Subspace Evasive Sets

Zeev Dvir[*]   Shachar Lovett [†]

Abstract

In this work we describe an explicit, simple, construction of large subsets of $\mathbb{F}^n$, where $\mathbb{F}$ is a finite field, that have small intersection with every k-dimensional affine subspace. Interest in the explicit construction of such sets, termed *subspace-evasive* sets, started in the work of Pudlák and Rödl [PR04] who showed how such constructions over the binary field can be used to construct explicit Ramsey graphs. More recently, Guruswami [Gur11] showed that, over large finite fields (of size polynomial in n), subspace evasive sets can be used to obtain explicit list-decodable codes with optimal rate and constant list-size. In this work we construct subspace evasive sets over large fields and use them, as described in [Gur11], to reduce the list size of folded Reed-Solomon codes form $\mathsf{poly}(n)$ to a constant.

1 Introduction

1.1 Subspace evasive sets

Defined formally, a (k, c)-subspace evasive set $S \subset \mathbb{F}^n$ has intersection of size at most c with every k-dimensional affine subspace $H \subset \mathbb{F}^n$. This definition makes sense over finite fields, as well as over infinite fields. Over finite fields, a simple probabilistic argument shows that a random set S of size $|\mathbb{F}|^{(1-\epsilon)n}$ will have intersection of size at most $c(k, \epsilon) = O(k/\epsilon)$ with any k-dimensional affine subspace H. In this work we give the first explicit construction of a subspace-evasive set S of size $|\mathbb{F}|^{(1-\epsilon)n}$ that has intersection size at most $c(k, \epsilon) = (k/\epsilon)^k$ with every k-dimensional affine subspace H. This is stated in the next theorem. We postpone the exact definition of the term *explicit* to the following sections (see Theorem 3.2 for the formal statement of this theorem and Section 4 for a discussion of explicitness).

Theorem 1 (Main theorem). *For any finite field $\mathbb{F}$ and parameters $k \geq 1, \epsilon > 0$ there exists an explicit construction of a set $S \subset \mathbb{F}^n$ of size $|S| > |\mathbb{F}|^{(1-\epsilon)n}$ that is $(k, c(k, \epsilon))$-subspace evasive with $c(k, \epsilon) = (k/\epsilon)^k$.*

While being far from the optimal bound of $O(k/\epsilon)$ and despite being exponential in k, the bound we obtain is useful when k is small and the field is sufficiently large. As we will see below, this is precisely the setting that was raised by Guruswami in connection to error correcting codes.

The main ingredient in our construction is an explicit family of degree d polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$, for all $k \leq n \leq |\mathbb{F}|$, such that for every injective (i.e full rank) affine map $\ell : \mathbb{F}^k \mapsto \mathbb{F}^n$ the system of equations

$$f_1(\ell(t_1, \ldots, t_k)) = 0$$
$$\vdots$$
$$f_k(\ell(t_1, \ldots, t_k)) = 0.$$

has at most d^k solutions. The degree d can be any number between n and $|\mathbb{F}|$. Using algebraic-geometry terminology, the set of common zeros of $f_1, \ldots, f_k$ forms an $(n-k)$-dimensional variety which has finite intersection with any k dimensional affine sub-space. We call such varieties *everywhere-finite* varieties (see Section 2 for a longer discussion of this particular choice of name).

Constructing subspace evasive sets as in Theorem 1 is then obtained by partitioning the n coordinates of the space into blocks of size k/ϵ and applying the basic construction (of an everywhere-finite variety) on each block independently. The polynomials we use in the basic construction are extremely simple (weighted sums of powers of variables) which makes the final construction explicit enough to be useful for the list-decoding application described in [Gur11] (allowing for both efficient encoding *and* list-decoding). Our proofs are elementary and do not use any sophisticated algebraic machinery (apart from Bezout's theorem).[1]

1.2 List-decodable codes

An error-correcting code allows one to encode a message into a codeword so that encodings of different messages differ in many coordinates. This allows one to recover the original message from an encoding that is corrupted in a small number of coordinates. More formally, A code is a subset $C \subset \Sigma^m$, where Σ is some finite alphabet. The *rate* of the code is denoted $R = \frac{\log |C|}{m \log |\Sigma|}$ and the *distance* of the code, denoted ρ, is the minimal Hamming distance between two codewords divided by m. It is easy to show that $\rho < 1 - R$ and that *unique decoding* (i.e decoding a message uniquely from a corrupted codeword) is only possible from a fraction $(1-R)/2$ of errors. When the number of errors goes beyond $(1-R)/2$ one has to be satisfied with *list-decoding*, in which a short list of possible messages is returned (i.e all messages whose encodings are close to the received word). Non explicitly, one can show the existence of a code that can be list-decoded from $1 - R - \epsilon$ errors with list-size bounded by $O(1/\epsilon)$. Obtaining an explicit construction of such a code (with efficient encoding/decoding) is a major open problem in coding theory. The first work to give explicit codes that can be list-decoded from $1 - R - \epsilon$ errors was the paper of Guruswami and Rudra [GR08] which builds on earlier work by Parvaresh and Vardi [PV05]. Their work showed that a certain family of codes, called *folded Reed-Solomon (RS) codes* can be list-decoded from $1 - R - \epsilon$ errors with list size bounded by $m^{O(1/\epsilon)}$, where m is the number of coordinates (or block length) of the code.

In a recent work, Guruswami [Gur11] gave a new list-decoding algorithm for folded RS codes which have some nice advantages over previous decoding algorithms. Among these advantages is the property that the list of possible messages, returned by the decoder, is contained in a low

---

[1]We do use Weil's exponential sum estimates to analyze a certain variant of the construction but this part of the proof can be omitted by choosing the polynomials $f_1, \ldots, f_k$ more carefully (as described in Section 4).

dimensional subspace. More precisely, the code represents messages as elements of $\mathbb{F}^n$, where $\mathbb{F}$ is a finite field of size $q \sim n$, and the list returned by the decoder is (quite surprisingly) a *subspace* of dimension $O(1/\epsilon)$. This immediately gives the size bound for the list of $q^{O(1/\epsilon)}$ mentioned above but also shows a way for improving further the list size. Guruswami observed that restricting the messages to come from a $((1/\epsilon), c(\epsilon))$-evasive set $S \subset \mathbb{F}^n$, instead of coming from the entire space $\mathbb{F}^n$, will reduce the list size to $c(\epsilon)$ and remove the dependency on the block length. In order for the rate to not degrade by much we need the size of S to be sufficiently large, say $|S| > |\mathbb{F}|^{(1-\epsilon)n}$.

For this application to produce codes with efficient encoding/decoding, the evasive set S must satisfy two explicitness conditions. The first is that messages can be encoded and decoded efficiently into S. The second condition is that, given a subspace (say, as a list of basis vectors), one can efficiently compute the intersection of this subspace with S. Our construction of subspace evasive sets satisfies both of these conditions (see Section 4) and so we obtain the following theorem.

Theorem 2. *For every R and ϵ, there exists an explicit family of codes $C \subset \Sigma^m$ with rate R that can be list-decoded from a fraction $1 - R - \epsilon$ of errors in quadratic time and with list size $(1/\epsilon)^{O(1/\epsilon)}$.*

The use of evasive sets to enhance list-decoding is completely black-box and only uses the property that the returned list is a subspace of a certain dimension in a sufficiently large field. We give the proof of Theorem 2 in Section 5, stating the relevant claims from [Gur11] that are needed for the black-box application.

Following [Gur11], Guruswami and Wang [GW11] showed another family of codes with optimal distance list decoding and with the additional property that the list returned by the decoder is a subspace. This family of codes, called derivative codes (also called multiplicity codes in [KSY11]), obtains roughly the same parameters as folded RS codes and can be also combined with our construction of evasive sets in the same way to reduce the list size.

1.3   Affine and two-source extractors

The work of Pudlák and Rödl [PR04] showed that constructing $(n/2, c)$-subspace evasive sets $S \subset \mathbb{F}_2^n$ gives explicit constructions of bipartite Ramsey graphs. These are bipartite graphs that do not contain bipartite cliques or independent sets of certain size. A recent work of Ben-Sasson and Zewi [BSZ11] explored this connection further and showed (under some number theoretic conjectures) that such sets can also be used to construct two-source *extractors* which are strong variants of bipartite Ramsey graphs. Another application given in [BSZ11] was to the construction of *affine extractors* which are functions that have uniform output whenever the input chosen uniformly from a subspace of sufficiently high dimension. Both of these applications require that the construction be over a field of two elements. Our construction requires the field to be at least of size n and so is not useful for these applications. An important direction for progress is to generalize our construction for smaller fields. Alternatively, one can try to generalize the approach of [BSZ11] to larger fields and then try to use our construction to obtain better extractors (affine or two-source).

1.4   Organization

Section 2 contains the main construction of everywhere-finite varieties (Theorem 2.4). In Section 3, we show how to compose this basic construction to obtain our main theorem, Theorem 3.2, which

gives explicit evasive sets. In Section 4 we prove several claims which deal with the explicitness of our construction, and use them, in Section 5 to derive Theorem 2. Appendix A contains some basic results on Fourier analysis that are used in part of Section 3.

2 Everywhere-finite varieties

Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ its algebraic closure (recall that the algebraic closure is always infinite, even if $\mathbb{F}$ is finite). A variety in $\overline{\mathbb{F}}^n$ is the set of common zeros of one or more polynomials. Given k polynomials $f_1, \ldots, f_k \in \overline{\mathbb{F}}[x_1, \ldots, x_n]$, we denote the variety they define as

$$\mathbf{V}(f_1, \ldots, f_k) := \{x \in \overline{\mathbb{F}}^n \mid f_1(x) = \ldots = f_k(x) = 0\}.$$

The *dimension* of a variety is a generalization of the notion of dimension for subspaces and can be thought of, informally, as the number of 'degrees of freedom' the variety has. In particular, k generic polynomials $f_1, \ldots, f_k$ define a variety $\mathbf{V}(f_1, \ldots, f_k)$ of dimension $n - k$. It is well known that the intersection of an $(n - k)$-dimensional variety $V \subset \overline{\mathbb{F}}^n$ with a generic k dimensional affine subspace $H \subset \overline{\mathbb{F}}^n$ is finite[2]. In the following we will not rely on any of these properties and keep the discussion self-contained. Our main result in this section is a construction of an explicit variety V where this holds for *all* affine subspaces H of dimension k. Using Bezout's theorem (Theorem 2.2) and the bound on the degrees of the polynomials defining V we will also get an explicit uniform bound on the size of the intersections $|\mathbf{V} \cap H|$. We start with the formal definition.

Definition 2.1 (Everywhere-finite variety)**.** *Let* $f_1, \ldots, f_k \in \overline{\mathbb{F}}[x_1, \ldots, x_n]$ *be polynomials. The variety* $\mathbf{V} = \mathbf{V}(f_1, \ldots, f_k)$ *is* everywhere-finite *if for any affine subspace* $H \subset \overline{\mathbb{F}}^n$ *of dimension* k, *the intersection* $\mathbf{V} \cap H$ *is finite.*

The importance of showing that the intersection is finite comes from Bezout's theorem, which allows one to give explicit bounds on the intersection size, given that it is finite. This result can be found in most introductory texts on Algebraic Geometry [Sha94] (for an elementary proof of this particular formulation see [Sch95]).

Theorem 2.2 (Bezout)**.** *Let* $g_1, \ldots, g_k \in \overline{\mathbb{F}}[t_1, \ldots, t_k]$ *be polynomials. If* $\mathbf{V}(g_1, \ldots, g_k)$ *is finite then*

$$|\mathbf{V}(g_1, \ldots, g_k)| \leq \prod_{i=1}^{k} \deg(g_i).$$

For everywhere-finite varieties this gives the following immediate corollary.

Corollary 2.3. *Let* $f_1, \ldots, f_k \in \overline{\mathbb{F}}[x_1, \ldots, x_n]$ *be polynomials such that* $\mathbf{V} = \mathbf{V}(f_1, \ldots, f_k)$ *is everywhere-finite. Then for any* k-*dimensional affine subspace* $H \subset \overline{\mathbb{F}}^n$ *we have*

$$|\mathbf{V} \cap H| \leq \prod_{i=1}^{k} \deg(f_i).$$

---

[2]For a precise definition of dimension and proofs of its basic properties we refer the reader to any elementary text on Algebraic Geometry (e.g [Sha94]).

Proof. Let the k-dimensional affine subspace H be given as the image of an affine map $\ell = (\ell_1, \ldots, \ell_n) : \overline{\mathbb{F}}^k \to \overline{\mathbb{F}}^n$. Let $g_i \in \overline{\mathbb{F}}[t_1, \ldots, t_k]$ denote the restriction of f_i to H, i.e.

$$g_i(t_1, \ldots, t_k) := f_i(\ell_1(t_1, \ldots, t_k), \ldots, \ell_n(t_1, \ldots, t_k)).$$

Clearly $\mathbf{V} \cap H = \mathbf{V}(g_1, \ldots, g_k)$ and $\deg(g_i) \leq \deg(f_i)$. The corollary now follows from Theorem 2.2. $\square$

We will now describe an explicit construction of an everywhere-finite variety. We will need the following definition: A $k \times n$ matrix (where $k \leq n$) is *k-regular* if all its $k \times k$ minors are regular (i.e have non-zero determinant). For example, if $\mathbb{F}$ is a field with at least n distinct nonzero elements $\gamma_1, \ldots, \gamma_n$ then $A_{i,j} = \gamma_j^i$ is k-regular.

Theorem 2.4 (Construction of an everywhere-finite variety). *Let $1 \leq k \leq n$ be parameters and $\mathbb{F}$ be a field. Let A be a $k \times n$ matrix with coefficients in $\mathbb{F}$ which is k-regular. Let $d_1 > d_2 > \ldots > d_n \geq 1$ be integers. Let the polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ be defined as follows:*

$$f_i(x_1, \ldots, x_n) := \sum_{j=1}^{n} A_{i,j} \cdot x_j^{d_j}.$$

Then $\mathbf{V} = \mathbf{V}(f_1, \ldots, f_k)$ is everywhere-finite. In particular, for any k-dimensional affine subspace $H \subset \overline{\mathbb{F}}^n$ we have $|\mathbf{V} \cap H| \leq (d_1)^k$.

We prove Theorem 2.4 in the remainder of this section. Let $H \subset \overline{\mathbb{F}}^n$ be a k-dimensional affine subspace. Our goal is to show that $\mathbf{V} \cap H$ is finite, and then the size bound follows from Corollary 2.3. The first step is to present H as the image of an affine map $\ell : \overline{\mathbb{F}}^k \mapsto \overline{\mathbb{F}}^n$ with a convenient choice of basis. In the following let $t = (t_1, \ldots, t_k) \in \overline{\mathbb{F}}^k$ and $x = (x_1, \ldots, x_n) \in \overline{\mathbb{F}}^n$.

Claim 2.5. *There exists an affine map $\ell = (\ell_1, \ldots, \ell_n) : \overline{\mathbb{F}}^k \to \overline{\mathbb{F}}^n$ whose image is H and such that the following holds. There exist k indices $1 \leq j_1 < j_2 < \ldots < j_k \leq n$ such that*

1. *For all $i \in [k]$, $\ell_{j_i}(t) = t_i$.*

2. *If $j < j_1$ then $\ell_j(t) \in \overline{\mathbb{F}}$ (i.e ℓ_j is constant).*

3. *If $j < j_i$ for $i > 1$ then $\ell_j(t)$ is an affine function just of the variables $t_1, t_2, \ldots, t_{i-1}$.*

Proof. Let $\ell' : \overline{\mathbb{F}}^k \to \overline{\mathbb{F}}^n$ be an arbitrary affine map whose image is H. We construct ℓ by a basis change of ℓ' which puts it in an upper-echelon form. That is, let j_1 be the minimal index such that $\ell'_{j_1}(t)$ is not constant. We take $\ell_{j_1}(t) = t_1$. Let j_2 be the minimal index after j_1 such that $\ell'_{j_2}(t)$ is not an affine function of $\ell'_{j_1}(t)$. We take $\ell_{j_2}(t) = t_2$, and we have that $\ell_j(t)$ for $j_1 < j < j_2$ are affine functions of t_1. Generally, let j_i be the minimal index after j_{i-1} such that $\ell'_{j_i}(t)$ is not an affine function of $\ell'_{j_1}(t), \ldots, \ell'_{j_{i-1}}(t)$. We take $\ell_{j_i}(t) = t_i$ and have that $\ell_j(t)$ for $j_{i-1} < j < j_i$ are affine functions of $t_1, \ldots, t_{i-1}$. Obviously, for $j > j_k$ we have that $\ell_j(t)$ are affine functions of all $t_1, \ldots, t_k$. $\square$

Let $\ell = (\ell_1, \ldots, \ell_n) : \overline{\mathbb{F}}^k \to \overline{\mathbb{F}}^n$ be given by Claim 2.5 and let $1 \leq j_1 < j_2 < \ldots < j_k \leq n$ be the indices given by the claim. Let $J := \{j_1, \ldots, j_k\}$. Our goal is to show that the following system has a finite number of solutions:

$$f_i(\ell_1(t_1, \ldots, t_k), \ldots, \ell_n(t_1, \ldots, t_k)) = 0, \ i \in [k].$$

Clearly, applying an invertible linear transformation on the set $f_1, \ldots, f_k$ (replacing each f_i with a linear combination of $f_1, \ldots, f_k$) will not affect the number of solutions. Our next step is to find such a linear transformation that will put the f_i's in a more convenient form, eliminating some of their coefficients.

Claim 2.6. *Let $f(x) = (f_1(x), \ldots, f_k(x))$. There exist k linearly independent vectors $u_1, \ldots, u_k \in \overline{\mathbb{F}}^k$ such that, for all $i \in [k]$,*

$$\langle u_i, f(x) \rangle = x_{j_i}^{d_{j_i}} + \sum_{j \in [n] \setminus J} c_{ij} \cdot x_j^{d_j}, \tag{1}$$

where the coefficients c_{ij} are elements of $\overline{\mathbb{F}}$.

Proof. Recall that by definition $f_i(x) = \sum_{j=1}^{n} A_{i,j} \cdot x_j^{d_j}$ where A is a k-regular matrix. Let A' be the $k \times k$ minor of A given by restriction to columns $j_1, \ldots, j_k$. Since A is k-regular we have that A' is regular. Let $u_1, \ldots, u_k \in \mathbb{F}^k$ denote the rows of $(A')^{-1}$. We thus have that $u_i A' = e_i$ where e_i is the i-th unit vector. That is, $\langle u_i, f(x) \rangle = x_{j_i}^{d_{j_i}} + \sum_{j \notin J} c_{ij} \cdot x_j^{d_j}$ where c_{ij} is the inner product of u_i and the j-th column of A. $\qquad\square$

Let $u_1, \ldots, u_k$ be the vectors given by Claim 2.6 and denote

$$\tilde{f}_i(x) := \langle u_i, f(x) \rangle.$$

Let us also denote

$$g_i(t_1, \ldots, t_k) := \tilde{f}_i(\ell_1(t_1, \ldots, t_k), \ldots, \ell_n(t_1, \ldots, t_k)).$$

Recall that, from the above discussion, our goal is to show that the system $\{g_i(t) = 0 : i \in [k]\}$ has a finite number of solutions in $\overline{\mathbb{F}}^k$. By Claims 2.5 and 2.6 we have that

$$g_i(t) = t_i^{d_{j_i}} + \sum_{j \in [n] \setminus J} c_{ij} \cdot \ell_j(t)^{d_j}. \tag{2}$$

We now perform one final transformation on our system. Contrary to the previous transformations which were linear transformations, this will be a polynomial transformation. Let

$$D := \prod_{i=1}^{k} d_{j_i}$$

and let

$$D_i := \frac{D}{d_{j_i}}.$$

For $i \in [k]$ define
$$h_i(t_1, \ldots, t_k) := g_i\left(t_1^{D_1}, \ldots, t_k^{D_k}\right).$$

We first note that in order to show that $\mathbf{V}(g_1, \ldots, g_k)$ is finite it suffices to show that $\mathbf{V}(h_1, \ldots, h_k)$ is finite.

Claim 2.7. $|\mathbf{V}(g_1, \ldots, g_k)| \leq |\mathbf{V}(h_1, \ldots, h_k)|$.

Proof. For each $w \in \mathbf{V}(g)$ we can define $w' \in \mathbf{V}(h)$ by letting w_i' be some D_i root of w_i (it exists since $\overline{\mathbb{F}}$ is algebraically closed). Clearly distinct elements in $\mathbf{V}(g)$ are mapped to distinct elements in $\mathbf{V}(h)$. $\square$

The reason for these transformations is that the final polynomials h_i have a specifically nice form: they are the sum of t_i^D with a polynomial of lower total degree.

Claim 2.8. *For all $i \in [k]$ we have that*
$$h_i(t_1, \ldots, t_k) = t_i^D + r_i(t_1, \ldots, t_k)$$

where $\deg(r_i) < D$.

Proof. By definition
$$h_i(t) = g_i(t_1^{D_1}, \ldots, t_k^{D_k}) = t_i^D + \sum_{j \in [n] \setminus J} c_{ij} \cdot \ell_j(t_1^{D_1}, \ldots, t_k^{D_k})^{d_j}.$$

To prove the claim we need to show that $\deg(\ell_j(t_1^{D_1}, \ldots, t_k^{D_k})) < D/d_j$ for all $j \notin J$. If $j < j_1$ then ℓ_j is constant. Otherwise let $i \in [k]$ be maximal such that $j > j_i$. By Claim 2.5 we have that $\ell_j(t)$ is an affine function of $t_1, \ldots, t_i$. Since $D_1 < \ldots < D_k$ we have that
$$\deg(\ell_j(t_1^{D_1}, \ldots, t_k^{D_k})) \leq D_i = \frac{D}{d_{j_i}} < \frac{D}{d_j}$$

since $d_1 > \ldots > d_n$. $\square$

To complete the proof of Theorem 2.4 we need to show that $\mathbf{V}(h_1, \ldots, h_k)$ is finite. This follows from a general bound for polynomials of the form $h_i(t) = t_i^D + r_i(t)$ where $\deg(r_i) < D$.

Lemma 2.9. *Let $h_1, \ldots, h_k \in \overline{\mathbb{F}}[t_1, \ldots, t_k]$ be polynomials such that $h_i(t) = t_i^D + r_i(t)$ where $\deg(r_i) < D$. Then $\mathbf{V}(h_1, \ldots, h_k) \leq D^k$.*

Lemma 2.9 follows immediately from the following two claims. In the following, let $R := \overline{\mathbb{F}}[t_1, \ldots, t_k]$ be the ring of polynomials; $I := \langle h_1, \ldots, h_k \rangle$ be the ideal in R generated by $h_1, \ldots, h_k$; and $M := R/I$ be their quotient. Note that M is a vector space over $\overline{\mathbb{F}}$.

Claim 2.10. $|\mathbf{V}(h_1, \ldots, h_k)| \leq \dim M$.

Proof. Assume by contradiction there exist $w_1, \ldots, w_m \in \mathbf{V}(h_1, \ldots, h_k)$ where $m > \dim(M)$. Let $q_i \in \overline{\mathbb{F}}[t_1, \ldots, t_k]$ be polynomials such that $q_i(w_i) = 1$ and $q_i(w_j) = 0$ for all $j \neq i$. Let $\tilde{q}_i$ be the image of q_i in M. Since $m > \dim(M)$ there must exist a nonzero linear dependency among $\tilde{q}_1, \ldots, \tilde{q}_m$. That is, there exist $c_1, \ldots, c_m \in \overline{\mathbb{F}}$ not all zero such that

$$\sum_{i \in [m]} c_i \cdot \tilde{q}_i(t) = 0 \quad (\text{in } M).$$

Equivalently put,

$$\sum_{i \in [m]} c_i \cdot q_i(t) \in I.$$

The key observation is that for any polynomial $h(t) \in I$ we have that $h(w) = 0$ for all $w \in \{w_1, \ldots, w_m\}$. This is because $h_i(w) = 0$ for all $i \in [k]$ by assumption. Thus substituting $t = w_j$ we get that

$$0 = \sum_{i \in [m]} c_i \cdot q_i(w_j) = c_j,$$

which contradicts the assumption that not all $c_1, \ldots, c_m$ are nonzero. $\qquad \square$

Claim 2.11. $\dim M \leq D^k$.

Proof. We will show that M is spanned by the image in I of the monomials $t_1^{e_1} \ldots t_k^{e_k}$ where $0 \leq e_1, \ldots, e_k \leq D - 1$. Thus in particular $\dim M \leq D^k$. In order to do so, we need to show that if $q(t)$ is a polynomial then there exists a polynomial $\tilde{q}(t)$ such that $q - \tilde{q} \in I$ and the degree of each variable in $\tilde{q}$ is at most $D - 1$. It suffices to show that if $q(t)$ has some variable of degree at least D then we can find $\tilde{q}$ such that $q - \tilde{q} \in I$ and such that $\deg(\tilde{q}) < \deg(q)$. The claim then follows by iterating this process until all variables have degrees below D. Moreover, it suffices to prove this in the case where q is a monomial, as this process can be applied to each monomial individually.

Thus, let $q(t) = t_1^{e_1} \ldots t_k^{e_k}$ be a monomial where $e_i \geq D$ for some $i \in [k]$. Define

$$\tilde{q}(t) = t_i^{e_i - D}(t_i^D - h_i(t)) \cdot \prod_{j \neq i} t_j^{e_j}.$$

We have that $\deg(\tilde{q}) < \deg(q)$ since $\deg(h_i(t) - t_i^D) < D$ by assumption; and $q(t) - \tilde{q}(t) = h_i(t) t_i^{e_i - D} \prod_{j \neq i} t_j^{e_j} \in I$ as required. $\qquad \square$

3 Subspace Evasive sets

In this section we construct subspace evasive sets, based on the construction of everywhere-finite varieties given in Theorem 2.4. We first recall the definition of subspace evasive sets.

Definition 3.1 (Subspace evasive sets)**.** *Let $S \subset \mathbb{F}^n$. We say S is (k, c)-subspace evasive if for all k-dimensional affine subspaces $H \subset \mathbb{F}^n$ we have $|S \cap H| \leq c$.*

8

We next give some necessary definitions. For polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_m]$ we define their common solutions in $\mathbb{F}^m$ (as opposed to their solutions over the algebraic closure) as

$$\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) := \mathbf{V}(f_1, \ldots, f_k) \cap \mathbb{F}^m = \{x \in \mathbb{F}^m : f_1(x) = \ldots = f_k(x) = 0\}.$$

We say that a $k \times m$ matrix is *strongly-regular* if all its $r \times r$ minors are regular for all $1 \leq r \leq k$. For example, if $\mathbb{F}$ is a field with at least m distinct nonzero elements $\gamma_1, \ldots, \gamma_m$ then $A_{i,j} = \gamma_j^i$ is strongly-regular.

Theorem 3.2. *Let $k \geq 1, \epsilon > 0$ and $\mathbb{F}$ be a finite field. Let $m := k/\epsilon$ and assume m is integer and m divides n. Let A be a $k \times m$ matrix with coefficients in $\mathbb{F}$ which is strongly-regular. Let $d_1 > \ldots > d_m$ be integers. For $i \in [k]$ let*

$$f_i(x_1, \ldots, x_m) := \sum_{j=1}^{m} A_{i,j} \cdot x_j^{d_j},$$

and define $S \subset \mathbb{F}^n$ to be the (n/m)-times cartesian product of $\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) \subset \mathbb{F}^m$. That is

$$
\begin{aligned}
S &= \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) \times \ldots \times \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) \\
&= \{x \in \mathbb{F}^n : f_i(x_{tm+1}, \ldots, x_{tm+m}) = 0, \ \forall \ 0 \leq t < n/m, \ 1 \leq i \leq k\}.
\end{aligned}
$$

Then S is $(k, (d_1)^k)$-subspace evasive. Moreover,

1. *If $\epsilon \leq 1/10$, $d_1 \leq |\mathbb{F}|^{1/4}$ and $|\mathbb{F}|^m \geq n^8$ then $|S| \geq \frac{1}{3}|\mathbb{F}|^{(1-\epsilon)n}$.*

2. *If at least k of the degrees $d_1, \ldots, d_m$ are co-prime to $|\mathbb{F}| - 1$ then $|S| = |\mathbb{F}|^{(1-\epsilon)n}$.*

We prove Theorem 3.2 in the remainder of this section. We first show that $\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)$ has small intersection with affine subspaces of dimension *at most k* (this is a stronger statement than the one we proved in Section 2 since the dimension of the subspace can be smaller than k).

Claim 3.3. *Let $H \subset \mathbb{F}^m$ be an r-dimensional affine subspace for $r \leq k$. Then $|\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) \cap H| \leq (d_1)^r$.*

Proof. Note that $\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) \cap H = \mathbf{V}(f_1, \ldots, f_k) \cap H$ since $H \subset \mathbb{F}^m$. We will show that in fact $|\mathbf{V}(f_1, \ldots, f_r) \cap H| \leq (d_1)^r$, from which the claim will follow since $\mathbf{V}(f_1, \ldots, f_k) \subset \mathbf{V}(f_1, \ldots, f_r)$. Now, since the matrix A is strongly-regular, its restriction to the first r rows is r-regular; hence $\mathbf{V}(f_1, \ldots, f_r)$ is everywhere-finite (as an $(n-r)$-dimensional variety) and, by Bezout's Theorem (Theorem 2.2), we have $|\mathbf{V}(f_1, \ldots, f_r) \cap H| \leq (d_1)^r$. $\qquad\square$

We now prove that $S = \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)^{(n/m)}$ is subspace evasive for dimensions up to k.

Claim 3.4. *Let $H \subset \mathbb{F}^n$ be an r-dimensional affine subspace for $r \leq k$. Then $|S \cap H| \leq (d_1)^r$.*

Proof. Let $\mathbf{V}_{\mathbb{F}} = \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)$. We prove the claim by induction of the number of blocks $b = n/m$. If $b = 1$ then $S = \mathbf{V}_{\mathbb{F}}$ and the claim follows from Claim 3.3. We thus assume that $b > 1$. Decompose H as a disjoint union of subspaces based on the restriction to the first m coordinates $x_1, \ldots, x_m$

(i.e. the first block). That is, let $T := \{(x_1, \ldots, x_m) : (x_1, \ldots, x_n) \in H\}$ and for each $t \in T$ let $H_t := \{(x_1, \ldots, x_n) \in H : (x_1, \ldots, x_m) = t\}$. Thus $H = \cup_{t \in T} H_t$ and we have that

$$|\mathbf{V}_{\mathbb{F}}^{n/m} \cap H| = \sum_{t \in \mathbf{V}_{\mathbb{F}} \cap T} |\mathbf{V}_{\mathbb{F}}^{(n/m)-1} \cap H_t|.$$

Now, since H is an affine subspace so is T. Let $r' = dim(T)$ where $0 \leq r' \leq r$. We also have that H_t is an $(r - r')$-dimensional affine subspace for all $t \in T$. Now by Claim 3.3 we have that $|\mathbf{V}_{\mathbb{F}} \cap T| \leq (d_1)^{r'}$; and by induction we have that $|\mathbf{V}_{\mathbb{F}}^{(n/m)-1} \cap H_t| \leq (d_1)^{r-r'}$ for all $t \in T$. Hence $|\mathbf{V}_{\mathbb{F}}^{n/m} \cap H| \leq (d_1)^r$ as claimed. $\qquad\square$

We now turn to prove the 'Moreover' part of Theorem 3.2, namely to lower bound the size of S. To do so, it is enough to bound the size of $\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)$ (since S is a product of such sets). We begin with the unrestricted case, where all we assume are some (rather weak) bounds on the size of the field. We refer the reader to Appendix A for the notations/preliminaries on Fourier analysis and Weil's theorem used in the proof.

Claim 3.5. *Assume that $\epsilon \leq 1/10$, $d_1 \leq |\mathbb{F}|^{1/4}$ and $|\mathbb{F}|^m \geq n^8$. Then $|\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)| \geq (1 - 1/n)|\mathbb{F}|^{m-k}$. In particular $|S| \geq |\mathbb{F}|^{(1-\epsilon)n}/3$.*

Proof. Let $x = (x_1, \ldots, x_m) \in \mathbb{F}^m$ be chosen uniformly. Our goal is to estimate the probability that $\sum_{j=1}^m A_{i,j} \cdot x_j^{d_j} = 0$ for all $i \in [k]$. Equivalently, let $X^{(j)} \in \mathbb{F}^k$ be a random variable defined as $X_i^{(j)} := A_{i,j} \cdot x_j^{d_j}$ and let $X := X^{(1)} + \ldots + X^{(m)}$. We need to estimate the probability that $X = 0^k$.

To this end, we apply Fourier analysis (for definitions see Appendix A). Assume $\mathbb{F} = \mathbb{F}_q$ where $q = p^\ell$. The characters of $\mathbb{F}^k$ are given by $\chi_a(x) = e_p(\text{Tr}(\langle a, x \rangle))$ for $a \in \mathbb{F}^k$ where $\text{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace operator. Since $X^{(1)}, \ldots, X^{(m)}$ are independent we have that

$$\widehat{X}(a) = \mathbb{E}[\chi_a(X)] = \mathbb{E}[\chi_a(\sum_{j=1}^m X^{(j)})] = \prod_{j=1}^m \mathbb{E}[\chi_a(X^{(j)})] = \prod_{j=1}^m \widehat{X^{(j)}}(a).$$

We proceed to estimate the Fourier coefficients of $X^{(j)}$. Let $A^{(j)} \in \mathbb{F}^k$ denote the j-th column of A. We have that

$$\widehat{X^{(j)}}(a) = \mathbb{E}_{x_j \in \mathbb{F}}[e_p(\text{Tr}(\langle a, A^{(j)} \rangle \cdot x_j^{d_j}))].$$

Thus, if the inner product of a and $A^{(j)}$ is nonzero, we have by the Weil bound (Theorem A.1) that

$$\left| \widehat{X^{(j)}}(a) \right| \leq \frac{d_j - 1}{\sqrt{|\mathbb{F}|}} \leq |\mathbb{F}|^{-1/4}.$$

Since we assume A is strongly-regular, for any nonzero $a \in \mathbb{F}^m$ there could by at most $k-1$ columns of A which are orthogonal to a; hence we deduce that for any nonzero a,

$$\left| \widehat{X}(a) \right| \leq (|\mathbb{F}|^{-1/4})^{(m-k+1)} \leq |\mathbb{F}|^{-k-m/8} \leq (1/n) \cdot |\mathbb{F}|^{-k}$$

by our choice of parameters. We now apply these bounds to estimate the probability that $X = 0$. We have that $\Pr[X = 0] = |\mathbb{F}|^{-k} \sum_a \widehat{X}(a)$ and $\widehat{X}(0) = 1$; hence

$$\left| \Pr[X = 0] - \mathbb{F}^{-k} \right| \leq \mathbb{F}^{-k} \sum_{a \neq 0} |\widehat{X}(a)| \leq (1/n) \cdot |\mathbb{F}|^{-k}.$$

Thus $|\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)| \geq (1 - 1/n)\mathbb{F}^{m-k} = (1 - 1/n)\mathbb{F}^{(1-\epsilon)m}$ and $|S| = |\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)|^{n/m} \geq (1/e) \cdot |\mathbb{F}|^{(1-\epsilon)n}$. $\qquad\square$

We now prove the second item of the 'Moreover' part of Theorem 3.2 in which we assume that at least k of the degrees $d_1, \ldots, d_n$ are co-prime to $|\mathbb{F}| - 1$ and use this extra condition to obtain a precise quantity for the size of S. In Section 4 we show that this condition on the degrees is relatively easy to satisfy if we are the ones choosing the field $\mathbb{F}$.

Claim 3.6. *If at least k of the degrees $d_1, \ldots, d_m$ are co-prime to $|\mathbb{F}^*| = |\mathbb{F}| - 1$ then $|\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)| = |\mathbb{F}|^{m-k}$. This implies $|S| = |\mathbb{F}|^{(1-\epsilon)n}$.*

Proof. Let $\mathbf{V}_{\mathbb{F}} = \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)$. Let $d_{j_1}, \ldots, d_{j_k}$ be degrees among $d_1, \ldots, d_m$ co-prime to $|\mathbb{F}| - 1$ and let $J = \{j_1, \ldots, j_k\}$. We will show that for any setting of $\{x_j : j \notin J\}$ there exists a unique setting of $\{x_j : j \in J\}$ which makes $x \in \mathbf{V}_{\mathbb{F}}$. This will clearly show that $|\mathbf{V}_{\mathbb{F}}| = |\mathbb{F}|^{m-k}$ as claimed.

Substitute $x_j = c_j \in \mathbb{F}$ for all $j \notin J$. We have that $x \in \mathbf{V}_{\mathbb{F}}$ if

$$\sum_{j \in J} A_{i,j} \cdot x_j^{d_j} = -\sum_{j \notin J} A_{i,j} \cdot c_j^{d_j} \qquad \forall i \in [k].$$

Let A' be the $k \times k$ minor of A given by restricting A to columns in J. Let $y = (x_{j_1}^{d_{j_1}}, \ldots, x_{j_k}^{d_{j_k}})$ and let $b \in \mathbb{F}^k$ be given by $b_i = -\sum_{j \notin J} A_{i,j} \cdot c_j^{d_j}$. Then $x \in \mathbf{V}_{\mathbb{F}}$ if

$$A'y = b.$$

We have that A' is regular since A is strongly regular; hence there exists a unique solution $y \in \mathbb{F}^k$ for the linear system $A'y = b$. We now apply our assumption that each degree d_{j_i} is co-prime to $|\mathbb{F}^*| = |\mathbb{F}| - 1$. This implies that raising to the d_{j_i} power in $\mathbb{F}$ is an automorphism of $\mathbb{F}^*$. That is, for each y_i there exists a unique solution to $x_{j_i}^{d_{j_i}} = y_i$ where $x_{j_i} \in \mathbb{F}$. $\qquad\square$

4 Explicitness of the construction

In this section we discuss the explicitness of our construction of subspace evasive sets. The construction of everywhere-finite varieties accomplished in Theorem 2.4 is given as the zero set of explicitly defined polynomials. One can use our construction over any finite field, including $\mathbb{F} = \mathbb{F}_{2^\ell}$ which is convenient for applications. The construction requires an explicit strongly regular $k \times n$ matrix A. Such a matrix can be easily obtained when $|\mathbb{F}| > n$ by taking $A_{i,j} = \gamma_j^i$ where $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ are n nonzero distinct elements in $\mathbb{F}$ (this is because each $k \times k$ sub-matrix is a Vandermonde matrix).

4.1 Efficient encoding of vectors as elements of S

It is trivial to decide in polynomial time if a given point $x \in \mathbb{F}^n$ is in S or not. The first non-trivial issue regarding explicitness is how to sample an element of the set uniformly. More precisely, for an evasive set $S \subset \mathbb{F}^n$ of size $|\mathbb{F}|^r$ we would like to have an efficiently computable bijection $\varphi : \mathbb{F}^r \mapsto S$. This is needed for the list-decoding application (see Section 5) because we would like to encode

messages as strings in S without losing much in the rate of the code and so that we can efficiently recover the original messages from their representation as elements of S. We now show how one can sample from the variety $\mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)$ efficiently (this is enough since the construction of evasive sets is a Cartesian product of such sets). We show this is simple when at least k of the degrees $d_1, \ldots, d_m$ are co-prime to $|\mathbb{F}| - 1$ (we will show below that this condition is easy to obtain).

Claim 4.1. *Assume that at least k of the degrees $d_1, \ldots, d_m$ are co-prime to $|\mathbb{F}| - 1$. Then there is an easy to compute bijection $\varphi : \mathbb{F}^{m-k} \to \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k) \subset \mathbb{F}^m$. Moreover, there are $m - k$ coordinates in the output of φ that compute the identity mapping $Id : \mathbb{F}^{m-k} \mapsto \mathbb{F}^{m-k}$.*

Proof. The proof is similar to the proof of Claim 3.6. Let $d_{j_1}, \ldots, d_{j_k}$ be degrees among $d_1, \ldots, d_m$ co-prime to $|\mathbb{F}| - 1$ and let $J = \{j_1, \ldots, j_k\}$. We showed in Claim 3.6 that for any setting for $\{x_j : j \notin J\}$ there exists a unique setting of $\{x_j : j \in J\}$ which makes $x \in \mathbf{V}_{\mathbb{F}}(f_1, \ldots, f_k)$. We now show that given this setting, the values of $\{x_j : j \in J\}$ can be found efficiently. Thus taking φ to be the identity map from $\mathbb{F}^{m-k}$ to $\mathbb{F}^{[m] \setminus J}$ and completing it uniquely to $\mathbb{F}^m$ will give the required map. As we showed in Claim 3.6 we have $x_{j_i}^{d_{j_i}} = y_j$ where $y = (y_1, \ldots, y_m)$ is a unique solution to a linear system $A'y = b$, where A', b are easy to compute and A' is regular. The value of y can be found by solving a linear system; and the value of x_{j_i} can be retrieved since $x_{j_i} = y_j^{e_j}$ where e_j is the inverse of d_{j_i} modulo $|\mathbb{F}| - 1$ (which exists by assumption). $\qquad\square$

4.2 Computing the intersection with a given subspace

Another important explicitness issue is how to efficiently compute the intersection of a (k, c)-subspace evasive set $S \subset \mathbb{F}^n$ with a given affine subspace H of dimension k. This question comes up in the list-decoding application when we obtain a subspace (given in some basis) that is supposed to contain all possible decodings of a corrupted codeword and we wish to 'filter-out' this subspace to obtain the list of elements in it that are also in S. One way of doing this is to go over all elements in H and to check for each whether or not it is in S (in our case by evaluating the k polynomials and checking that they are all zero). Using the specific structure of our construction we can do much better and output the set $S \cap H$ in polynomial time in the size of the intersection.

Claim 4.2. *Let $S \subset \mathbb{F}^n$ be the (k, c)-subspace evasive set constructed in Theorem 3.2 (for some choice of the parameter m and degrees $d_1 > \ldots > d_m$). There exists an algorithm that, given a basis for any affine subspace H of dimension k, outputs $S \cap H$ in time polynomial in the output size.*

Proof. This follows from powerful algorithms that can solve a system of polynomial equations (over finite fields) in time polynomial in the size of the output, *provided that the number of solutions is finite in the algebraic closure* (i.e the 'zero-dimensional' case). See for example [Laz92, FGLM93]. In our basic construction of an everywhere finite variety, given as the common zero set of k polynomials $f_1, \ldots, f_k$ in n variables $x_1, \ldots, x_n$, the intersection with a k dimensional affine subspace reduces to solving a system of k equations in k variables – simply substitute $x_i = \ell_i(t_1, \ldots, t_k)$, where H is the image of the degree one map $\ell : \mathbb{F}^k \mapsto \mathbb{F}^n$. For the construction of the evasive set (which is the direct product of these simple varieties) we can use an iterative argument (similar to the proof of Theorem 3.2). Recall that in our construction we partitioned the set of coordinates into consecutive blocks of length m – each containing an independent copy of a the variety $\mathbf{V}(f_1, \ldots, f_k)$. In the

first step we solve a system of equations for the projection of H on the first m coordinates. If the dimension of this projection is r_1 then this step will take time polynomial in $(d_1)^{r_1}$ which is the bound on the number of solutions. For every fixing of the first m coordinates to a solution obtained in this step, we reduce the dimension of H by r_1 and obtain a new subspace H' on the remaining coordinates. Continuing in the same fashion with H' on the second block we can compute all solutions in time $\mathsf{poly}((d_1)^{r_1}) \cdot \mathsf{poly}((d_1)^{r_2}) \cdot \cdots \cdot \mathsf{poly}((d_1)^{r_\ell})$, where $r_1 + r_2 + \ldots + r_\ell = k$. This will add up to a total of $\mathsf{poly}((d_1)^k)$ running time, which is polynomial in the number of solutions. $\quad\square$

4.3 Generating a field with k degrees co-prime to $|\mathbb{F}| - 1$

We now address the condition, appearing in Theorem 3.2 and in Claim 4.1, that at least k of the degrees $d_1 > \ldots > d_m$ used in the construction are co-prime to $|\mathbb{F}| - 1$. We will want to satisfy this condition, while still maintaining am reasonable bound on d_1 (which is important since it determines the intersection size with subspaces). For certain fields it may be the case that $|\mathbb{F}| - 1$ has many small divisors, in which case d_1 might have to be large. However, if one has the freedom of 'picking' the field size (as we do in the application to list-decoding) then this problem can be avoided. In essence, we need a (deterministic) way of generating a field $\mathbb{F}$ of size within some specified range and with at least k small integers co-prime to $|\mathbb{F}| - 1$. The best bound on the k integers is $O(k)$ which can be obtained, for example, using 'safe' primes or primes of the form $2q+1$ for q prime. Since we do not know how to find a safe prime in a specified range (or even to show that infinitely many such primes exist!) we will have to resort to an asymptotically weaker bound as is given by the following claim.

Claim 4.3. *There exists a constant $C > 0$ such that the following holds: There is a deterministic algorithm that, given integer inputs k, n so that $n > k^{C \log \log k}$, runs in $\mathsf{poly}(n)$ time and returns a prime p and k integers $k^{C \log \log k} > d_1 > d_2 > \ldots > d_k > 1$ such that:*

> *1. For all $i \in [k]$, $\gcd(p - 1, d_i) = 1$.*

> *2. $n < p \leq n \cdot k^{C \log \log k}$.*

Proof. Let K be the product of the first $\lceil \log_2(k + 1) \rceil$ odd primes. By the prime number theorem, $K < k^{C' \log \log k}$ for some constant $C' > 0$. Let $K > d_1 > \ldots > d_k$ be k distinct odd divisors of K. We will show how to chose the prime p as in the claim using results on the distribution of primes in arithmetic progressions (see [IK04] for more details). Property 1. will follow if our prime p will satisfy the congruence $p = 2 \mod K$. Since K and 2 are co-prime, we know (see [IK04]) that the number of primes smaller than x satisfying this congruence is asymptotically $\frac{1}{\phi(K)} \cdot \frac{x}{\ln x}$, where ϕ is Euler's totient function. From this it follows that there exists a prime in the range $[n, 2nK]$ that satisfies the congruence $p = 2 \mod K$ and, consequently, $p - 1$ is co prime to all the divisors of K. Finding this p in time polynomial in n is trivial since we can just try all integers in the range and test them for primality. $\quad\square$

5   Proof of Theorem 2

In [Gur11], Guruswami considers an explicit family of codes (folded Reed-Solomon codes) that are defined as the image of an explicit mapping

$$\mathcal{C} : \mathbb{F}^n \to (\mathbb{F}^r)^{m/r}$$

where $\mathbb{F} = \mathbb{F}_q$ is any finite field of size q and $1 \leq m \leq q - 1$ is a multiple of r. Since our application is black-box (and applies to any code that shares the decoding properties listed below, such as the codes from [GW11]) we omit the precise description of the code and refer the reader to [Gur11] for more details on the actual definition of C.

In this setting, n is the message length, $\Sigma = \mathbb{F}^r$ is the alphabet, $N = m/r$ is the block length and $R = n/m$ is the rate. Let $\epsilon > 0$ be a sufficiently small constant and set $k \approx 1/\epsilon$ and $r \approx 1/\epsilon^2$. Guruswami shows (Theorem 7 in [Gur11]) that for the above choice of parameters:

1. The mapping $\mathcal{C}$ can be computed in polynomial time.

2. There exists a polynomial time algorithm that, given $y \in (\mathbb{F}^r)^{m/r}$, returns a basis to a subspace $H \subset \mathbb{F}^n$ of dimension k which contains all points $x \in \mathbb{F}^n$ whose encoding $\mathcal{C}(x)$ has normalized hamming distance at most $1 - R - \epsilon$ from y. (In fact, this algorithm runs in time quadratic in its output length.)

We now describe how to combine this code C with our construction of subspace evasive sets (Theorem 3.2) to obtain a code C' with shorter list size and without loosing too much in the decoding radius. Let $S \subset \mathbb{F}^n$ be a $(k, c = c(k, \epsilon))$ subspace-evasive set obtained from Theorem 3.2. Using Claim 4.3, we can construct a finite field $\mathbb{F}$ of size between n and $O_\epsilon(n)$ so that the first k degrees $d_1, d_2, \ldots, d_k$ used in the construction are co-prime to $|\mathbb{F}| - 1$. From Claim 4.1 we know that there is an efficiently computable bijection $\varphi : \mathbb{F}^{(1-\epsilon)n} \to S \subset \mathbb{F}^n$. Consider the composed code $\mathcal{C}' : \mathbb{F}^{(1-\epsilon)n} \to (\mathbb{F}^r)^{m/r}$ defined as

$$\mathcal{C}'(x) = \mathcal{C}(\varphi(x)).$$

Let R' denote the rate of C'. Then

$$R' = (1 - \epsilon)n/m = (1 - \epsilon) \cdot R \geq R - \epsilon.$$

First, we claim that the composed code $\mathcal{C}'$ can be list-decoded with list size $c(1/\epsilon, \epsilon) = (1/\epsilon)^{O(1/\epsilon)}$ from a fraction

$$1 - R - \epsilon \geq 1 - R' - 2\epsilon$$

of errors. This is since for every $y \in (\mathbb{F}^r)^{m/r}$, the subspace $H \subset \mathbb{F}^n$ returned by the list-decoding algorithm for $\mathcal{C}$ contains at most c messages who lie in S.

In order to maintain the efficiency of encoding and list-decoding of $\mathcal{C}'$, we need to guarantee three properties:

(i) Encoding: the map φ should be computable in polynomial time.

(ii) Decoding: the inverse map φ^{-1} should be computable in polynomial time.

14

(iii) List-decoding: for every subspace $H \subset \mathbb{F}^n$ of dimension s, we can find in polynomial time the intersection $S \cap H \subset \mathbb{F}^n$.

The first two items are guaranteed by Claim 4.1, and the third by Claim 4.2. Using the property that the decoded given by Guruswami runs in quadratic time we get that the composed code C' can be list-decoded (with the above parameters) in quadratic time (for all constant $\epsilon > 0$). This completes the proof of Theorem 3.2.

6 Acknowledgments

References

[BSZ11]   E. Ben-Sasson and N. Zewi. From affine to two-source extractors via approximate duality. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 177–186, New York, NY, USA, 2011. ACM.

[FGLM93] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *J. Symb. Comput.*, 16:329–344, October 1993.

[GR08]   V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *Information Theory, IEEE Transactions on*, 54(1):135 –150, 2008.

[Gur11]   V. Guruswami. Linear-algebraic list decoding of folded reed-solomon codes. *Computational Complexity, Annual IEEE Conference on*, 0:77–85, 2011.

[GW11]   V. Guruswami and C. Wang. Optimal rate list decoding via derivative codes. In *APPROX-RANDOM*, pages 593–604, 2011.

[IK04]   H. Iwaniec and E. Kowalski. *Analytic number theory.* Colloquium Publications. American Mathematical Society, 2004.

[KSY11]   S. Kopparty, S. Saraf, and S. Yekhanin. High-rate codes with sublinear-time decoding. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 167–176, New York, NY, USA, 2011. ACM.

[Laz92]   D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13(2):117 – 131, 1992.

[PR04]   P. Pudlák and V. Rödl. Pseudorandom sets and explicit construction of Ramsey graphs. *Quaderni di Matematica*, 13:327–346, 2004.

[PV05] F. Parvaresh and A. Vardy. Correcting errors beyond the guruswami-sudan radius in polynomial time. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '05, pages 285–294, Washington, DC, USA, 2005. IEEE Computer Society.

[Sch95] J. Schmid. On the affine bezout inequality. *Manuscripta Mathematica*, 88(1):225–232, 1995.

[Sch04] W.M. Schmidt. *Equations over finite fields: an elementary approach.* Kendrick Press, 2004.

[Sha94] I. R. Shafarevich. *Basic algebraic geometry.* Springer-Verlag New York, Inc., New York, NY, USA, 1994.

[Wei48] A. Weil. Sur les courbes algebriques et les varietes qui s'en deduisent. *Actualities Sci. et Ind.*, (1041), 1948.

A Fourier analysis

Let $\mathbb{F}$ be a finite field. An additive character (e.g. Fourier basis) of $\mathbb{F}$ is a function $\chi : \mathbb{F} \to \mathbb{C}$ such that $\chi(x+y) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{F}$. The set of characters form an orthogonal basis of functions from $\mathbb{F}$ to $\mathbb{C}$. Let $e_p(x) := e^{2\pi i x/p}$. The set of characters of $\mathbb{F} = \mathbb{F}_{p^\ell}$ for p prime and $\ell \geq 1$ is given by $\chi_a(x) = e_p(\mathrm{Tr}(ax))$ for $a \in \mathbb{F}_{p^\ell}$, where the trace $\mathrm{Tr} : \mathbb{F}_{p^\ell} \to \mathbb{F}_p$ is defined as $\mathrm{Tr}(x) = \sum_{i=0}^{e-1} x^{p^i}$. The constant function 1 is a trivial character for any field; any other character is called non-trivial. More generally, the characters of the vector space $\mathbb{F}^m$ are given by $\chi_a(x) = e_p(\mathrm{Tr}(\langle a, x \rangle))$ where $a = (a_1, \ldots, a_m) \in \mathbb{F}^m$, $x = (x_1, \ldots, x_m) \in \mathbb{F}^m$ and $\langle a, x \rangle = a_1 x_1 + \ldots + a_m x_m$.

Let X be a random variable taking values in $\mathbb{F}^m$. Its Fourier coefficients $\widehat{X}(a)$ for $a \in \mathbb{F}^m$ are given by

$$\widehat{X}(a) := \sum_{x \in \mathbb{F}^m} \Pr[X = x]\chi_a(x);$$

and for any $x \in \mathbb{F}^m$, the Fourier inversion formula gives that

$$\Pr[X = x] = |\mathbb{F}|^{-m} \sum_{a \in \mathbb{F}^m} \widehat{X}(a)\overline{\chi_a(x)}.$$

Character sums The following result by Weil [Wei48] (see also [Sch04]) is a strong tool which gives a bound on the average of a nontrivial character evaluated over the output of a low degree polynomial.

Theorem A.1 (Weil)**.** *Let $f(x)$ be a non-constant degree d polynomial over a finite field $\mathbb{F}$. Let $\chi : \mathbb{F} \to \mathbb{C}$ be a nontrivial additive character. Then $|\mathbb{E}_{x \in \mathbb{F}}[\chi(x)]| \leq \frac{d-1}{\sqrt{|\mathbb{F}|}}$.*