

Affine Dispersers from Subspace Polynomials

Eli Ben-Sasson^{*}
Computer Science Department,
Technion — Israel Institute of Technology,
Haifa, 32000, Israel.
eli@cs.technion.ac.il

Swastik Kopparty[†]
CSAIL, MIT
Cambridge, MA 02139.
swastik@mit.edu

ABSTRACT

An affine disperser over \mathbb{F}_2^n for sources of dimension d is a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that for any affine space $S \subseteq \mathbb{F}_2^n$ of dimension at least d , we have $\{f(s) : s \in S\} = \mathbb{F}_2$. Affine dispersers have been considered in the context of deterministic extraction of randomness from structured sources of imperfect randomness. Previously, explicit constructions of affine dispersers were known for every $d = \Omega(n)$, due to Barak et. al. [2] and Bourgain [10] (the latter in fact gives stronger objects called affine extractors).

In this work we give the first explicit affine dispersers for *sublinear* dimension. Specifically, our dispersers work even when $d = \Omega(n^{4/5})$. The main novelty in our construction lies in the method of proof, which relies on elementary properties of *subspace polynomials*. In contrast, the previous works mentioned above relied on sum-product theorems for finite fields.

Categories and Subject Descriptors

G.3 [Mathematics of Computing]: Probability and Statistics—*Random number generation*

General Terms

Algorithms, Theory

1. INTRODUCTION

Roughly speaking, a *one-output-bit seedless disperser* (often called a deterministic disperser) for a “structured” family \mathcal{F} of subsets of \mathbb{F}_2^n , is a function $\text{Disp} : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ satisfying the property that on any subset $X \in \mathcal{F}$, $X \subset \mathbb{F}_2^n$ the function Disp takes more than one value, i.e., $\{\text{Disp}(x) : x \in$

^{*}Research of both authors supported in part by a European Community International Reintegration Grant, an Alon Fellowship, and grants by the Israeli Science Foundation and by the US-Israel Binational Science Foundation.

[†]Research supported in part by NSF Award CCR-0514915.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

STOC’09, May 31–June 2, 2009, Bethesda, Maryland, USA.
Copyright 2009 ACM 978-1-60558-506-2/09/05 ...\$5.00.

$X\} = \mathbb{F}_2$. Dispersers have been intensively studied in recent years in the context of extracting randomness from imperfect sources of randomness. The goal of these studies has been to obtain dispersers computable in polynomial time, and today several constructions of seedless dispersers for various structured families of subsets are known, including for “bit-fixing” and “samplable” sources [13, 14, 22, 17]. We refer the reader to [2] for more information on seedless dispersers and their connection to extractors and expanders. A particularly interesting family of structured subsets that has been considered in this context, and is also the focus of our paper, is the family of affine subspaces. A *disperser for affine sources* is a function Disp as above that is guaranteed to be nonconstant on every affine subspace of \mathbb{F}_2^n that has sufficiently large dimension. Dispersers for spaces of dimension greater than $n/2$ are relatively easy to construct [6]. However, for spaces of dimension smaller than $n/2$ the problem becomes much harder, and to date, only two such constructions are known [2, 10] (A related, though incomparable, result of Gabizon and Raz [15] constructs extractors for affine sources over “large” finite fields, where “large” means $|\mathbb{F}| \gg n$). Both these works show how to construct, for any $\epsilon > 0$, a affine disperser for any affine space \mathcal{A} of dimension $> \epsilon n$. In fact, the construction of [10] is an extractor, i.e., the output of the dispersing function, on a uniformly random element of \mathcal{A} , is close to an unbiased coin. Both constructions use recent sum-product theorems over finite fields [12, 11] and related results from additive combinatorics, in addition to several other non-trivial concepts.

Results.

Our main result (Theorem 2.2) is the explicit construction of an affine disperser that disperses spaces of dimension $o(n)$. Specifically, our disperser works for spaces of dimension at least $\Omega(n^{4/5})$. The structure of our main affine disperser is as follows. The n input bits are broken into r blocks, each with an equal number k of bits, and each block is interpreted as specifying an element of the finite field \mathbb{F}_{2^k} . The r elements thus obtained in \mathbb{F}_{2^k} are now substituted into a certain polynomial over \mathbb{F}_{2^k} , and its output, which is an element of \mathbb{F}_{2^k} , is projected onto \mathbb{F}_2 via an \mathbb{F}_2 -linear projection (such as taking its first bit).

The techniques we use allow for a host of results with a similar flavor. Let us informally describe a few of them. The simplest-to-prove result is a “univariate” affine disperser below the notorious $n/2$ barrier. By “univariate” we mean that the function we use to compute the disperser is naturally viewed as a univariate polynomial. For example, we

show that the function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, where $f(x)$ is computed by first interpreting x as an element of \mathbb{F}_{2^n} , and then outputting the first bit of x^7 (any nontrivial linear combination of the bits will do) is a disperser for dimension at least $2n/5 + \Omega(1)$, as long as n is odd. (In followup work we show that this function is in fact an affine *extractor*, see the remark following Theorem 2.5.) We point out that if n is even, then \mathbb{F}_{2^n} has subfields of dimension $n/2$, and this implies that the above construction will not disperse that subfield. Indeed, when x is in a subfield, then x^7 will be in the same subfield, and hence some linear combinations of the bits of x^7 will be 0. In the next section we comment on the role that the oddness of n , and more generally, the absence of subfields, plays in our proofs.

Another result that is particularly easy to describe is our *same-source affine disperser*. We say that a multi-input function $f : (\mathbb{F}_2^n)^t \rightarrow \mathbb{F}_2$ is a same-source affine disperser for dimension d if for every d -dimensional space $\mathcal{A} \subseteq \mathbb{F}_2^n$ we have $\{f(x_1, \dots, x_t) \mid x_i \in \mathcal{A}\} = \mathbb{F}_2$, i.e., if f is a disperser for the set of sources that are the t -wise direct product of a d -dimensional affine space. We show that the function $f(x_1, \dots, x_t)$ which views x_i as an element in \mathbb{F}_{2^n} and outputs the first bit of $\prod_{i=1}^t x_i$ is a same-source affine disperser for any \mathcal{A} of dimension $d > 1$ that is not contained in a subfield of \mathbb{F}_{2^n} , as long as $t > 2n/d$. And, as we argue in Section 2, the number of copies t needed to ensure f is indeed a disperser is nearly optimal, up to the small multiplicative constant of 2, because there exist d -dimensional subspaces for which the product of $n/d - 1$ any elements from the subspace is a field element whose first bit is 0.

On subspaces and polynomials.

Our analysis makes use of a class of polynomials called *subspace polynomials*. These polynomials were first studied by Ore in the 1930's [19, 20]. They have numerous applications in the study of finite fields and in the theory of error correcting codes (See Berlekamp [9, Chapter 11] and Lidl and Niederreiter [18, Chapter 3, Section 4]). More recently, they have been used within computational complexity to construct short PCPs [4, 8, 5] and to study the limits of list-decodability of the Reed-Solomon code [7].

The polynomials studied in this last line of works are what we call the *kernel-subspace*¹ polynomial associated to a linear subspace $L \subseteq \mathbb{F}_{2^n}$, which is a polynomial whose set of roots equals L . In this work we analyze our dispersers using elementary properties of the *image-subspace polynomial* of a linear subspace L . These polynomials have the property that their image, i.e., the set of values they take over \mathbb{F}_{2^n} , equals L . Our proofs begin by first reformulating the property of being an affine disperser in terms of these polynomials. We then use a simple-to-prove, yet extremely powerful, structural lemma about these polynomials, to get our main results.

Pseudorandomness from the absence of subfields.

Recently, starting with the work of Barak, Impagliazzo and Wigderson [1], there have been a number of works [23, 16, 3] that utilize results from additive combinatorics in the explicit construction of extractors and dispersers. A common theme of these works is the use of results such as the

¹The terms “kernel-” and “image-subspace polynomials” were suggested by Prahladh Harsha and we thank him for introducing this nomenclature.

sum-product theorem of Bourgain, Katz and Tao [12] and the related multilinear exponential sum estimates of Bourgain, Glibichuk and Konyagin [11]. Such sum-product theorems enable the extreme pseudorandom properties of *finite fields without large subfields* to be systematically exploited.

In our work, we offer a different algebraic incarnation of this phenomenon. Specifically, we show that the absence of large subfields directly affects the structure of the image-subspace polynomials of the field. Image-subspace polynomials are *linearized*, which means that they are of the form $\sum_{i=0}^{n-1} a_i X^{2^i}$. Roughly speaking, our main structural lemma (Lemma 4.7) says that a subspace polynomial whose image is a subspace \mathcal{A} of dimension d cannot have d consecutive coefficients a_i that are all zero. Moreover, and this is the crucial part, if \mathcal{A} is not contained in a subfield of \mathbb{F}_{2^n} , then the polynomial cannot have even $d - 1$ consecutive coefficients that are all zero. This lemma has a short proof (appearing in Section 4.2), yet is extremely powerful. Surprisingly, reducing the maximal length of a sequence of zero-coefficients by 1 (from d to $d - 1$) for spaces that are not contained in subfields allows us to improve upon state-of-the-art constructions of affine dispersers using arguably simpler techniques.

1.1 Proof Strategy

We now give a brief description of the basic proof strategy that we use to prove that a function is an affine disperser. We demonstrate the steps involved in the special case of the function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, $f(x) = \text{Tr}(x^7)$ (where $\text{Tr} : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is the Trace map). We will show in Theorem 2.5 that if n is prime (so that \mathbb{F}_{2^n} has no proper subfields), then for any affine space $\mathcal{A} \subseteq \mathbb{F}_{2^n}$ of dimension $\geq 2n/5 + \Omega(1)$, we have $f|_{\mathcal{A}}$ is nonconstant.

Part I — Reduce to showing that a certain polynomial h is not a constant polynomial: We first parameterize the affine space \mathcal{A} using subspace polynomials. Let $Q(X)$ be the image-subspace of \mathcal{A} , so that $\mathcal{A} = \{Q(x) : x \in \mathbb{F}_{2^n}\}$. In terms of the polynomial $Q(X)$, we want to show that the composed map $f \circ Q : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is non-constant. Let $h(X)$ be the polynomial $\text{Tr}(Q(X)^7) \bmod \langle X^{2^n} - X \rangle$, so that $h(x) = f(Q(x))$ for each $x \in \mathbb{F}_{2^n}$ (by Proposition 3.1). Thus to show that h is a nonconstant map, it suffices to show that $h(X)$ is a nonconstant polynomial. We do this in the next two steps of our proof strategy, by finding a monomial of positive degree that appears in $h(X)$ with a nonzero coefficient.

Part II — Express the coefficients of h in terms of the coefficients of the subspace polynomials: To show that h has a monomial of positive degree with a nonzero coefficient, it will be convenient to get an explicit expression for the coefficients themselves. Such an explicit expression can be obtained by direct substitution. In all the cases we consider, there is a good deal of structure in the resulting formulae. For example, for the polynomial we obtained while studying $f(x) = \text{Tr}(x^7)$, we have the following lemma.

LEMMA 1.1. *Let $Q(X) = \sum_{i=0}^{n-1} a_i X^{2^i}$ and let $h(X) = \text{Tr}(Q(X)^7) \bmod \langle X^{2^n} - X \rangle$. Then for distinct j, k, l , the coefficient of $X^{2^j + 2^k + 2^l}$ in $h(X)$ is given by the expression:*

$$\sum_{r=0}^{n-1} \text{Perm} \begin{pmatrix} a_{j-r} & a_{k-r} & a_{l-r} \\ a_{j-r-1}^2 & a_{k-r-1}^2 & a_{l-r-1}^2 \\ a_{j-r-2}^4 & a_{k-r-2}^4 & a_{l-r-2}^4 \end{pmatrix}^{2^r}, \quad (1)$$

where Perm is the matrix permanent.

Part III — Argue combinatorially that some coefficient of h must be nonzero: Finally, we show that some positive degree monomial of h has a nonzero coefficient. Using the regular form of the coefficients of the polynomial h , for example as given in Lemma 1.1, and the structural results about the coefficients of subspace polynomials, this part of the argument reduces to the combinatorics of cyclic shifts on \mathbb{Z}_n . More to the point, we use our main structural lemma (Lemma 4.7) to prove that the matrix appearing in the first summand (corresponding to $r = 0$) in equation (1) is lower triangular with nonzero entries on its diagonal, hence its permanent is nonzero, whereas the matrices appearing in all other summands in equation (1) (corresponding to $r = 1, \dots, n - 1$) contain a zero column, hence have a zero permanent.

2. MAIN RESULTS

We begin by describing the function $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ which we will prove is a good affine disperser over \mathbb{F}_p and before doing so we formally define a disperser. Throughout this paper, for $f : X \rightarrow Y$ a function and $S \subset X$ a set, let $f(S) = \{f(s) \mid s \in S\}$.

DEFINITION 2.1 (\mathbb{F}_p -AFFINE DISPERSER). *Let \mathbb{F}_p denote the finite field of prime size p . A function $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ is said to be a \mathbb{F}_p -affine disperser for dimension d if for all affine spaces $\mathcal{A} \subseteq \mathbb{F}_p^m$ of dimension $\dim(\mathcal{A}) > d$, we have $|f(\mathcal{A})| > 1$.*

The standard definition of a disperser, as appearing in, say, [21], requires that $f(\mathcal{A}) = \mathbb{F}_p$. Notice that for the case of $p = 2$ the two definitions match. All our constructions give \mathbb{F}_p -dispersers according to Definition 2.1 so to simplify notation we simply refer to them as *affine dispersers*. We now get back to describing our main disperser.

The integers n, r and t are parameters of the construction to be specified later. As in [10], we partition the m -bit input x into r blocks (x_1, \dots, x_r) of n bits each (we assume n divides m by discarding a few bits of the source, if necessary). We will pick n to be prime, so that \mathbb{F}_{p^n} has no nontrivial subfields. Each block x_i is interpreted as an element of \mathbb{F}_{p^n} by using a linear isomorphism from \mathbb{F}_p^n to \mathbb{F}_{p^n} . We raise each element x_i to a distinct suitable power and let y_i denote the result of this powering. Next, we take the t^{th} symmetric polynomial of y_1, \dots, y_r , where this polynomial is defined as

$$\text{Sym}_r^t(Y_1, \dots, Y_r) = \sum_{I \subseteq [r], |I|=t} \prod_{i \in I} Y_i.$$

Finally, we view $z = \text{Sym}_r^t(y_1, \dots, y_r) \in \mathbb{F}_{p^n}$ as a vector in \mathbb{F}_p^n by using a linear isomorphism from \mathbb{F}_{p^n} to \mathbb{F}_p^n and output the first element of this vector. In fact, any fixed nontrivial \mathbb{F}_p -linear combination of the elements of this vector will do. A particularly convenient way to get such a linear combination is to take the *trace* function $\text{Tr}(Z) = \sum_{i=0}^{n-1} Z^{p^i}$. We now formally state our main result.

THEOREM 2.2 (EXPLICIT AFFINE DISPERSERS). *Given integer m fix parameters n, r, t as follows. Let n be the smallest prime bigger than $2 \cdot m^{3/5}$. Let $r = \lceil m/n \rceil$ and let $t = \lceil \sqrt{r} \rceil$. (We have $n \approx m^{3/5}$, $r \approx m^{2/5}$ and $t \approx m^{1/5}$.) Embedding \mathbb{F}_p^m in $(\mathbb{F}_{p^n})^r$ using a \mathbb{F}_p -linear injective mapping, the function $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ defined by*

$$f(x_1, \dots, x_r) = \text{Tr} \left(\text{Sym}_r^t \left(x_1^{1+p}, x_2^{1+p+p^2}, \dots, x_r^{1+p+p^2+\dots+p^{r-1}} \right) \right)$$

is a affine disperser for dimension $> 6m^{4/5}$, i.e., for all affine $\mathcal{A} \subseteq \mathbb{F}_p^m$ with $\dim(\mathcal{A}) > 6m^{4/5}$ we have $|f(\mathcal{A})| > 1$.

Remark All statements in this section hold even when the trace function Tr is replaced by any other nontrivial homomorphism $\psi : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$. This is equivalent to saying that any nontrivial linear combination of the “bits” of output of the polynomial of which we take trace, will also lead to a disperser. Yet another way of stating this is that the polynomial inside the trace has the property that on every space \mathcal{A} of sufficient dimension, its output is not contained in any nontrivial subspace of \mathbb{F}_p^n .

Notice f can be computed in polynomial time in p and m because Sym_r^t can be computed efficiently in the said time via interpolation. In particular, our construction is more computationally efficient than that of [10] (where the running time for spaces of dimension en is $n^{2^{\Omega(1/\epsilon)}}$).

We prove Theorem 2.2 in Section 6. The main technical lemma that underlies this construction is stated in Section 5 and proved in Section 7.

The method by which we prove Theorem 2.2 is quite general, and in the next two subsections we show that a few natural variations of this function can also be shown to be good affine dispersers in various settings.

2.1 Independent affine source dispersers

Informally, we say a function $f : (\mathbb{F}_p^n)^t \rightarrow \mathbb{F}_p$ is a *disperser for independent affine sources* if on every set of affine spaces $\mathcal{A}_1, \dots, \mathcal{A}_t \subseteq \mathbb{F}_p^n$ of “sufficiently large” accumulated dimension, we have $|f(\prod_{i=1}^t \mathcal{A}_i)| > 1$, where $\prod_{i=1}^t \mathcal{A}_i = \{(x_1, \dots, x_t) \mid x_i \in \mathcal{A}_i\}$. We describe dispersers for two families of independent affine sources. The first family is that of “same-source” sets, i.e., when $\mathcal{A}_1, \dots, \mathcal{A}_t$ are all the same subspace \mathcal{A} . Our function is particularly easy to describe. Given t samples $x_1, \dots, x_t \in \mathbb{F}_{p^n}$, we take (say) the first bit of their product.

Notice that our disperser will fail to disperse from \mathcal{A} that is contained in a *proper subfield* of \mathbb{F}_{p^n} . Thus, throughout this paper we say that a subspace $\mathcal{A} \subseteq \mathbb{F}_{p^n}$ is contained in an *affine shift of a proper subfield* if $\mathcal{A} \subseteq b \cdot \mathbb{F}_{p^k} + c = \{a'b + c \mid a' \in \mathbb{F}_{p^k}\}$ where $k < n$ divides n and $b, c \in \mathbb{F}_{p^n}$. Notice that every one-dimensional affine space is (contained in) an affine shift of a proper subfield, namely, \mathbb{F}_p .

THEOREM 2.3 (SAME-SOURCE AFFINE DISPERSER). *Let $f : \mathbb{F}_{p^n}^t \rightarrow \mathbb{F}_p$ be given by*

$$f(x_1, \dots, x_t) = \text{Tr} \left(\prod_{i=1}^t x_i \right).$$

Then for any \mathbb{F}_p -affine space $\mathcal{A} \subseteq \mathbb{F}_{p^n}$ which is not contained in an affine shift of a proper subfield of \mathbb{F}_{p^n} , with $\dim(\mathcal{A}) > \frac{2n}{t}$, we have $|f(\mathcal{A}^t)| > 1$.

The previous theorem can be interpreted (using the remark following Theorem 2.2) as a kind of *sum-product statement*. One way to state sum-product theorems, such as those of [12, 11] is to say that if a set $\mathcal{A} \subset \mathbb{F}$ does not expand significantly under addition, i.e., if $|\mathcal{A} + \mathcal{A} + \dots + \mathcal{A}| \approx |\mathcal{A}|$, then the set \mathcal{A} must expand under multiplication, i.e. $|\mathcal{A} \times \mathcal{A} \times \dots \times \mathcal{A}| \gg |\mathcal{A}|$. Theorem 2.3 says that if \mathcal{A} does not expand at all under addition, then its product (taken sufficiently many times) must span \mathbb{F} . What seems remarkable is that the dimension of \mathcal{A} can be as small as 2 and

the only cases for which our construction fails to disperse is when \mathcal{A} is itself contained in an affine shift of a proper nontrivial subfield of \mathbb{F} . Notice also that we need to take at least $n/\dim(\mathcal{A})$ products to disperse. To see this take α to generate a standard basis for \mathbb{F}_{p^n} , i.e., let $\alpha^0, \dots, \alpha^{n-1}$ span \mathbb{F}_{p^n} over \mathbb{F}_p . Taking $\mathcal{A} = \text{span}(\alpha^0, \alpha^1)$ we notice that $\mathcal{A}^{n-2} = \text{span}(\alpha^0, \dots, \alpha^{n-2})$ is contained in a $n-1$ -dimensional subspace of \mathbb{F}_{p^n} .

The following construction reduces the number of copies of \mathcal{A} that we need from $2n/\dim(\mathcal{A})$ to $n/\dim(\mathcal{A})$ and also deals with arbitrary, and not necessarily identical, subspaces. In fact, the affine disperser of Theorem 2.2 is analyzed by viewing it as the gluing together of many overlapping copies of (cousins of) the independent affine disperser below. The proof of the following theorem appears in Section 5. The proof of the previous Theorem 2.3 follows along the same lines and hence omitted from this extended abstract.

THEOREM 2.4 (INDEPENDENT AFFINE DISPERSER). *Let $f : \mathbb{F}_{p^n}^t \rightarrow \mathbb{F}_p$ be given by*

$$f(x_1, \dots, x_t) = \text{Tr} \left(\prod_{i=1}^t x_i^{1+p} \right).$$

Let $\mathcal{A}_1, \dots, \mathcal{A}_t \subseteq \mathbb{F}_{p^n}$ be \mathbb{F}_p -affine spaces of dimensions d_1, \dots, d_t respectively, where each \mathcal{A}_i is not contained in a affine shift of a proper subfield of \mathbb{F}_{p^n} . If $\sum_{i=1}^t (d_i - 2) > n$, then $|f(\prod_i \mathcal{A}_i)| > 1$.

2.2 Univariate Affine Dispersers

Our final set of results is a description of two constructions of affine dispersers based on univariate polynomials. Here we treat our input $x \in \mathbb{F}_{p^n}$ as a single element of the field \mathbb{F}_{p^n} . We raise it to a suitable power and take (say) the first bit of this power.

THEOREM 2.5 (UNIVARIATE AFFINE DISPERSER I). *Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be given by*

$$f(x) = \text{Tr}(x^{1+p+p^2}).$$

Then for any \mathbb{F}_p -affine space $\mathcal{A} \subseteq \mathbb{F}_{p^n}$ with $\dim(\mathcal{A}) > \frac{2n}{5} + 10$ that is not contained in a affine shift of a proper subfield of \mathbb{F}_{p^n} , we have $|f(\mathcal{A})| > 1$.

Remark In recent work we show that the function $f(x)$ described in the previous theorem is in fact an affine extractor for dimension greater than $\frac{2n}{5} + 10$. By this we mean that there exists $\epsilon > 0$ such that for any \mathbb{F}_p -affine space $\mathcal{A} \subseteq \mathbb{F}_{p^n}$ with $\dim(\mathcal{A}) \geq \frac{2n}{5} + 10 + d$ we have $|\mathbb{E}_{x \in \mathcal{A}} \omega^{f(x)}| \leq (p/d)^\epsilon$ where ω is any complex primitive root of unity of order p .

THEOREM 2.6 (UNIVARIATE AFFINE DISPERSER II). *Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ be given by*

$$f(x) = \text{Tr}(x^{1+p+p^2+p^3}).$$

Then for any \mathbb{F}_p -affine space $\mathcal{A} \subseteq \mathbb{F}_{p^n}$, with $\dim(\mathcal{A}) > \frac{n}{3} + 10$ that is not contained in a affine shift of a proper subfield of \mathbb{F}_{p^n} , we have $|f(\mathcal{A})| > 1$.

The proofs of these statements are quite similar. The proofs are omitted from this extended abstract.

3. PRELIMINARIES

Let \mathbb{F}_q denote the finite field of size q . If $q = p^n$ for prime p then \mathbb{F}_q is a degree n extension of \mathbb{F}_p . A set $\mathcal{A} \subseteq \mathbb{F}_{p^n}$ is said to be a \mathbb{F}_p -linear subspace if $\alpha a + \beta b \in \mathcal{A}$ for all $a, b \in \mathcal{A}$ and $\alpha, \beta \in \mathbb{F}_p$. A \mathbb{F}_p -affine subspace is a set of the form $c + \mathcal{A} = \{c + a \mid a \in \mathcal{A}\}$ for \mathcal{A} a \mathbb{F}_p -linear subspace. When the ambient subfield is clear from context we will simply speak of *linear* and *affine* subspaces of \mathbb{F}_{p^n} .

Throughout this paper capital letters such as X_i are used for formal variables whereas x_i denotes a field-element. For a polynomial $h(X_1, \dots, X_r) \in \mathbb{F}_{p^n}[X_1, \dots, X_r]$, abusing notation we define

$$h(X_1, \dots, X_r) \pmod{\langle (X_i^{p^n} - X_i)_{i \in [r]} \rangle}$$

to be the polynomial obtained by starting with $h(X_1, \dots, X_r)$, and for each $i \in [r]$, replacing the current polynomial by its reduction mod $X_i^{p^n} - X_i$. Equivalently, h' is the polynomial obtained by starting with h and repeatedly replacing, for each i , every occurrence of $X_i^{p^n}$ by X_i . The following proposition, stated without proof, will be used repeatedly in our arguments.

PROPOSITION 3.1. *Let $h(X_1, \dots, X_r) \in \mathbb{F}_{p^n}[X_1, \dots, X_r]$. Let*

$$h'(X_1, \dots, X_r) = h(X_1, \dots, X_r) \pmod{\langle (X_i^{p^n} - X_i)_{i \in [r]} \rangle}.$$

Then for any $x \in \mathbb{F}_{p^n}^r$ we have $h(x) = h'(x)$.

Consequently, $|h(\mathbb{F}_{p^n}^r)| > 1$ if and only if $h'(X_1, \dots, X_r)$ is a polynomial of degree greater than 0.

For a nonnegative integer i , let $\text{wt}_p(i)$ denote the sum of the digits of i in the base- p representation. If $m(X_1, \dots, X_t) \in \mathbb{F}_{p^n}[X_1, \dots, X_t]$ is the monomial $\prod_{i=1}^t X_i^{\beta_i}$, we define the \mathbb{F}_p -degree of m in the variable X_i to be $\text{wt}_p(\beta_i)$. We define the *total \mathbb{F}_p -degree* of the monomial m to be the sum of the \mathbb{F}_p -degrees of m in each variable X_i . We then define the \mathbb{F}_p -degree of a polynomial to be the maximum \mathbb{F}_p degree of any of its monomials. The following facts about \mathbb{F}_p -degree can be readily verified.

PROPOSITION 3.2. *Let $P(X_1, \dots, X_t), Q(X_1, \dots, X_t)$ be polynomials in $\mathbb{F}_{p^n}[X_1, \dots, X_t]$ with \mathbb{F}_p -degrees d_1, d_2 respectively, with $d_1, d_2 < n$.*

- *The \mathbb{F}_p -degree of $P(X_1, \dots, X_t) \cdot Q(X_1, \dots, X_t)$ is at most $d_1 \cdot d_2$.*
- *The \mathbb{F}_p -degree of $P(X_1, \dots, X_t)^{p^r} \pmod{\langle (X_i^{p^n} - X_i)_{i \in [t]} \rangle}$ equals d_1 .*

4. PROPERTIES OF SUBSPACE POLYNOMIALS

We start this section by reviewing elementary properties of linearized and subspace polynomials. We follow this in Subsections 4.2, 4.3 by proving some key structural results about subspace polynomials. These results, though relatively easy to obtain, will play a pivotal role in our analysis of affine dispersers.

4.1 A Brief Introduction to the Theory of Subspace Polynomials

The information in this subsection was first described in the work of [19, 20]. We state the minimal set of definitions

and claims that will be needed to analyze our constructions and we refer the reader interested in a more thorough introduction to the subject to [18, Chapter 4] and to [9, Chapter 11].

A polynomial $P \in \mathbb{F}_{p^n}[X]$ is said to be *linearized* if and only if

$$P(X) = \sum_{i=0}^{n-1} a_i X^{p^i}, a_i \in \mathbb{F}_{p^n}$$

which is equivalent to saying that $P(\beta b + \gamma c) = \beta P(b) + \gamma P(c)$ for all $b, c \in \mathbb{F}_{p^n}$ and $\beta, \gamma \in \mathbb{F}_p$. By extension, a polynomial is said to be *affine linearized* if $P(X) = \hat{P}(X) + \hat{a}$ where \hat{P} is linearized and $\hat{a} \in \mathbb{F}_{p^n}$. Thus, the affine linearized polynomials in X over \mathbb{F}_{p^n} are precisely the polynomials of \mathbb{F}_p -degree at most 1. Often, when there is no risk of confusion, we shall abuse notation and speak of “affine polynomials” by which we mean “affine linearized polynomials”.

LEMMA 4.1. *Let $\psi : \mathbb{F}_p^n \rightarrow \mathbb{F}_{p^n}$ be a linear bijection. There is a one-to-one correspondence between affine transformations from \mathbb{F}_p^n to \mathbb{F}_p^n and affine linearized polynomials in $\mathbb{F}_{p^n}[X]$, i.e., for every affine $\phi : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ there exists a unique affine linearized polynomial P_ϕ satisfying $P_\phi(\psi(b)) = \psi(\phi(b))$ for all $b \in \mathbb{F}_p^n$.*

We shall take particular interest in a special class of polynomials that split completely in \mathbb{F}_{p^n} to a set of roots that forms a \mathbb{F}_p -affine subspace of \mathbb{F}_{p^n} .

DEFINITION 4.2 (KERNEL-SUBSPACE POLYNOMIAL). *Let $L \subseteq \mathbb{F}_{p^n}$ be a affine subspace of dimension d . Define $P_L(X) \in \mathbb{F}_{p^n}[X]$, the kernel-subspace polynomial of L , to be the polynomial:*

$$P_L(X) = \prod_{\alpha \in L} (X - \alpha).$$

LEMMA 4.3 (SUBSPACE POLYNOMIALS ARE AFFINE). *If $L \subseteq \mathbb{F}_{p^n}$ is a affine subspace of dimension d then $P_L(X)$ is a monic affine linearized polynomial of degree p^d . Furthermore, P_L is linearized iff L is a linear space.*

Every kernel-subspace polynomial P_L corresponds to a affine transformation whose kernel is L , so by linearity $P(\mathbb{F}_{p^n})$ is a affine subspace of \mathbb{F}_{p^n} of dimension $n - \dim(L)$. Surprisingly, the images of all d -dimensional subspace polynomials are precisely all the $n - d$ dimensional subspaces of \mathbb{F}_{p^n} . These *image-subspace* polynomials will be the starting point of our analysis of affine dispersers.

LEMMA 4.4 (IMAGE-SUBSPACE POLYNOMIALS). *If $L \subseteq \mathbb{F}_{p^n}$ is a affine subspace of dimension d then there exists a monic affine linearized polynomial $Q_L(X)$ with $\deg(Q_L) = p^{n-d}$, called the image-subspace polynomial of L , such that*

$$L = Q_L(\mathbb{F}_{p^n}) \triangleq \{Q_L(c) \mid c \in \mathbb{F}_{p^n}\}.$$

Moreover, if $P_L(X)$ is the subspace polynomial of L then

$$P_L(Q_L(X)) \equiv Q_L(P_L(X)) \equiv X^{p^n} - X. \quad (2)$$

Thus the kernel of $Q_L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ equals the image of $P_L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$. In particular $Q_L(X)$ has p^{n-d} roots in \mathbb{F}_{p^n} , and is thus also the subspace polynomial of some subspace.

4.2 Structure of the coefficients of subspace polynomials

The following claims will be needed to prove our main structural lemma. In what follows, let $\overline{\mathbb{F}}_p$ denote the algebraic closure of \mathbb{F}_p .

CLAIM 4.5. *Let $k > 1$, and suppose $a, c \in \mathbb{F}_{p^n}$ are such that $a^{p^k} - ca = 0$. Then, letting b be any $(p^k - 1)$ -th root of c in $\overline{\mathbb{F}}_p$, we have $a \in b \cdot \mathbb{F}_{p^k}$.*

PROOF. If $a = 0$ then the claim is trivial. Otherwise, we have $a^{p^k} = ca$, and hence $a^{p^k-1} = c$. Thus $(a/b)^{p^k-1} = 1$, which implies that $a/b \in \mathbb{F}_{p^k}$. \square

CLAIM 4.6. *For linearized polynomial $Q(X) = \sum_{j=0}^{n-1} a_j X^{p^j} + \hat{a} \in \mathbb{F}_{p^n}[X]$ and integer t , we have*

$$(Q(X))^{p^t} \pmod{X^{p^n} - X} \equiv \sum_{j=0}^{n-1} (a_{((j-t) \bmod n)})^{p^t} X^{p^j} + \hat{a}^{p^t}.$$

PROOF. The transformation $Z \mapsto Z^{p^t}$ is a \mathbb{F}_p -linear operator which sends X^{p^r} to $X^{p^{(r+t) \bmod n}}$ and sends $a \in \mathbb{F}_{p^n}$ to a^{p^t} . \square

We now state and prove our main structural lemma about the zero/nonzero pattern of consecutive coefficients of subspace polynomials.

LEMMA 4.7 (MAIN STRUCTURAL LEMMA). *Let L be a d dimensional linear subspace in \mathbb{F}_{p^n} . Let $Q_L(X) = \sum_{j=0}^{n-1} a_j X^{p^j} + \hat{a}$ be the image-subspace polynomial of L .*

1. *For any integer r and set $J = \{(r+j) \bmod n \mid j = 0, \dots, d-1\}$ of d consecutive indices in \mathbb{Z}_n , there is some $j \in J$ with $a_j \neq 0$. In particular, a_0 and a_{n-d} are nonzero.*
2. *Suppose that L is not contained in any constant multiple of a proper subfield of \mathbb{F}_{p^n} , i.e. $L \not\subseteq \beta \cdot \mathbb{F}_{p^k}$ for any $\beta \in \mathbb{F}_{p^n}$ and any $\mathbb{F}_{p^k} \subset \mathbb{F}_{p^n}$. Then for any integer $r \neq n-d+1$ and set $J = \{(r+j) \bmod n \mid j = 0, \dots, d-2\}$ of $d-1$ consecutive indices in \mathbb{Z}_n , there is some $j \in J$ with $a_j \neq 0$.*

PROOF. For the first part, suppose $a_j = 0$ for all $j \in J$. Note that by Lemma 4.4, Q_L has p^{n-d} distinct roots in \mathbb{F}_{p^n} . Let $Q'(X) := Q_L(X)^{p^{n-(r+d)}} \pmod{X^{p^n} - X}$. Then, by Claim 4.6 we conclude $Q'(X) = \sum_{j=0}^{n-1} a_{j+r+d-n}^{p^{n-(r+d)}} X^{p^j}$. Now for any $j \in [n-d, n-1]$, we have $a_{j+r+d-n} = 0$ by assumption, and thus $Q'(X)$ is of degree at most p^{n-d-1} . In addition, by Proposition 3.1, $Q'(\alpha) = Q_L(\alpha)^{p^{n-(r+d)}} = 0$ for every $\alpha \in \mathbb{F}_{p^n}$ for which $Q_L(\alpha) = 0$, and hence Q' has at least p^{n-d} roots. This is a contradiction.

In particular, since by definition $a_{n-d+1}, \dots, a_{n-1}$ forms a sequence of $d-1$ consecutive coefficients that are all zero, we conclude both a_{n-d} and a_0 must be nonzero.

For the second part, suppose $a_j = 0$ for all $j \in J$. Again, by Lemma 4.4, Q_L has p^{n-d} distinct roots in \mathbb{F}_{p^n} . Let $k = n - (r+d) + 1 \neq 0$. Then as above the polynomial $Q'(X) := Q_L(X)^{p^k} \pmod{X^{p^n} - X}$ is nonzero of degree at most p^{n-d} . In addition, $Q'(\alpha) = Q_L(\alpha)^{p^k} = 0$ for every $\alpha \in \mathbb{F}_{p^n}$ for which $Q_L(\alpha) = 0$. As Q' and Q_L are of the same degree

p^{n-d} , there is a constant $c \in \mathbb{F}_{p^n}$ such that $Q'(X) - cQ_L(X)$ is of degree at most p^{n-d-1} and vanishes on the p^{n-d} roots of $Q_L(X)$. Thus the polynomial $Q'(X) - cQ_L(X)$ is identically zero. Recalling the definition of $Q'(X)$, we have just showed that $Q_L(X)^{p^k} - cQ_L(X) = 0 \pmod{X^{p^n} - X}$. Thus for each $\alpha \in \mathbb{F}_{p^n}$, we have $Q_L(\alpha)^{p^k} - cQ_L(\alpha) = 0$. Now, since the image of Q_L is L , by Claim 4.5 we conclude that $L \subseteq b \cdot \mathbb{F}_{p^k}$ (where $b \in \overline{\mathbb{F}_p}$ is a $p^k - 1$ -th root of c). This almost gives the desired contradiction, but for the possibility that $b \notin \mathbb{F}_{p^n}$, and that \mathbb{F}_{p^k} may not be a subfield of \mathbb{F}_{p^n} .

Let $\beta \in L \setminus \{0\}$. For any $\alpha \in L$, we have $\alpha/\beta \in (b \cdot \mathbb{F}_{p^k}) / (b \cdot \mathbb{F}_{p^k})$, and hence $\alpha/\beta \in \mathbb{F}_{p^k}$. Thus $\beta^{-1} \cdot L \subseteq \mathbb{F}_{p^k} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\gcd(k,n)}}$, where $(k,n) = \gcd(k,n)$. Thus $L \subseteq \beta \cdot \mathbb{F}_{p^{\gcd(k,n)}}$, contradicting the hypothesis on L . \square

4.3 Structure of products of subspace polynomials

In our subsequent arguments, we will need time and again to prove that a polynomial P that is the trace of products of linearized polynomials, is not a constant. In this subsection we describe a lemma that will allow us to argue such statements by showing that a well-chosen monomial of P has a nonzero coefficient. We start with a definition.

DEFINITION 4.8 (ASSOCIATED MATRIX). For $Q(X) = \sum_{i=0}^{n-1} a_i X^{p^i}$ a linearized polynomial over \mathbb{F}_{p^n} , we define its associated matrix $M_Q \in \mathbb{F}_{p^n}^{\{0, \dots, n-1\} \times \{0, \dots, n-1\}}$ by setting the (i, j) -entry of M_Q to be $(a_{j-i})^{p^i}$, where both rows and columns are indexed by $\{0, 1, \dots, n-1\}$ and index arithmetic, as well as powers of p are computed modulo n . Explicitly, M_Q is the following matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & \dots & a_{n-1} \\ (a_{n-1})^p & (a_0)^p & (a_1)^p & \dots & \dots & (a_{n-2})^p \\ (a_{n-2})^{p^2} & (a_{n-1})^{p^2} & (a_0)^{p^2} & \dots & \dots & (a_{n-3})^{p^2} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ (a_1)^{p^{n-1}} & (a_2)^{p^{n-1}} & (a_3)^{p^{n-1}} & \dots & \dots & (a_0)^{p^{n-1}} \end{pmatrix}.$$

The utility of the above definition lies in the following claim that follows immediately from Claim 4.6 (we omit the proof).

CLAIM 4.9. The (i, j) -entry of M_Q is the coefficient of X^{p^j} in the linearized polynomial $(Q(X))^{p^i} \pmod{X^{p^n} - X}$.

To state the main lemma of this subsection we need the following notation. For A, B nonempty subsets of $\{0, \dots, n-1\}$ let $M[A, B]$ be the minor corresponding to rows A and columns B . For integer r let $A + r = \{s + r \pmod{n} \mid s \in A\}$

LEMMA 4.10. Let $A_1, \dots, A_t, B_1, \dots, B_t \subseteq \{0, \dots, n-1\}$ satisfy $|A_i| = |B_i| > 0$ for $i = 1, \dots, t$. Let $\alpha_i = \sum_{j \in A_i} p^j, \beta_i = \sum_{k \in B_i} p^k$. Let $Q_1(X_1), \dots, Q_t(X_t)$ be linearized polynomials with associated matrices M_1, \dots, M_t respectively. Then the coefficient c_m of the monomial $m = \prod_{i=1}^t X_i^{\beta_i}$ in

$$R(X_1, \dots, X_t) = \text{Tr} \left(\prod_{i=1}^t (Q_i(X_i))^{\alpha_i} \right) \pmod{\langle (X_i^{p^n} - X_i)_{i \in [t]} \rangle}$$

is given by the expression

$$c_m = \sum_{r=0}^{n-1} \left(\prod_{i=1}^t \text{Perm}(M_i[A_i + r, B_i]) \right).$$

The proof of this lemma is by direct expansion, and is omitted from this extended abstract.

5. ANALYSIS OF INDEPENDENT SOURCE AFFINE DISPERSER

We are ready to prove our main results described in Section 2. In this section we prove Theorem 2.4, restated below. We point out that although the analysis is simpler than that involved in the proof of our main disperser (Theorem 2.2), it is at the heart of the more complicated construction.

THEOREM 2.4 (INDEPENDENT SOURCE AFFINE DISPERSER, RESTATED) Let $f : \mathbb{F}_{p^n}^t \rightarrow \mathbb{F}_p$ be given by

$$f(x_1, \dots, x_t) = \text{Tr} \left(\prod_{i=1}^t x_i^{1+p} \right).$$

Let $\mathcal{A}_1, \dots, \mathcal{A}_t \subseteq \mathbb{F}_{p^n}$ be \mathbb{F}_p -affine spaces of dimensions d_1, \dots, d_t respectively, where each \mathcal{A}_i is not contained in an affine shift of a proper subfield of \mathbb{F}_{p^n} . If $\sum_{i=1}^t (d_i - 2) > n$, then $|f(\prod_i \mathcal{A}_i)| > 1$.

PROOF. We follow the steps outlined in our strategy (Section 1.1). First, we notice that

$$f(\mathcal{A}_1, \dots, \mathcal{A}_t) = f(Q_1(\mathbb{F}_{p^n}), \dots, Q_t(\mathbb{F}_{p^n}))$$

where $Q_i(X_i)$ is the image-subspace polynomial of \mathcal{A}_i . By Proposition 3.1, in order to show $|f(\mathcal{A}_1, \dots, \mathcal{A}_t)| > 1$ it suffices to show that

$$R(X_1, \dots, X_t) \stackrel{\text{def}}{=} \text{Tr} \left(\prod_{i=1}^t (Q_i(X_i))^{\alpha_i} \right) \pmod{\langle (X_i^{p^n} - X_i)_{i \in [t]} \rangle}$$

has a monomial of degree > 0 that has a nonzero coefficient. We use Lemma 4.10 to understand what the coefficients of certain monomials look like. Finally, we use the structural properties of image-subspace polynomials given in Lemma 4.7 to find a nonzero monomial of R and complete the proof.

The key step in our proof is given by the following theorem. We state a somewhat more general form than needed for the proof of Theorem 2.4. The added generality will be useful in the proof of Theorem 2.2. (The general form we refer to deals with large powers α_i whereas for Theorem 2.4 setting all α_i to $1 + p$ would be sufficient.)

THEOREM 5.1. (INDEPENDENT SOURCE DISPERSER: ALGEBRAIC VERSION) Let $\mathcal{A}_1, \dots, \mathcal{A}_t \subseteq \mathbb{F}_{p^n}$ be affine subspaces of dimensions $d_1, \dots, d_t > 1$, none of which are contained in an affine shift of a proper subfield of \mathbb{F}_{p^n} . Let $Q_i(X_i) \in \mathbb{F}_{p^n}[X_i]$ be the image-subspace polynomial of \mathcal{A}_i . Let e_1, \dots, e_t satisfy $1 \leq e_i < d_i - 1$ and let $\alpha_i = \sum_{j=0}^{e_i} p^j$. Let

$$R(X_1, \dots, X_t) \stackrel{\text{def}}{=} \text{Tr} \left(\prod_{i=1}^t (Q_i(X_i))^{\alpha_i} \right) \pmod{\langle (X_i^{p^n} - X_i)_{i \in [t]} \rangle} \quad (3)$$

If $\sum_{i=1}^t (d_i - (e_i + 1)) > n - \max d_i + 1$, then $R(X_1, \dots, X_t)$ has a monomial $\prod_{i=1}^t X_i^{\beta_i}$ with $\text{wt}_p(\beta_i) = e_i + 1$, which has a nonzero coefficient. In particular, $R : \mathbb{F}_{p^n}^t \rightarrow \mathbb{F}_p$ is a nonconstant function.

Before giving the proof of Theorem 5.1, let us first show how to use it to complete the proof of Theorem 2.4. We

may assume without loss of generality that $d_i > 2$ by fixing nonzero elements of those spaces that have dimension 2. Next, we set in Theorem 5.1 values $e_1 = \dots = e_t = 1$ which gives $\alpha_1 = \dots = \alpha_t = 1 + p$ and notice using Proposition 3.1 that $R(\mathbb{F}_{p^n}^t)$ defined in (3) is exactly the set we are interested in, namely $f(\mathcal{A}_1, \dots, \mathcal{A}_t)$. Since $\sum(d_i - 2) = \sum(d_i - (e_i + 1)) > n$ so we conclude from Theorem 5.1 that $|f(\mathcal{A}_1, \dots, \mathcal{A}_t)| > 1$ and this completes the proof of Theorem 2.4. \square

5.1 Proof of Theorem 5.1

PROOF OF THEOREM 5.1. Let $A_i = \{0, \dots, e_i\}$. By Lemma 4.10, if $B_1, \dots, B_t \subset \{0, \dots, n-1\}$, $|B_i| = e_i + 1$ and $\beta_i = \sum_{k \in B_i} p^k$, then the coefficient of $m = \prod_{i=1}^t X_i^{\beta_i}$ in R , which is denoted henceforth by c_m , equals

$$\sum_{r=0}^{n-1} \left(\prod_{i=1}^t \text{Perm}(M_i[A_i + r, B_i]) \right). \quad (4)$$

We will find suitable powers β_i with $\text{wt}_p(\beta_i) = e_i + 1$ such that $c_m \neq 0$. We define β_i by specifying B_i with $|B_i| = e_i + 1$ and setting $\beta_i = \sum_{k \in B_i} p^k$.

Assume wlog $d_1 = \max d_i$. To define B_i let $\ell_1 = 0$ and for $1 < i \leq t$ let $\ell_i = \ell_{i-1} + d_i - (e_i + 1) \pmod n$. In other words, $\ell_i = \sum_{i' < i} (d_{i'} - (e_{i'} + 1)) \pmod n$ where $\ell_1 = 0$. Let $Q_i(X_i) = \sum_{j=0}^{n-1} a_{i,j} X_i^j + \hat{a}_i$. Our definition of B_i splits into two cases, depending on whether a_{i,ℓ_i} is nonzero or zero. In the first case we set B_i to be the set $\{\ell_i, n - d_i + 1, n - d_i + 2, \dots, n - d_i + e_i\}$. In the second case let j_i be the smallest index greater than ℓ_i such that a_{i,j_i} is nonzero. Similarly, let j'_i be the largest index smaller than ℓ_i such that a_{i,j'_i} is nonzero. Let $q_i = j_i - j'_i - 1$ be the number of zero valued indices between j'_i and j_i . Let $s_i = \min\{q_i, e_i\}$. We set B_i to be the set

$$\{j_i\} \cup \{j'_i + 1, \dots, j'_i + s_i\} \cup \{n - d_i + s_i + 1, \dots, n - d_i + e_i\}.$$

The last set might be empty in case $s_i = e_i$.

Our proof follows from the following two claims. We point out that the noncontainment of \mathcal{A}_i in a proper subfield is crucially used via the structural Lemma 4.7 in the proof of Claim 5.3.

CLAIM 5.2. $\text{Perm}(M_i[A_i, B_i]) \neq 0$ for $i = 1, \dots, t$.

CLAIM 5.3. For all $r \in \{1, \dots, n-1\}$ there exists $i \in \{1, \dots, t\}$ such that $\text{Perm}(M_i[A_i + r, B_i]) = 0$.

By Claim 5.2 the first summand of (4), corresponding to $r = 0$, is nonzero. By Claim 5.3 all other summands are zero. This completes the proof of Theorem 5.1. \square

6. THE AFFINE DISPERSER

In this section we prove Theorem 2.2. We start by examining what happens to $\mathcal{A} \subset \mathbb{F}_p^{nr}$ when it is partitioned into r blocks of size n . Then we prove the main theorem, by essentially reducing it to the case of independent affine sources described in Theorem 5.1.

6.1 Preparatory lemmas

Our first lemma, already used by Bourgain [10] in his construction of affine extractors, gives a certain kind of direct sum decomposition of \mathbb{F}_p -affine subspaces of \mathbb{F}_p^r .

LEMMA 6.1 ([10]). Let $\mathcal{A} \subseteq (\mathbb{F}_p^n)^r$ be an \mathbb{F}_p -affine subspace. Let $\gamma \in \mathcal{A}$. Then there exist linear spaces $Y_1, \dots, Y_r \subseteq \mathbb{F}_p^n$ and linear maps $\sigma_{ij} : Y_j \rightarrow \mathbb{F}_p^n$ such that:

$$\mathcal{A} = \{(x_1, \dots, x_r) \mid \exists y_i \in Y_i \text{ such that } x_i = \gamma_i + y_i + \sum_{j < i} \sigma_{ij}(y_j)\}$$

and $\dim \mathcal{A} = \sum_{i \in [r]} \dim Y_i$.

The next lemma should be thought of as a complement to Theorem 5.1. It expands the class of sources on which the function R given in that theorem is nonconstant. This expanded class is what we will use in the proof of our main theorem. The proof is omitted.

LEMMA 6.2. For each $i \in [r]$, let $P_i(X_i) \in \mathbb{F}_{p^n}[X_i]$ be a linearized polynomial. For each $j < i$, let $P_{ij}(X_j) \in \mathbb{F}_{p^n}[X_j]$ be a linearized polynomial. Let $\gamma \in \mathbb{F}_{p^n}^r$. Let $I_0 \subseteq [r]$ with $I_0 = \{i_1 < i_2 < \dots < i_t\}$. Let $e_{i_1}, \dots, e_{i_t} > 1$ be integers and let $\alpha_i = \sum_{k=0}^{e_i} p^k$, for $i \in I_0$. Let $g(X_1, \dots, X_r) \in \mathbb{F}_{p^n}[X_1, \dots, X_r]$ be the polynomial

$$\text{Tr} \left(\prod_{i \in I_0} \left(P_i(X_i) + \sum_{j < i} P_{ij}(X_j) + \gamma_i \right)^{\alpha_i} \right) \pmod{\langle X_i^q - X_i \rangle_{i \in [r]}}.$$

Let $g'(X_1, \dots, X_r) \in \mathbb{F}_{p^n}[X_1, \dots, X_r]$ be the polynomial

$$\text{Tr} \left(\prod_{i \in I_0} P_i(X_i)^{\alpha_i} \right) \pmod{\langle X_i^q - X_i \rangle_{i \in [r]}}.$$

Then for any $(\beta_{i_1}, \dots, \beta_{i_t})$ where $\text{wt}_p(\beta_{i_k}) = e_{i_k} + 1$, the coefficients of the monomial $\prod_{i \in I_0} X_i^{\beta_i}$ in g and in g' are equal.

6.2 Proof of Theorem 2.2

We can now analyze our main affine disperser construction. Theorem 2.2 will follow by setting the proper parameters into the following theorem.

THEOREM 6.3. (AFFINE DISPERSER — NON-PARAMETERIZED VERSION) Let $t < r$ be integers. Let n be prime with $n \geq r(r+1)/t$. For each $i \in [r]$, let $e_i = r + 1 - i$ and let $\alpha_i = \sum_{k=0}^{e_i} p^k$. Let $f : \mathbb{F}_p^{nr} \rightarrow \mathbb{F}_p$ be given by

$$f(x_1, \dots, x_r) = \text{Tr} \left(\sum_{I \subseteq [r], |I|=t} \prod_{i \in I} x_i^{\alpha_i} \right).$$

Let $\mathcal{A} \subseteq \mathbb{F}_p^{nr}$ be any \mathbb{F}_p -affine space with $\dim(\mathcal{A}) > \frac{nr}{t} + nt + r(r+1)$. Then $|f(\mathcal{A})| > 1$.

Before proving this theorem let us show how it implies Theorem 2.2.

PROOF OF THEOREM 2.2. For our selection of parameters n, t, r we notice the assumptions of Theorem 6.3 hold. Indeed, by Bertrand's postulate we can bound n from above by $4m^{3/5}$, hence $m^{2/5}/2 > r \geq m^{2/5}/4$. Notice that for our setting of parameters $r(r+1)/t \leq \sqrt{r}(r+1) \leq m^{3/5} < n$ and if $d > 6m^{4/5}$ then we have

$$\frac{nr}{t} + nt + r(r+1) \leq \frac{4}{\sqrt{2}} m^{4/5} + \frac{4}{\sqrt{2}} m^{4/5} + \frac{1}{4} m^{4/5} + o(m^{4/5}) < d.$$

Thus, the function f in Theorem 6.3 has the property that for any \mathcal{A} with $\dim(\mathcal{A}) > 6m^{4/5}$, we have $|f(\mathcal{A})| > 1$. Finally notice f as defined in Theorem 6.3 is identical to f defined in Theorem 2.2, up to renaming of the variables x_i . This completes the proof. \square

PROOF OF THEOREM 6.3. Our proof strategy is again as outlined in the Introduction. Our first goal is to find a polynomial mapping $H : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^r$ such that $H(\mathbb{F}_p^n) = \mathcal{A}$. We will then show that the composed function $f \circ H$ is a non-constant map, by showing that in its representation as a polynomial, there is a positive degree monomial with a nonzero coefficient.

To define the mapping H , we first decompose the affine space \mathcal{A} using Lemma 6.1. Let $\gamma \in \mathcal{A}$. Then by that lemma, we may find a collection of \mathbb{F}_p -linear subspaces $Y_1, \dots, Y_r \subseteq \mathbb{F}_p^n$ and linear maps $\sigma_{ij} : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ for $i, j \in [r]$ with $i < j$ such that:

$$\mathcal{A} = \{(x_1, \dots, x_r) \mid \exists y_i \in Y_i \text{ such that } x_i = \gamma_i + y_i + \sum_{j < i} \sigma_{ij}(y_j)\}$$

and $\dim \mathcal{A} = \sum_{i \in [r]} \dim Y_i$.

Let $Q_i(X) \in \mathbb{F}_p^n[X]$ be the image-subspace polynomial of Y_i . Let $Q_{ij}(X)$ be the linearized polynomial (guaranteed to exist by Lemma 4.4) such that $Q_{ij}(x) = \sigma_{ij}(Q_i(x))$ for each $x \in \mathbb{F}_p^n$. Let $R_i(X_1, \dots, X_r) \in \mathbb{F}_p^n[X_1, \dots, X_r]$ be the polynomial $Q_i(X_i) + \sum_{j < i} Q_{ij}(X_j) + \gamma_i$. Then by the above comments, the image of the function H mapping $x = (x_1, \dots, x_r) \in \mathbb{F}_p^n$ to $(R_1(x), \dots, R_r(x))$ is precisely \mathcal{A} .

Now let $h(X_1, \dots, X_r) \in \mathbb{F}_p^n[X_1, \dots, X_r]$ be the polynomial representing $f \circ H$, namely $h(X_1, \dots, X_r)$ equals

$$\begin{aligned} & f(R_1(X_1, \dots, X_r), \dots, R_r(X_1, \dots, X_r)) \pmod{\langle X_i^q - X_i \rangle_{i \in [r]}} \\ &= \sum_{I \subseteq [r], |I|=t} \text{Tr} \left(\prod_{i \in I} R_i(X_1, \dots, X_r)^{\alpha_i} \right) \pmod{\langle X_i^q - X_i \rangle_{i \in [r]}} \end{aligned} \quad (5)$$

By Proposition 3.1, we have $h(\mathbb{F}_p^r) = f(\mathcal{A})$.

Therefore, to show that $|f(\mathcal{A})| > 1$, it suffices to show that $|h(\mathbb{F}_p^r)| > 1$. We do this by showing that $h(X_1, \dots, X_r)$ has a monomial of positive degree with a nonzero coefficient and invoking Proposition 3.1.

To find this monomial, we consider the representation (5) of the polynomial $h(X_1, \dots, X_r)$. We will first find a set $I_0 \subseteq [r]$, with $|I_0| = t$, of ‘‘blocks with high entropy’’. Then via Theorem 5.1, we will argue that the summand in (5) corresponding to I_0 is a nonzero polynomial, with certain monomial \mathcal{M} having a nonzero coefficient. We will then show that no other summand in the sum (5) can have the monomial \mathcal{M} with a nonzero coefficient, thus establishing that \mathcal{M} appears in h with a nonzero coefficient, as desired.

We proceed with implementing this plan. Let $d_i = \dim(Y_i)$ and let $d = \dim(\mathcal{A}) > \frac{nr}{t} + nt + r(r+1)$. We have $\sum_i d_i = d$. Let $S = \{i \in [r] \mid d_i > r + 1\}$. Then we get

- $|S| \geq t$ (since each $d_i \leq n$ and $\sum d_i > nt + r(r+1)$).
- $\sum_{i \in S} d_i \geq \sum_{i \in [r]} (d_i - r - 1) = d - r(r+1) \geq nr/t + nt$.

Thus there exists $I_0 \subseteq S$ (and hence each $i \in I_0$ has $d_i > r + 1$) with $|I_0| = t$ such that

$$\sum_{i \in I_0} (d_i - (r+1)) \geq \left(\sum_{i \in S} d_i \right) \frac{t}{r} - (r+1)t \geq n + nt^2/r - (r+1)t \geq n, \quad (6)$$

where the last inequality used the hypothesis that $n \geq r(r+1)/t$.

Let us focus on the term

$$g(X_1, \dots, X_r) = \text{Tr} \left(\prod_{i \in I_0} R_i(X_1, \dots, X_r)^{\alpha_i} \right) \pmod{\langle X_i^q - X_i \rangle_{i \in [r]}}$$

in the representation (5) of the polynomial $h(X_1, \dots, X_r)$.

Putting $g'(X_1, \dots, X_r) = \text{Tr} \left(\prod_{i \in I_0} Q_i(X_i)^{\alpha_i} \right) \pmod{\langle X_i^q - X_i \rangle_{i \in [r]}}$ and noting that each $e_i + 1 \leq r + 1$, Equation (6) and Theorem 5.1 imply that there is a monomial $\mathcal{M} = \prod_{i \in I_0} X_i^{\beta_i}$ with $\text{wt}_p(\beta_i) = \text{wt}_p(\alpha_i) = e_i + 1$, which has a nonzero coefficient in g' . Lemma 6.2 now implies that the coefficient of \mathcal{M} in g is exactly the same as the coefficient of \mathcal{M} in g' , and hence nonzero.

We now show that in the representation (5) of the polynomial $h(X_1, \dots, X_r)$, no summand other than g can have a nonzero coefficient for the monomial \mathcal{M} . First notice that each $R_i(X_1, \dots, X_r)$ is a polynomial only in the variables X_1, X_2, \dots, X_i , and is a sum of monomials of the form aX_k^p plus possibly a constant term (i.e., monomials of total \mathbb{F}_p -degree at most 1).

Let $J \subseteq [r]$ with $|J| = t$, and consider the expression $\text{Tr}(\prod_{j \in J} R_j(X_1, \dots, X_r)^{\alpha_j}) \pmod{\langle (X_i^p - X_i)_{i \in [r]} \rangle}$. By definition, it equals:

$$\text{Tr} \left(\prod_{j \in J} \prod_{l=0}^{e_j} R_j(X_1, \dots, X_j)^{p^l} \right) \pmod{\langle (X_i^p - X_i)_{i \in [r]} \rangle}.$$

Suppose the monomial \mathcal{M} appeared in the above polynomial with a nonzero coefficient. Then, opening up the Tr , there is some $w \in [n - 1]$ such that \mathcal{M} appears in

$$\prod_{j \in J} \prod_{l=0}^{e_j} R_j(X_1, \dots, X_j)^{p^{l+w}} \pmod{\langle (X_i^p - X_i)_{i \in [r]} \rangle}$$

with a nonzero coefficient. Letting $R_{jl} = R_j^{p^{l+w}}$, we may rewrite the last polynomial as

$$\prod_{j \in J} \prod_{l=0}^{r-j+1} R_{jl}(X_1, \dots, X_j) \pmod{\langle (X_i^p - X_i)_{i \in [r]} \rangle},$$

where each R_{jl} is a sum of monomials of total \mathbb{F}_p -degree at most 1. Each monomial \mathcal{M}' that appears in this product is obtained by choosing, for each $j \in J$ and $l \in [0, r - j + 1]$, a monomial from $R_{jl}(X_1, \dots, X_j)$, and multiplying all these monomials out. Since we know that \mathcal{M} appears in this product, let us focus on the choices made in order for \mathcal{M} to appear. We set $\lambda_j(l) = i$ if for (j, l) we chose a monomial from $R_{jl}(X_1, \dots, X_j)$ whose variable is indexed by i (i.e., we chose some aX_i^p). Observe that the \mathbb{F}_p -degree in X_i of \mathcal{M} is at most the number of (j, l) pairs for which $\lambda_j(l) = i$ (which may be compactly written as $\sum_{j \in J} |\lambda_j^{-1}(i)|$). However, we know that for any $i \in I_0$, the \mathbb{F}_p -degree of \mathcal{M} in the variable X_i is $e_i + 1$ (which equals $r + 2 - i$). The following combinatorial claim (whose proof is omitted) now shows that J must be equal to I_0 .

CLAIM 6.4. *Let $I_0 \subseteq [r]$ with $|I_0| = t$. Suppose $J \subseteq [r]$ with $|J| = t$, and that there exist functions $\lambda_j : \{0, 1, \dots, r + 1 - j\} \rightarrow \{1, \dots, j\}$ for $j \in J$, with the property that for each $i \in I_0$,*

$$\sum_{j \in J} |\lambda_j^{-1}(i)| \geq r + 2 - i.$$

Then $J = I_0$.

Therefore, we have shown that there is precisely one summand, namely the one corresponding to I_0 , in the representation (5) of $h(X_1, \dots, X_r)$ that has a nonzero coefficient for the monomial \mathcal{M} . Thus \mathcal{M} appears in h with a nonzero coefficient, and thus $|h(\mathbb{F}_p^r)| > 1$, as desired. \square

7. PROOFS OF CLAIMS

PROOF OF CLAIM 5.2. Notice that, by definition, $M_i[A_i, B_i]$ is a $(e_i + 1) \times (e_i + 1)$ matrix constructed by taking the minor corresponding to the first $e_i + 1$ rows of M_i and the columns indexed by B_i . We claim this matrix is in fact lower triangular with nonzero entries on its diagonal, which immediately proves our claim. To see that $M_i[A_i, B_i]$ is such a matrix, consider B_i . To simplify notation in this proof, let $a_j = a_{i,j}$ be the coefficient of X^{p^j} in $Q(X_i)$. There are two cases.

$\mathbf{a}_{\ell_i} \neq \mathbf{0}$: We have $B_i = \{\ell_i, n - d_i + 1, \dots, n - d_i + e_i\}$. Consider the indices j of the coefficients a_j residing in the various entries of $M_i[A_i, B_i]$. (The exact power p^s to which each coefficient a_j is raised is not important for our proof.) By assumption $e_i < d_i$ so the entries above the diagonal of $M_i[A_i, B_i]$ have indices belonging to

$$\{n - d_i + 1, \dots, n - d_i + e_i\} \subseteq \{n - d_i + 1, \dots, n - 1\}$$

and this proves $M_i[A_i, B_i]$ is lower triangular. Regarding the diagonal, at the topmost left entry we have $a_{\ell_i} \neq 0$ and at all subsequent positions we have a_{n-d_i} raised to various powers. By Lemma 4.7 $a_{n-d_i} \neq 0$ and this completes the proof of this case.

$\mathbf{a}_{\ell_i} = \mathbf{0}$: In this case we have $B_i = \{j_i\} \cup \{j_i' + 1, \dots, j_i' + s_i\} \cup \{n - d_i + s_i + 1, \dots, n - d_i + e_i\}$ where

$$j_i = \min \{j > \ell_i \mid a_{i,j} \neq 0\} \text{ and } j_i' = \max \{j < \ell_i \mid a_{i,j} \neq 0\}.$$

The uppermost left $(s_i + 1) \times (s_i + 1)$ submatrix of $M_i[A_i, B_i]$ in this case is

$$\begin{pmatrix} a_{j_i} & a_{j_i'+1} & \cdots & a_{j_i'+s_i} \\ a_{j_i-1}^p & a_{j_i'}^p & \cdots & a_{j_i'+s_i-1}^p \\ \vdots & \vdots & \ddots & \vdots \\ a_{j_i-s_i}^{p^{s_i}} & a_{(j_i'+1)-s_i}^{p^{s_i}} & \cdots & a_{j_i'}^{p^{s_i}} \end{pmatrix}$$

which is lower triangular because the $a_{j_i'+1}, \dots, a_{j_i'+s_i}$ are all zero, and the diagonal of this submatrix is nonzero because $a_{j_i}, a_{j_i'}$ are nonzero. The last $e_i - s_i$ columns of the matrix (if they exist) are identical to the same last columns of the previous case and this shows that $M_i[A_i, B_i]$ is lower triangular with nonzero diagonal. This completes the proof of Claim 5.2. \square

PROOF OF CLAIM 5.3. In what follows we denote for $c < d$ by $[c, d]$ the set of integers in the interval $[c, d]$ and by $[c, d] \bmod n$ the set $\{i \bmod n \mid i \in [c, d]\}$. We start by observing that

$$M_i[A_i + r, \{k\}] = \begin{pmatrix} (a_{i,k-r})^{p^r} \\ (a_{i,k-(r+1)})^{p^{r+1}} \\ \vdots \\ (a_{i,k-(r+e_i)})^{p^{r+e_i}} \end{pmatrix}.$$

More to the point, the set of coefficient-indices of Q_i appearing in the k -column of $M_i[A_i + r, \{0, \dots, n - 1\}]$ is precisely

$[k - (r + e_i), \leq k - r] \bmod n$. So the structural Lemma 4.7 implies that for $k \in B_i$ and r that satisfy

$$[k - (r + e_i), k - r] \bmod n \subseteq [n - d_i + 1, n - 1] \quad (7)$$

the matrix $M_i[A_i + r, B_i]$ contains a zero column. So we get the following proposition.

PROPOSITION 7.1. *Whenever $k \in B_i$ and*

$$r \in [k + 1, k + d_i - (e_i + 1)] \bmod n$$

then $M_i[A_i + r, B_i]$ contains an all-zero column.

Thus, to prove the claim it suffices to show

$$[1, n - 1] \subseteq \bigcup_{i=1}^t \cup_{k \in B_i} [k + 1, k + (d_i - e_i) - 1]. \quad (8)$$

(Notice that Claim 5.2 implies the containment in the previous equation is in fact an equality.)

Indeed, since $\ell_1 = 0$ we have $B_1 = \{0\} \cup [n - d_1 + 1, n - d_1 + e_1]$, which implies by Proposition 7.1 that $M_1[A_1 + r, B_1]$ contains a zero column for r belonging to

$$[1, d_1 - (e_1 + 1)] \cup [n - d_1 + 2, n - 1] = [\ell_1 + 1, \ell_2] \cup [n - d_1 + 2, n - 1]. \quad (9)$$

Let t' be the minimal i such that $\sum_{i' \leq i} (d_{i'} - (e_{i'} + 1)) \geq n - d_1 + 1$, noticing such t' exists by assumption. In this case we have $\sum_{i' \leq t'} (d_{i'} - (e_{i'} + 1)) < n$ and so $\ell_{t'+1} = \sum_{i' \leq t'} (d_{i'} - (e_{i'} + 1))$.

We claim that for $1 < i \leq t'$ we have

$$\bigcup_{k \in B_i} [k + 1, k + d_i - (e_i + 1)] \supseteq [\ell_i + 1, \ell_{i+1}]. \quad (10)$$

which, together with (9), proves (8) and complete the proof of our claim. There are two cases to consider when proving (10).

$\mathbf{a}_{i, \ell_i} \neq \mathbf{0}$: In this case $\ell_i \in B_i$ so the claim follows from Proposition 7.1 by recalling $\ell_{i+1} - 1 = \ell_i + d_i - (e_i + 1)$.

$\mathbf{a}_{i, \ell_i} = \mathbf{0}$: There are two subcases to consider.

Case 1: $q_i < e_i$. In this case

$$B_i = \{j_i\} \cup [j_i' + 1, j_i' + q_i] \cup [n - d_i + q_i + 1, n - d_i + e_i].$$

Substituting $j_i' + (q_i + 1)$ for j_i and reordering elements of B_i we get

$$B_i = [j_i' + 1, j_i' + q_i + 1] \cup [n - d_i + q_i + 1, n - d_i + e_i].$$

We conclude $\ell_i \in B_i$ so by Proposition 7.1 our proof is complete, as in the case of $\mathbf{a}_{i, \ell_i} \neq \mathbf{0}$ above.

Case 2: $q_i \geq e_i$. In this case we have

$$B_i = \{j_i\} \cup [j_i' + 1, j_i' + e_i].$$

Substituting $j_i = j_i' + q_i + 1$ we get

$$B_i = [j_i' + 1, j_i' + e_i] \cup \{j_i' + q_i + 1\}$$

Now we use the fact that \mathcal{A}_i is not contained in an affine shift of a proper subfield. We notice that since $i \leq t'$ we have by maximality of d_1 that

$$j_i' < \ell_i \leq n - d_1 \leq n - d_i$$

which implies (using the maximality of d_1 again) that $j'_i + 1 \neq n - d_i + 1$. As \mathcal{A}_i is not contained in an affine shift of a proper subfield and $j'_i + 1 \neq n - d_i + 1$, our Structural Lemma 4.7 implies that $j_i - j'_i \leq d_i - 1$, or, equivalently, $j_i \leq j'_i + d_i - 1$.

Taking all but the last element of B_i in the previous equation notice

$$\bigcup_{k \in [j'_i + 1, j'_i + e_i]} [k + 1, k + d_i - (e_i + 1)] \supseteq [j'_i + 2, j'_i + d_i - 1],$$

which contains j_i . Now, since $j'_i < \ell_i < j_i$ when we reinsert j_i into B_i we conclude

$$\begin{aligned} \bigcup_{k \in B_i} [k + 1, k + d_i - (e_i + 1)] &\supseteq [j'_i + 2, j_i + d_i - (e_i + 1)] \\ &\supseteq [\ell_i + 1, \ell_{i+1}]. \end{aligned}$$

This completes the last case and with it the proof of Claim 5.3 is complete. \square

Acknowledgements.

This work was initiated while both authors visited Alex Samorodnitsky at the Hebrew University, Jerusalem. He took an active part in the initial stages of this research yet declined to be a co-author. We are grateful to Alex for his hospitality and support and for many enlightening discussions. We thank Jaikumar Radhakrishnan for helpful discussions.

8. REFERENCES

- [1] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting randomness using few independent sources. In *FOCS*, pages 384–393, Washington, DC, USA, 2004. IEEE Computer Society.
- [2] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating independence: New constructions of condensers, ramsey graphs, dispersers, and extractors. In *STOC*, pages 1–10, 2005.
- [3] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for sub-polynomial entropy and ramsey graphs beating the frankl-wilson construction. In *STOC*, pages 671–680, New York, NY, USA, 2006. ACM.
- [4] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. Vadhan. Robust PCPs of proximity, shorter PCPs and applications to coding. In ACM, editor, *STOC*, pages 1–10, 2004.
- [5] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. P. Vadhan. Short PCPs verifiable in polylogarithmic time. In *IEEE Conference on Computational Complexity*, pages 120–134, 2005.
- [6] E. Ben-Sasson, S. Hoory, E. Rozenman, and S. Vadhan. Extractors for affine sources, unpublished manuscript. 2001.
- [7] E. Ben-Sasson, S. Kopparty, and J. Radhakrishnan. Subspace polynomials and list decoding of reed-solomon codes. In *FOCS*, pages 207–216, 2006.
- [8] E. Ben-Sasson and M. Sudan. Simple PCPs with poly-log rate and query complexity. In *STOC*, pages 266–275, New York, NY, USA, 2005. ACM Press.
- [9] E. R. Berlekamp. *Algebraic Coding Theory*. Mc Graw-Hill, revised 1984 edition, 1968.
- [10] J. Bourgain. On the construction of affine extractors. *Geometric and Functional Analysis*, 17(1):33–57, 2007.
- [11] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc. (2)*, 73(2):380–398, 2006.
- [12] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.
- [13] B. Chor, O. Goldreich, J. Håstad, J. Friedman, S. Rudich, and R. Smolensky. The bit extraction problem of t-resilient functions (preliminary version). In *FOCS*, pages 396–407. IEEE, 1985.
- [14] Gabizon, Raz, and Shaltiel. Deterministic extractors for bit-fixing sources by obtaining an independent seed. *SICOMP: SIAM Journal on Computing*, 36, 2006.
- [15] A. Gabizon and R. Raz. Deterministic extractors for affine sources over large fields. In *FOCS*, pages 407–418, Washington, DC, USA, 2005. IEEE Computer Society.
- [16] J. Kamp, A. Rao, S. P. Vadhan, and D. Zuckerman. Deterministic extractors for small-space sources. In *STOC*, pages 691–700, 2006.
- [17] J. Kamp and D. Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. *SIAM J. Comput.*, 36(5):1231–1247, 2007.
- [18] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
- [19] O. Ore. On a special class of polynomials. *Trans. Amer. Math. Soc.*, 35(3):559–584, 1933.
- [20] O. Ore. Contributions to the theory of finite fields. *Trans. Amer. Math. Soc.*, 36(2):243–274, 1934.
- [21] R. Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.
- [22] L. Trevisan and S. P. Vadhan. Extracting randomness from samplable distributions. In *FOCS*, pages 32–42, 2000.
- [23] D. Zuckerman. Linear degree extractors and the inapproximability of max clique and chromatic number. In *STOC*, pages 681–690, New York, NY, USA, 2006. ACM.