alpha\in I}|\{a\in A_\alpha : g_{h(\alpha)}(a)\in B\}| - \rho(B)\cdot|A|\right| > 2\epsilon|A|\right) < \epsilon$$

where the probability is over all possible choices of $h\in H$, with uniform probability distribution. Observe that

$$\sum_{\alpha\in I}|\{a\in A_\alpha : g_{h(\alpha)}(a)\in B\}| = |\{a\in A : g_{h(\text{lsb}(a))}(a)\in B\}|$$

It follows that for all but an $\epsilon$ fraction of the $h\in H$

$$\left||\{a\in A : g_{h(\text{lsb}(a))}(a)\in B\}| - \rho(B)\cdot|A|\right| \leq 2\epsilon|A|$$

The theorem follows. ■

## B.2 Extracting High Min-Entropy – Proof of Theorem 6

Clearly, the family $F$ satisfies the succinctness and efficiency requirements. We now turn to prove that it satisfies the extraction property. We fix an arbitrary random variable $X \in \{0,1\}^n$, of min-entropy $n-k$, and consider the distribution $(f, f(X))$, when $f$ is randomly chosen in $F$. Once we bound the statistical difference between $(f, f(X))$ and $(f, U_m)$ by $\epsilon$, where $U_m$ is the uniform distribution over $\{0,1\}^m$, the theorem follows (by a counting argument).

Let $Z$ be a random variable representing the distribution on the $m$ most significant bits of $X$; i.e., $Z = \mathrm{msb}(X)$. For each $z \in \{0,1\}^m$, let $Y_z$ be a random variable representing the distribution on $\mathrm{lsb}(X)$ conditioned on $Z = z$; i.e., $X = Y_Z \cdot Z$. We call *bad* those $z$'s in $\{0,1\}^m$ for which $Y_z$ has 'too high' min-entropy. Namely, for $\delta > 0$ to be fixed later, let the set of bad prefixes be denoted by

$$B_\delta \stackrel{\text{def}}{=} \{z \in \{0,1\}^m : \exists y \text{ s.t. } \mathrm{Prob}(Y_z = y) > \delta\}$$

The reader can easily verify, using the min-entropy bound on $X$, that

$$\mathrm{Prob}(Z \in B_\delta) < \frac{2^{m-(n-k)}}{\delta}$$

Also, it can be verified that for every $z$

$$\mathrm{Prob}(Z = z) < 2^{-(m-k)}$$

We now turn to bound the statistical difference between the distributions $(f, f(X))$ and $(f, U_m)$, where $f \in_R F$. Denote the statistical difference between distributions $D_1$ and $D_2$ by $\Delta(D_1, D_2)$ (i.e., $\Delta(D_1, D_2) \stackrel{\text{def}}{=} \sum_\alpha |\mathrm{Prob}(D_1 = \alpha) - \mathrm{Prob}(D_2 = \alpha)|$. Then

$$\begin{aligned}
\Delta((f, f(X)), (f, U_m)) &= \mathrm{Exp}_{f \in_R F}(\Delta(f(X), U_m)) \\
&\leq \mathrm{Exp}_{f \in_R F}(\Delta(f(X'), U_m)) + \Delta(X, X')
\end{aligned}$$

where $X'$ is the random variable induced by $X$ subject to $Z \neq B_\delta$. By the above, $\Delta(X, X') < 2\frac{2^{-(n-m-k)}}{\delta}$. Let $A$ be the matrix representing the transition probabilities in a random step on the graph $G$; i.e., $Ap$ describes the probability distribution after one random step on the graph $G$, starting with the distribution $p$. Here and in the sequel, we abuse notation and refer to random variables and distributions as to vectors in the natural manner (i.e., the $i^{\text{th}}$ component of the vector $p$ is $p(i)$ and the $i^{\text{th}}$ component of the vector $X$ is the probability that $X = i$). Each column in $A$ has $d$ non-zero entries and each such entry holds the value $\frac{1}{d}$. For every $h \in H$, let $A_h$ be the matrix that results from $A$ by modifying the non-zero entries as follows. The $i^{\text{th}}$ non-zero entry in column $z$ is changed from $\frac{1}{d}$ to $\mathrm{Prob}(h(Y_z) = i)$. Note that $A_h Z$ equals $g_{h(Y_Z)}(Z)$ which in turn equals $f(X)$ for the function $f$ associated with the hashing function $h$. Thus, letting $Z' = \mathrm{msb}(X')$,

$$\begin{aligned}
\mathrm{Exp}_{f \in_R F}(\Delta(f(X'), U_m)) &= \mathrm{Exp}_{h \in_R H}(\Delta(A_h Z', U_m)) \\
&\leq \Delta(AZ', U_m) + \mathrm{Exp}_{h \in_R H}(\Delta(A_h Z', AZ')) \\
&\leq \Delta(Z', Z) + \Delta(AZ, U_m) + \mathrm{Exp}_{h \in_R H}(\Delta(A_h Z', AZ'))
\end{aligned}$$

Using the Leftover Hash Lemma Universal Hashing we get, for each $z \neq B_\delta$,

$$\mathrm{Exp}_{h \in_R H}(\Delta(h(Y_z), D)) < \sqrt[3]{\delta d}$$

where $D$ is uniformly distributed over $\{1, ..., d\}$. Fixing $\delta \stackrel{\mathrm{def}}{=} \frac{\epsilon^3}{d}$, we get for every probability vector $p$, and in particular for $p$ induced by $Z'$

$$\mathrm{Exp}_{h \in_R H}(\Delta(A_h p, Ap)) < \epsilon$$

Finally, it is left to bound $\Delta(AZ, U_m)$. This is done using the Expander Smoothing Lemma. We get

$$\Delta(AZ, U_m) < \sqrt{2^k} \cdot \frac{\lambda}{d} < \epsilon$$

Combining all the above bounds, we get

$$\Delta((f, f(X)), (f, U_m)) \quad < \quad 4 \cdot \frac{2^{-(n-m-k)}}{\delta} + \epsilon + \epsilon$$

Substituting $\delta$ for $\frac{\epsilon^3}{d}$, with $d = (\frac{2^k}{\epsilon})^c$ and using $n - m - k = 2 + ck + (4 + c) \cdot \log(1/\epsilon)$, the first term is bounded by $\epsilon$ too, and we are done. The theorem follows. ■

### B.3 Extracting Low Min-Entropy – Proof of Theorem 8

Suppose, on the contrary to the claim of the theorem, that, for a random variable $X = (X_1, ..., X_t)$ as in the hypothesis, for an $\epsilon$ fraction of the $f$'s in $F$ the random variable $f(X)$ is $\epsilon$-away (in norm-1) from the uniform distribution. Then, it follows that there is a subset $S' \subseteq S$ of $\epsilon|S|$ sequences so that, for each $\bar{s} \stackrel{\mathrm{def}}{=} (s_1, ..., s_t) \in S'$, the random variable $\sum_{i=1}^t X_i s_i$ is $\epsilon$-away from the uniform distribution. Passing to the Fourier basis[3], it follows that for each such $\bar{s} \in S'$, there exists some $j \in \{1, ..., p-1\}$, satisfying

$$\|\mathrm{Exp}(\omega^{j \sum_{i=1}^t X_i s_i})\| > \frac{\epsilon}{p}$$

where $\|c\|$ denotes the norm-2 of the complex number $c$. This means that for some fixed $j$ (say $j = 1$ wlog) the above inequality holds for all sequences in a subset $S'' \subseteq S'$ of size $\epsilon|S|/p$.

By partitioning these sequences according to the approximate direction of the exponential sum and applying a pigeon-hole argument[4], we obtain a set $B \subseteq S''$ of cardinality $\Omega(\epsilon|S|/p)$ so

[3] Additional details follow. Let $v$ (representing here the difference between the probability function of $\sum_{i=1}^t X_i s_i$ and the uniform distribution) be a sum-zero $p$-dimentional vector with norm-1 greater than $\epsilon$. Then the norm-2 of $v \stackrel{\mathrm{def}}{=} (v_1, ..., v_p)$ is at least $\epsilon/p$. The Fourier coefficients for the vector $v$ are $\hat{v} = (\hat{v_1}, ..., \hat{v_p})$, where $\hat{v_j} = \frac{1}{\sqrt{p}} \sum_i \omega^{ji} \cdot v_i$, and the norm-2 of $v$ and $\hat{v}$ are equal. Thus, the max-norm of $\hat{v}$ is at least $\epsilon/p^{1.5}$. It follows that there exists a $j$ so that $\| \sum_i v_i \omega^{ji} \| \geq \epsilon/p$ and this $j$ cannot be $p$ (since $\sum_i v_i \omega^{pi} = \sum_i v_i = 0$).

[4] E.g., partition the vectors according quaters of the plain and consider the direction halving the quater with largest number of vectors.

that

$$\|\frac{1}{|B|}\sum_{(s_1,...,s_t)\in B}\mathrm{Exp}(\omega^{\sum_{i=1}^{t}X_i s_i})\| = \Omega(\epsilon/p) \tag{2}$$

Contradiction follows by contrasting Eq. 2 with the following lemma, which generalizes Lindsey's Lemma (cf., [12, p. 88] and [2]).

**Lemma 5** *Let $A$ be an $N$-by-$M$ matrix of complex numbers, so that each row has inner-product equal to $M$ and each pair of different rows have inner-product*[5] *bounded (in norm-2) by $\epsilon' M$. Let $u$ be an $N$-dimensional probability vector with each components bounded above by $\delta$, and $v$ be an $M$-dimensional probability vector with each components being either $\frac{1}{K}$ or zero. Then,*

$$\|uAv^{\top}\| \leq \sqrt{(\epsilon'+\delta)\cdot\frac{M}{K}}$$

Lindsey's Lemma is obtained from the above by requiring the rows of $A$ to be orthogonal (i.e., $\epsilon' = 0$) and considering only flat distributions (i.e., each $u_i$ being either $\delta$ or 0).

**proof:** Denote, $\Delta \stackrel{\mathrm{def}}{=} \|uAv^{\top}\|$. Then, using Cauchy Schwarz Inequality, we get

$$\begin{aligned}\Delta^2 &\leq (v\cdot v^{\top})\cdot((uA)\cdot(uA)^{\top}) \\ &= \frac{1}{K}\cdot((\sum_i u_i A_i)\cdot(\sum_i u_i A_i)^{\top})\end{aligned}$$

where $A_i$ is the $i^{\mathrm{th}}$ row of the matrix $A$. Using the hypothesis concerning the inner-product of the rows of $A$ we obtain the bound

$$\begin{aligned}\Delta^2 &\leq \frac{1}{K}\cdot\left(\sum_{i\neq j}u_i u_j \epsilon' M + \sum_i u_i^2 M\right) \\ &= \frac{M}{K}\cdot\left(\epsilon'\sum_{i,j}u_i u_j + \sum_i u_i^2\right)\end{aligned}$$

Using $\sum_{i,j}u_i u_j = (\sum_i u_i)^2 = 1$ and maximizing $\sum_i u_i^2$ over all admissible $u$'s (i.e., $\sum_i u_i = 1$ and $0 \leq u_i \leq \delta$ for each $i$), we get $\Delta^2 \leq \frac{M}{K}\cdot(\epsilon'+\delta)$ and the lemma follows. □

Contradiction to Eq. 2 follows by considering the $p^t$-by-$|S|$ matrix with rows corresponding to elements of $GF(p)^t$ and columns corresponding to elements of $S$. The $(i,j)^{\mathrm{th}}$ entry in the matrix consists of $\omega^{\sum_{k=1}^{t}x_k s_k}$, where $(x_1,...,x_t)$ is the $i^{\mathrm{th}}$ sequence in $GF(p)^t$ and $(s_1,...,s_t)$ is the $j^{\mathrm{th}}$

[5] Note that inner-product of complex vectors is defined as component-wise complex multiplication of one vector by the conjugate of the other.

sequence in $S$. Let $u$ be a vector describing the probability distribution of the random variable $X$ (i.e., $u_x = \text{Prob}(X = x)$) and $\delta = 2^{-k}$ (the upper bound on probability for $X$). Let $v$ be the (normalized) vector charecterizing the set $B$ (i.e., $v_i$ equals $\frac{1}{|B|}$ if $i \in B$ and 0 otherwise). Note that the inner-product of different rows corresponding to sequences $x = (x_1, ..., x_t)$ and $y = (y_1, ..., y_t)$ equals $\sum_{s \in S} \omega^{\sum_{k=1}^{t}(x_k - y_k)s_k}$, which, by construction of the sample space $S$, has norm-2 bounded by $\epsilon'|S|$. Applying Lemma 5 and using the definition of $\epsilon'$, $\delta$, $M$ and $K$ (i.e., $\epsilon' = \frac{\epsilon^3}{p^5}$, $\delta = 2^{-k} \leq \epsilon^3 \cdot 2^{-5m} \approx \frac{\epsilon^3}{p^5}$, $|M| = |S|$ and $K = |B| = \Omega(\epsilon|S|/p)$ we get

$$\begin{aligned} \| \frac{1}{|B|} \sum_{(s_1,...,s_t) \in B} \text{Exp}(\omega^{\sum_{i=1}^{t} X_i s_i}) \| &\leq \sqrt{(\epsilon' + \delta) \cdot \frac{M}{K}} \\ &= O(\epsilon/p^2) \end{aligned}$$

which contradicts Eq. 2. The theorem follows. ■

# C Proofs of Lower Bounds

## C.1 For mixing families – proof of Theorem 2

**proof:** Otherwise, let $F = \{f_i : 1 \leq i \leq d\}$ be a family of functions over $\{0,1\}^n$, contradicting the claim. We construct a graph with vertex set $\{0,1\}^n$ and edges set $\{(x, f(x)) : x \in \{0,1\} \wedge f \in F\}$. Clearly, the graph has an independent set of size $N/d$, where $N \stackrel{\text{def}}{=} 2^n$. Consequently, there are two sets, $A$ and $B$, each of cardinality $N/2d$, so that there exists no function $f \in F$ and $x \in A$ so that $f(x) \in B$. The theorem follows (in a strong sense!). ■

## C.2 For extraction families – proof of Theorem 9

**proof:** Let $F = \{f_i : 1 \leq i \leq m\}$ be a family of functions as in the hypothesis of the theorem. Assume, on the contrary that $m \leq n - k$. Our argument proceeds in $m$ iterations. In the first iteration we consider the function $f_1$ and omit the strings $x \in \{0,1\}^n$ which are mapped by $f_1$ to the less likely value. In the $i^{\text{th}}$ iteration we omit the strings according to the mapping by $f_i$. After $m$ iterations we are left with a set $B$ of at least $2^k$ strings such that for every $x, y \in B$ and $f \in F$ it holds that $f(x) = f(y)$.

We now turn to the second inequality. Assume, on the contrary that $m \leq (1/\epsilon) - 1$. Without loss of generality, we assume that $m$ is odd (otherwise consider $m - 1$ of the functions in $F$). It follows that for every $x$, there exists a bit $\sigma$, so that $\text{Prob}_{f \in_R F}(f(x) = \sigma) > \frac{1+\epsilon}{2}$. Thus, there exists a bit $\sigma$, so that for at least half of the $x$'s (in $\{0,1\}^n$) the above holds. Let $X$ be a random variable uniformly distributed on these "bad" $x$'s, we get $\text{Exp}_{f \in F}(\text{Prob}(f(X) = \sigma) > \frac{1+\epsilon}{2}$, and the theorem follows. ■

# D Details for the Application to Sampling

Following the intuitive description in the main text, we define the approximation problem as follows.

**Definition 4** (The Approximation Problem): *Let* $\nu : \{0,1\}^n \mapsto [0,1]$ *be an arbitrary function,* $\bar{\nu} \stackrel{\text{def}}{=} \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \nu(x)$ *and* $\epsilon > 0$. *The* approximation problem *consists of presenting a randomized algorithm that on input* $n$ *and* $\epsilon$, *and oracle access to* $\nu$, *makes at most* $O(1/\epsilon^2)$ *oracle calls and outputs a rational number* $\tilde{\nu}$ *so that*

$$\text{Prob}(|\tilde{\nu} - \bar{\nu}| > \epsilon) < \frac{1}{3}$$

*In the* generalized approximation problem *the algorithm is given an additional parameter* $\delta > 0$, *is allowed to makes* $O(\delta/\epsilon^2)$ *oracle calls and is required to output a rational number* $\tilde{\nu}$ *so that*

$$\text{Prob}(|\tilde{\nu} - \bar{\nu}| > \epsilon) < \delta$$

As said in the main text, a solution to the approximation problem of randomness complexity $2n$ has been known [10]. The same holds for the generalized approximation problem. Note that in the generalized problem the number of oracle calls grows inversely proportional to the error probability $\delta$. We remark that a "better" avenue for dealing with very small error probability is suggested in [21, 7, 5]. Specifically, Bellare et. al. [5] show how to use any solution for the generalized problem in order to derive an algorithm that makes $O(\frac{\log(1/\delta)}{\epsilon^2})$ oracle calls, uses additional $O(\log(1/\delta))$ coins (beyond the coins used by the basic algorithm) and produces an estimate that, with probability $1-\delta$, is within a $\epsilon$ of $\bar{\nu}$. Hence, we concentrate on the randomness complexity of the approximation problem (as defined above).

**Theorem 12** *The generalized approximation problem can be solved within randomness complexity* $n + O(\log(1/\epsilon)) + O(\log(1/\delta))$.

PROOF: The idea is to use a sequence of approximately pairwise independent random sample points. These sample points are generated by selecting a sequence of pairwise independent functions from a family constructed in Theorem 1 and applying each function to a single string that is uniformly selected in $\{0,1\}^n$. (We remark that the constructions of almost $k$-wise independent sample spaces, and specifically the ones in [25, 3, 14, 13], are of no help here.)

We begin by considering the special case of Boolean functions; namely, we assume that $\nu : \{0,1\}^n \mapsto \{0,1\}$. Next, we define $A \stackrel{\text{def}}{=} \{x : \nu(x) = 1\}$. Hence, the problem reduces to approximating $|A|/N$, where $N \stackrel{\text{def}}{=} 2^n$. Using a family of functions, $F$, guaranteed by Theorem 1 (while replacing $\epsilon$ by $\epsilon'$ to be determined later), we know that for every set $B$ and all but an $\epsilon'$ fraction of the $f \in F$ we have

$$|\text{Prob}(X_n \in A \wedge f(X_n) \in B) - \rho(A)\rho(B)| < 2\epsilon'$$

where $\rho(S) \stackrel{\text{def}}{=} \frac{|S|}{2^n}$ and $X_n$ is a random variable uniformly distributed in $\{0,1\}^n$. One can easily conclude that for all but a $2\epsilon'$ fraction of the pairs, $(f, f')$, of functions in $F$ it holds

$$|\text{Prob}(f'(X_n) \in A \wedge f(X_n) \in A) - \rho(A)^2| < 4\epsilon'$$

Hence, setting $m = \frac{2}{\delta\epsilon^2}$ and randomly selecting a sequence of pairwise independent functions, $f_1, ..., f_m \in F$, we get that with probability at least $1 - m^2\epsilon'$, for every pair of functions $f_i, f_j$ $(i \neq j)$

$$|\text{Prob}(f_i(X_n) \in A \wedge f_j(X_n) \in A) - \rho(A)^2| < 4\epsilon' \tag{3}$$

At this point, we set $\epsilon'$ so that $m^2\epsilon' < \delta/4$ and $4\epsilon' < \epsilon^2\delta/4$. Note that $\epsilon' = \text{poly}(\epsilon, \delta)$ will do, and consequently $\log(1/\epsilon') = O(\log(1/\epsilon)) + O(\log(1/\delta))$.

The algorithm is now obvious. We pick uniformly in $\{0,1\}^n$ a *seed*, denoted $s$, and independently of it, we generate an $m$-long sequence of pairwise independent functions, $f_1, ..., f_m \in F$. Our sample is the sequence $s_1, ..., s_m$, where $s_i = f_i(s)$. As our estimate, we output the average of $\nu$ over this sample; namely, $\tilde{\nu} \stackrel{\text{def}}{=} \frac{1}{m}\sum_{i=1}^{m} \nu(s_i)$. To analyze the performance of this algorithm, we use an analysis analogous to the one used for pairwise independent sampling. Namely, we define a sequence of $m$ random variables, $\zeta_1, ..., \zeta_m$, so that

$$\zeta_i = \begin{cases} 1 & \text{if } f_i(X_n) \in A \\ 0 & \text{otherwise} \end{cases}$$

Using the Chebyshev Inequality, we get

$$\begin{aligned} \text{Prob}(|\tilde{\nu} - \bar{\nu}| > \epsilon) &= \text{Prob}\left(|\sum_{i=1}^{m} \zeta_i - \sum_{i=1}^{m} \text{Exp}(\zeta_i)| > \epsilon m\right) \\ &< \frac{\text{Var}(\sum_i \zeta_i)}{(\epsilon m)^2} \\ &< \frac{\sum_i \text{Exp}(\zeta_i^2)}{\epsilon^2 m^2} \\ &\quad + \frac{\sum_{i \neq j} \text{Exp}(\zeta_i\zeta_j) - \text{Exp}(\zeta_i) \cdot \text{Exp}(\zeta_j)}{\epsilon^2 m^2} \end{aligned}$$

The first term in the last expression is bounded by $\delta/2$, since $\text{Exp}(\zeta_i^2) \leq 1$ and $m = 2/(\delta\epsilon^2)$. To bound the second term note that $\text{Exp}(\zeta_i) = \rho(A)$ and $\text{Exp}(\zeta_i\zeta_j) = \text{Prob}(f_i(X_n) \in A \wedge f_j(X_n) \in A)$, for every $i, j$. Using Eq. 3 for most of choices of the $f_i, f_j$ pairs and adding an error term for the others, we bound the second term in the above expression by $\delta/2$. This concludes the analysis of the simple case of Boolean functions.

We now generalize the proof to deal with arbitrary functions $\nu$, rather than Boolean ones. We use the same algorithm, except for a different setting of the parameter $\epsilon'$, and analyze it with more care. The definition of the random variables, $\zeta_i$, is modified as follows. Let $t \stackrel{\text{def}}{=} \lceil \frac{1}{\epsilon} \rceil + 1$. We define $t+1$ sets $A_j \stackrel{\text{def}}{=} \{x : \frac{j-1}{t} \leq \nu(x) < \frac{j}{t}\}$, for $1 \leq j \leq t+1$, and set $\zeta_i = \frac{j-1}{t}$ if $f_i(X_n) \in A_j$.

We proceed by considering only functions $\nu:\{0,1\}^n \mapsto \{\frac{j-1}{t} : 1 \leq j \leq t+1\}$, rounding-up any other function in the obvious manner. This, by itself, introduces an $\epsilon/2$ error in the approximation. Following the same ideas as before, we show that for all but a $\delta/4$ fraction of the pairs, $(f, f')$, of functions in $F$ it holds for every $1 \leq r, s \leq t$

$$|\text{Prob}(f'(X_n) \in A_r \wedge f(X_n) \in A_s) - \rho(A_r)\rho(A_s)| < \frac{\epsilon^2\delta}{4t^2}$$

The rest of the analysis now follows as before, since again we will have

$$\frac{\sum_{i \neq j} \text{Exp}(\zeta_i\zeta_j) - \text{Exp}(\zeta_i) \cdot \text{Exp}(\zeta_j)}{\epsilon^2 m^2} < \frac{(m^2/2) \cdot (\epsilon^2\delta/4)}{\epsilon^2 m^2} + \frac{\delta}{4} = \frac{\delta}{2}$$

The theorem follows. ■

## A Simpler Sampler for the Boolean Case

For the case of Boolean functions, a much simpler sampler, meeting the complexity bounds of the sampler presented above, exists. In fact, this simpler sampler has even lower randomness complexity (specifically $n$ instead of $n + O(\log(1/\epsilon))$). Our sampling procedure is exactly the one that was presented by Karp, Pippinger and Sipser for hitting a witness set [22], yet the analysis is somewhat more involved. Furthermore, to get an algorithm which samples the universe only on $O(\delta/\epsilon^2)$ points, it is crucial to use a Ramanujan graph in role of the expander in the Karp-Pippinger-Sipser method. Again, we present a sampler for constant $\delta$ and derive the result for general $\delta$ using the method of Bellare et. al. [5].

### Construction

As said, the sampling algorithm uses, in an essential way, an explicit construction of a Ramanujan (expander) graph [23]; namely, expanders with second eigenvalue, $\lambda$, satisfying $\lambda \leq 2\sqrt{d}$, where $d$ denotes the degree. Specifically, we use an expander of degree $d = 4/\delta\epsilon^2$ and associate the vertex set of the expander with $\{0,1\}^n$. The sampling algorithm consists of uniformly selecting a vertex, $v$, (of the expander) and averaging over the values assigned (by $\nu$) to the neighbours of $v$; namely,

$$\tilde{\nu} \stackrel{\text{def}}{=} \frac{1}{d} \sum_{u \in \mathcal{N}(v)} \nu(u)$$

where $\mathcal{N}(v)$ denotes the set of neighbours of vertex $v$.

### Analysis

We denote by $B$ the set of *bad* choices for the algorithm; namely, the set of vertices that once selected by the algorithm yield a wrong estimate. That is, $v \in B$ if

$$\left| \frac{1}{d} \sum_{u \in \mathcal{N}(v)} \nu(u) - \bar{\nu} \right| > \epsilon$$

Denote by $B'$ the subset of $v \in B$ for which

$$\frac{1}{d} \sum_{u \in \mathcal{N}(v)} \nu(u) > \bar{\nu} + \epsilon \tag{4}$$

It follows that each $v \in B'$ has $\epsilon d$ too many neighbours in the set $A \stackrel{\text{def}}{=} \{u : \nu(u) = 1\}$; namely,

$$|\{u \in \mathcal{N}(v) : u \in A\}| > (\rho(A_i) + \epsilon) \cdot d \tag{5}$$

where $\rho(A) \stackrel{\text{def}}{=} \frac{|A|}{N}$ and $N \stackrel{\text{def}}{=} 2^n$. Using the Expander Mixing Lemma ones gets that

$$\begin{aligned}
\epsilon \cdot \rho(B') &= \left| \frac{|B'| \cdot (\rho(A) + \epsilon)d}{dN} - \rho(B) \cdot \rho(A) \right| \\
&\leq \left| \frac{|(B' \times A) \cap E|}{|E|} - \frac{|A|}{|V|} \cdot \frac{|B|}{|V|} \right| \\
&\leq \frac{\lambda}{d} \cdot \frac{\sqrt{|A| \cdot |B'|}}{N} \\
&\leq \frac{2}{\sqrt{d}} \cdot \sqrt{\rho(A) \cdot \rho(B')}
\end{aligned}$$

and $\rho(B') \leq \delta \rho(A)$ follows. Using a similar argument, we can show that and $\rho(B - B') \leq \delta(1 - \rho(A))$. Thus, $\rho(B) \leq \delta$ and the claim follows. ■