Electronic Colloquium on Computational Complexity, Report No. 129 (2011)

Extractors for Polynomials Sources over Constant-Size Fields of Small Characteristic

Eli Ben-Sasson* Ariel Gabizon†

September 22, 2011

Abstract

Let $\mathbb{F}_q$ be the field of q elements, where $q = p^\ell$ for prime p. Informally speaking, a *polynomial source* is a distribution over $\mathbb{F}_q^n$ sampled by low degree multivariate polynomials. In this paper, we construct extractors for polynomial sources over fields of constant size q assuming $p \ll q$.

More generally, suppose a distribution X over $\mathbb{F}_q^n$ has support size q^k and is sampled[1] by polynomials of individual degree d and total degree D. Then we can extract random bits with error ϵ from X whenever $q = \Omega(D^2 \cdot (p \cdot d)^{6n/k}/\epsilon^2)$. For instance, when p, D and the 'entropy rate' n/k are constant, we get an extractor over constant-size fields with constant error. The only previous construction by Dvir, Gabizon and Wigderson [8] required a field of size polynomial in n.

Our proof follows similar lines to that of DeVos and Gabizon [6] on extractors for affine sources, i.e., polynomial sources of degree 1. Like [6], our result makes crucial use of a theorem of Hou, Leung and Xiang [10] giving a lower bound on the dimension of products of subspaces. The key insights that enable us to extend these results to the case of polynomial sources of degree greater than 1 are

1. A source with support size q^k must have a linear span of dimension at least k, and in the setting of low-degree polynomial sources it suffices to increase the dimension of this linear span.
2. Distinct Frobenius automorphisms of a (single) low-degree polynomial source are 'pseudo-independent' in the following sense: Taking the product of distinct automorphisms (of the very same source) increases the dimension of the linear span of the source.

*Department of Computer Science, Technion, Haifa, Israel and Microsoft Research New-England, Cambridge, MA. eli@cs.technion.ac.il. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 240258.

†Department of Computer Science, Technion, Haifa, Israel. ariel.gabizon@gmail.com

[1] See the introduction for formal definitions and results.

ISSN 1433-8092

1 Introduction

This paper is part of a long and active line of research devoted to the problem of "randomness extraction": Given a family of distributions all guaranteed to have a certain structure, devise a method that can convert a sample from any distribution in this family to a sequence of uniformly distributed bits — or at least a sequence *statistically close* to the uniform distribution. Usually, it is easy to prove that a random function would be a good extractor for the given family with high probability, and the challenge is to give an explicit construction of such an extractor.

The first example of a randomness extraction problem was given by von-Neumann [17], who gave an elegant solution to the following problem: How can a biased coin with unknown bias be used to generate 'fair' coin tosses? In this case the input distribution consists of independent identically distributed bits which makes the extraction task simpler. Since then many families of more complex distributions were studied. Also, the concept of randomness extraction has proven to be useful for various applications. The reader is referred to the introduction of [6] for more details on the classes of distributions studied, references and motivation.

Polynomial sources In this paper we construct extractors for *polynomial sources* — distributions that are sampled by applying low-degree polynomials to uniform inputs as defined next. Throughout this paper if Ω is a finite set we let U_Ω denote the uniform distribution on Ω.

Definition 1 (Polynomial sources and extractors)**.** *Fix integers n, d, k with $k \leq n$ and a field $\mathbb{F}_q$. We define $\mathcal{M}[n, d, k]$ to be the set of mappings $f : \mathbb{F}_q^r \mapsto \mathbb{F}_q^n$, where r is an integer counting the number of inputs to the source and*

$$f(Z_1, \ldots, Z_r) = (f_1(Z_1, \ldots, Z_r), \ldots, f_n(Z_1, \ldots, Z_r))$$

such that

- *for every $i \in [n]$, f_i is a polynomial in $\mathbb{F}_q[Z_1, \ldots, Z_r]$ of individual degree at most d.*
- *The range, or support, of f is of size at least q^k. Formally,*

$$|\{f(z_1, \ldots, z_r) \mid (z_1, \ldots, z_r) \in \mathbb{F}_q^r\}| \geq q^k.$$

A (n, k, d)-polynomial source *is a distribution of the form $f(U_{\mathbb{F}_q^r})$ for some and $f \in \mathcal{M}[n, k, d]$ with r inputs. (When the parameters n, k, d are clear from context we shall omit them and, simply, use the term "polynomial source".)*

Let Ω be some finite set. A function $E : \mathbb{F}_q^n \mapsto \Omega$ is a (k, d, D, ϵ)-polynomial source extractor *if for every $f \in \mathcal{M}[n, d, k]$ of total degree at most D and r inputs, $E(f(U_{\mathbb{F}_q^r}))$ is ϵ-close to uniform, where a distribution P on Ω is* ϵ-close to uniform *if for every $A \subseteq \Omega$*

$$|\Pr_{x \leftarrow P}(x \in A) - |A|/|\Omega|| \leq \epsilon.$$

Remark 1.1. *A few words are in order regarding the above definitions.*

- *The number of inputs used by our source — denoted by r in the definitions above — does not affect the parameters of our extractors or dispersers hence we omit this parameter from the definition of polynomial sources and extractors.*
- *In the context of extractors what might have seemed more natural is to require the distribution $f(U_{\mathbb{F}_q^r})$ to have* min-entropy[2] *$k \cdot \log q$. Our requirement on the size of the range of f is weaker, and suffices for our construction to work.*
- *Individual degree plays a larger role than total degree in our results. In fact, the first stage of our construction — constructing a non-constant polynomial over $\mathbb{F}_q$- requires a field of size depending* only *on individual degree. This is why it is more convenient to limit individual degree and not total degree in the definition of $\mathcal{M}[n, d, k]$.*

1.1 Previous work and our result

Polynomial source extractors are a generalization of affine source extractors — where the source is sampled by a degree one map. There has been much work recently on affine source extractors [2, 3, 19, 9, 6, 11] and related objects called affine source dispersers [1, 16] where the output is required to be non-constant but not necessarily close to uniform. Regarding a related, though different, class of algebraic sources, Dvir [7] constructs extractors for distributions that are uniform over low-degree algebraic varieties which are sets of common zeros of a system of low-degree multivariate polynomials.

The only previous work on polynomial sources is by Dvir, Gabizon and Wigderson [8]. [8] concentrated on extracting as many bits as possible from the source, for which they required a large field size. Specifically, given a polynomial mapping $f : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ of total degree D whose output on a uniform input has min-entropy $k \cdot \log q$, [8] can extract $\Omega(k \cdot \log q)$ bits that are statistically close to uniform assuming q is prime[3] and $q > (poly(D, k) \cdot n)^{O(k)}$. If we are intersted in extracting just one bit, [8] still require a field size polynomial in n.

In this work, we construct polynomial source extractors over much smaller fields, assuming the characteristic of the field is significantly smaller than the field size.

Theorem 1 (Main — Extractor)**.** *Fix a field $\mathbb{F}_q$ of characteristic p, integers $d, D, 4 \leq k \leq n$ where $n \geq 25$, and a positive integer $m < 1/2 \cdot \log_p q$. Let $\alpha = 3D \cdot (p \cdot d)^{3n/k}$. Assume that $q \geq 2 \cdot \alpha^2$. There is an explicit (k, d, D, ϵ)-polynomial source extractor $E : \mathbb{F}_q^n \mapsto \mathbb{F}_p^m$ with error $\epsilon = p^{m/2} \cdot \alpha \cdot q^{-1/2}$.*

In particular, when $D, n/k$ and p are constant we get a polynomial source extractor for constant field size. We state such an instantiation.

[2]The min-entropy of a distribution P is the largest ℓ such that for every fixed x, $\Pr(P = x) \leq 2^{-\ell}$. This is the standard measure of randomness in the context of extractors originating from Chor and Goldreich [5].

[3]It seems the same method works for a non-prime q assuming the characteristic of the field is large.

Corollary 1.2 (Extractor for quadratic sources of min-entropy rate half over fields of characteristic 2)**.** *There is a universal constant C such that the following holds. For any $\epsilon > 0$ and any $q > C/\epsilon^2$ which is a power of 2, there is an explicit $(n/2, 2, 2, \epsilon)$-polynomial source extractor $E : \mathbb{F}_q^n \mapsto \{0,1\}$*
.

Non-boolean dispersers for smaller fields Along the way of our proof we construct a weaker object called a *non-boolean disperser*. A non-boolean disperser maps the source into a relatively small (but not $\{0,1\}$) domain and guarantees the output is non-constant. The advantage of this part of the construction is that it works for smaller fields than the extractor, and moreover, the field size for which it works depends only on the *individual* degrees of the source polynomials. In the theorem and corollary below we use an implicit isomorphism of $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$. See an explanation of this in the beginning of Section 3.

Theorem 2 (Main — Disperser)**.** *Fix a prime power $q = p^\ell$. Fix integers $k \leq n$ and $d < s$ such that n is prime and s is a power of p. Fix a non-trivial $\mathbb{F}_q$-linear map $T : \mathbb{F}_q^n \mapsto \mathbb{F}_q$. Let $u = \lceil (n-k)/(k-1) \rceil$. Define $P : \mathbb{F}_q^n \mapsto \mathbb{F}_q$ by $P(x) \triangleq T(x^{1+s+s^2+\ldots+s^u})$. Assume that $q > d \cdot \frac{s^{u+1}-1}{s-1}$. Then, for any $f(\mathbf{Z}) = f(Z_1, \ldots, Z_r) \in \mathcal{M}[n,k,d]$, $P(f(\mathbf{Z}))$ is a non-constant function from $\mathbb{F}_q^r$ into $\mathbb{F}_q$.*

We instantiate this result for the smallest field it works for — $\mathbb{F}_4$.

Corollary 1.3 (Disperser for min-entropy rate half over $\mathbb{F}_4$)**.** *Let n be prime. Define the function $P : \mathbb{F}_4^n \mapsto \mathbb{F}_4$ as follows. Think of the input x as an element of $\mathbb{F}_{4^n}$ and compute x^3. Now output the first coordinate of the vector x^3. Then for any $f \in \mathcal{M}[n, \lceil n/2+1 \rceil, 1]$ — that is any multilinear $f \in \mathbb{F}_{4^n}[Z_1, \ldots, Z_r]$ that has support size at least $4^{\lceil n/2+1 \rceil}$, the polynomial $P(f(Z_1, \ldots, Z_r))$ is a non-constant function from $\mathbb{F}_4^r$ into $\mathbb{F}_4$.*

2 Overview of the Proof

Our goal is to describe an explicit function $E : \mathbb{F}_q^n \to \{0,1\}^m$ such that for any (n,k,d)-polynomial source X we have that $E(X)$ is ϵ-close to the uniform distribution on $\{0,1\}^m$ and we do this in two steps. First we construct a function E_0, called a *non-boolean disperser*, that is guaranteed to be non-constant on X, i.e., such that the distribution $Y = E_0(X)$ has support size greater than 1. This part is done in Section 4. Then we apply a second function E_1 to the output of E_0 and prove that the distribution $E_1(Y) = E_1(E_0(X))$ is ϵ-close to uniform. This "disperser–to–extractor" part is described in Sections 5 and 6. We now informally describe the two functions assuming for simplicity the field $\mathbb{F}_q$ is of characteristic 2 and that n is prime. Before starting let us recall the notion of a Frobenius automorphism. If $\mathbb{K}$ is a finite field of characteristic 2 then the mapping

$$\sigma_i : \mathbb{K} \to \mathbb{K}, \quad \sigma_i(z) = z^{2^i}$$

is a *Frobenius automorphism of $\mathbb{K}$ over $\mathbb{F}_2$*. (These mappings can be defined over larger fields as well, cf. Section 3.3.) The three elementary properties of this mapping that we use below are first its $\mathbb{F}_2$*-linearity* — that $\sigma_i(a+b) = \sigma_i(a) + \sigma_i(b)$, second its *distinctness*, i.e., that if $\mathbb{K}$ is an extension

of $\mathbb{F}_2$ of degree at least t and $0 \leq i < j \leq t-1$ then σ_i and σ_j are different, and third its *dimension-preservation:* If $\mathbb{K} \supset \mathbb{F}_q \supset \mathbb{F}_2$ then $A \subset \mathbb{K}$ and $\sigma_i(A) \triangleq \{\sigma_i(a) \mid a \in A\}$ span spaces of equal dimension over $\mathbb{F}_q$ (see Claim 3.1).

A different view on low-degree sources The first part of our analysis uses a somewhat nonstandard view of low-degree sources that we need to highlight. The random variable X ranges over $\mathbb{F}_q^n$ and is the output of n degree-d polynomials over $\mathbb{F}_q$. Let $\mathbb{F}_q^{\leq d}[Z_1, \ldots, Z_r]$ denote the set monomials over $\mathbb{F}_q$ of individual degree at most d where $d < q$. (We use Z variables to denote inputs of the polynomial source and X variables for its output.) Suppose the ith coordinate of X is

$$X_i = P^{(i)}(Z_1, \ldots, Z_r) = \sum_{M \in \mathbb{F}_q^{\leq d}[Z_1, \ldots, Z_r]} a_M^{(i)} \cdot M(Z_1, \ldots, Z_r)$$

where $a_M^{(i)} \in \mathbb{F}_q$ and $Z_1, \ldots, Z_r$ are independent random variables distributed uniformly over $\mathbb{F}_q$. Applying an $\mathbb{F}_q$-linear bijection $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$, let $a_M = \phi(a_M^{(1)}, \ldots, a_M^{(n)})$ denote the sequence of coefficients of the monomials M, viewed now as a single element in $\mathbb{F}_{q^n}$. Our nonstandard view is that our source is

$$X = P(Z_1, \ldots, Z_r) = \sum_{M \in \mathbb{F}_q^{\leq d}[Z_1, \ldots, Z_r]} a_M \cdot M(Z_1, \ldots, Z_r) \tag{1}$$

where the coefficients a_M and the random variable X come from the "large" field $\mathbb{F}_{q^n}$ but the random variables $Z_1, \ldots, Z_r$ still range over the "small" field $\mathbb{F}_q$. This large-field-small-field view will be important in what comes next. In particular, we shall use the following claim which reduces the problem of constructing a non-boolean disperser to that of constructing a polynomial whose coefficients span $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Claim 2.1 (Full-span polynomials are non-constant coordinate-wise)**.** *Suppose P has individual degree smaller than q. If the set of coefficients $A = \{a_M \mid \deg(M) > 0\}$ appearing in (1) spans $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ then $X_i = P^{(i)}(Z_1, \ldots, Z_r)$ is a non-constant function for every $i \in \{1, \ldots, n\}$.*

Proof. By way of contradiction. If $P^{(i)}$ is constant on $\mathbb{F}_q^r$ and has individual degrees smaller than q, then all its nonzero coefficients are zero in which case A spans a strict subspace of $\mathbb{F}_{q^n}$. □

Non-boolean disperser We start with the simplest nontrivial case to which our techniques apply and construct a non-boolean disperser for homogeneous multilinear quadratic sources with min-entropy rate greater than half over the finite field with 4 elements (this is a special case of Corollary 1.3). Using $\binom{r}{2}$ to denote the set $\{(i,j) \mid 1 \leq i < j \leq r\}$ and writing X as in (1) we get

$$X = \sum_{(i,j) \in \binom{r}{2}} a_{ij} Z_i Z_j, \quad a_{ij} \in \mathbb{F}_{4^n} \tag{2}$$

where $Z_1, \ldots, Z_r$ are uniformly and independently distributed over $\mathbb{F}_4$ and X has support of size greater than $4^{n/2}$. Let

$$A = \left\{ a_{ij} \mid (i,j) \in \binom{r}{2} \right\} \tag{3}$$

denote the set of coefficients appearing in (2). In light of Claim 2.1 it suffices to construct E_0 such that $E_0(X)$, when written as a polynomial over $Z_1, \ldots, Z_r$, has a set of coefficients that spans $\mathbb{F}_{4^n}$ over $\mathbb{F}_4$. (Then we "project" this polynomial onto, say, the first coordinate and get a non-constant function mapping into $\mathbb{F}_4$, i.e., a non-boolean disperser.)

To do this we take the approach of DeVos and Gabizon [6] which uses the theorem of Hou, Leung and Xiang [10]. Assuming n is prime, this theorem implies that if $A, B \subset \mathbb{F}_{q^n}$ are sets spanning spaces of respective dimensions d_1, d_2 over $\mathbb{F}_q$, then the set of products

$$A \cdot B \triangleq \{a \cdot b \mid a \in A, b \in B\}$$

spans a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of dimension at least $\min\{n, d_1 + d_2 - 1\}$. Returning to our case and taking A as in (3), our first observation is that $\dim(\mathrm{span}(A)) > n/2$ because X is contained in $\mathrm{span}(A)$. So the theorem of [10] mentioned above implies that $\mathrm{span}(A \cdot A) = \mathbb{F}_{4^n}$. Consider what would happen if we could sample *twice* from X independently and take the product of the two samples in $\mathbb{F}_{4^n}$. Using $X', Z'_1, \ldots, Z'_r$ to express the second sample we write this product as

$$X \cdot X' \;=\; \left(\sum_{(i,j)\in\binom{r}{2}} a_{ij} Z_i Z_j \right) \cdot \left(\sum_{(i',j')\in\binom{r}{2}} a_{i'j'} Z'_i Z'_j \right).$$

Opening the right-hand-side as a polynomial in $Z_1, \ldots, Z_r, Z'_1, \ldots, Z'_r$ we see that its set of coefficients is $A \cdot A$ which spans $\mathbb{F}_{4^n}$ over $\mathbb{F}_4$, as desired[4].

Unfortunately we only have access to a *single* sample of X and have to make use of it. We use the fact that $\mathbb{F}_4$ is a degree 2 extension of a smaller field ($\mathbb{F}_2$) and hence has two distinct Frobenius automorphisms. And here comes our second observation: Taking the product of 2 distinct Frobenius automorphisms of a *single* sample of X has a similar effect to that of taking two independent samples of X! Indeed, take the product of $\sigma_0(X)$ and $\sigma_1(X)$ and, using the linearity of Frobenius mapping, expand as

$$\begin{aligned} X \cdot X^2 \;&=\; \left(\sum_{(i,j)\in\binom{r}{2}} a_{ij} Z_i Z_j \right) \cdot \left(\sum_{(i',j')\in\binom{r}{2}} a^2_{ij} Z^2_i Z^2_j \right) \\ &=\; \sum_{(i,j),(i',j')\in\binom{r}{2}} a_{ij} a^2_{i'j'} Z_i Z_j Z^2_{i'} Z^2_{j'}. \end{aligned}$$

[4]The same argument would work as well over the two-element field $\mathbb{F}_2$. The extension field is needed to deal with the case of a single source as explained next.

The main point is that every element in the set of products of A and $A^2 \triangleq \{a^2 \mid a \in A\}$ appears as the coefficient of a monomial in the polynomial above and these monomials are distinct over $\mathbb{F}_4$. And the dimension-preservation of σ_1 implies that $\dim(\mathrm{span}(A^2)) = \dim(\mathrm{span}(A)) > n/2$. Consequently, the theorem of [10] implies that $A \cdot A^2$ spans $\mathbb{F}_{4^n}$ over $\mathbb{F}_4$, so by Claim 2.1 the function $E_0(X)$, which outputs the first coordinate of $X \cdot X^2$, is non-constant for X and this completes the sketch of our non-boolean disperser for the special case of homogenous, quadratic, multilinear polynomials over $\mathbb{F}_4$.

To extend this argument to general polynomial sources of individual degree $\leq d$ we carefully select a set of t distinct Frobenius automorphisms $\sigma_{i_0}, \ldots, \sigma_{i_{t-1}}$ (assuming $\mathbb{F}_q$ is an extension-field of degree at least t) such that the mapping $f : (\mathbb{F}_q^{\leq d}[Z_1, \ldots, Z_r])^t \to \mathbb{F}_q[Z_1, \ldots, Z_r]$ given by

$$f(M_0, \ldots, M_{t-1}) = \prod_{j=0}^{t-1} \sigma_{i_j}(M_j) \mod (Z_1^q - Z_1, \ldots, Z_r^q - Z_r)$$

is injective. Then we argue, just as in the case above, that the function $g(X) \triangleq \prod_{j=0}^{t-1} \sigma_{i_j}(X)$ expands to a sum of distinct monomials with coefficients ranging over the product set $\hat{A} = \sigma_{i_0}(A) \cdots \sigma_{i_{t-1}}(A)$ where $\sigma(A) = \{\sigma(a) \mid a \in A\}$. The theorem of [10] is applied t times to conclude that $\hat{A}$ spans $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Now we apply Claim 2.1 and get that the first coordinate of $g(X)$ (viewing $g(X)$ as a tuple of n polynomials over $\mathbb{F}_q$) is a non-constant function. Details are provided in Section 4.

From dispersers to extractors This part is based on the work of Gabizon and Raz [9] and uses an important theorem of Weil [18]. This theorem implies the following. Suppose we evaluate a polynomial $g \in \mathbb{F}_q[Z_1, \ldots, Z_r]$ of small-enough degree $\deg(g) < \sqrt{q}$ on a uniformly random sample in $\mathbb{F}_q^r$ and then take the first bit of this evaluation (when viewing it as a vector over $\mathbb{F}_2$). Then, this bit will either be constant — we then say g is "degenerate" — or close to the uniform distribution. Assuming our source is low-degree and the field size q is sufficiently large we can argue that $\deg(E_0(X)) < \sqrt{q}$ because X is low-degree by assumption and E_0 is low-degree by construction. So to apply Weil's Theorem and get an extractor we only need to ensure that we have in hand a non-degenerate polynomial. Alas, we have relatively little control over the polynomial source so need to transform it somehow into a non-degenerate one in a black-box manner. Here we apply another observation, its proof is due to Swastik Kopparty, which says that $(E_0(X))^v$ is non-degenerate for odd[5] $v > 2$. This part is explained in Section 5. So we take $E_1(Y)$ to be the first[6] bit of Y^3 and using this observation and Weil's Theorem conclude that $E_1(E_0(X))$ is close to uniform. Analysis of the resulting extractor is given in Section 6.

[5]For characteristic $p > 2$ the criteria for v is a bit different: we need $p \not| v$.

[6]In fact, we can output several bits. See Subsection 3.1 for details.

3 Preliminaries

Notation: When we discuss identities between polynomials we only mean identities as *formal polynomials*. We will frequently alternate between viewing $\mathbf{x} \in \mathbb{F}_q^n$ as an element of either $\mathbb{F}_q^n$ or the field $\mathbb{F}_{q^n}$. When we do this we assume it is using an implicit bijective map $\phi : \mathbb{F}_q^n \mapsto \mathbb{F}_{q^n}$ that is an isomorphism of vector spaces. That is, $\phi(t_1 \cdot a_1 + t_2 \cdot a_2) = t_1 \cdot \phi(a_1) + t_2 \cdot \phi(a_2)$ for any $t_1, t_2 \in \mathbb{F}_q$ and $a_1, a_2 \in \mathbb{F}_q^n$. Such ϕ is efficiently computable using standard representations of $\mathbb{F}_{q^n}$. (For details see for example the book of Lidl and Niederreiter [12].) For a set Ω we denote by U_Ω the uniform distribution on Ω.

3.1 Weil Bounds for Additive Character Sums

The seminal work of Weil [18] on the 'Reimann hypothesis for curves over finite fields' implies very useful bounds on character sums. As we will see in this section, these bounds enable us to extract randomness from certain 'low-degree distributions'.

For background on characters of finite fields see [15] or Subsection 3.2 of [9]. The following version of the Weil bound was proved by Carlitz and Uchiyama [4].

Theorem 1 (Weil-Carlitz-Uchiyama bound)**.** *Let $q = p^\ell$ for prime p and an integer ℓ. Let ψ be a non-trivial additive character of $\mathbb{F}_q$ (that is, not identically 1). Let $f(Z)$ be a polynomial in $\mathbb{F}_q[Z]$ of degree d. Suppose that f is not of the form $h^p + h + c$ for any $h \in \mathbb{F}_q[Z]$ and $c \in \mathbb{F}_q$. Then*

$$\left| \sum_{z \in \mathbb{F}_q} \psi(f(z)) \right| \leq (d-1) \cdot q^{1/2}.$$

We require the following generalization of Vazirani's XOR Lemma from Rao [14], appearing there as Lemma 4.2.

Lemma 3.1 (Rao's XOR lemma)**.** *Let X be a distribution on a finite abelian group G s.t. $|\mathrm{E}(\psi(X))| \leq \epsilon$ for any non-trivial character ψ of G. Then X is $\epsilon \cdot \sqrt{|G|}$-close to uniform on G.*

The above lemma implies it suffices to bound additive character sums of a distribution over $\mathbb{F}_q$ in order to extract randomness. This is formalized in lemma below. To state the lemma we first define how to extract a few entries of an element in $\mathbb{F}_{p^\ell}$.

Definition 2 (Prefix projection)**.** *Let $q = p^\ell$ for prime p and an integer ℓ. Fix an isomorphism between $\mathbb{F}_q$ and $\mathbb{F}_p^\ell$ and view $x \in \mathbb{F}_q$ as $(x_1, \ldots, x_\ell) \in \mathbb{F}_p^\ell$. Fix an integer $m \leq \ell$. We define the* prefix projection function $E_m : \mathbb{F}_q \mapsto \mathbb{F}_p^m$ *by $E_m(x) = E_m((x_1, \ldots, x_\ell)) \triangleq (x_1, \ldots, x_m)$.*

Lemma 3.2 (XOR lemma for prefix projections)**.** *Let $q = p^\ell$ for prime p and an integer ℓ. Let X be a distribution on $\mathbb{F}_q$ such that $|\mathrm{E}(\psi(X))| \leq \epsilon$ for any non-trivial additive character ψ of $\mathbb{F}_q$. Then $E_m(X)$ is $p^{m/2} \cdot \epsilon$-close to uniform.*

Proof. Let $\omega \in \mathbb{C}$ be a primitive p'th root of unity. The additive characters of $\mathbb{F}_q$ are exactly the functions $\psi : \mathbb{F}_q \mapsto \mathbb{C}$ of the form $\psi(a) = \omega^{T(a)}$ where $T : \mathbb{F}_q \mapsto \mathbb{F}_p$ is an $\mathbb{F}_p$-linear function and

$T(a)$ is interpreted as an integer in $\{0, \ldots, p-1\}$. The additive characters of $\mathbb{F}_p^m$ are just a subset of these, namely the functions $\psi : \mathbb{F}_p^m \mapsto \mathbb{C}$ of the form $\psi(a) = \omega^{T(a)}$ where $T : \mathbb{F}_p^m \mapsto \mathbb{F}_p$ is an $\mathbb{F}_p$-linear function. (Recall that we identify $\mathbb{F}_q$ with $\mathbb{F}_p^\ell$.) It follows that $|\mathrm{E}(\psi(E_m(X)))| \leq \epsilon$ for any non-trivial additive character of $\mathbb{F}_p^m$. From Lemma 3.1, we have that $E_m(X)$ is $p^{m/2} \cdot \epsilon$-close to uniform.

□

Summing up the previous results we reach the statement that will be later used in analyzing our extractors.

Corollary 3.3 (Weil-Carlitz-Uchiyama for prefix projections)**.** *Let $q = p^\ell$ for prime p and an integer ℓ. Let $f(Z)$ be a polynomial in $\mathbb{F}_q[Z]$ of degree d. Suppose that f is not of the form $h^p + h + c$ for any $h \in \mathbb{F}_q[Z]$ and $c \in \mathbb{F}_q$. Then $E_m(f(U_{\mathbb{F}_q}))$ is $p^{m/2} \cdot d/\sqrt{q}$-close to uniform.*

Proof. Follows immediately from Theorem 1 and Lemma 3.2. □

3.2 Dimension Expansion of Products

Recall that $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_q$ isomorphic to $\mathbb{F}_q^n$. For a set $A \subseteq \mathbb{F}_{q^n}$ we denote by $\dim(A)$ the dimension of the $\mathbb{F}_q$-span of A. For sets $A, B \subseteq \mathbb{F}_{q^n}$ let $A \cdot B \triangleq \{a \cdot b \mid a \in A, b \in B\}$. Hou, Leung and Xiang [10] show that such products expand in dimension. The following theorem is a corollary of Theorem 2.4 of [10].

Theorem 3 (Dimension expansion of products)**.** *Let $\mathbb{F}_q$ be any field, and let n be prime.*[7] *Let A and B be non-empty subsets of $\mathbb{F}_{q^n}$ such that $A, B \neq \{0\}$. Then*

$$\dim(A \cdot B) \geq \min\{n, \dim(A) + \dim(B) - 1\}$$

In particular, if $A_1, \ldots, A_m$ are non-empty subsets of $\mathbb{F}_{q^n}$ such that for all $1 \leq i \leq m$, $dim(A_i) \geq k$ for some $k \geq 1$. Then

$$\dim(A_1 \cdots A_m) \geq \min\{n, k \cdot m - (m-1)\}.$$

Remark 3.4. *The definition of $A \cdot B$ is somewhat different from that in [10] where it is defined only for subspaces, and as the* span *of all possible products. The definition above will be more convenient for us. It is easy to see that Theorem 2.4 of [10] implies the theorem above with our definition. Still, we give a self-contained proof.*[8]

Proof. First we note that it is enough to prove the theorem for linear subspaces A and B of dimension at least one: Given arbitrary sets A and B, let $A' \triangleq \mathrm{span}(A)$ and $B' \triangleq \mathrm{span}(B)$. If A and B both

[7] The theorem of [10] works also for non-prime n in which case the inequality involves the size of a certain subfield of $\mathbb{F}_{q^n}$.

[8] Also, see Section 3.2 of [6] for a self-contained proof using the definition of [10].

contain a non-zero element (as required in the theorem), then A' and B' are linear subspaces of dimension at least one. So we have that

$$\dim(A' \cdot B') \geq \min\{n, \dim(A') + \dim(B') - 1\} = \min\{n, \dim(A) + \dim(B) - 1\}.$$

Now, we observe that $\mathrm{span}(A' \cdot B') \subseteq \mathrm{span}(A \cdot B)$: An element of $A' \cdot B'$ has the form

$$(\sum_i t_i \cdot a_i) \cdot (\sum_j s_j \cdot b_j) = \sum_{i,j} t_i \cdot s_j \cdot a_i \cdot b_j,$$

where $a_i \in A, b_j \in B$ and $t_i, s_j \in \mathbb{F}_q$. This is obviously in $\mathrm{span}(A \cdot B)$. So $A' \cdot B' \subseteq \mathrm{span}(A \cdot B)$, and this implies $\mathrm{span}(A' \cdot B') \subseteq \mathrm{span}(A \cdot B)$. Therefore, the equation above implies

$$\dim(A \cdot B) \geq \min\{n, \dim(A) + \dim(B) - 1\}.$$

We now turn to proving the theorem for linear subspaces A and B of dimension at least one. We proceed by induction on $\dim(A)$. As a base, observe that the result holds trivially when $\dim(A) = 1$. For the inductive step, we may then assume that $\dim(A) > 1$. We may also assume that $B \neq \mathbb{F}_{q^n}$ as the theorem is immediate in this case.

Note that we may freely replace A by $g \cdot A$ (or B by $g \cdot B$) for some $g \in \mathbb{F}_{q^n}$ as this has no effect on $\dim(A)$, $\dim(B)$, or $\dim(A \cdot B)$. By this operation, we may assume that $1 \in A \cap B$. Since $\dim(A) > 1$, we may choose $a \in A \setminus \mathbb{F}_q$. Let ℓ be the smallest nonnegative integer so that $a^\ell \notin B$ (this must exist since $\mathbb{F}_{q^n} = \mathrm{span}(1, a, a^2, \ldots, a^{n-1})$ for any $a \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ when n is prime, and $B \neq \mathbb{F}_{q^n}$) and note that $\ell > 0$ by the assumption that $1 \in B$. Next, replace B by the set $a^{-(\ell-1)} \cdot B$. It now follows that $1 \in B$ and $a \notin B$, so $A \cap B$ is a proper nonempty subset of A.

Consider the $\mathbb{F}_q$-linear subspaces $A \cap B$ and $A + B$ and observe that $(A \cap B) \cdot (A + B) \subseteq \mathrm{span}(A \cdot B)$. The next equation follows from this and the induction hypothesis applied to $A \cap B$ and $A + B$.

$$\begin{aligned} \dim(A \cdot B) &\geq \dim((A \cap B) \cdot (A + B)) \\ &\geq \min\{n, \dim(A \cap B) + \dim(A + B) - 1\} \\ &= \min\{n, \dim(A) + \dim(B) - 1\}. \end{aligned}$$

This completes the proof. □

3.3 Frobenius Automorphisms of $\mathbb{F}_q$

Let $q = p^\ell$ for prime p and let $i \geq 0$ be an integer. Raising to power p^i in $\mathbb{F}_q$ is known as a Frobenius automorphism of $\mathbb{F}_q$ over $\mathbb{F}_p$ and will play an important role. We record two useful and well-known properties of this automorphism that will be used in our proofs.

- **Linearity:** $\forall a, b \in \mathbb{F}_q$, $(a + b)^{p^i} = a^{p^i} + b^{p^i}$.

- **Bijection:** The map $x \mapsto x^{p^i}$ over $\mathbb{F}_q$ is bijective. In particular, for $c \in \mathbb{F}_q$, c^{1/p^i} is always (uniquely) defined.

A useful fact following from these properties is that 'taking the p'th power' of a set does not change its dimension.

Claim 3.1 (Dimension preservation)**.** *Let $q = p^\ell$ from prime p and an integer ℓ. For an integer $i \geq 1$ and a set $A \subseteq \mathbb{F}_{q^n}$ let $A^{p^i} \triangleq \{a^{p^i} \mid a \in A\}$. Then* $\dim(A) = \dim(A^{p^i})$.

Proof. Let $\{a_1, \ldots, a_k\} \subseteq A$ be a basis for the $\mathbb{F}_q$-span of A. Choose any $c_1, \ldots, c_k \in \mathbb{F}_q$ that are not all zero. Then,

$$\sum_{j=1}^{k} c_j \cdot a_j^{p^i} = \left(\sum_{j=1}^{k} c_j^{1/p^i} \cdot a_j \right)^{p^i} \neq 0.$$

Thus $\{a_1^{p^i}, \ldots, a_k^{p^i}\}$ are independent over $\mathbb{F}_q$ and therefore $\dim(A^{p^i}) \geq \dim(A)$. The reverse inequality is similar. □

4 The Main Construction

As before, we use r to denote the number of inputs of $f(Z_1, \ldots, Z_r) \in \mathcal{M}[n, d, k]$. We denote by $\mathcal{D}$ the product set $\{0, \ldots, d\}^r$. We use bold letters to denote variables that are vectors in $\mathbb{F}_q^r$. For example, $\mathbf{Z} = (Z_1, \ldots, Z_r)$. For an element $S = (s_1, \ldots, s_r) \in \mathcal{D}$ we use the notation

$$\mathbf{Z}^S \triangleq Z_1^{s_1} \cdots Z_r^{s_r}.$$

Fix $f = (f_1(\mathbf{Z}), \ldots, f_n(\mathbf{Z})) \in \mathcal{M}[n, d, k]$. For $1 \leq j \leq n$, we write

$$f_j(\mathbf{Z}) = \sum_{S \in \mathcal{D}} a_{j,S} \cdot \mathbf{Z}^S.$$

With the notation above, for $S \in \mathcal{D}$ let $a_S \triangleq (a_{1,S}, \ldots, a_{n,S}) \in \mathbb{F}_q^n$. Using the isomorphism of the vectors spaces $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$, we can view a_S as an element of $\mathbb{F}_{q^n}$ and write

$$f(\mathbf{Z}) = \sum_{S \in \mathcal{D}} a_S \cdot \mathbf{Z}^S. \tag{4}$$

That is, we view f as a multivariate polynomial with coefficients in $\mathbb{F}_{q^n}$. A crucial observation is that when f has large support the coefficients of f have large dimension.

Lemma 4.1 (Large support implies large span)**.** *Let $f \in \mathcal{M}[n, d, k]$. As in (4), write $f(\mathbf{Z}) = \sum_{S \in \mathcal{D}} a_S \cdot \mathbf{Z}^S$ where $a_S \in \mathbb{F}_{q^n}$. Then* $\dim\{a_S\}_{S \in \mathcal{D} \setminus \{\mathbf{0}\}} \geq k$.

Proof. The range of f over inputs in $\mathbb{F}_q^r$ is contained in an affine shift of the $\mathbb{F}_q$-linear span of $\{a_S\}_{S \in \mathcal{D} \setminus \{\mathbf{0}\}}$. Since this range is of size at least q^k, we must have $\dim\{a_S\}_{S \in \mathcal{D} \setminus \{\mathbf{0}\}} \geq k$. □

A simple but crucial observation from [6] is that a polynomial with coefficients in $\mathbb{F}_{q^n}$ whose non-constant coefficients span $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be 'projected' to a non-constant polynomial with coefficients in $\mathbb{F}_q$. We formalize this in the definition and lemma below.

Definition 3 (Full-span polynomial)**.** *We say that a polynomial $G \in \mathbb{F}_{q^n}[\mathbf{Z}] = \mathbb{F}_{q^n}[Z_1, \ldots, Z_r]$ has* full span *if the coefficients of the non-constant monomials of G span $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Lemma 4.2 (Disperser for full-span polynomials)**.** *Suppose $G \in \mathbb{F}_{q^n}[\mathbf{Z}]$ has full span. Let $T : \mathbb{F}_{q^n} \mapsto \mathbb{F}_q$ be a non-trivial $\mathbb{F}_q$-linear mapping. Then $T(G(\mathbf{Z}))$, as a function from $\mathbb{F}_q^r$ to $\mathbb{F}_q$, is a non-constant polynomial in $\mathbb{F}_q[\mathbf{Z}]$ whose total and individual degrees are at most those of G.*

Proof. We write $G(\mathbf{Z}) = \sum_{S \in \mathcal{R}} a_S \cdot \mathbf{Z}^S$ for $a_S \in \mathbb{F}_{q^n}$, where $\mathcal{R} \subset \mathbb{N}^r$ denotes the set of tuples corresponding to the monomials of G. For every $\mathbf{x} = (x_1, \ldots, x_r) \in \mathbb{F}_q^r$, we have

$$T(G(\mathbf{x})) = T\left(\sum_{S \in \mathcal{R}} a_S \cdot \mathbf{x}^S\right) = \sum_{S \in \mathcal{R}} T(a_S) \cdot \mathbf{x}^S,$$

where the last inequality used the $\mathbb{F}_q$-linearity of T. Thus $T(G(\mathbf{Z}))$ agrees on all inputs in $\mathbb{F}_q^r$ with the polynomial $F(\mathbf{Z}) \triangleq \sum_{S \in \mathcal{R}} T(a_S) \cdot \mathbf{Z}^S$ which is in $\mathbb{F}_q[\mathbf{Z}]$. The full span of G means that $\dim\{a_S\}_{S \in \mathcal{R} \setminus \{\mathbf{0}\}} = n$. Since T is a nontrivial linear map there is some $S \in \mathcal{R}$ such that $T(a_S) \neq 0$ and $S \neq \mathbf{0}$ and so F is a non-constant polynomial. As the monomials with non-zero coefficients in F are a subset of the monomials with non-zero coefficients in G, it is clear that F's total and individual degrees are at most those of G. □

The previous lemma implies that to construct a disperser for polynomial sources it suffices to produce a function that increases the span of low-degree polynomials, which is what we do in the next theorem which is of paramount importance in this paper.

Theorem 4 (Product of distinct Froebenius automorphisms increases span)**.** *Fix a prime power $q = p^\ell$. Fix integers $k \leq n$ and $d < s$ such that n is prime and s is a power of p. (In particular, raising to power s^i is a Frobenius automorphism of $\mathbb{F}_q$ over $\mathbb{F}_p$.) Let $u = \lceil (n-k)/(k-1) \rceil$. Then for any $f(Z_1, \ldots, Z_r) \in \mathcal{M}[n, k, d]$, the polynomial*

$$f^{1+s+s^2+\ldots+s^u}(Z_1, \ldots, Z_r) = f(Z_1, \ldots, Z_r) \cdot f^s(Z_1, \ldots, Z_r) \cdots f^{s^u}(Z_1, \ldots, Z_r)$$

has full span.

Proof. Fix $f \in \mathcal{M}[n, k, d]$. As in (4), write $f(\mathbf{Z}) = \sum_{S \in \mathcal{D}} a_S \cdot \mathbf{Z}^S$ with $a_S \in \mathbb{F}_{q^n}$.

$$f^{1+s+s^2+\ldots+s^u}(\mathbf{Z}) = \left(\sum_{S \in \mathcal{D}} a_S \cdot \mathbf{Z}^S\right)^{1+s+s^2+\ldots+s^u} = \prod_{i=0}^{u} \left(\sum_{S \in \mathcal{D}} a_S \cdot \mathbf{Z}^S\right)^{s^i}$$

In what follows we use the notation $S_i = (S_{i,1}, \ldots, S_{i,r})$ and $S_i \cdot s^i = (S_{i,1} \cdot s^i, \ldots, S_{i,r} \cdot s^i)$. Using

the linearity of Frobenius automorphisms we continue the derivation and get

$$= \prod_{i=0}^{u}\left(\sum_{S\in\mathcal{D}} a_S^{s^i}\cdot \mathbf{Z}^{S\cdot s^i}\right) = \sum_{S_0,\ldots,S_u\in\mathcal{D}}\prod_{i=0}^{u} a_{S_i}^{s^i}\cdot\prod_{i=0}^{u}\mathbf{Z}^{S_i\cdot s^i} = \sum_{S_0,\ldots,S_u\in\mathcal{D}}\prod_{i=0}^{u} a_{S_i}^{s^i}\cdot\prod_{i=0}^{u}\prod_{j=1}^{r} Z_j^{S_{i,j}\cdot s^i}$$
$$= \sum_{S_0,\ldots,S_u\in\mathcal{D}} A_{S_0,\ldots,S_u}\cdot M_{S_0,\ldots,S_u}(\mathbf{Z}),$$

where $A_{S_0,\ldots,S_u} = \prod_{i=0}^{u} a_{S_i}^{s^i}$ and $M_{S_0,\ldots,S_u}(\mathbf{Z}) = \prod_{i=0}^{u}\prod_{j=1}^{r} Z_j^{S_{i,j}\cdot s^i}$. The crucial observation is that if $(S_0,\ldots,S_u)$ and $(S'_0,\ldots,S'_u)$ are two distinct tupples of elements of $\mathcal{D}$ then the monomials $M_{S_0,\ldots,S_u}(\mathbf{Z})$ and $M_{S'_0,\ldots,S'_u}(\mathbf{Z})$ are distinct as well: Consider $j\in\{1,\ldots,r\}$ such that $S_{i,j}\neq S'_{i,j}$ for some $0\leq i\leq u$. Then Z_j is raised to power $\sum_{i=0}^{u} S_{i,j}\cdot s^i$ in $M_{S_0,\ldots,S_u}(\mathbf{Z})$ and to power $\sum_{i=0}^{u} S'_{i,j}\cdot s^i$ in $M_{S'_0,\ldots,S'_u}(\mathbf{Z})$. These powers are different as for all $0\leq i\leq u$, $S_{i,j}, S'_{i,j}\leq d<s$; And there is only one way to write an integer in base s with 'coefficients' smaller than s.
Define $A\triangleq\{A_{S_0,\ldots,S_u}\mid S_0,\ldots,S_u\in\mathcal{D}\setminus\{\mathbf{0}\}\}$. For $0\leq i\leq u$, define $B^{s^i}\triangleq\{a_S^{s^i}\mid S\in\mathcal{D}\setminus\{\mathbf{0}\}\}$. Note that $A = B^{s^0}\cdots B^{s^u}$. For all $0\leq i\leq u$, by Lemma 4.1 and Claim 3.1 we have $\dim(B^{s^i})\geq k$. Therefore, by Theorem 3 we get

$$\dim(A)\geq\min\{n, k\cdot(u+1)-u\} = n.$$

Our theorem follows by noticing that the coefficients of the non-constant monomials in $f^{1+s+s^2+\ldots+s^u}$ contain the set A, hence $f^{1+s+\ldots+s^u}$ has full span. □

Combining the lemma and theorem above we 'project' into $\mathbb{F}_q$ and get a non-constant polynomial with coefficients in $\mathbb{F}_q$.

Theorem 5. *Fix a prime power $q=p^\ell$. Fix integers $k\leq n$ and $d<s$ such that n is prime and s is a power of p. Fix a non-trivial $\mathbb{F}_q$-linear map $T:\mathbb{F}_{q^n}\mapsto\mathbb{F}_q$. Let $u=\lceil(n-k)/(k-1)\rceil$. Define $P:\mathbb{F}_{q^n}\mapsto\mathbb{F}_q$ by $P(x)\triangleq T(x^{1+s+s^2+\ldots+s^u})$. Fix any $f(Z_1,\ldots,Z_r)\in\mathcal{M}[n,k,d]$ of total degree D. Then $P(f(\mathbf{Z}))$, as a function on $\mathbb{F}_q^r$, is a non-constant polynomial in $\mathbb{F}_q[\mathbf{Z}]$ of total degree at most $D\cdot(1+s+s^2+\ldots+s^u)<D\cdot s^{u+1}$ and individual degree at most $d\cdot(1+s+s^2+\ldots+s^u)=d\cdot\frac{s^{u+1}-1}{s-1}$.*

Proof. Follows immediately from Lemma 4.2 and Theorem 4. □

An immediate corollary is a construction of a 'non-boolean disperser' for polynomial sources.

Corollary 4.3. *Fix a prime power $q=p^\ell$. Fix integers $k\leq n$ and $d<s$ such that n is prime and s is a power of p. Fix a non-trivial $\mathbb{F}_q$-linear map $T:\mathbb{F}_{q^n}\mapsto\mathbb{F}_q$. Let $u=\lceil(n-k)/(k-1)\rceil$. Define $P:\mathbb{F}_{q^n}\mapsto\mathbb{F}_q$ by $P(x)\triangleq T(x^{1+s+s^2+\ldots+s^u})$. Assume that $q>d\cdot\frac{s^{u+1}-1}{s-1}$. Then, for any $f(Z_1,\ldots,Z_r)\in\mathcal{M}[n,k,d]$ we have that $P(f(\mathbf{Z}))$ is a non-constant function from $\mathbb{F}_q^r$ into $\mathbb{F}_q$.*

Proof. Follows immediately from Theorem 5 by noticing that if $P(f)$ is a non-constant polynomial whose individual degrees are smaller than q, then it is a non-constant function from $\mathbb{F}_q^r$ into $\mathbb{F}_q$. □

5 A useful criteria for the Weil bound

To get our main result we shall apply the Weil-Carlitz-Uchiyama bound for prefix prjections (Corollary 3.3) to a certain polynomial $f \in \mathbb{F}_q[Z]$, and so we have to ensure that f is not of the 'degenerate' form h^p+h+c precluded by that bound. The common way to do this is to require $\gcd(\deg(f), p) = 1$ (cf. [9, 6]). However we have less control on the degree of the polynomial f we need to work with. For this reason, the following lemma will be very helpful to us. It gives us a simple way to 'alter' f and get a polynomial that is not of the form $h^p + h + c$. The proof of the following lemma was shown to us by Swastik Kopparty.

Lemma 5.1 (Criteria for non-degenerateness)**.** *Let $q = p^\ell$ for prime p and let $v \geq 2$ be an integer such that $p \nmid v$. Let $f \in \mathbb{F}_q[Z]$ be a non-constant polynomial. If f is of the form g^v for some $g \in \mathbb{F}_q[Z]$, it is not of the form $h^p + h + c$ for any $h \in \mathbb{F}_q[Z]$ and $c \in \mathbb{F}_q$.*

Proof. Suppose by way of contradiction there exists $f \in \mathbb{F}_q[Z]$ of degree $d \geq 1$ such that $f = g^v = h^p + h + c$ for some $g, h \in \mathbb{F}_q[Z]$ and $c \in \mathbb{F}_q$. Fix such an f with minimal degree $d \geq 1$. It follows that $\deg(g) = d/v$ and $\deg(h) = d/p$. Taking a derivative in $\mathbb{F}_q[Z]$ we get

$$f'(Z) = v \cdot g^{v-1}(Z) \cdot g'(Z) = h'(Z).$$

Notice that $v \neq 0$ in $\mathbb{F}_q$ since $p \nmid v$. If $g' \not\equiv 0$ then this implies $\deg(h') \geq (v-1) \cdot \deg(g) = \frac{v-1}{v} \cdot d$. But $\deg(h') < d/p < \frac{v-1}{v} \cdot d$ (for the last inequality we use $p \nmid v$ and $v \geq 2$). So g' and h' are the zero polynomial. It is not hard to see that this implies that all powers in g and h are multiples of p. So $g = g_1^p$ and $h = h_1^p$ for some $g_1, h_1 \in \mathbb{F}_q[Z]$. We now have

$$f = (g_1^p)^v = (h_1^p)^p + h_1^p + c.$$

This implies

$$g_1^v = h_1^p + h_1 + c^{1/p}.$$

(recall that a p'th root always exists in $\mathbb{F}_q$.) Since g_1 has positive degree smaller than $\deg(f) = d$, this contradicts the minimality of d and proves the theorem. □

Reducing the multivariate case to the univariate case, we get the version of the Weil bound we need.

Lemma 5.2. *Let $q = p^\ell$ for a prime p and integer $\ell > 0$. Let $f(Z_1, \ldots, Z_r) \in \mathbb{F}_q[Z_1, \ldots, Z_r]$ be a non-constant polynomial of total degree $d < q$. Assume that $f = g^v$ for an integer $v \geq 2$ with $p \nmid v$ and some $g \in \mathbb{F}_q[Z_1, \ldots, Z_r]$. Let $m < \ell$ be a positive integer. Then $E_m(f(U_{\mathbb{F}_q^r}))$ is ϵ-close to uniform for $\epsilon = p^{m/2} \cdot d \cdot q^{-1/2}$.*

Proof. We note first that there must be an $a = (a_1, \ldots, a_r) \in \mathbb{F}_q^r$ such that the univariate 'line restriction' polynomial $f_a(t) \triangleq f(a \cdot t) = f(a_1 \cdot t, \ldots, a_r \cdot t)$ has degree *exactly* d: The coefficient of t^d in f_a is $f^d(a)$ where f^d is the d-homogeneous part of f, i.e., the sum of monomials of degree exactly d in f. By the Schwartz-Zippel lemma as $d < q$, there is an $a \in \mathbb{F}_q^r$ such that $f^d(a) \neq 0$ and

therefore $f_a(t)$ has degree d. Fix such an $a \in \mathbb{F}_q^r$. It now follows that for all $b = (b_1, \ldots, b_r) \in \mathbb{F}_q^r$, $f_{a,b}(Z) \triangleq f(a \cdot Z + b) = f(a_1 \cdot Z + b_1, \ldots, a_r \cdot Z + b_r)$ is non-constant — as the coefficient of Z^d in $f_{a,b}$ is the same as the coefficient of Z^d in f_a. Furthermore, for any $b \in \mathbb{F}_q^r$

$$f_{a,b} = f(a_1 \cdot Z + b_1, \ldots, a_r \cdot Z + b_r) = g^v(a_1 \cdot Z + b_1, \ldots, a_r \cdot Z + b_r),$$

and so $f_{a,b}$ is a v'th power of a polynomial in $\mathbb{F}_q[Z]$, and so by Lemma 5.1 is not of the form $h^p + h + c$ for any $h \in \mathbb{F}_q[Z]$ and $c \in \mathbb{F}_q$. As the distribution $f(U_{\mathbb{F}_q^r})$ is a convex combination of the distributions $f_{a,b}(U_{\mathbb{F}_q})$ for the different 'shifts' $b \in \mathbb{F}_q^r$, the claim now follows from the Weil-Carlitz-Uchiyama bound for prefix projections (Corollary 3.3). □

6 A polynomial source extractor

We can now state and prove our main technical theorem, which immediately implies our main theorem on extractors for polynomial sources (Theorem 1).

Theorem 6 (Main — Extractors, parameterized version)**.** *Fix a field $\mathbb{F}_q$ of characteristic p, integers $d, D, 2 \leq k \leq n$ where $n \geq 25$, and a positive integer $m < 1/2 \cdot \log_p q$. Let $\alpha = 3D \cdot (p \cdot d)^{\frac{1.2 \cdot n - k}{k-1} + 2}$. Assume that $q \geq 2 \cdot \alpha^2$. There is an explicit (k, d, D, ϵ)-polynomial source extractor $E : \mathbb{F}_q^n \mapsto \mathbb{F}_p^m$ with error $\epsilon = p^{m/2} \cdot \alpha \cdot q^{-1/2}$.*

Theorem 1 follows from the previous theorem by noticing that for $4 \leq k \leq n$,

$$\frac{1.2 \cdot n - k}{k-1} + 2 \leq 3n/k.$$

Proof of Theorem 6. Choose a prime $n \leq n' \leq 1.2 \cdot n$ (which always exists for $n \geq 25$ according to Nagura's improvement of the Bertrand-Chebychev Theorem [13]). Given $f(Z_1, \ldots, Z_r) \in \mathcal{M}[n, k, d]$ of total degree D we think of f as an element of $\mathcal{M}[n', k, d]$ by padding its output with zeros. Let s be the smallest power of p greater than d. Note that $s \leq p \cdot d$. Let $P : \mathbb{F}_q^{n'} \mapsto \mathbb{F}_q$ be the polynomial in Theorem 5 using s as above. If $p = 2$ let $v = 3$ and otherwise let $v = 2$. Let $E : \mathbb{F}_q^n \mapsto \mathbb{F}_p^m$ be defined as $E(\mathbf{x}) \triangleq E_m(P^v(\mathbf{x}))$. From Theorem 5 we conclude that $P(f(\mathbf{Z}))$ is non-constant of degree at most $D \cdot s^{u+1}$ where $u = \lceil (n' - k)/(k-1) \rceil \leq \frac{1.2 \cdot n - k}{k-1} + 1$. Hence, from Lemma 5.2 we see that $E_m(P^v(f(U_{\mathbb{F}_q^r})))$ is ϵ-close to uniform for

$$\epsilon = p^{m/2} \cdot v \cdot D \cdot s^{u+1} \cdot q^{-1/2} \leq p^{m/2} \cdot 3D \cdot (p \cdot d)^{\frac{1.2 \cdot n - k}{k-1} + 2} \cdot q^{-1/2} = p^{m/2} \cdot \alpha \cdot q^{-1/2}.$$

□

Acknowledgements

We thank Swastik Kopparty for the proof of Lemma 5.1. We thank Swastik Kopparty and Shubhangi Saraf for helpful discussions. We thank Zeev Dvir for reading a previous version of this paper. The

first author thanks Emanuele Viola for raising this question.

References

[1] E. Ben-Sasson and S. Kopparty. Affine dispersers from subspace polynomials. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 65–74, 2009.

[2] Eli Ben-Sasson, S. Hoory, E. Rozenman, S. Vadhan, and A. Wigderson. Extractors for affine sources. Unpublished Manuscript, 2001.

[3] J. Bourgain. On the construction of affine extractors. *Geometric & Functional Analysis*, 17 Number 1:33–57, 2007.

[4] L. Carlitz and S. Uchiyama. Bounds for exponential sums. *Duke Math. J.*, 24, 1957.

[5] 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.

[6] M. DeVos and A. Gabizon. Simple affine extractors using dimension expansion. In *Proceedings of the 25th Annual IEEE Conference on Computational Complexity*, page 63, 2010.

[7] Z. Dvir. Extractors for varieties. 2009.

[8] Z. Dvir, A. Gabizon, and A. Wigderson. Extractors and rank extractors for polynomial sources. *Computational Complexity*, 18(1):1–58, 2009.

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

[10] X. Hou, K.H. Leung, and Q. Xiang. A generalization of an addition theorem of kneser. *Journal of Number Theory*, 97:1–9, 2002.

[11] X. Li. A new approach to affine extractors and dispersers. 2011.

[12] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1994.

[13] J. Nagura. On the interval containing at least one prime number. *Proceedings of the Japan Academy*, 28:177–181, 1952.

[14] A. Rao. An exposition of bourgain's 2-source extractor. *ECCC technical report*, 2007.

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

[16] R. Shaltiel. Dispersers for affine sources with sub-polynomial entropy. 2011.

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

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

[19] A. Yehudayoff. Affine extractors over prime fields. *Manuscript*, 2009.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de