Extensions to the method of multiplicities, with applications to Kakeya sets and mergers

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1109/FOCS.2009.40">http://dx.doi.org/10.1109/FOCS.2009.40</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Citable link</td>
<td><a href="http://hdl.handle.net/1721.1/59284">http://hdl.handle.net/1721.1/59284</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher’s policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.</td>
</tr>
</tbody>
</table>
Extensions to the Method of Multiplicities, with applications to Kakeya Sets and Mergers

Zeev Dvir*  Swastik Kopparty†  Shubhangi Saraf‡  Madhu Sudan§

Abstract—We extend the “method of multiplicities” to get the following results, of interest in combinatorics and randomness extraction.

1) We show that every Kakeya set (a set of points that contains a line in every direction) in $\mathbb{F}_q^n$ must be of size at least $q^n/2^\Omega(n)$. This bound is tight to within a $2 + o(1)$ factor for every $n$ as $q \to \infty$, compared to previous bounds that were off by exponential factors in $n$.

2) We give an improved construction of “randomness mergers”. Mergers are seeded functions that take as input $\Lambda$ (possibly correlated) random variables in $\{0, 1\}^\Lambda$ and a short random seed, and output a single random variable in $\{0, 1\}^\Lambda$ that is statistically close to having entropy $(1 - \delta)\cdot N$ when one of the $\Lambda$ input variables is distributed uniformly. The seed we require is only $(1/\delta) \cdot \log \Lambda$-bits long, which significantly improves upon previous construction of mergers.

3) We show how to construct randomness extractors that use logarithmic length seeds while extracting $1 - o(1)$ fraction of the min-entropy of the source. Previous results could extract only a constant fraction of the entropy while maintaining logarithmic seed length.

The “method of multiplicities”, as used in prior work, analyzed subsets of vector spaces over finite fields by constructing somewhat low degree interpolating polynomials that vanish on every point in the subset with high multiplicity. The typical use of this method involved showing that the interpolating polynomial also vanished on some points outside the subset, and then used simple bounds on the number of zeroes to complete the analysis. Our augmentation to this technique is that we prove, under appropriate conditions, that the interpolating polynomial vanishes with high multiplicity on the subset $K$. This requirement often forces one to use polynomials of higher degree than in the polynomial method, but it gains in the second step by using the high multiplicity of zeroes to conclude “more easily” that the polynomial is zero at other points. This typically leads to a tighter analysis of the combinatorial parameters of interest. The method has been applied widely in list-decoding starting with Sudan [Sud97] and subsequent works. Recently the method has been applied to analyze “extractors” by Guruswami, Umans, and Vadhan [GUV07]. Most relevant to this current paper are its applications to lower bound the cardinality of “Kakeya sets” by Dvir [Dvi08], and the subsequent constructions of “mergers” and “extractors” by Dvir and Wigderson [DW08]. (We will elaborate on some of these results shortly.)

The method of multiplicities, as we term it, may be considered an extension of this method. In this extension one constructs polynomials that vanish with high multiplicity on the subset $K$. This requirement often forces one to use polynomials of higher degree than in the polynomial method, but it gains in the second step by using the high multiplicity of zeroes to conclude “more easily” that the polynomial is zero at other points. This typically leads to a tighter analysis of the combinatorial parameters of interest. This method has been applied widely in list-decoding starting with the work of Guruswami and Sudan [GS99] and continuing through many subsequent works, most significantly in the works of Parvaresh and Vardy [PV05] and Guruswami and Rudra [GR06] leading to rate-optimal list-decodable codes. Very recently this method was also applied to improve the lower bounds on the size of “Kakeya sets” by Saraf and Sudan [SS08].

The main contribution of this paper is an extension to this method, that we call the extended method of multiplicities, which develops this method (hopefully) fully to derive even tighter bounds on the combinatorial parameters. In our
extension, we start as in the method of multiplicities to construct a polynomial that vanishes with high multiplicity on every point of \( K \). But then we extend the second step where we exploit the algebraic conditions to show that the polynomial vanishes with \textit{high multiplicity} on some points outside \( K \) as well. Finally we extend the third step to show that this gives better bounds on the combinatorial parameters of interest.

By these extensions we derive nearly optimal lower bounds on the size of Kakeya sets and qualitatively improved analysis of mergers leading to new extractor constructions. We also rederive algebraically a known bound on the list-size in the list-decoding of Reed-Solomon codes. We describe these contributions in detail next, before going on to describe some of the technical observations used to derive the extended method of multiplicities (which we believe are of independent interest).

1.1. Kakeya Sets over Finite Fields

Let \( \mathbb{F}_q \) denote the finite field of cardinality \( q \). A set \( K \subset \mathbb{F}_q^n \) is said to be a Kakeya set if it “contains a line in every direction”. In other words, for every “direction” \( b \in \mathbb{F}_q^n \) there should exist an “offset” \( a \in \mathbb{F}_q^n \) such that the “line” through \( a \) in direction \( b \), i.e., the set \( \{ a + tb | t \in \mathbb{F}_q \} \), is contained in \( K \). A question of interest in combinatorics/algebra/geometry, posed originally by Wolff [Wol99], is: “What is the size of the smallest Kakeya set, for a given choice of \( q \) and \( n \)?”

The trivial upper bound on the size of a Kakeya set is \( q^n \) and this can be improved to roughly \( \frac{1}{n} q^n + O(q^{n-1}) \), see [SS08] for a proof of this bound due to Dvir, also discovered independently by Thas [That99]. An almost trivial lower bound is \( q^{n/2} \) (every Kakeya set “contains” at least \( q^{n/2} \) lines, but there are at most \( |K|^2 \) lines that intersect \( K \) at least twice). Till recently even the exponent of \( q \) was not known precisely (see [Dvi08] for details of work prior to 2008). This changed with the result of [Dvi08] (combined with an observation of Alon and Tao) who showed that for every \( n \), \( |K| \geq c_n q^n \), for some constant \( c_n \) depending only on \( n \).

Subsequently the work [SS08] explored the growth of the constant \( c_n \) as a function of \( n \). The result of [Dvi08] shows that \( c_n \geq 1/n! \), and [SS08] improve this bound to show that \( c_n \geq 1/(2.6)^n \). This still leaves a gap between the upper bound and the lower bound and we effectively close this gap.

\textbf{Theorem 1:} If \( K \) is a Kakeya set in \( \mathbb{F}_q^n \) then \( |K| \geq \frac{1}{q^2} q^n \).

Note that our bound is tight to within a \( 2 + o(1) \) multiplicative factor as long as \( q = \omega(2^n) \) and in particular when \( n = O(1) \) and \( q \to \infty \).

1.2. Randomness Mergers and Extractors

A general quest in the computational study of randomness is the search for simple primitives that manipulate random variables to convert their randomness into more useful forms. The exact notion of utility varies with applications. The most common notion is that of “extractors” that produce an output variable that is distributed statistically close to uniformly on the range. Other notions of interest include “condensers”, “dispersers” etc. One such object of study (partly because it is useful to construct extractors) is a “randomness merger”. A randomness merger takes as input \( \Lambda \), possibly correlated, random variables \( A_1, \ldots, A_\Lambda \), along with a short uniformly random seed \( B \), which is independent of \( A_1, \ldots, A_\Lambda \), and “merges” the randomness of \( A_1, \ldots, A_\Lambda \). Specifically the output of the merger should be statistically close to a high-entropy-rate source of randomness provided at least one of the input variables \( A_1, \ldots, A_\Lambda \) is uniform.

Mergers were first introduced by Ta-Shma [TS96a] in the context of explicit constructions of extractors. A general framework was given in [TS96a] that reduces the problem of constructing good extractors into that of constructing good mergers. Subsequently, in [LRVW03], mergers were used in a more complicated manner to create extractors which were optimal to within constant factors. The mergers of [LRVW03] had a very simple algebraic structure: the output of the merger was a random linear combination of the blocks over a finite vector space. The [LRVW03] merger analysis was improved in [DS07] using the connection to the finite field Kakeya problem and the (then) state of the art results on Kakeya sets.

The new technique in [Dvi08] inspired Dvir and Wigderson [DW08] to give a very simple, algebraic, construction of a merger which can be viewed as a derandomized version of the [LRVW03] merger. They associate the domain of each random variable \( A_i \) with a vector space \( \mathbb{F}_q^n \). With the \( \Lambda \)-tuple of random variables \( A_1, \ldots, A_\Lambda \), they associate a curve \( C: \mathbb{F}_q \to \mathbb{F}_q^n \) of degree \( \leq \Lambda \) which ‘passes’ through all the points \( A_1, \ldots, A_\Lambda \) (that is, the image of \( C \) contains these points). They then select a random point \( u \in \mathbb{F}_q \) and output \( C(u) \) as the “merged” output. They show that if \( q \geq \log(\Lambda \cdot n) \) then the output of the merger is statistically close to a distribution of entropy-rate arbitrarily close to 1 on \( \mathbb{F}_q^n \).

While the polynomial (or at least linear) dependence of \( q \) on \( \Lambda \) is essential to the construction above, the requirement \( q \geq \log(n) \) appears only in the analysis. In our work we remove this restriction to show:

\textbf{Informal Theorem [Merger]:} For every \( \Lambda, q \) the output of the Dvir-Wigderson merger is close to a source of entropy rate \( 1 - \log_q \Lambda \). In particular there exists an explicit merger for \( \Lambda \) sources (of arbitrary length) that outputs a source with entropy rate \( 1 - \delta \) and has seed length \( (1/\delta) \cdot \log(\Lambda/\epsilon) \) for any error \( \epsilon \).
The above theorem (in its more formal form given in Theorem 16) allows us to merge $\Lambda$ sources using seed length which is only logarithmic in the number of sources and does not depend entirely on the length of each source. Earlier constructions of mergers required the seed to depend either linearly on the number of blocks [LRW03], [Zuc07] or to depend also on the length of each block [DW08].

One consequence of our improved merger construction is an improved construction of extractors. Recall that a $(k, \epsilon)$-extractor $E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is a deterministic function that takes any random variable $X$ with min-entropy at least $k$ over $\{0, 1\}^n$ and an independent uniformly distributed seed $Y \in \{0, 1\}^d$ and converts it to the random variable $E(X, Y)$ that is $\epsilon$-close in statistical distance to a uniformly distributed random variable over $\{0, 1\}^m$. Such an extractor is efficient if $E$ is polynomial time computable.

A diverse collection of efficient extractors are known in the literature (see the survey [Sha02] and the more recent [GUV07], [DW08] for references) and many applications have been found for explicit extractor is various research areas spanning theoretical computer science. Yet all previous constructions lost a linear fraction of the min-entropy of the source (i.e., achieved $m = (1-\epsilon)k$ for some constant $\epsilon > 0$) or used super-logarithmic seed length ($d = \omega(\log n)$).

We show that our merger construction yields, by combining with several of the prior tools in the arsenal of extractor constructions, an extractor which extracts a $1 - \frac{1}{\text{polylog}(n)}$ fraction of the minentropy of the source, while still using $O(\log n)$-length seeds. We now state our extractor result in an informal way (see Theorem 20 for the formal statement).

Informal Theorem [Extractor]: There exists an explicit $(k, \epsilon)$-extractor for all min-entropies $k$ with $O(\log n)$ seed, entropy loss $O(k/\text{polylog}(n))$ and error $\epsilon = 1/\text{polylog}(n)$, where the powers in the $\text{polylog}(n)$ can be arbitrarily high constants.

1.3. List-Decoding of Reed-Solomon Codes

The Reed-Solomon list-decoding problem is the following: Given a sequence of points

$$ \{ (\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n) \in \mathbb{F}_q \times \mathbb{F}_q, $$

and parameters $k$ and $t$, find the list of all polynomials $p_1, \ldots, p_L$ of degree at most $k$ that agree with the given set of points on $t$ locations, i.e., for every $j \in \{1, \ldots, L\}$ the set $\{i|p_j(\alpha_i) = \beta_i\}$ has at least $t$ elements. (Strictly speaking the problem requires $\alpha_i$’s to be distinct, but we will consider the more general problem here.) The associated combinatorial problem is: How large can the list size, $L$, be for a given choice of $k, t, n, q$ (when maximized over all possible set of distinct input points)?

A somewhat nonstandard, yet reasonable, interpretation of the list-decoding algorithms of [Sud97], [GS99] is that they give algebraic proofs, by the polynomial method and the method of multiplicities, of known combinatorial upper bounds on the list size, when $t > \sqrt{kn}$. Their proofs happen also to be algorithmic and so lead to algorithms to find a list of all such polynomials.

However, the bound given on the list size in the above works does not match the best known combinatorial bound. The best known bound to date seems to be that of Cassuto and Bruck [CB04] who show that, letting $R = k/n$ and $\gamma = t/n$, if $\gamma^2 > R$, then the list size $L$ is bounded by $O(\frac{n^2}{R})$ (in contrast, the Johnson bound and the analysis of [GS99] gives a list size bound of $O(\frac{n}{\sqrt{R}})$, which is asymptotically worse for, say, $\gamma = (1 + O(1))\sqrt{R}$ and $R$ tending to $0$).

In the full version of this paper [DKSS09, Theorem 34], we recover the bound of [CB04] using our extended method of multiplicities.

1.4. Technique: Extended method of multiplicities

The common insight to all the above improvements is that the extended method of multiplicities can be applied to each problem to improve the parameters. Here we attempt to describe the technical novelties in the development of the extended method of multiplicities.

For concreteness, let us take the case of the Kakeya set problem. Given a set $K \subseteq \mathbb{F}^n_q$, the method first finds a non-zero polynomial $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ that vanishes with high multiplicity $m$ on each point of $K$. The next step is to prove that $P$ vanishes with fairly high multiplicity $\ell$ at every point in $\mathbb{F}^m_q$ as well. This step turns out to be somewhat subtle (and is evidenced by the fact that the exact relationship between $m$ and $\ell$ is not simple). Our analysis here crucially uses the fact that the (Hasse) derivatives of the polynomial $P$, which are the central to the notion of multiplicity of roots, are themselves polynomials, and also vanish with high multiplicity at points in $K$. This fact does not seem to have been needed/used in prior works and is central to ours.

A second important technical novelty arises in the final step of the method of multiplicities, where we need to conclude that if the degree of $P$ is “small”, then $P$ must be identically zero. Unfortunately in our application the degree of $P$ may be much larger than $q$ (or $nq$, or even $q^n$). To prove that it is identically zero we need to use the fact that $P$ vanishes with high multiplicity at every point in $\mathbb{F}^m_q$, and this requires some multiplicity-enhanced version of the standard Schwartz-Zippel lemma. We prove such a strengthening, showing that the expected multiplicity of zeroes of a degree
We start with some notation. We use $[n]$ to denote the set \{1,\ldots,n\}. For a vector $i = \langle i_1,\ldots,i_n \rangle$ of non-negative integers, its weight, denoted $\text{wt}(i)$, equals $\sum_{j=1}^{n} i_j$.

Let $\mathbb{F}$ be any field, and $\mathbb{F}_q$ denote the finite field of $q$ elements. For $X = \langle X_1,\ldots,X_n \rangle$, let $\mathbb{F}[X]$ be the ring of polynomials in $X_1,\ldots,X_n$ with coefficients in $\mathbb{F}$. For a polynomial $P(X)$, we let $H_P(X)$ denote the homogeneous part of $P(X)$ of highest total degree.

For a vector of non-negative integers $i = \langle i_1,\ldots,i_n \rangle$, let $X^i$ denote the monomial $\prod_{j=1}^{n} X_j^{i_j} \in \mathbb{F}[X]$. Note that the (total) degree of this monomial equals $\text{wt}(i)$. For $n$-tuples of non-negative integers $i$ and $j$, we use the notation

\[ \binom{i}{j} = \prod_{k=1}^{n} \binom{i_k}{j_k}. \]

Note that the coefficient of $Z^i W^{r-i}$ in the expansion of $\langle Z + W \rangle^r$ equals $\binom{r}{i}$.

**Definition 2 (Hasse Derivative):** For $P(X) \in \mathbb{F}[X]$ and non-negative vector $i$, the $i$th (Hasse) derivative of $P$, denoted $P^{(i)}(X)$, is the coefficient of $Z^i$ in the polynomial $\tilde{P}(X,Z) = P(X+Z) \in \mathbb{F}[X,Z]$.

Thus,

\[ P(X+Z) = \sum_i P^{(i)}(X) Z^i. \quad (1) \]

We are now ready to define the notion of the (zero-)multiplicity of a polynomial at any given point.

**Definition 3 (Multiplicity):** For $P(X) \in \mathbb{F}[X]$ and $a \in \mathbb{F}^n$, the multiplicity of $P$ at $a \in \mathbb{F}^n$, denoted $\text{mult}(P,a)$, is the largest integer $M$ such that for every non-negative vector $i$ with $\text{wt}(i) < M$, we have $P^{(i)}(a) = 0$ (if $M$ may be taken arbitrarily large, we set $\text{mult}(P,a) = \infty$).

Note that $\text{mult}(P,a) \geq 0$ for every $a$. Also, $P(a) = 0$ if and only if $\text{mult}(P,a) \geq 1$.

The above notations and definitions also extend naturally to a tuple $P(X) = \langle P_1(X),\ldots,P_m(X) \rangle$ of polynomials with $P^{(i)} \in \mathbb{F}[X]^m$ denoting the vector $\langle P_1^{(i)},\ldots,P_m^{(i)} \rangle$. In particular, we define $\text{mult}(P,a) = \min_{j \in [m]} \{\text{mult}(P_j,a)\}$.

The definition of multiplicity above is similar to the standard (analytic) definition of multiplicity with the difference that the standard partial derivative has been replaced by the Hasse derivative. The Hasse derivative is also a reasonably well-studied quantity (see, for example, [HKT08, pages 144-155]) and seems to have first appeared in the CS literature (without being explicitly referred to by this name) in the work of Guruswami and Sudan [GS99]. It typically behaves like the standard derivative, but with some key differences that make it more useful/informative over finite fields. For completeness we review basic properties of the Hasse derivative and multiplicity in the following subsections.

### 2.2. Properties of Hasse Derivatives

The following proposition lists basic properties of the Hasse derivatives. Parts (1)-(3) below are the same as for the analytic derivative, while Part (4) is not! Part (4) considers the derivatives of the derivatives of a polynomial and shows a different relationship than is standard for the analytic derivative. However crucial for our purposes is that it shows that the $j$th derivative of the $i$th derivative is zero if (though not necessarily only if) the $(i+j)$-th derivative is zero.

**Proposition 4 (Basic Properties of Derivatives):** Let $P(X), Q(X) \in \mathbb{F}[X]^m$ and let $i, j$ be vectors of nonnegative integers. Then:

1) $P^{(i)}(X) + Q^{(i)}(X) = (P + Q)^{(i)}(X)$. 

Organization of this paper. In Section 2 we define the notion of the multiplicity of the roots of a polynomial, using the notion of the Hasse derivative. We present some basic facts about multiplicities and Hasse derivatives, and also present the multiplicity based version of the Schwartz-Zippel lemma. In Section 3 we present our lower bounds for Kakeya sets. In Section 4 we extend this analysis for “curves” and for “statistical” versions of the Kakeya property. This leads to our analysis of the Dvir-Wigderson merger in Section 5. We then show how to use our mergers to construct the novel extractors in Section 6.

### 2. Preliminaries

In this section we formally define the notion of “multiplicity of zeroes” along with the companion notion of the “Hasse derivative”. We also describe basic properties of these notions, concluding with the “multiplicity-enhanced version” of the Schwartz-Zippel lemma. Due to space limitations proofs are omitted and may be found in the full version [DKSS09].

### 2.1. Basic definitions

For a vector of non-negative integers $i = \langle i_1,\ldots,i_n \rangle$ of non-negative integers, its weight, denoted $\text{wt}(i)$, equals $\sum_{j=1}^{n} i_j$.

Let $\mathbb{F}$ be any field, and $\mathbb{F}_q$ denote the finite field of $q$ elements. For $X = \langle X_1,\ldots,X_n \rangle$, let $\mathbb{F}[X]$ be the ring of polynomials in $X_1,\ldots,X_n$ with coefficients in $\mathbb{F}$. For a polynomial $P(X)$, we let $H_P(X)$ denote the homogeneous part of $P(X)$ of highest total degree.

For a vector of non-negative integers $i = \langle i_1,\ldots,i_n \rangle$, let $X^i$ denote the monomial $\prod_{j=1}^{n} X_j^{i_j} \in \mathbb{F}[X]$. Note that the (total) degree of this monomial equals $\text{wt}(i)$. For $n$-tuples of non-negative integers $i$ and $j$, we use the notation

\[ \binom{i}{j} = \prod_{k=1}^{n} \binom{i_k}{j_k}. \]

Note that the coefficient of $Z^i W^{r-i}$ in the expansion of $\langle Z + W \rangle^r$ equals $\binom{r}{i}$.
2) If $P$ is homogeneous of degree $d$, then $P^{(i)}$ is homogeneous of degree $d - w(i)$.

3) $(H_{P^{(i)}})(X) = H_{P^{(i)}}(X)$

4) $(P^{(i)})^{(j)}(X) = (i+j)P^{(i+j)}(X)$.

We now translate some of the properties of the Hasse derivative into properties of the multiplicities.

**Lemma 5 (Basic Properties of multiplicities):** If $P(X) \in \mathbb{F}[X]$ and $a \in \mathbb{F}^n$ are such that $\text{mult}(P, a) = m$, then $\text{mult}(P^{(i)}, a) \geq m - w(i)$.

We now discuss the behavior of multiplicities under composition of polynomial tuples. Let $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_k)$ be formal variables. Let $P(X) = (P_1(X), \ldots, P_m(X)) \in \mathbb{F}[X]^m$ and $Q(Y) = (Q_1(Y), \ldots, Q_l(Y)) \in \mathbb{F}[Y]^l$. We define the composition polynomial $P \circ Q(Y) \in \mathbb{F}[Y]^m$ to be the polynomial $P(Q_1(Y), \ldots, Q_l(Y))$. In this situation we have the following proposition.

**Proposition 6:** Let $P(X), Q(Y)$ be as above. Then for any $a \in \mathbb{F}^t$,

$$\text{mult}(P \circ Q, a) \geq \text{mult}(P, Q(a)) \cdot \text{mult}(Q - Q(a), a).$$

In particular, since $\text{mult}(Q - Q(a), a) \geq 1$, we have $\text{mult}(P \circ Q, a) \geq \text{mult}(P, Q(a))$.

Applying the above to $P(X)$ and $Q(T) = a + Tb \in \mathbb{F}[T]^n$, we get the following corollary.

**Corollary 7:** Let $P(X) \in \mathbb{F}[X]$ where $X = (X_1, \ldots, X_n)$.
Let $a, b \in \mathbb{F}^n$. Let $P_{a,b}(T)$ be the polynomial $P(a + T\cdot b) \in \mathbb{F}[T]$. Then for any $t \in \mathbb{F}$,

$$\text{mult}(P_{a,b}, t) \geq \text{mult}(P, a + t \cdot b).$$

### 2.3. Strengthening of the Schwartz-Zippel Lemma

We are now ready to state the strengthening of the Schwartz-Zippel lemma. In the standard form this lemma states that the probability that $P(a) = 0$ when $a$ is drawn uniformly at random from $S^n$ is at most $d/|S|$, where $P$ is a non-zero degree $d$ polynomial and $S \subseteq \mathbb{F}$ is a finite set. Using $\text{min}\{1, \text{mult}(P, a)\}$ as the indicator variable that is 1 if $P(a) = 0$, this lemma can be restated as saying $\sum_{a \in S^n} \text{min}\{1, \text{mult}(P, a)\} \leq d \cdot |S|^{n-1}$. Our version below strengthens this lemma by replacing $\text{min}\{1, \text{mult}(P, a)\}$ with $\text{mult}(P, a)$ in this inequality.

**Lemma 8:** Let $P \in \mathbb{F}[X]$ be a non-zero polynomial of total degree at most $d$. Then for any finite $S \subseteq \mathbb{F}$,

$$\sum_{a \in S^n} \text{mult}(P, a) \leq d \cdot |S|^{n-1}.$$

While we omit the proof, we mention briefly the idea. As in the “standard” proof of the Schwartz-Zippel lemma, we use induction on $n$. We write the polynomial $P(X)$ as a polynomial in $x_n$ with coefficients being polynomials in $x_1, \ldots, x_{n-1}$. Let the degree of this polynomial in $x_n$ be $t$ and the coefficient of $x_n^t$ be $P_t(x_1, \ldots, x_{n-1})$. For every $a_1, \ldots, a_{n-1} \in S$, we show that $\sum_{a_n \in S} \text{mult}(P_t(a_1, \ldots, a_{n-1}), a_n) \leq t + \text{mult}(P_t, a_1, \ldots, a_{n-1}) \cdot |S|$. (This replaces the step in the standard proof that shows that the number of zeroes of $P$ with the first $n - 1$ coordinates set to $a_1, \ldots, a_{n-1}$ is at most $t$ if $P_t(a_1, \ldots, a_{n-1})$ is non-zero.) The lemma follows easily, once we have this inequality.

The following corollary simply states the above lemma in contrapositive form, with $S = \mathbb{F}_q$.

**Corollary 9:** Let $P \in \mathbb{F}_q[X]$ be a polynomial of total degree at most $d$. If $\sum_{a \in \mathbb{F}_q} \text{mult}(P, a) > d \cdot q^{n-1}$, then $P(X) = 0$.

### 3. A LOWER BOUND ON THE SIZE OF KAKEYA SETS

We now give a lower bound on the size of Kakeya sets in $\mathbb{F}_q^n$. We implement the plan described in Section 1. Specifically, in Proposition 10 we show that we can find a somewhat low degree non-zero polynomial that vanishes with high multiplicity on any given Kakeya set, where the degree of the polynomial grows with the size of the set. Next, in Claim 12 we show that the homogenous part of this polynomial vanishes with fairly high multiplicity everywhere in $\mathbb{F}_q^n$. Using the strengthened Schwartz-Zippel lemma, we conclude that the homogenous polynomial is identically zero if the Kakeya set is too small, leading to the desired contradiction. The resulting lower bound (slightly stronger than Theorem 1) is given in Theorem 11.

**Proposition 10:** Given a set $K \subseteq \mathbb{F}^n$ and non-negative integers $m, d$ such that $m + n - 1 \cdot |K| < (\frac{d+1}{d})^n$, there exists a non-zero polynomial $P = P_{m,K} \in \mathbb{F}[X]$ of total degree at most $d$ such that $\text{mult}(P, a) \geq m$ for every $a \in K$.

The proof is by a simple counting argument and omitted here.

**Theorem 11:** If $K \subseteq \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq \left(\frac{q}{2-\ell/q}\right)^n$.

**Proof:** Let $\ell$ be a large multiple of $q$ and let $m = 2\ell - \ell/q$ and $d = \ell q - 1$. These three parameters ($\ell, m$, and $d$) will be used as follows: $d$ will be the bound on the degree of a polynomial $P$ which vanishes on $K$, $m$ will be the multiplicity of the zeros of $P$ on $K$ and $\ell$ will be the multiplicity of the zeros of the homogenous part of $P$ which we will deduce by restricting $P$ to lines passing through $K$.

Note that by the choices above we have $d < \ell q$ and $(m - \ell)q > d - \ell$. We prove below that $|K| \geq \left(\frac{d+1}{m+n-1}\right)^n$. Assume for contradiction that $|K| < \left(\frac{d+1}{m+n-1}\right)^n$. Then, by Proposition 10 there exists a non-zero polynomial $P(X) \in \mathbb{F}_q[X]$ such that...
\( F[X] \) of total degree exactly \( d^* \), where \( d^* \leq d \), such that \( \text{mult}(P, x) \geq m \) for every \( x \in K \). Note that \( d^* \geq \ell \) since \( d^* \geq m \) (since \( P \) is nonzero and vanishes to multiplicity \( \geq m \) at some point), and \( m \geq \ell \) by choice of \( m \). Let \( H_P(X) \) be the homogeneous part of \( P(X) \) of degree \( d^* \). Note that \( H_P(X) \) is nonzero. The following claim shows that \( H_P \) vanishes to multiplicity \( \ell \) at each point of \( F_q^n \).

**Claim 12:** For each \( b \in F_q^n \),
\[
\text{mult}(H_P, b) \geq \ell.
\]

**Proof:** Fix \( i \) with \( \text{wt}(i) = w \leq \ell - 1 \). Let \( Q(X) = P^{(i)}(X) \). Let \( d' \) be the degree of the polynomial \( Q(X) \), and note that \( d' \leq d^* - w \).

Let \( a = a(b) \) be such that \( \{a + tb \mid t \in F_q \} \subset K \). Then for all \( t \in F_q \), by Lemma 5, \( \text{mult}(Q, a + tb) \geq m - w \). Since \( w \leq \ell - 1 \) and \( (m - \ell) \cdot q > d^* - \ell \), we get that \( (m - w) \cdot q > d^* - w \).

Let \( Q_{a,b}(T) \) be the polynomial \( Q(a + T b) \in F_q[T] \). Then \( Q_{a,b}(T) \) is a univariate polynomial of degree at most \( d' \), and by Corollary 7, it vanishes at each point of \( F_q \) with multiplicity \( m - w \). Since
\[
(m - w) \cdot q > d^* - w \geq \text{deg}(Q_{a,b}(T))
\]
we conclude that \( Q_{a,b}(T) = 0 \). Hence the coefficient of \( T^{d'} \) in \( Q_{a,b}(T) \) is 0. Let \( H_Q \) be the homogenous component of \( Q \) of highest degree. Observe that the coefficient of \( T^{d'} \) in \( Q_{a,b}(T) \) is \( H_Q(b) \). Hence \( H_Q(b) = 0 \).

However \( H_Q(X) = (H_P)^{(i)}(X) \) (by item 2 of Proposition 4). Hence \( (H_P)^{(i)}(b) = 0 \). Since this is true for all \( i \) of weight at most \( \ell - 1 \), we conclude that \( \text{mult}(H_P, b) \geq \ell \).

Applying Corollary 9, and noting that \( \ell q^n > d^* q^{n-1} \), we conclude that \( H_P(X) = 0 \). This contradicts the fact that \( P(X) \) is a nonzero polynomial.

Hence, \( |K| \geq \frac{(d^* + n)}{m^{n-\ell}} \). It is straightforward to show that the bound above is at least \( (q/(2 - 1/q))^n \) as we take the limit when \( \ell \to \infty \).

**4. STATISTICAL KAKEYA FOR CURVES**

Next we extend the results of the previous section to a form conducive to analyze the mergers of Dvir and Wigderson [DW08]. The extension changes two aspects of the consideration in Kakeya sets, that we refer to as “statistical” and “curves”. We describe these terms below.

In the setting of Kakeya sets we were given a set \( K \) such that for every direction, there was a line in that direction such that every point on the line was contained in \( K \). In the statistical setting we replace both occurrences of the “every” quantifier with a weaker “for many” quantifier. So we consider sets that satisfy the condition that for many directions, there exists a line in that direction intersecting \( K \) in many points.

A second change we make is that we now consider curves of higher degree and not just lines. We also do not consider curves in various directions, but rather curves passing through a given set of special points. We start with formalizing the terms “curves”, “degree” and “passing through a given point”.

A curve of degree \( \Lambda \) in \( F_q^n \) is a tuple of polynomials \( C(X) = (C_1(X), \ldots, C_n(X)) \in F_q[X]^n \) such that \( \max_{i \in [n]} \text{deg}(C_i(X)) = \Lambda \). A curve \( C \) naturally defines a map from \( F_q \) to \( F_q^n \). For \( x \in F_q^n \), we say that a curve \( C \) passes through \( x \) if there is a \( t \in F_q \) such that \( C(t) = x \).

We now state and prove our statistical version of the Kakeya theorem for curves.

**Theorem 13 (Statistical Kakeya for curves):** Let \( \Lambda > 0, \eta > 0 \). Let \( \Lambda > 0 \) be an integer such that \( \eta q > \Lambda \). Let \( S \subset F_q^n \) be such that \( |S| = \eta q^n \). Let \( K \subset F_q^n \) be such that for each \( x \in S \), there exists a curve \( C_x \) of degree at most \( \Lambda \) that passes through \( x \), and intersects \( K \) in at least \( \eta q \) points. Then,
\[
|K| \geq \frac{\lambda q}{\Lambda \left( \frac{\lambda q - 1}{\eta q} \right) + 1}.
\]

In particular, if \( \Lambda \geq \eta \) we get that \( |K| \geq \left( \frac{\eta q}{\Lambda + 1} \right)^n \).

The proof is similar to that of Theorem 11 and omitted from this version.

**5. IMPROVED MERGERS**

In this section we state and prove our main result on randomness mergers.

**5.1. Definitions and Theorem Statement**

We start by recalling some basic quantities associated with random variables. The statistical distance between two random variables \( X \) and \( Y \) taking values from a finite domain \( \Omega \) is defined as
\[
\max_{S \subset \Omega} |\Pr[X \in S] - \Pr[Y \in S]|.
\]

We say that \( X \) is \( \epsilon \)-close to \( Y \) if the statistical distance between \( X \) and \( Y \) is at most \( \epsilon \), otherwise we say that \( X \) and \( Y \) are \( \epsilon \)-far. The min-entropy of a random variable \( X \) is defined as
\[
H_{\infty}(X) \equiv \min_{x \subset \text{supp}(X)} \log_2 \left( \frac{1}{\Pr[X = x]} \right).
\]
We say that a random variable $X$ is $\varepsilon$-close to having min-entropy $m$ if there exists a random variable $Y$ of min-entropy $m$ such that $X$ is $\varepsilon$-close to $Y$.

A “merger” of randomness takes a $\Lambda$-tuple of random variables and “merges” their randomness to produce a high-entropy random variable, provided the $\Lambda$-tuple is “somewhere-random” as defined below.

**Definition 14 (Somewhere-random source):** For integers $A$ and $N$, a simple $(N,\Lambda)$-somewhere-random source is a random variable $A = (A_1, \ldots, A_\Lambda)$ taking values in $S^\Lambda$, where $S$ is some finite set of cardinality $2^N$, such that for some $i_0 \in [\Lambda]$, the distribution of $A_{i_0}$ is uniform over $S$. A $(N,\Lambda)$-somewhere-random source is a convex combination of simple $(N,\Lambda)$-somewhere-random sources. (When $N$ and $\Lambda$ are clear from context we refer to the source as simply a “somewhere-random source”.)

We are now ready to define a merger.

**Definition 15 (Merger):** For positive integer $\Lambda$ and set $S$ of size $2^N$, a function $f : S^\Lambda \times \{0,1\}^d \rightarrow S$ is called an $(m,\varepsilon)$-merger of $(N,\Lambda)$-somewhere-random sources, if for every $(N,\Lambda)$-somewhere-random source $A = (A_1, \ldots, A_\Lambda)$ taking values in $S^\Lambda$, and for $B$ being uniformly distributed over $\{0,1\}^d$, the distribution of $f((A_1, \ldots, A_\Lambda), B)$ is $\varepsilon$-close to having min-entropy $m$.

A merger thus has five parameters associated with it: $N, \Lambda, m, \varepsilon$ and $d$. The general goal is to give explicit constructions of mergers of $(N,\Lambda)$-somewhere-random sources for every choice of $N$ and $\Lambda$, for as large an $m$ as possible, and with $\varepsilon$ and $d$ being as small as possible. Known mergers attain $m = (1-\varepsilon)N$ for arbitrarily small $\varepsilon$ and $\delta$ and our goal will be to achieve $\delta = o(1)$ as a function of $N$, while $\varepsilon$ is an arbitrarily small positive real number. Thus our main concern is the growth of $d$ as a function of $N$ and $\Lambda$. Prior to this work, the best known bounds required either $d = \Omega(\log N + \log \Lambda)$ or $d = \Omega(\log \Lambda)$. We only require $d = \Omega(\log \Lambda)$.

**Theorem 16:** For every $\varepsilon, \delta > 0$ and integers $N, \Lambda$, there exists a $((1-\delta)N, \varepsilon$)-merger of $(N,\Lambda)$-somewhere-random sources, computable in polynomial time, with seed length $d = \frac{1}{\delta} \cdot \log_2 \left(\frac{2\Lambda}{\varepsilon}\right)$.

### 5.2. The Curve Merger of $[DW08]$ and its analysis

The merger that we consider is a very simple one proposed by Dvir and Wigderson $[DW08]$, and we improve their analysis using our extended method of multiplicities. We note that they used the polynomial method in their analysis; and the basic method of multiplicities doesn’t seem to improve their analysis.

The curve merger of $[DW08]$, denoted $f_{DW}$, is obtained as follows. Let $q \geq \Lambda$ be a prime power, and let $n$ be any integer. Let $\gamma_1, \ldots, \gamma_\Lambda \in \mathbb{F}_q$ be distinct, and let $c_i(T) \in \mathbb{F}_q[T]$ be the unique degree $\Lambda - 1$ polynomial with $c_i(\gamma_i) = 1$ and for all $j \neq i$, $c_i(\gamma_j) = 0$. Then for any $x = (x_1, \ldots, x_\Lambda) \in (\mathbb{F}_q^n)^\Lambda$ and $u \in \mathbb{F}_q$, the curve merger $f_{DW}$ maps $(\mathbb{F}_q^n)^\Lambda \times \mathbb{F}_q$ to $\mathbb{F}_q^n$ as follows:

$$f_{DW}((x_1, \ldots, x_\Lambda), u) = \sum_{i=1}^\Lambda c_i(u)x_i.$$

In other words, $f_{DW}((x_1, \ldots, x_\Lambda), u)$ picks the (canonical) curve passing through $x_1, \ldots, x_\Lambda$ and outputs the $u$th point on the curve.

**Theorem 17:** Let $q \geq \Lambda$ and $A$ be somewhere-random source taking values in $(\mathbb{F}_q^n)^\Lambda$. Let $B$ be distributed uniformly over $\mathbb{F}_q$, with $A, B$ independent. Let $C = f_{DW}(A, B)$. Then for

$$q \geq \left(\frac{2\Lambda}{\varepsilon}\right)^\frac{1}{3},$$

$C$ is $\varepsilon$-close to having min-entropy $(1-\delta) \cdot n \cdot \log_2 q$.

Theorem 16 easily follows from the above. We note that $[DW08]$ proved a similar theorem assuming $q \geq \text{poly}(n, \Lambda)$, forcing their seed length to grow logarithmically with $n$ as well.

**Proof of Theorem 16:** Let $q = 2^d$, so that $q \geq \left(\frac{2\Lambda}{\varepsilon}\right)^\frac{1}{3}$, and let $n = N/d$. Then we may identify identify $\mathbb{F}_q$ with $\{0,1\}^d$ and $\mathbb{F}_q^n$ with $\{0,1\}^N$. Take $f$ to be the function $f_{DW}$ given earlier. Clearly $f$ is computable in the claimed time. Theorem 17 shows that $f$ has the required merger property.

We now prove Theorem 17.

**Proof of Theorem 17:** Without loss of generality, we may assume that $A$ is a simple somewhere-random source. Let $m = (1-\delta)N \cdot \log_2 q$. We wish to show that $f_{DW}(A, B)$ is $\varepsilon$-close to having min-entropy $m$.

Suppose not. Then there is a set $K \subseteq \mathbb{F}_q^n$ with $|K| \leq 2^m = q^{(1-\delta)N} \leq \left(\frac{\varepsilon q}{2\Lambda}\right)^n$ such that

$$\Pr_{\mathbb{A},\mathbb{B}}[f(A, B) \in K] \geq \varepsilon.$$

Suppose $A_{i_0}$ is uniformly distributed over $\mathbb{F}_q^n$. Let $A_{-i_0}$ denote the random variable

$$(A_1, \ldots, A_{i_0-1}, A_{i_0+1}, \ldots, A_\Lambda).$$

By an averaging argument, with probability at least $\lambda = \varepsilon/2$ over the choice of $A_{i_0}$, we have

$$\Pr_{A_{-i_0}, B}[f(A, B) \in K] \geq \eta,$$

where $\eta$ is a positive number depending only on $\varepsilon$. Let $A_\Lambda$ denote the random variable

$$(A_1, \ldots, A_{i_0-1}, A_{i_0+1}, \ldots, A_\Lambda).$$

We may assume that $A_{\Lambda}$ is everywhere-random; otherwise, replace $A_{\Lambda}$ with $A_{\Lambda} - \eta$. Let $S$ be a subset of $\{0,1\}^d$ with $\Pr_{x \in S}[x \in \{0,1\}^d] = \varepsilon$. We may assume that $A_{\Lambda}$ is everywhere-random; otherwise, replace $A_{\Lambda}$ with $A_{\Lambda} - \eta$. Let $S$ be a subset of $\{0,1\}^d$ with $\Pr_{x \in S}[x \in \{0,1\}^d] = \varepsilon$.

We may assume that $A_{\Lambda}$ is everywhere-random; otherwise, replace $A_{\Lambda}$ with $A_{\Lambda} - \eta$. Let $S$ be a subset of $\{0,1\}^d$ with $\Pr_{x \in S}[x \in \{0,1\}^d] = \varepsilon$. Then for every $u \in S$ such that $\Pr_{x \in S}[x \in \{0,1\}^d] = \varepsilon$, we have

$$\Pr_{A_{\Lambda}}[f(A, B) \in K| u] \geq \eta.$$
where η = ε/2. Since A_{i_0} is uniformly distributed over \( F_q^n \), we conclude that there is a set \( S \) of cardinality at least \( \lambda q^n \) such that for any \( x \in S \),
\[
\Pr[f(A, B) \in K \mid A_{i_0} = x] \geq \eta.
\]

Fixing the values of \( A_{-i_0} \), we conclude that for each \( x \in S \), there is a \( y = y(x) = (y_1, \ldots, y_A) \) with \( y_{i_0} = x \) such that \( \Pr_y[f(y, B) \in K] \geq \eta \). Define the degree \( A - 1 \) curve \( C(x) = f(y(x), T) = \sum_{j=1}^A y_j c_j(T) \). Then \( C_x \) passes through \( x \), since \( C_x(\gamma_{i_0}) = \sum_{j=1}^A y_j c_j(\gamma_{i_0}) = y_{i_0} = x \), and \( \Pr_{C_x \in F_q}[C_x(B) \in K] \geq \eta \) by definition of \( C_x \).

Thus \( S \) and \( K \) satisfy the hypothesis of Theorem 13. We now conclude that \(|K| \geq \left( \frac{\lambda q^n}{(A - 1)^{-1} + 1} \right)^n > \left( \frac{q^\lambda}{2^n} \right)^n \). This is a contradiction, and the proof of the theorem is complete.

**The Somewhere-High-Entropy case:** It is possible to extend the merger analysis given above also to the case of somewhere-high-entropy sources. In this scenario the source is comprised of blocks, one of which has min entropy at least \( c \). One can then prove an analog of Theorem 17 saying that the output of \( f_{DW} \) will be close to having min entropy \((1 - \delta) \cdot r \) under essentially the same conditions on \( q \). The proof is done by hashing the source using a random linear function into a smaller dimensional space and then applying Theorem 17 (in a black box manner). The reason why this works is that the merger commutes with the linear map (for details see [DW08]).

### 6. Extractors with sub-linear entropy loss

In this section we use our improved analysis of the Curve Merger to show the existence of an explicit extractor with logarithmic seed and sub linear entropy loss.

We will call a random variable \( X \) distributed over \( \{0, 1\}^n \) with min-entropy \( k \) an \((n, k)\)-source.

**Definition 18 (Extractor):** A function \( E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) is a \((k, \epsilon)\)-extractor if for every \((n, k)\)-source \( X \), the distribution of \( E(X, U_d) \) is \( \epsilon \)-close to uniform, where \( U_d \) is a random variable distributed uniformly over \( \{0, 1\}^d \), and \( X, U_d \) are independent. An extractor is called explicit if it can be computed in polynomial time.

It is common to refer to the quantity \( k - m \) in the above definition as the entropy loss of the extractor. The next theorem asserts the existence of an explicit extractor with logarithmic seed and sub linear entropy loss.

**Theorem 19 (Basic extractor with sub-linear entropy loss):** For every \( c_1 \geq 1 \), for all positive integers \( k < n \) with \( k \geq \log \log(n) \), there exists an explicit \((k, \epsilon)\)-extractor \( E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) with \( d = O(c_1 \cdot \log(n)) \), \( k - m = O\left( \frac{\log(n)}{\log \log(n)} \right) \), and \( \epsilon = O\left( \frac{1}{\log \log(n)} \right) \).

The extractor of this theorem is constructed by composing several known explicit constructions of pseudorandom objects with the merger of Theorem 16. In Section 6.1 we describe the construction of our basic extractor. The basic extractor can be strengthened to extract even more randomness by the ‘repeated extraction’ technique of Wigderson and Zuckerman [WZ99]. This yields an extractor with entropy loss \( k - m = O(k \log\epsilon \cdot n) \) as asserted in the following theorem, whose proof may be found in the full version.

**Theorem 20 (Final extractor with sub-linear entropy loss):** For every \( c_1, c_2 \geq 1 \), for all positive integers \( k < n \), there exists an explicit \((k, \epsilon)\)-extractor \( E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) with \( d = O(c_1 c_2 \cdot \log(n)) \), \( k - m = O\left( \frac{k}{\log^2(n)} \right) \), and \( \epsilon = O\left( \frac{1}{\log \log(n)} \right) \).

6.1. Proof of Theorem 19

Note that we may equivalently view an extractor \( E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) as a randomized algorithm \( E : \{0, 1\}^n \rightarrow \{0, 1\}^m \) which is allowed to use \( d \) uniformly random bits. We will present the extractor \( E \) as such an algorithm which takes 5 major steps.

Before giving the formal proof we give a high level description of our extractor. Our first step is to apply the lossless condenser of [GUV07] to output a string of length \( 2k \) with min entropy \( k \) (thus reducing our problem to the case \( k = \Omega(n) \)). The construction continues along the lines of [DW08]. In the second step, we partition our source (now of length \( n' = 2k \)) into \( \Lambda = \log(n) \) consecutive blocks \( X_1, \ldots, X_\Lambda \in \{0, 1\}^{n'}/\Lambda \) of equal length. We then consider the \( \Lambda \) possible divisions of the source into a prefix of \( j \) blocks and suffix of \( \Lambda - j \) blocks for \( j \) between 1 and \( \Lambda \).

By a result of Ta-Shma [TS96b], after passing to a convex combination, one of these divisions is a \((k', k_2)\) block source with \( k' \) being at least \( k - O(k/\Lambda) \) and \( k_2 \) being at least poly-logarithmic in \( k \). In the third step we use a block source extractor (from [RSW00]) on each one of the possible \( \Lambda \) divisions (using the same seed for each division) to obtain a somewhere random source with block length \( k' \). The fourth step is to merge this somewhere random source into a single block of length \( k' \) and entropy \( k' \cdot (1 - \delta) \) with \( \delta \) sub-constant. In view of our new merger parameters, and the fact that \( \Lambda \) (the number of blocks) is small enough, we can get away with choosing \( \delta = \log \log(n)/\log(n) \) and keeping the seed logarithmic and the error poly-logarithmic. To finish the construction (the fifth step) we need to extract almost all the entropy from a source of length \( k' \) and entropy \( k' \cdot (1 - \delta) \). This can be done (using known techniques) with logarithmic seed and an additional entropy loss of \( O(\delta \cdot k') \).

We now formally prove Theorem 19. We begin by reducing to the case where \( n = O(k) \) using the lossless condensers of [GUV07].
Theorem 21 (Lossless condenser [GUV07]): For all integers positive $k$ with $k = \omega(\log(n))$, there exists an explicit function $C_{\text{GUV}} : \{0, 1\}^n \times \{0, 1\}^d \to \{0, 1\}^{n'}$ with $n' = 2k$, $d' = O(\log(n))$, such that for every $(n,k)$-source $X$, $C(X, U_d)$ is $(1/n)$-close to an $(n', k)$-source, where $U_d$ is distributed uniformly over $\{0, 1\}^d$, and $X, U_d$ are independent.

Step 1: Pick $U_d$ uniformly from $\{0, 1\}^d$.
Compute $X' = C_{\text{GUV}}(X, U_d)$.

By the above theorem, $X'$ is $(1/n)$-close to an $(n', k)$-source, where $n' = 2k$. Our next goal is to produce a somewhere-block source. We now define this formally.

Definition 22 (Block Source): Let $X = (X_1, X_2)$ be a random source over $\{0, 1\}^m \times \{0, 1\}^n$. We say that $X$ is a $(k_1, k_2)$-block source if $X_1$ is an $(n_1, k_1)$-source and for each $x_1 \in \{0, 1\}^{n_1}$ the conditional random variable $X_2|X_1 = x_1$ is an $(n_2, k_2)$-source.

Definition 23 (Somewhere-block source): Let $X = (X_1, \ldots, X_\Lambda)$ be a random variable such that each $X_j$ is distributed over $\{0, 1\}^{m_j} \times \{0, 1\}^{n_j}$, for each $1 \leq j \leq \Lambda$. We say that $X$ is a simple $(k_1, k_2)$-somewhere-block source if there exists $i \in [\Lambda]$ such that $X_i$ is a $(k_1, k_2)$-block source.

We next use the block source extractor from [RSW00] to convert the above somewhere-block source to a somewhere-random source.

Theorem 25 ([RSW00]): Let $n' = n_1 + n_2$ and let $k', k_2$ be such that $k_2 > \log^4(n_1)$. Then there exists an explicit function $E_{\text{RSW}} : \{0, 1\}^{n_1} \times \{0, 1\}^{n_2} \times \{0, 1\}^d \to \{0, 1\}^{m''}$ with $m'' = k', d'' = O(\log(n'))$, such that for any $(k', k_2)$-block source $X$, $E_{\text{RSW}}(X, U_d')$ is $(n_1)^{-\Omega(1)}$-close to the uniform distribution over $\{0, 1\}^{m''}$, where $U_d'$ is distributed uniformly over $\{0, 1\}^d$, and $X, U_d'$ are independent.

Step 3: Pick $U_{d''}$ uniformly from $\{0, 1\}^{d''}$.
For each $j \in [\Lambda]$, compute $X_j'' = E_{\text{RSW}}(X_j', U_{d''})$.

By the above theorem, $X''$ is $n_1^{-\Omega(1)}$-close to a somewhere-random source. We are now ready to use the merger $M$ from Theorem 16. We invoke that theorem with entropy-loss $\delta = \log\log(n)/\log(n)$ and error $\epsilon = \frac{1}{\log^4(n)}$, and hence $M$ has a seed length of $d''' = O\left(\frac{1}{\delta} \log \frac{\Lambda}{\epsilon}\right) = O(c_1 \log(n))$.

Step 4: Pick $U_{d'''}$ uniformly from $\{0, 1\}^{d'''}$.
Compute $X''' = M(X'', U_{d''})$.

By Theorem 16, $X'''$ is $O\left(\frac{1}{\log^4(n)}\right)$-close to a $(k', 1-\delta)k'$-source. Note that $\delta = o(1)$, and thus $X'''$ has nearly full entropy. We now apply an extractor for sources with extremely-high entropy rate, given by the following lemma.

Lemma 26: For any $k'$ and $\delta > 0$, there exists an explicit $(k'(1-\delta), k'(1-\delta)^{\Omega(1)})$-extractor $E_{\text{HIGH}} : \{0, 1\}^{k'} \times \{0, 1\}^{d'''} \times \{0, 1\}^{(1-\delta)k'}$ with $d''' = O(\log(k'))$.

The proof of this lemma follows easily from Theorem 25. Roughly speaking, the input is partitioned into blocks of length $k' - \delta k - \log^4 k'$ and $\delta k + \log^4 k'$. It follows that this partition is close to a $(k'(1 - 2\delta) - \log^4 k', \log^4 k')$-block source. This block source is then passed through the block-source extractor of Theorem 25.

Step 5: Pick $U_{d''''}$ uniformly from $\{0, 1\}^{d''''}$.
Compute $X'''' = E_{\text{HIGH}}(X''', U_{d''''})$.

Output $X''''$.

This completes the description of the extractor $E$. It remains to note that $d$, the total number of random bits used, is at
most \(d' + d'' + d''' + d'''' = O(c_1 \log n)\), and that the output \(X''''\) is \(O\left(\frac{1}{\log^2 n}\right)\)-close to uniformly distributed over
\[\{0, 1\}^{(1-3\delta)k'} = \{0, 1\}^{k-O(k \cdot \log \log n)}\).

This completes the proof of Theorem 19.

We summarize the transformations in the following table:

<table>
<thead>
<tr>
<th>Transformation</th>
<th>Seed Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>(C_{GUV})</td>
<td>(O(\log(n)))</td>
</tr>
<tr>
<td>(B_{TS}^{O(\log(n))})</td>
<td>(O(\log(n)))</td>
</tr>
<tr>
<td>(E_{RGW})</td>
<td>(O(\log(k)))</td>
</tr>
<tr>
<td>(U_{k'} - o(k))</td>
<td>(O(\log(k)))</td>
</tr>
<tr>
<td>Our Merger</td>
<td>(O(\log(n)))</td>
</tr>
</tbody>
</table>

References:


