Deterministic Extractors for Affine Sources over Large Fields

Ariel Gabizon* Weizmann Institute

Ran Raz† Weizmann Institute

May 13, 2005

Abstract

An (n, k)-*affine source* over a finite field $\mathbb{F}$ is a random variable $X = (X_1, ..., X_n) \in \mathbb{F}^n$, which is uniformly distributed over an (unknown) k-dimensional affine subspace of $\mathbb{F}^n$. We show how to (deterministically) extract practically all the randomness from affine sources, for any field of size larger than n^c (where c is a large enough constant). Our main results are as follows:

1. **(For arbitrary k):** For any n, k and any $\mathbb{F}$ of size larger than n^{20}, we give an explicit construction for a function $D : \mathbb{F}^n \to \mathbb{F}^{k-1}$, such that for any (n, k)-affine source X over $\mathbb{F}$, the distribution of $D(X)$ is ϵ-close to uniform, where ϵ is polynomially small in $|\mathbb{F}|$.
2. **(For $k = 1$):** For any n and any $\mathbb{F}$ of size larger than n^c, we give an explicit construction for a function $D : \mathbb{F}^n \to \{0, 1\}^{(1-\delta)\log_2 |\mathbb{F}|}$, such that for any $(n, 1)$-affine source X over $\mathbb{F}$, the distribution of $D(X)$ is ϵ-close to uniform, where ϵ is polynomially small in $|\mathbb{F}|$. Here, $\delta > 0$ is an arbitrary small constant, and c is a constant depending on δ.

1 Introduction

Let $\mathbb{F}$ be a finite field of size q and let n be an integer. The famous Hales-Jewett theorem [14] implies that if n is large enough compared to q then in any two-coloring of the vector space $\mathbb{F}^n$ there exists a monochromatic line[1]. On the other hand, if q is significantly larger than n (say, $q \geq 3n \log_2 n$) then a random two-coloring of the vector space $\mathbb{F}^n$ doesn't have monochromatic lines (with high probability). Assume that q is large enough (say, $q \geq n^{20}$). Can one give an **explicit** two-coloring of $\mathbb{F}^n$ that doesn't have monochromatic lines ? More generally, can one give an explicit coloring $D : \mathbb{F}^n \to \{0, 1\}$, such that every line will have roughly the same number of zeros and ones ?

*Research supported by Israel Science Foundation (ISF) grant.

†Research supported by Israel Science Foundation (ISF) grant.

[1] A line is a 1-dimensional affine subspace of $\mathbb{F}^n$.

The problem of extracting randomness from affine sources is a more general problem. Fix n, k and $\mathbb{F}$. Assume that X is uniformly distributed over an **unknown** k-dimensional affine subspace of $\mathbb{F}^n$. The goal is to give an explicit example for a function $D : \mathbb{F}^n \to \Omega$ (for some finite set Ω), such that the distribution of $D(X)$ is ϵ-close to uniform. Naturally, we would like Ω to be as large as possible and ϵ to be as small as possible.

1.1 Affine source extractors

Denote by $\mathbb{F}_q$ the finite field with q elements. Denote by $\mathbb{F}_q^n$ the n-dimensional vector space over $\mathbb{F}_q$.
Definition 1 (affine source). *A distribution X over $\mathbb{F}_q^n$ is an $(n,k)_q$-affine source if it is uniformly distributed over an affine subspace of dimension k. That is, X is sampled by choosing $t_1, \ldots, t_k$ uniformly and independently in $\mathbb{F}_q$ and calculating*

$$\sum_{j=1}^{k} t_j \cdot a^{(j)} + b$$

for some $a^{(1)}, \ldots, a^{(k)}, b \in \mathbb{F}_q^n$ such that $a^{(1)}, \ldots, a^{(k)}$ are linearly independent.

For a finite set Ω, we denote by U_Ω the uniform distribution on Ω. We say that two distributions P and Q over Ω are ϵ-close (denoted by $P \stackrel{\epsilon}{\sim} Q$) if for every event $A \subseteq \Omega$, $|\Pr_P(A) - \Pr_Q(A)| \leq \epsilon$.
Definition 2 (deterministic affine source extractor). *A function $D : \mathbb{F}_q^n \to \Omega$ is a deterministic (k, ϵ)-affine source extractor if for every $(n,k)_q$-affine source X the distribution $D(X)$ is ϵ-close to uniform. That is*[2]*,*

$$D(X) \stackrel{\epsilon}{\sim} U_\Omega.$$

1.2 Our results

We construct deterministic extractors for affine sources over large fields. Specifically, we work with a field size that is polynomially large in n. We give constructions that extract practically all the randomness in all cases. We have two main constructions. The first is designed for $k \geq 2$ and the second for $k = 1$.

Our first construction gives a deterministic affine source extractor that extracts $k-1$ random elements in $\mathbb{F}_q$ from any $(n,k)_q$-affine source, provided q is a large enough polynomial in n. Note that we didn't make any attempt to optimize the constants 20 and 21 in the following theorem (as they depend on each other).
Theorem 1. *There exists a constant q_0 such that for any field $\mathbb{F}_q$ and integers n, k with $q > \max[q_0, n^{20}]$, there is an explicit deterministic (k, ρ)-affine source extractor $D : \mathbb{F}_q^n \to \mathbb{F}_q^{k-1}$, with $\rho \leq q^{-1/21}$.*

[2] Our extractors will sometimes output bits and sometimes output field elements. Therefore, the definition here uses a general output domain.

Our second result is for $k = 1$. It gives a deterministic affine source extractor that extracts all the randomness except for an entropy loss of $2\log_2(n/\epsilon) + o(\log_2 q)$ bits.

Theorem 2. *For any field $\mathbb{F}_q$, integer n and $\epsilon > 0$, there is an explicit deterministic $(1, \epsilon)$-affine source extractor $D : \mathbb{F}_q^n \to \{0,1\}^d$, with $d = \lfloor \log_2 q - 2\log_2(n/\epsilon) - 2\log_2\log_2 q - 4 \rfloor$.*

We note the following possible instantiations of the theorem.

- Assuming $q > n^c$, we can extract a $(1-\delta)$ fraction of the source randomness, where $\delta > 0$ is an arbitrarily small constant, and c is a constant[3] depending on δ.
- Using any $q \geq n^2 \cdot \log_2^3 n$ and $\epsilon = 1/4$ with a one bit output, we get an explicit two-coloring of $\mathbb{F}_q$ such that no line is monochromatic.

The main drawback of Theorem 1 is the large error. The error that we achieve is polynomially small in q. However, the error ρ does not decrease as k increases. (We might have hoped to have error exponentially small in k.) This is because, as will be explained in section 2, the first stage of our construction extracts randomness from an $(n, 1)_q$-affine source. The error of the entire construction is bounded from below by the error of this stage.

1.3 Previous work

The only previous work that we are aware of studied the problem over the field $\mathbb{F}_2$ (i.e., $GF[2]$) [4]. In that work, Barak, Kindler, Shaltiel, Sudakov and Wigderson show how to extract one non-constant bit for k slightly sub-linear in n. In other words, their result gives a two-coloring of $\mathbb{F}_2^n$, in which no affine subspace of linear dimension (or slightly sub-linear dimension) is monochromatic. It is also known how to extract one random bit when $k > n/2$ [5].

1.4 Background

Our results can be put in the broader context of *deterministic extractors*. A "deterministic randomness extractor" is a function that "extracts" an (almost) uniformly distributed output from "weak sources of randomness" which may be very far from uniform. More precisely, let $\mathcal{C}$ be a class of distributions on some finite set Ω. D is a deterministic randomness extractor for the class $\mathcal{C}$, if for every distribution X in $\mathcal{C}$, the distribution of $D(X)$ is close to uniform. The distributions $X \in \mathcal{C}$ are often referred to as "weak random sources". That is, distributions that "contain" some randomness. Given a class $\mathcal{C}$, the goal of this field is to design *explicit* (that is, efficiently computable) deterministic extractors that extract as much randomness as possible.

Various classes $\mathcal{C}$ of distributions were studied in the literature: The first construction of deterministic extractors can be traced back to von Neumann [33] who showed how to use many independent tosses of a biassed coin (with unknown bias) to obtain an unbiased coin. Blum [6] considered

[3] See Lemma 5.5 for an exact formulation of such an instantiation.

sources that are generated by a finite Markov-chain. Santha and Vazirani [22], Vazirani [30, 31], Chor and Goldreich [7], Barak et al. [3], Barak et al. [4], Dodis et al. [10] and Raz [20] studied sources that are composed of several independent samples from various classes of distributions. Trevisan and Vadhan [28] studied sources which are "samplable" by small circuits. Chor et al. [8], Kamp and Zuckerman [15] and Gabizon et al. [12] studied "bit-fixing sources" in which a subset of the bits is fixed and the rest of the bits are chosen randomly and independently.

A negative result was given by Santha and Vazirani [22] that exhibit a very natural class of high min-entropy sources[4] that does not have deterministic extractors. This led to the development of a different notion of extractors called "seeded extractors". Such extractors are allowed to use a short seed of few truly random bits when extracting randomness from a source. (The notion of "seeded extractors" emerged from attempts to simulate probabilistic algorithms using weak random sources [32, 7, 9, 35, 36] and was explicitly defined by Nisan and Zuckerman [18].) Unlike deterministic extractors, seeded extractors can extract randomness from the most general class of sources: Sources with high min-entropy. The reader is referred to [19, 17, 24, 29] for various surveys on randomness extractors.

2 Overview of techniques

The basic scheme of our construction is as follows: We construct a deterministic affine source extractor that extracts a few bits. We then use these bits to run a "seeded extractor" that extracts almost all the randomness from the source. (Usually, seeded extractors require a seed that is independent of the source. We will construct a "special kind" of seeded extractor that can work well even with a seed that is correlated with the affine source). The proof that this composition of extractors works uses an argument similar to [12]. We now elaborate on the components in this scheme.

2.1 Extracting many bits from lines

As described above, the first step of our construction is to extract a few bits deterministically. We do this by showing a method to extract any constant fraction of the randomness from an $(n, 1)_q$-affine source, assuming $q > n^c$ for large enough c. We first describe how to extract one bit when q is slightly more than quadratic in n.

Extracting a single bit: We want to extract one random bit from an $(n, 1)_q$-affine source, assuming $q = n^{2+\gamma}$ for some $\gamma > 0$. Consider first the easier task of outputting a non-constant bit or even a non-constant value over a larger domain, say $\mathbb{F}_q$. This can be achieved by the following method: Given input $x = (x_1, \ldots, x_n) = (a_1 \cdot t + b_1, \ldots, a_n \cdot t + b_n) \in \mathbb{F}_q^n$ (where $a_i, b_i \in \mathbb{F}_q$ are constant and t is chosen uniformly at random in $\mathbb{F}_q$), we compute the expression $\sum_{i=1}^n x_i^i = \sum_{i=1}^n (a_i \cdot t + b_i)^i$.

[4] Min-entropy is a measure of the amount of randomness in the source. A distribution has min-entropy k if it gives no particular element probability greater than 2^{-k}.

We know that $a_i \neq 0$ for some i. Assume for simplicity that $a_n \neq 0$. The n'th summand is a polynomial of degree n in the variable t. Since the other summands do not contain n'th powers, the entire expression is a non-constant polynomial in t (the large field size comes in here). Since t is chosen uniformly in $\mathbb{F}_q$, our output will be non-constant. Actually, by computing this expression we have "converted" our distribution into a "low degree distribution" of the form $f(U_{\mathbb{F}_q})$, that is, a distribution sampled by choosing t uniformly in $\mathbb{F}_q$ and computing $f(t)$ for some low degree polynomial f (low degree in relation to the field size). Noticing this, the way to a random bit becomes easy using well known theorems[5] of Weil [34] about character sums. Loosely speaking, the *characters* of a finite field $\mathbb{F}_q$ are functions from $\mathbb{F}_q$ to the complex numbers that preserve the field addition or multiplication. Weil's theorems show that field characters of order 2 (see subsection 3.2 for definitions) are actually "deterministic extractors" for such "low degree distributions" (unless the polynomial is of a certain restricted form). Thus, our extractor works by "converting" the source distribution into a "low degree distribution"[6] $f(U_{\mathbb{F}_q})$, and then applying a character of order 2.

Extracting many bits: As explained in subsection 3.2, we will need to work a bit differently for fields of even and odd size. For simplicity, let us consider now the case of an even sized field. As described in subsection 3.2, when q is even, we use Weil's theorems to show that the trace function $Tr : \mathbb{F}_q \to \{0,1\}$ (defined in subsection 3.2) outputs an almost unbiased bit when given a sample from a "low degree distribution" $f(U_{\mathbb{F}_q})$, where f is a polynomial of odd degree. Furthermore, Tr is an additive function; that is[7], $Tr(a+b) = Tr(a) \oplus Tr(b)$. Our extractor works as follows: In a way similar to the one bit case, we use our source to produce samples from several "low degree distributions" of the form $U(f'_j)$ where the (f'_j)s have odd degree. We then apply Tr on each sample. This gives us several bits that are each individually close to uniform. We want to ensure that their joint distribution is also close to uniform. For this purpose, we make sure the (f'_j)s have the property that the sum of any subset of them is also a polynomial of odd degree. We use this property together with the additivity of Tr to show that the parity of any subset of the output bits is close to uniform. We then use the Vazirani Xor Lemma to conclude that the output distribution is close to uniform. The case of an odd sized field is similar but requires a bit more work.

2.2 Linear seeded affine source extractors

Our goal is to construct deterministic affine source extractors. As a component in our construction, we use linear **seeded** extractors for affine sources. That is, seeded extractors that work only on affine sources (and not on general high min-entropy sources). Furthermore, the extractors are linear, meaning that for any fixed seed, the extractor is a linear function of the source.

[5]These theorems have already been very fruitful in computer science, e.g., in explicit constructions of ϵ-biased spaces [2], tournaments [13, 1] and pseudorandom graphs [16].

[6]We use a slightly different expression than the one given here to ensure that f will not be of a certain restricted form on which Weil's theorems don't apply.

[7]Here '$+$' denotes addition in $\mathbb{F}_q$ and '$\oplus$' denotes addition mod 2.

Definition 3 (linear seeded affine source extractor). *A function $E : \mathbb{F}_q^n \times \{0,1\}^d \to \mathbb{F}_q^m$ is a linear seeded (k, ϵ)-affine source extractor if*

1. *For every $(n,k)_q$-affine source X, the distribution $E(X, U_d)$ is ϵ-close to uniform. That is,*

$$E(X, U_d) \overset{\epsilon}{\sim} U_{\mathbb{F}_q^m}.$$

2. *For a fixed seed, E is a linear function. That is, for any $a^{(1)}, a^{(2)} \in \mathbb{F}_q^n, t_1, t_2 \in \mathbb{F}_q$ and $y \in \{0,1\}^d$, we have*

$$E(t_1 \cdot a^{(1)} + t_2 \cdot a^{(2)}, y) = t_1 \cdot E(a^{(1)}, y) + t_2 \cdot E(a^{(2)}, y).$$

We now describe our construction of linear seeded affine source extractors. Fix any affine subspace $A \subseteq \mathbb{F}_q^n$ of dimension k. It is not hard to show that a random linear mapping $T : \mathbb{F}_q^n \to \mathbb{F}_q^k$, or equivalently, a random $k \times n$ matrix over $\mathbb{F}_q$, will map A (uniformly) onto $\mathbb{F}_q^k$, with probability at least $1 - \frac{1}{q-1}$. Our construction of linear seeded affine source extractors can be viewed as a derandomization of this property. Assuming $q > n^3$, we construct a set of **less than q** matrices with a similar property. That is, for any affine subspace $A \subseteq \mathbb{F}_q^n$ of dimension k, most of the matrices in this set will map A onto $\mathbb{F}_q^k$. The construction is very simple: Pick any subset $U \subseteq \mathbb{F}_q$ with $|U| > n^3$. The set of matrices will be the "power matrices" of the elements of U. That is, for each $u \in U$ we will have a $k \times n$ matrix T_u where $(T_u)_{j,i} = u^{ji}$ (where ji is the product of j and i as integers).

For general high min-entropy sources, it is known that encoding the source string with an error correcting code and outputting random locations of the encoding makes a good extractor. Some extractor constructions for general high min-entropy sources, specifically the breakthrough construction of Trevisan[27] and it's improvement by Raz, Reingold and Vadhan[21] and also the very elegant constructions of Ta-Shma, Zuckerman and Safra[26] and Shaltiel and Umans[25], can be viewed as using the random seed to select locations from an encoding of the source in a derandomized way. From this angle, our construction may be viewed as selecting locations from the Reed-Solomon encoding[8] of the (affine) source in a derandomized way. Specifically, we choose the first location u randomly from a large enough subset $U \subseteq \mathbb{F}_q$. The other locations are simply the powers of u, i.e., $u^2, u^3, \ldots, u^k$.

Remark 2.1. *We note that some extractor constructions for general high min-entropy sources, for example, the constructions of [21, 25, 26, 27] discussed above, are already linear seeded affine source extractors. They are designed to work over the binary field but seem to be easily adaptable to large fields. Why not use one of these constructions? This is a possibility. However, our construction is considerably simpler and achieves better parameters for the case of affine sources. In particular, using one of the above mentioned constructions would not have enabled us to extract almost all the randomness (as we will need an affine source extractor that can do so with a seed of length $O(\log n)$).*

[8]The Reed-Solomon encoding of $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ at location $u \in \mathbb{F}_q$, is defined as $\sum_{i=1}^n x_i \cdot u^i$.

2.3 Using the correlated randomness as a seed

As stated earlier, we wish to use the few bits extracted by the deterministic affine source extractor D (described in subsection 2.1) as a seed for the linear seeded affine source extractor E described in subsection 2.2. In principal, this is problematic as a seeded extractor is only guaranteed to work when its seed is independent of the source. We want to use a seed that is a **function** of the source. However, using an argument similar to [12], we show that when the seeded extractor is linear this does work. Let us sketch the argument: Given a fixed seed u, E is a linear mapping. Therefore, if X is an affine source, then given a possible output value a, the distribution X conditioned on $E(x,u) = a$ is *also* an affine source (as we have just added another linear constraint on the support of X). Hence, the distribution $D(X)$, even when conditioned on $E(x,u) = a$, is still close to uniform. Using simple manipulations of probability distributions, this can be used to show that the distribution $E(X, D(X))$ is close to the distribution $E(X, U_d)$ (and therefore close to uniform).

3 Preliminaries

Notation: We use $[n]$ to denote the set $\{1,\ldots,n\}$. Let Ω, Π be some finite sets. For $x \in \Omega^n$ and $i \in [n]$, we denote by x_i the i'th coordinate of x. Similarly, for a function $D : \Pi \to \Omega^n$ and $i \in [n]$, we denote by D_i the function D restricted to the i'th output coordinate. Logarithms will always be taken base 2. We denote by $\mathbb{F}_q$ the finite field of q elements. We denote by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$ and by $\mathbb{F}_q[t]$ the ring of formal polynomials over $\mathbb{F}_q$. We denote by $\mathbb{F}_q^n$ the vector space of dimension n over $\mathbb{F}_q$. Given a $k \times n$ matrix T over $\mathbb{F}_q$, we also view T as a mapping from $\mathbb{F}_q^n$ to $\mathbb{F}_q^k$ and denote $T(x) \triangleq T \cdot x$, for $x \in \mathbb{F}_q^n$.

3.1 Probability distributions

Notation for probability distributions: Let Ω be some finite set. Let P be a distribution on Ω. For $B \subseteq \Omega$, we denote $P(B)$, i.e., the probability of B according to P, by $\Pr_P(B)$ or $\Pr(P \subseteq B)$; When $B \in \Omega$, we will also use the notation $\Pr(P = B)$. Given a function $A : \Omega \to U$, we denote by $A(P)$ or by $[A(t)]_{t \leftarrow P}$ the distribution induced on U when sampling t by P and calculating $A(t)$. We will use the same notation for expressions not explicitly named as functions. For example, for a distribution P on $\mathbb{F}_q$ we will denote by $P + 1$ or by $[t+1]_{t \leftarrow P}$ the distribution induced on $\mathbb{F}_q$ by sampling t by P and adding 1. When we write $t_1, \ldots, t_k \leftarrow P$, we mean that $t_1, \ldots, t_k$ are chosen *independently* according to P. We denote by U_Ω the uniform distribution on Ω. For an integer n, we denote by U_n the uniform distribution on $\{0,1\}^n$. We abuse notation and denote by U_q the uniform distribution on $\mathbb{F}_q$. In any expression involving U_Ω or U_n and other distributions, the instance of U_n or U_Ω is independent of the other distributions. For a distribution P on Ω^d and $j \in [d]$, we denote by P_j the restriction of P to the j'th coordinate. We denote by $Supp(P)$ the support of P. The *statistical distance* between two distributions P and Q on Ω, denoted by $|P-Q|$, is defined as

$$|P-Q| \triangleq \max_{S\subseteq\Omega}\left|\Pr_P(S)-\Pr_Q(S)\right| = \frac{1}{2}\sum_{w\in\Omega}\left|\Pr_P(w)-\Pr_Q(w)\right|.$$

We say that P is *ϵ-close* to Q, denoted $P \overset{\epsilon}{\sim} Q$, if $|P-Q|\le\epsilon$. We denote the fact that P and Q are identically distributed by $P \sim Q$.

We define conditional distributions.

Definition 4 (Conditional distributions). *Let P be a distribution on Ω. Let $C\subseteq\Omega$ be an event such that $\Pr_P(C)>0$. We define the distribution $(P|C)$ by*

$$\Pr_{(P|C)}(B) = \frac{\Pr_P(B\cap C)}{\Pr_P(C)}$$

for any $B\subseteq\Omega$. Given a function $A:\Omega\to U$, we denote by $(A(P)|C)$ the distribution $A((P|C))$.

We will need the notion of a convex combination of distributions.

Definition 5 (Convex combination of distributions). *Given distributions $P_1,\dots,P_t$ on a set Ω and coefficients $\mu_1,\dots,\mu_t\ge 0$ such that $\sum_{i=1}^t \mu_i = 1$, we define the distribution $P\triangleq\sum_{i=1}^t \mu_i\cdot P_i$ by*

$$\Pr_P(B) = \sum_{i=1}^t \mu_i\cdot\Pr_{P_i}(B)$$

for any $B\subseteq\Omega$.

We will need a few technical lemmas on probability distributions.

The following lemma shows that convex combinations of similar distributions with similar coefficients are statistically close.

Lemma 3.1. *Let t be any integer. Let $P_1,\dots,P_t$ and $Q_1,\dots,Q_t$ be sequences of distributions on a set Ω such that for every $i\in[t]$, $P_i \overset{\epsilon}{\sim} Q_i$. Let μ and ν be distributions on $[t]$ with $|\mu-\nu|\le\delta$. Let $P\triangleq\sum_{i=1}^t \Pr(\mu=i)\cdot P_i$, $Q\triangleq\sum_{i=1}^t\Pr(\nu=i)\cdot Q_i$. Then $P \overset{2\cdot\delta+\epsilon}{\sim} Q$.*

Proof. Denote $\mu_i=\Pr(\mu=i)$ and $\nu_i=\Pr(\nu=i)$. Given $B\subseteq\Omega$, we have

$$\left|\Pr_P(B)-\Pr_Q(B)\right| = \left|\sum_{i=1}^t\mu_i\cdot\Pr_{P_i}(B)-\sum_{i=1}^t\nu_i\cdot\Pr_{Q_i}(B)\right|$$

$$\le\sum_{i=1}^t\left|\mu_i\cdot\Pr_{P_i}(B)-\nu_i\cdot\Pr_{Q_i}(B)\right|\le\sum_{i=1}^t\left|\mu_i\cdot\Pr_{P_i}(B)-\nu_i\cdot\Pr_{P_i}(B)+\nu_i\cdot\Pr_{P_i}(B)-\nu_i\cdot\Pr_{Q_i}(B)\right|$$

$$\le\sum_{i=1}^t|\mu_i-\nu_i|+\nu_i\left|\Pr_{P_i}(B)-\Pr_{Q_i}(B)\right|\le 2\cdot\delta+\sum_{i=1}^t\nu_i\left|\Pr_{P_i}(B)-\Pr_{Q_i}(B)\right|\le 2\cdot\delta+\epsilon.$$

□

Lemma 3.2. *Let $P_1, \ldots, P_t$ be a sequence of distributions on a set Ω. Let μ be a distribution on $[t]$. Let $P \triangleq \sum_{i=1}^{t} \Pr(\mu = i) \cdot P_i$. Assume that the probability given by μ to the non-uniform P_i's is at most ϵ, i.e., $\Pr_{i \leftarrow \mu}(P_i \nsim U_\Omega) \leq \epsilon$. Then*

$$P \overset{\epsilon}{\sim} U_\Omega.$$

Proof. By the assumption of the lemma, $P = (1-\delta) \cdot U_\Omega + \delta \cdot V$ for some $\delta \leq \epsilon$ and distribution V on Ω. Let $B \subseteq \Omega$ be some event.

$$\left| \Pr_P(B) - \Pr_{U_\Omega}(B) \right| = \left| \delta \cdot \Pr_V(B) + (1-\delta) \cdot \Pr_{U_\Omega}(B) - \Pr_{U_\Omega}(B) \right| \leq \delta \cdot \left| \Pr_V(B) - \Pr_{U_\Omega}(B) \right| \leq \delta \leq \epsilon.$$

□

3.2 Characters of finite fields

Loosely speaking, given an abelian group G, a *character* on G is a map from G to complex roots of unity that preserves the group action. The characters of a finite field are the characters of the additive and multiplicative[9] groups of the field.

Definition 6 (Additive character). *A function $\psi : \mathbb{F}_q \to \mathbb{C}$ is an additive character of $\mathbb{F}_q$ if $|\psi(a)| = 1$ for every $a \in \mathbb{F}_q$ and*

$$\psi(a+b) = \psi(a)\psi(b)$$

for every $a, b \in \mathbb{F}_q$. The order of ψ is the smallest integer d such that $(\psi(a))^d = 1$ for every $a \in \mathbb{F}_q$.

Definition 7 (Multiplicative character). *A function $\chi : \mathbb{F}_q \to \mathbb{C}$ is a multiplicative character of $\mathbb{F}_q$ if $|\chi(a)| = 1$ for every $a \in \mathbb{F}_q^*$ and $\chi(0) = 0$ and*

$$\chi(ab) = \chi(a)\chi(b)$$

for every $a, b \in \mathbb{F}_q$. The order of χ is the smallest integer d such that $(\chi(a))^d = 1$ for every $a \in \mathbb{F}_q^*$.

We will concentrate on characters of order 2. Even sized fields have additive characters of order 2 and odd sized fields have a multiplicative character of order 2. We define a character of order 2 for each case and also a "boolean version" of the character (i.e., a function with range $\{0, 1\}$) that we will use in our extractor construction.

Definition 8 (Additive character of order 2). *Let $q = 2^l$ for some integer l. The function $Tr : \mathbb{F}_q \to \{0, 1\}$ is defined to be the trace of $\mathbb{F}_q$ over $\mathbb{F}_2$. That is*[10]*,*

$$Tr(a) = a + a^2 + a^{2^2} + \ldots + a^{2^{l-1}}.$$

We define the additive character $\psi_1 : \mathbb{F}_q \to \{1, -1\}$ by $\psi_1(a) = -1^{Tr(a)}$.

[9] A character χ of $\mathbb{F}_q^*$ is extended to 0 by $\chi(0) = 0$.

[10] It is known (and can be easily proved) that $Tr(a) \in \{0, 1\}$ for every $a \in \mathbb{F}_q$ (we interpret the field elements 0 and 1 as the corresponding boolean values).

Definition 9 (Multiplicative character of order 2). *Let $q = p^l$ for some integer l and odd prime p. We define the multiplicative character $\chi_1 : \mathbb{F}_q \to \{-1, 0, 1\}$ to be 1 for a non-zero quadratic residue, -1 for a quadratic non-residue, and 0 on 0. More concisely,*

$$\chi_1(a) = a^{\frac{q-1}{2}}.$$

We define the function $QR : \mathbb{F}_q \to \{0, 1\}$ by $QR(a) = 1$ if $\chi_1(a) = -1$, and $QR(a) = 0$ otherwise. That is, $QR(a) = 1$ for quadratic non-residues and 0 otherwise.

It is obvious that χ_1 and ψ_1 have order at most 2. It can be shown that their order is exactly 2.

Very useful theorems of Weil [34] state that for any low degree polynomial f that is not of a certain restricted form, the values of a field character "cancel out" over the range of f (when viewed as a multi-set). We state two special cases of these theorems. The theorems can be found in [23]. The first theorem deals with additive characters.

Theorem 3. *[23][Theorem $2E$, page 44] Let ψ be a non-trivial additive character of $\mathbb{F}_q$ (that is, not identically 1). Let $f(t)$ be a polynomial in $\mathbb{F}_q[t]$ of degree m. Suppose that $gcd(m, q) = 1$, then*

$$\left|\sum_{t\in\mathbb{F}_q} \psi(f(t))\right| \leq mq^{1/2}.$$

The second theorem deals with multiplicative characters.

Theorem 4. *[23][Theorem $2C'$, page 43] Let χ be a multiplicative character of $\mathbb{F}_q$ of order $d > 1$. Let $f(t)$ be a polynomial in $\mathbb{F}_q[t]$ of degree m. Suppose that $f(t)$ is not of the form $c \cdot g(t)^d$ for any $c \in \mathbb{F}_q$ and $g(t) \in \mathbb{F}_q[t]$. Then*

$$\left|\sum_{t\in\mathbb{F}_q} \chi(f(t))\right| \leq mq^{1/2}.$$

For the case of a field character of order 2, Weil's theorems actually show that the character is a "deterministic extractor"[11] for distributions of the form $f(U_q)$ for almost any low degree polynomial f. We formalize this in the following corollaries of Theorems 3 and 4 stated for the boolean versions of the characters ψ_1 and χ_1.

Corollary 3.3. *Let q be a power of 2. Let $f \in \mathbb{F}_q[t]$ be a polynomial of odd degree m. Then*

$$Tr(f(U_q)) \overset{\frac{m}{2\sqrt{q}}}{\sim} U_1.$$

Proof.

$$\left|\sum_{t\in\mathbb{F}_q} \psi_1(f(t))\right| = \left|\sum_{t\in\mathbb{F}_q,\psi_1(f(t))=1} 1 - \sum_{t\in\mathbb{F}_q,\psi_1(f(t))=-1} 1\right|$$

[11] Characters of higher order are also extractors, but with larger error.

$$= q\cdot\left|\Pr_{t\leftarrow U_q}(\psi_1(f(t))=1) - \Pr_{t\leftarrow U_q}(\psi_1(f(t))=-1)\right| = q\cdot\left|\Pr_{t\leftarrow U_q}(Tr(f(t))=0) - \Pr_{t\leftarrow U_q}(Tr(f(t))=1)\right|$$

$$= q\cdot\left|2\cdot\Pr_{t\leftarrow U_q}(Tr(f(t))=0)-1\right| = 2q\cdot\left|\Pr_{t\leftarrow U_q}(Tr(f(t))=0)-1/2\right| = 2q\cdot\left|Tr(f(U_q))-U_1\right|.$$

Since $gcd(m,q)=1$, using Theorem 3 we have

$$|Tr(f(U_q))-U_1| = \frac{1}{2q}\cdot\left|\sum_{t\in\mathbb{F}_q}\psi_1(f(t))\right| \le \frac{1}{2q}\cdot mq^{1/2} = \frac{m}{2\sqrt{q}}.$$

□

The proof of the analogous claim for χ_1 is a bit more cumbersome as we have to deal with the artificial extension of χ_1 to $\mathbb{F}_q$ by $\chi_1(0)=0$. We will use the following definition.

Definition 10 (Square multiple). *We say that a polynomial $f(t)$ in $\mathbb{F}_q[t]$ is a square multiple in $\mathbb{F}_q[t]$ if $f(t)=c\cdot g(t)^2$ for some $c\in\mathbb{F}_q$ and $g(t)\in\mathbb{F}_q[t]$.*

Corollary 3.4. *Let $q=p^l$ for some integer l and odd prime p. Let $f(t)\in\mathbb{F}_q[t]$ be a polynomial of degree m that is not a square multiple in $\mathbb{F}_q[t]$. Then*

$$QR(f(U_q)) \overset{\frac{m}{\sqrt{q}}}{\sim} U_1.$$

Proof. Assume without loss of generality that $\sum_{t\in\mathbb{F}_q}\chi_1(f(t))\ge 0$. We have

$$\sum_{t\in\mathbb{F}_q}\chi_1(f(t)) = \left[\sum_{t\in\mathbb{F}_q,\chi_1(f(t))=1} 1 - \sum_{t\in\mathbb{F}_q,\chi_1(f(t))=-1} 1\right]$$

$$= q\cdot\left[\Pr_{t\leftarrow U_q}(\chi_1(f(t))=1) - \Pr_{t\leftarrow U_q}(\chi_1(f(t))=-1)\right]$$

$$= q\cdot\left[\Pr_{t\leftarrow U_q}(QR(f(t))=0) - \Pr_{t\leftarrow U_q}(f(t)=0) - \Pr_{t\leftarrow U_q}(QR(f(t))=1)\right]$$

$$= q\cdot\left[2\cdot\Pr_{t\leftarrow U_q}(QR(f(t))=0)-1\right] - q\cdot\Pr_{t\leftarrow U_q}(f(t)=0)$$

$$= 2q\cdot\left[\Pr_{t\leftarrow U_q}(QR(f(t))=0)-1/2\right] - q\cdot\Pr_{t\leftarrow U_q}(f(t)=0) = 2q\cdot|QR(f(U_q))-U_1| - q\cdot\Pr_{t\leftarrow U_q}(f(t)=0).$$

Since χ_1 is of order 2 and $f(t)$ is not of the form $c\cdot g(t)^2$ for any $c\in\mathbb{F}_q$ and $g(t)\in\mathbb{F}_q[t]$, using Theorem 4 we have

$$|QR(f(U_q))-U_1| = \frac{1}{2q}\cdot\sum_{t\in\mathbb{F}_q}\chi_1(f(t)) + (1/2)\cdot\Pr_{t\leftarrow U_q}(f(t)=0)$$

$$\le \frac{1}{2q}\cdot mq^{1/2} + \frac{m}{2q} \le \frac{m}{2\sqrt{q}} + \frac{m}{2\sqrt{q}} = \frac{m}{\sqrt{q}}.$$

□

4 Extracting one bit from lines

In the next section we show how to extract any constant fraction of the randomness from an $(n, 1)_q$-affine source, provided q is a large enough polynomial in n. For simplicity of the presentation, we first show how to extract one bit from an $(n, 1)_q$-affine source when q is slightly more than quadratic in n.

As explained in section 2, we first "convert" a uniform distribution on a one-dimensional affine subspace into a distribution of the form $f'(U_q)$, where f' is low degree polynomial; We then apply a (boolean version of a) field character of order 2. Weil's theorems guarantee that our output will be close to uniform. As explained in subsection 3.2, since we want a field character of order 2 we need to use an additive character for even sized fields and a multiplicative character for odd sized fields.

The following lemma shows how to extract one bit when the field size is even.

Lemma 4.1. *Let q be a power of 2. Fix any integer $n < \sqrt{q}$. Define the multivariate polynomial $f : \mathbb{F}_q^n \to \mathbb{F}_q$ by $f(x) = \sum_{i=1}^n x_i^{2i-1}$. The function $D_0 : \mathbb{F}_q^n \to \{0, 1\}$ defined by $D_0(x) = Tr(f(x))$ is a deterministic $(1, \epsilon)$-affine source extractor, where $\epsilon = n/\sqrt{q}$.*

Proof. Fix an $(n, 1)_q$-affine source X. Recall that $X \sim [t \cdot a + b]_{t \leftarrow U_q}$ for some $a, b \in \mathbb{F}_q^n$ such that $a \neq 0$. We have

$$D_0(X) \sim Tr(f(X)) \sim [Tr(f(t \cdot a_1 + b_1, \ldots, t \cdot a_n + b_n))]_{t \leftarrow U_q}$$

$$\sim \left[Tr \left(\sum_{i=1}^n (t \cdot a_i + b_i)^{2i-1} \right) \right]_{t \leftarrow U_q}.$$

Denote $f'(t) = \sum_{i=1}^n (t \cdot a_i + b_i)^{2i-1}$. Note that f' is a polynomial of odd degree m, where $m \leq 2n$. Therefore, using corollary 3.3 we have

$$D_0(X) \sim Tr(f'(U_q)) \overset{\frac{n}{\sqrt{q}}}{\approx} U_1.$$

□

The following lemma shows how to extract one bit when the field size is odd.

Lemma 4.2. *Let $q = p^l$ for some integer l and odd prime p. Fix any integer $n < \sqrt{q}/2$. Define the multivariate polynomial $f : \mathbb{F}_q^n \to \mathbb{F}_q$ by $f(x) = \sum_{i=1}^n x_i^{2i-1}$. The function $D_0 : \mathbb{F}_q^n \to \{0, 1\}$ defined by $D_0(x) = QR(f(x))$ is a deterministic $(1, \epsilon)$-affine source extractor, where $\epsilon = 2n/\sqrt{q}$.*

Proof. Fix an $(n, 1)_q$-affine source $X \sim [t \cdot a + b]_{t \leftarrow U_q}$. We have

$$D_0(X) \sim QR(f(X)) \sim [QR(f(t \cdot a_1 + b_1, \ldots, t \cdot a_n + b_n))]_{t \leftarrow U_q}$$

$$\sim \left[QR \left(\sum_{i=1}^n (t \cdot a_i + b_i)^{2i-1} \right) \right]_{t \leftarrow U_q}.$$

Denote $f'(t) = \sum_{i=1}^{n}(t \cdot a_i + b_i)^{2i-1}$. Note that $f'(t)$ is a polynomial of odd degree m (and therefore not a square multiple in $\mathbb{F}_q[t]$) where $m \le 2n$. Therefore, using corollary 3.4 we have

$$D_0(X) \;\sim\; QR(f'(U_q)) \;\overset{\frac{2n}{\sqrt{q}}}{\sim}\; U_1.$$

□

5 Extracting many bits from lines

In this section we prove Theorem 2. In particular, we show how to extract any constant fraction of the randomness from an $(n, 1)_q$-affine source provided q is a large enough polynomial in n. We will prove the correctness of our construction by showing that the parity of any subset of the output bits is almost unbiased. The following "Xor Lemma" due to Vazirani states that this indeed implies that the output is close to uniform. (For a proof see for example [11].)

Lemma 5.1. *Let X be a distribution on $\{0,1\}^d$. Assume that for every non-empty subset $S \subseteq [d]$*

$$\bigoplus_{j \in S} X_j \;\overset{\epsilon}{\sim}\; U_1$$

(where $\bigoplus$ denotes addition mod 2). Then

$$|X - U_d| \le \epsilon \cdot 2^{d/2}.$$

We first deal with fields of even size. As explained in section 2, we use the source distribution to produce samples from several "low degree distributions" of the form $f'_j(U_q)$, where the (f'_j)s are low degree polynomials of odd degree. We then apply the function Tr on each sample. We make sure that the (f'_j)s have the property that the sum of any subset of them is also a polynomial f' of odd degree. We use this property together with the additivity of Tr to show that the parity of any subset of the output bits is close to uniform. We then conclude using Lemma 5.1.

Lemma 5.2. *Let q be a power of 2. Fix any integers d and n. For every $j \in [d]$, define the multivariate polynomial $f_j : \mathbb{F}_q^n \to \mathbb{F}_q$ by $f_j(x) = \sum_{i=1}^{n} x_i^{2j+(2i-1)}$. The function $D : \mathbb{F}_q^n \to \{0,1\}^d$ defined by $D_j(x) = Tr(f_j(x))$ is a deterministic $(1, \epsilon)$-affine source extractor, where $\epsilon = \frac{(d+n)\cdot 2^{d/2}}{\sqrt{q}}$.*

Proof. Fix an $(n, 1)_q$-affine source $X \;\sim\; [t \cdot a + b]_{t \leftarrow U_q}$. Fix a non-empty subset $S \subseteq [d]$. We have

$$\bigoplus_{j \in S} D_j(X) \;\sim\; \bigoplus_{j \in S} Tr(f_j(X))$$

$$\sim\; Tr\left(\sum_{j \in S} f_j(X)\right)$$

$$\sim \left[Tr\left(\sum_{j\in S} \sum_{i=1}^{n} (t\cdot a_i + b_i)^{2j+(2i-1)} \right) \right]_{t\leftarrow U_q}.$$

Denote $f'(t) = \sum_{j\in S} \sum_{i=1}^{n} (t\cdot a_i + b_i)^{2j+(2i-1)}$. Note that f' is a polynomial of odd degree m where $m \leq 2d + 2n$. Therefore, using corollary 3.3 we have

$$\bigoplus_{j\in S} D_j(X) \sim Tr(f'(U_q)) \overset{\frac{d+n}{\sqrt{q}}}{\sim} U_1.$$

Using lemma 5.1 we get

$$|D(X) - U_d| \leq \frac{(d+n)\cdot 2^{d/2}}{\sqrt{q}}.$$

□

We now deal with fields of odd size. The proof is roughly analogous to the case of even sized fields but requires a bit more work.

We will need the following special case of a lemma from [23].

Lemma 5.3. *[23][Lemma $4B$, page 51] Let $q = p^l$ for some integer l and odd prime p. Let f(t) be a polynomial in $\mathbb{F}_q[t]$. The following are equivalent.*

- *$f(t)$ is a square multiple in $\mathbb{F}_q[t]$.*
- *$f(t) = c\cdot(t-\nu_1)^{e_1}\cdots(t-\nu_s)^{e_s}$ for some $\nu_1,\ldots,\nu_s \in \overline{\mathbb{F}}_q$ and $c\in\mathbb{F}_q$, where e_i is even for all $i\in[s]$.*

Lemma 5.4. *Let $q = p^l$ for some integer l and odd prime p. Fix any integers d and n such that $d \leq q$. Let $c_1,\ldots,c_d$ be distinct elements in $\mathbb{F}_q$. Define the multivariate polynomial $f_0 : \mathbb{F}_q^n \to \mathbb{F}_q$ by $f_0(x) = \sum_{i=1}^{n} x_i^{2i-1}$. For $j\in[d]$, define the multivariate polynomial $f_j : \mathbb{F}_q^n \to \mathbb{F}_q$ by $f_j(x) = f_0(x) + c_j$. The function $D : \mathbb{F}_q^n \to \{0,1\}^d$ defined by $D_j(x) = QR(f_j(x))$ is a deterministic $(1,\epsilon)$-affine source extractor, where $\epsilon = \frac{4dn\cdot 2^{d/2}}{\sqrt{q}}$.*

Proof. Fix an $(n,1)_q$-affine source $X \sim [t\cdot a + b]_{t\leftarrow U_q}$. Fix a non-empty subset $S\subseteq[d]$. For any $x = t\cdot a + b$ in $Supp(X)$, we have

$$\bigoplus_{j\in S} D_j(x) = \bigoplus_{j\in S} QR(f_j(x))$$

$$= \bigoplus_{j\in S} QR\left(\left(\sum_{i=1}^{n} (t\cdot a_i + b_i)^{2i-1} \right) + c_j \right).$$

For $j \in S$, denote $f'_j(t) = (\sum_{i=1}^{n}(t \cdot a_i + b_i)^{2i-1}) + c_j$. For $x = t \cdot a + b$, we call x *good* if $f'_j(t) \neq 0$ for every $j \in S$. For any good $x = t \cdot a + b$, we have

$$\bigoplus_{j \in S} D_j(x) = \bigoplus_{j \in S} QR(f'_j(t)) = QR\left(\prod_{j \in S} f'_j(t)\right).$$

Since there are at most $d \cdot 2n$ bad x's, we get

$$\left|\bigoplus_{j \in S} D_j(X) - QR\left(\prod_{j \in S} f'_j(U_q)\right)\right| \leq d \cdot 2n/q.$$

Denote $f'(t) = \prod_{j \in S} f'_j(t)$. We will show that $f'(t)$ is not a square multiple in $\mathbb{F}_q[t]$. Fix some $j_0 \in S$. Since f'_{j_0} has odd degree it is not a square multiple in $\mathbb{F}_q[t]$. Therefore, by Lemma 5.3 (and by the fact that any polynomial decomposes into linear factors in $\overline{\mathbb{F}}_q$), $f'_{j_0}(t) = c \cdot (t - \nu_1)^{e_1} \cdots (t - \nu_s)^{e_s}$ for distinct $\nu_1, \ldots, \nu_s \in \overline{\mathbb{F}}_q$, where e_k is odd for some $k \in [s]$. Assuming that $|S| \geq 2$, fix any $j_1 \in S$ where $j_1 \neq j_0$. For any $t \in \overline{\mathbb{F}}_q$, $f'_{j_0}(t) - f'_{j_1}(t) = c_{j_0} - c_{j_1} \neq 0$. Therefore, f'_{j_0} and f'_{j_1} do not have a common linear factor in $\overline{\mathbb{F}}_q$. Hence, the factor $(t - \nu_k)$ appears an odd number of times in $f'(t) = \prod_{j \in S} f'_j(t)$. Therefore, by Lemma 5.3 $f'(t)$ is not a square multiple in $\mathbb{F}_q$. Thus, using Corollary 3.4 we have

$$\left|\bigoplus_{j \in S} D_j(X) - U_1\right| \leq \left|\bigoplus_{j \in S} D_j(X) - QR\left(f'(U_q)\right)\right| + \left|QR\left(f'(U_q)\right) - U_1\right|$$

$$\leq \frac{d \cdot 2n}{q} + \frac{2dn}{\sqrt{q}} \leq \frac{4dn}{\sqrt{q}}.$$

Therefore, using Lemma 5.1 we have

$$|D(X) - U_d| \leq \frac{4dn \cdot 2^{d/2}}{\sqrt{q}}.$$

□

We restate and prove Theorem 2

Theorem 2 For any field $\mathbb{F}_q$, integer n and $\epsilon > 0$, there is an explicit deterministic $(1, \epsilon)$-affine source extractor $D : \mathbb{F}_q^n \to \{0,1\}^d$, with $d = \lfloor \log q - 2\log(n/\epsilon) - 2\log\log q - 4 \rfloor$.

Proof. Using Lemmas 5.2 and 5.4, we can get an explicit deterministic $(1, \epsilon)$-affine source extractor $D : \mathbb{F}_q^n \to \{0,1\}^d$ for any ϵ,n,q and d such that

$$\epsilon \geq \frac{4dn \cdot 2^{d/2}}{\sqrt{q}}.$$

Squaring, we get

$$\epsilon^2 \geq \frac{16d^2n^2 \cdot 2^d}{q}.$$

Taking the logarithm on both sides, we get

$$2\log(1/\epsilon) \geq 4 + 2\log d + 2\log n + d - \log q$$

Rearranging and using $d \leq \log q$, we get

$$d \leq \log q - 2\log(n/\epsilon) - 2\log\log q - 4.$$

□

We also prove the following instantiation of Lemmas 5.2 and 5.4 which we will use in the proof of Theorem 1. The following lemma states that we can extract any constant fraction of the randomness from an $(n,1)_q$-affine source, provided q is a large enough polynomial in n.

Lemma 5.5. *Fix any constant $0 < \delta < 1$. There exists a constant q_0 (depending on δ) such that for any integers q and n with $q > q_0$ and $q \geq n^{7/\delta}$, there is an explicit deterministic $(1,\epsilon)$-affine source extractor $D : \mathbb{F}_q^n \to \{0,1\}^d$ where $\epsilon \leq q^{-\delta/3}$ and $d = \lfloor (1-\delta)\log q \rfloor$.*

Proof. According to whether q is even or odd we use Lemma 5.2 or Lemma 5.4 with d and n as stated in the lemma. We get an explicit deterministic $(1,\epsilon)$-affine source extractor $D : \mathbb{F}_q^n \to \{0,1\}^d$ where

$$\epsilon \leq \frac{4dn \cdot 2^{d/2}}{\sqrt{q}} \leq \frac{4 \cdot (1-\delta)\log q \cdot q^{\delta/7} \cdot q^{\frac{1-\delta}{2}}}{\sqrt{q}}.$$

We take q large enough so that $q^{\delta/42} \geq 4 \cdot (1-\delta)\log q$. For such q, we have

$$\epsilon \leq \frac{q^{\delta/42+\delta/7+1/2-\delta/2}}{q^{1/2}} = q^{-\delta/3}.$$

□

6 A linear seeded extractor for affine sources

In this section we describe our construction of linear seeded affine source extractors. As described in section 2, this seeded extractor will be used as a component in our construction of deterministic affine source extractors.

Given $u \in \mathbb{F}_q$ and an integer k, we define a $k \times n$ matrix $T_{u,k}$ by $(T_{u,k})_{j,i} = u^{ji}$ (where ji is an integer product). That is,

$$T_{u,k}(x) = \left(\sum_{i=1}^{n} x_i \cdot u^i, \sum_{i=1}^{n} x_i \cdot u^{2i}, \ldots, \sum_{i=1}^{n} x_i \cdot u^{ki}\right)$$

for $x \in \mathbb{F}_q^n$.

The following theorem shows how to extract all the randomness from an $(n,k)_q$-affine source using a seed of length $\lceil \log n + 2\log k + \log(1/\epsilon) \rceil$, whenever $q > 2n \cdot k^2/\epsilon$.

Theorem 5. *Fix any field $\mathbb{F}_q$, integers n, k, and $\epsilon > 0$, such that $q \geq 2\frac{n \cdot k^2}{\epsilon}$. Let s be the smallest power of 2 such that $s \geq \frac{n \cdot k^2}{\epsilon}$. Let $U = \{u_1, \ldots, u_s\}$ be a set of distinct elements in $\mathbb{F}_q$. Let $d = \log s$. We identify $[s]$ with $\{0,1\}^d$. The function $E : \mathbb{F}_q^n \times \{0,1\}^d \to \mathbb{F}_q^k$ defined by*

$$E(x,y) = T_{u_y,k}(x) = \left(\sum_{i=1}^{n} x_i \cdot u_y^i, \sum_{i=1}^{n} x_i \cdot u_y^{2i}, \ldots, \sum_{i=1}^{n} x_i \cdot u_y^{ki} \right)$$

is a linear seeded (k, ϵ)-affine source extractor.

The theorem will be derived easily from the following lemma.

Lemma 6.1. *Fix any field $\mathbb{F}_q$ and integers n, k such that $q \geq n \cdot k^2$. Fix any affine subspace $A \subseteq \mathbb{F}_q^n$ of dimension k. There are at most $n \cdot k^2$ elements $u \in \mathbb{F}_q$ such that $T_u(A) \subsetneq \mathbb{F}_q^k$, where $T_u = T_{u,k}$.*

Proof. First note that if $A = A_1 + b$ where $b \in \mathbb{F}_q^n$ and A_1 is a linear subspace of dimension k, then $(T_u(A_1) = \mathbb{F}_q^k) \leftrightarrow (T_u(A) = \mathbb{F}_q^k)$. Therefore, we assume A is a linear subspace with basis $\{a^{(1)}, a^{(2)}, \ldots, a^{(k)}\}$ where $a^{(j)} \in \mathbb{F}_q^n$. Denote by B the $n \times k$ matrix

$$B = \left(a^{(1)}, a^{(2)}, \ldots, a^{(k)} \right).$$

We have

$$T_u(A) = T_u \cdot B(\mathbb{F}_q^k)$$

where $\cdot$ denotes the matrix product.

Denote by C_u the $k \times k$ matrix $T_u \cdot B$. That is,

$$(C_u)_{j,l} = \sum_{i=1}^{n} {a^{(l)}}_i \cdot u^{ji}.$$

$$C_u = \begin{pmatrix} \sum_{i=1}^n {a^{(1)}}_i \cdot u^i & \sum_{i=1}^n {a^{(2)}}_i \cdot u^i & \ldots & \sum_{i=1}^n {a^{(k)}}_i \cdot u^i \\ \sum_{i=1}^n {a^{(1)}}_i \cdot u^{2i} & \sum_{i=1}^n {a^{(2)}}_i \cdot u^{2i} & \ldots & \sum_{i=1}^n {a^{(k)}}_i \cdot u^{2i} \\ . & . & \ldots & . \\ . & . & \ldots & . \\ . & . & \ldots & . \\ \sum_{i=1}^n {a^{(1)}}_i \cdot u^{ki} & \sum_{i=1}^n {a^{(2)}}_i \cdot u^{ki} & \ldots & \sum_{i=1}^n {a^{(k)}}_i \cdot u^{ki} \end{pmatrix}$$

Recall that $(C_u(\mathbb{F}_q^k) = \mathbb{F}_q^k) \leftrightarrow (Det(C_u) \neq 0)$.

Let $f(u) = Det(C_u)$. We will show that $f(u)$ is a non-zero polynomial of degree at most $n \cdot k^2$. It follows that $Det(C_u) = 0$ for at most $n \cdot k^2$ u's and the lemma follows.

$$f(u) = Det(C_u) = \sum_{\sigma \in S_k} sgn(\sigma) \cdot f_\sigma(u),$$

where

$$f_\sigma(u) = \prod_{j=1}^{k} (C_u)_{j,\sigma(j)}.$$

For $j \in [k]$, we define $j_{\max}$ to be the maximal $i \in [n]$ such that ${a^{(j)}}_i$ is non-zero. Note that, using Gaussian elimination, we can find a basis $a^{(1)}, \ldots, a^{(k)}$ of A such that,

$$0 < 1_{\max} < 2_{\max} < \ldots < k_{\max}.$$

We assume without loss of generality that this is the case. Let $Id \in S_k$ be the identity permutation. We will show that for every $\sigma \neq Id$ in S_k, $deg(f_\sigma) < deg(f_{Id})$.

Assume for contradiction that there exists $\sigma \neq Id$ in S_k with $deg(f_\sigma) \geq deg(f_{Id})$. Fix such a permutation σ that maximizes $\deg(f_\sigma)$. (That is, $deg(f_\sigma) \geq deg(f_{\sigma'})$ for every $\sigma' \in S_k$). $(C_u)_{j,\sigma(j)}$ is a polynomial in u of degree $j \cdot \sigma(j)_{max}$. Therefore, $f_\sigma(u)$ has degree $\sum_{j=1}^{k} j \cdot \sigma(j)_{max}$. Since $\sigma \neq Id$, there exist $j_1 < j_2$ such that $\sigma(j_1) > \sigma(j_2)$. Let $\tau = \sigma \cdot (\sigma(j_1)\sigma(j_2))$, i.e., the permutation τ consists of applying σ and then "switching" between $\sigma(j_1)$ and $\sigma(j_2)$.

We have

$$deg(f_\tau) - deg(f_\sigma) = j_2(\sigma(j_1)_{max} - \sigma(j_2)_{max}) + j_1(\sigma(j_2)_{max} - \sigma(j_1)_{max})$$

$$= j_2(\sigma(j_1)_{max} - \sigma(j_2)_{max}) - j_1(\sigma(j_1)_{max} - \sigma(j_2)_{max})$$
$$= (j_2 - j_1)(\sigma(j_1)_{max} - \sigma(j_2)_{max}) > 0$$

which contradicts the maximality of $deg(f_\sigma)$.

Therefore, for any $\sigma \neq Id$, we have $deg(f_{Id}) > deg(f_\sigma)$. Thus, f_{Id} cannot be "canceled out" by the other summands in $f(u)$, and $f(u)$ is a non-zero polynomial of degree $deg(f_{Id}) = \sum_{j=1}^{k} j \cdot j_{max} \leq n \cdot \sum_{j=1}^{k} j = n \cdot \frac{k(k+1)}{2} \leq n \cdot k^2$. □

We can now easily prove the theorem.

Proof. (of Theorem 5) Fix any $(n,k)_q$-affine source X. Using Lemma 6.1 we get

$$\Pr_{y \leftarrow U_d}(E(X,y) \nsim U_{\mathbb{F}_q^k}) \leq \frac{n \cdot k^2}{|U|} \leq \epsilon.$$

Therefore, by lemma 3.2

$$E(X,U_d) \overset{\epsilon}{\sim} U_{\mathbb{F}_q^k}.$$

□

7 Composing extractors

Let E be a linear seeded affine source extractor. In this section, we show that we can use E with a correlated seed that we have extracted deterministically from our affine source.

Our starting point will be the following lemma which is a combination of Lemmas 2.5 and 2.6 in [12].[12] Fix a distribution X on $\mathbb{F}_q^n$ and functions T and D. Roughly speaking, the lemma states that if $D(X)$ is close to uniform even when conditioning on a certain output value of T, then the output distribution $T(X)$ is "almost not affected" by conditioning on a value of D.

Lemma 7.1. *Let X be a distribution on $\mathbb{F}_q^n$. Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and $D : \mathbb{F}_q^n \to \{0,1\}^d$ be any functions. Assume that for every $a \in Supp(T(X))$ we have $|(D(X)|T(x) = a) - U_d| \leq \epsilon$. Then for every $y \in Supp(D(X))$ we have*

$$(T(X)|D(x) = y) \overset{\epsilon \cdot 2^{d+1}}{\sim} T(X).$$

The following corollary of Lemma 7.1 shows that, for a fixed linear mapping T, the output distribution of T on an affine source X is "almost not affected" by conditioning on an output value of a deterministic affine source extractor D.

Corollary 7.2. *Fix any field $\mathbb{F}_q$, integers n, k, m, d, and $\epsilon > 0$, such that $k > m$ and $\epsilon < 2^{-(d+1)}$. Let $D : \mathbb{F}_q^n \to \{0,1\}^d$ be a deterministic $(1, \epsilon)$-affine source extractor. Let X be an $(n, k)_q$-affine source. Then for any linear mapping $T : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and $y \in \{0,1\}^d$,we have*

$$|(T(X)|D(x) = y) - T(X)| \leq \epsilon \cdot 2^{d+1}.$$

Proof. Fix any $a \in Supp(T(X))$. It is easy to see that $(X|T(x) = a)$ is an $(n, k')_q$-affine source for some $k' \geq 1$ (since $k > m$). Therefore,

$$(D(X)|T(x) = a) \overset{\epsilon}{\sim} U_d.$$

Fix any $y \in \{0,1\}^d$. Since $\epsilon < 2^{-d}$, we know that $y \in Supp(D(X))$. Thus, using lemma 7.1, we have

$$|(T(X)|D(x) = y) - T(X)| \leq \epsilon \cdot 2^{d+1}.$$

□

Corollary 7.2 works for any linear T and output value y. In particular, as observed in [12], T can be a function of y. We use this fact to compose a deterministic affine source extractor with a linear seeded affine source extractor, and get a new deterministic affine source extractor that extracts more randomness.

[12] In [12] they assume all distributions are over binary strings, but it is easy to see that the proof follows in the case stated here.

Theorem 6. *Fix any field $\mathbb{F}_q$, integers n, k, m, d, and $\epsilon, \epsilon' > 0$, such that $k > m$ and $\epsilon' < 2^{-(d+1)}$. Let $D' : \mathbb{F}_q^n \to \{0,1\}^d$ be a deterministic $(1, \epsilon')$-affine source extractor. Let $E : \mathbb{F}_q^n \times \{0,1\}^d \to \mathbb{F}_q^m$ be a linear seeded (k, ϵ)-affine source extractor. Then $D : \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined by*

$$D(x) = E(x, D'(x))$$

is a deterministic (k, ρ)-affine source extractor, where $\rho = 4\epsilon' \cdot 2^d + \epsilon$.

Proof. Fix an $(n, k)_q$-affine source X. Note that,

$$D(X) \;\sim\; E(X, D'(X)) \;\sim\; \sum_{y \in \{0,1\}^d} \Pr(D'(X) = y) \cdot (E(X, y) | D'(x) = y),$$

and

$$E(X, U_d) \;\sim\; \sum_{y \in \{0,1\}^d} \Pr(U_d = y) \cdot E(X, y).$$

We know that $|D'(X) - U_d| \leq \epsilon'$. Fix any $y \in \{0,1\}^d$. $T_y(x) = E(x, y)$ is a linear mapping from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$, where $m < k$. Therefore, by corollary 7.2, we have

$$|(E(X, y)|D'(x) = y) - E(X, y)| \leq \epsilon' \cdot 2^{d+1}.$$

By lemma 3.1, we have

$$|D(X) - E(X, U_d)| \leq 2\epsilon' + \epsilon' \cdot 2^{d+1}.$$

Therefore,

$$|D(X) - U_{\mathbb{F}_q^m}| \leq 2\epsilon' + \epsilon' \cdot 2^{d+1} + \epsilon \leq 4\epsilon' \cdot 2^d + \epsilon.$$

□

8 Putting it all together

In this section we present our main extractor construction.

Using Theorem 6, we compose the deterministic extractor of Lemma 5.5 and the seeded extractor of Theorem 5 to get a deterministic extractor that extracts almost all the randomness from an $(n, k)_q$-affine source assuming q is a large enough polynomial in n. We restate and prove Theorem 1.

Theorem 1 There exists a constant q_0 such that for any field $\mathbb{F}_q$ and integers n, k with $q > \max[q_0, n^{20}]$, there is an explicit deterministic (k, ρ)-affine source extractor $D : \mathbb{F}_q^n \to \mathbb{F}_q^{k-1}$, with $\rho \leq q^{-1/21}$.

Proof. We use Lemma 5.5 with $\delta = 4/5$. For large enough q and any $n \leq q^{\delta/7}$, we get an explicit deterministic $(1, \epsilon')$-affine source extractor $D' : \mathbb{F}_q^n \to \{0,1\}^{d'}$, where $d' = \lfloor (1/5)\log q \rfloor$ and $\epsilon' \leq q^{-4/15}$. We use Theorem 5 with parameters $q, n, k-1$ and $\epsilon = \frac{8n^3}{q^{1/5}}$. Note that,

$$\frac{2n \cdot k^2}{\epsilon} \leq \frac{2n^3 \cdot q^{1/5}}{8n^3} \leq q$$

as required in Theorem 5. We get a linear seeded (k, ϵ)-affine source extractor $E : \mathbb{F}_q^n \times \{0,1\}^d \to \mathbb{F}_q^{k-1}$, where $2^d \leq \frac{2n \cdot k^2}{\epsilon} \leq q^{1/5}/4 \leq 2^{d'}$. Since $d \leq d'$, we can use theorem 6 with D' and E and get an explicit deterministic (k, ρ)-affine source extractor $D : \mathbb{F}_q^n \to \mathbb{F}_q^{k-1}$, where

$$\rho = 4\epsilon' \cdot 2^d + \epsilon \leq 4q^{-4/15} \cdot q^{1/5}/4 + \frac{8n^3}{q^{1/5}}$$

$$\leq q^{-3/15} + 8 \cdot q^{3/20-1/5} \leq 9 \cdot q^{-1/20} \leq q^{-1/21}$$

for large enough q. $\square$

Acknowledgements

The first author is grateful to Zeev Dvir, Oded Goldreich, Dana Moshkovitz, Asaf Nussboim, Omer Reingold, Guy Rothblum, Ronen Shaltiel, Amir Shpilka, and Amir Yehudayoff for very helpful discussions. In particular, the first author would like to thank Oded Goldreich for a very helpful comment that significantly simplifed the presentation of the proof of Lemma 6.1. Finally, a big big thanks to Asaf Nussboim for introducing the first author to Weil's theorems.

References

[1] N. Alon. Tools from higher algebra. In *R. L. Graham & M. Grotschel & L. Lovasz (eds.), Handbook of Combinatorics, Elsevier and The MIT Press*, volume 2. 1995.

[2] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple constructions of almost k-wise independent random variables. In *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science*, volume II, pages 544–553, 1990.

[3] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting randomness from few independent sources. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, 2004.

[4] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating independence: New consturctions of condenesers, ramsey graphs, dispersers, and extractors. In *Submitted*, 2004.

[5] E. Ben-Sasson, S. Hoory, E. Rozenman, and S. Vadhan. Personal communication. 2001.

[6] Manuel Blum. Independent unbiased coin flips from a correlated biased source: a finite state Markov chain. In *Proceedings of the 25th Annual IEEE Symposium on Foundations of Computer Science*, pages 425–433, 1984.

[7] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, April 1988. Special issue on cryptography.

[8] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, and R. Smolensky. The bit extraction problem or t-resilient functions. In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science*, 1985.

[9] A. Cohen and A. Wigderson. Dispersers, deterministic amplification, and weak random sources. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, 1989.

[10] Y. Dodis, A. Elbaz, R. Oliveira, and R. Raz. Improved randomness extraction from two independent sources. In *RANDOM: International Workshop on Randomization and Approximation Techniques in Computer Science*. LNCS, 2004.

[11] A. Elbaz. Improved constructions for extracting quasi-random bits from sources of weak randomness. *MSc Thesis, Weizmann Institute*, 2003.

[12] A. Gabizon, R. Raz, and R. Shaltiel. Determinsitic extractors for bit-fixing sources by obtaining an independent seed. In *FOCS 2004*, 2004.

[13] R. L. Graham and J. H. Spencer. A constructive solution to a tournament problem. *Canad. Math. Bull.*, 14:45–48, 1971.

[14] A. Hales and R. Jewett. Regularity and positional games. *Trans. Amer. Math. Soc.*, 106:222–229, 1963.

[15] J. Kamp and D. Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, 2003.

[16] M. Naor, A. Nussboim, and E. Tromer. Efficiently constructible huge graphs that preserve first order properties of random graphs. In *TCC*, pages 66–85, 2005.

[17] N. Nisan and A. Ta-Shma. Extracting randomness: A survey and new constructions. *Journal of Computer and System Sciences*, 58, 1999.

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

[19] Noam Nisan. Extracting randomness: How and why: A survey. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity*, pages 44–58, 1996.

[20] R. Raz. Extractors with weak random seeds. 2005.

[21] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in trevisan's extractors. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 149–158, 1999.

[22] M. Santha and U. V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33:75–87, 1986.

[23] W. M. Schmidt. *Equations over Finite Fields: An Elementary Approach*, volume 536. Springer-Verlag, Lecture Notes in Mathematics, 1976.

[24] R. Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[25] R. Shaltiel and C. Umans. Simple extractors for all min-entropies and a new pseudo-random generator. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, 2001.

[26] A. Ta-Shma, D. Zuckerman, and S. Safra. Extractors from Reed-Muller codes. In IEEE, editor, *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 638–647, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. IEEE Computer Society Press.

[27] L. Trevisan. Construction of extractors using pseudorandom generators. In *Proceedings of the 31st ACM Symposium on Theory of Computing*, 1999.

[28] L. Trevisan and S. Vadhan. Extracting randomness from samplable distributions. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, 2000.

[29] S. Vadhan. Randomness extractors and their many guises. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 9–12, 2002.

[30] U. Vazirani. Efficient considerations in using semi-random sources. In *Proceedings of the 19th Annual ACM Symposium on the Theory of Computing*, 1987.

[31] U. Vazirani. Strong communication complexity or generating quasi-random sequences from two communicating semi-random sources. *Combinatorica*, 7:375–392, 1987.

[32] U. Vazirani and V. Vazirani. Random polynomial time is equal to semi-random polynomial time. Technical Report TR88-959, Cornell University, Computer Science Department, December 1988.

[33] John von Neumann. Various techniques used in connection with random digits. *Applied Math Series*, 12:36–38, 1951.

[34] A. Weil. On some exponential sums. In *Proc. Nat. Acad. Sci. USA*, volume 34, pages 204–207, 1948.

[35] D. Zuckerman. General weak random sources. In *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543, 1990.

[36] D. Zuckerman. Simulating BPP using a general weak random source. *Algorithmica*, 16(4/5):367–391, October/November 1996.