Electronic Colloquium on Computational Complexity, Report No. 60 (2013)

Explicit Subspace Designs

Venkatesan Guruswami[*] Swastik Kopparty[†]

March 2013

Abstract

A subspace design is a collection $\{H_1, H_2, \ldots, H_M\}$ of subspaces of $\mathbb{F}_q^m$ with the property that no low-dimensional subspace W of $\mathbb{F}_q^m$ intersects too many subspaces of the collection. Subspace designs were introduced by Guruswami and Xing (STOC 2013) who used them to give a randomized construction of optimal rate list-decodable codes over constant-sized large alphabets and sub-logarithmic (and even smaller) list size. Subspace designs are the only non-explicit part of their construction. In this paper, we give explicit constructions of subspace designs with parameters close to the probabilistic construction, and this implies the first deterministic polynomial time construction of list-decodable codes achieving the above parameters.

Our constructions of subspace designs are natural and easily described, and are based on univariate polynomials over finite fields. Curiously, the constructions are very closely related to certain good list-decodable codes (folded RS codes and univariate multiplicity codes). The proof of the subspace design property uses the polynomial method (with multiplicities): Given a target low-dimensional subspace W, we construct a nonzero low-degree polynomial P_W that has several roots for each H_i that non-trivially intersects W. The construction of P_W is based on the classical Wronskian determinant and the folded Wronskian determinant, the latter being a recently studied notion that we make explicit in this paper. Our analysis reveals some new phenomena about the zeroes of univariate polynomials, namely that polynomials with many structured roots or many high multiplicity roots tend to be linearly independent.

1 Introduction

This paper gives explicit constructions of certain pseudorandom objects known as subspace designs. A collection of linear subspaces $H_1, \ldots, H_M$ of the vector space $\mathbb{F}_q^m$ is called an (s, A)-subspace design if for every s-dimensional space $W \subseteq \mathbb{F}_q^m$, at most A of the H_i intersect W non-trivially. Being a subspace design is a kind of "well-spread-out" property, and so a random collection of linear spaces turns out to be a good subspace design with high probability. Like in the case of many other such design-like objects (error-correcting codes, combinatorial designs, expander graphs, dimension expanders, subspace-evasive sets), the main challenge is to develop techniques that can analyze this "well-spread-out" phenomenon, and to use this to give explicit constructions of such objects.

[*] Computer Science Department, Carnegie Mellon University, Pittsburgh, PA. Email: `guruswami@cmu.edu`. Research supported in part by a Packard Fellowship and NSF CCF-0963975.

[†] Departments of Mathematics & Computer Science, Rutgers University, New Brunswick, NJ. Email: `swastik.kopparty@rutgers.edu`

ISSN 1433-8092

Subspace designs were defined in a recent paper of Guruswami and Xing [10], who gave a randomized polynomial time (or a deterministic quasipolynomial time) construction of efficiently list-decodable error-correcting codes of optimal rate over *constant size* alphabets with *nearly-constant* list-size (the exact parameters are discussed below). The only step of their construction which required randomness/quasipolynomial time was in constructing appropriate subspace designs to pick a subcode of the underlying algebraic-geometric code. Using explicit subspace designs, we can make this construction deterministic polynomial time. This implies the *first explicit construction* for optimal rate list decoding over constant-sized (large) alphabets and a near-constant list size.

Starting with the constructions of Parvaresh-Vardy [16], and Guruswami-Rudra [7], there have been several recent works [6, 8, 12, 9, 10] constructing successively improved list-decodable error-correcting codes with rate R which can correct $(1 - R - \varepsilon)$ fraction errors in polynomial time. We do not survey the parameters of all these constructions here, and instead point the interested reader to the introductions of [10] or [11]. Below we mention the "maximal" results which are not dominated in terms of parameters, and then discuss the impact of this work on them. (The results are for $n^{O(1)}$ time list decoding up to error fraction $1 - R - \varepsilon$ with rate R; n refers to the block length of the code which we assume, for ease of notation when stating asymptotic bounds, to be sufficiently large compared to $1/\varepsilon$.)

1. For randomized (Monte Carlo) constructions that work with high probability, subcodes based on hierarchical subspace evasive (h.s.e) sets of folded algebraic-geometric codes [9] or AG codes with evaluation points with coordinates in a subfield [10], achieve constant alphabet size (of $\exp(\tilde{O}(1/\varepsilon^2))$) and constant list size (of $O(1/\varepsilon)$). The alphabet size is nearly best possible ($\exp(1/\varepsilon)$ being a lower bound), and the list size matches the bound achieved by pure random codes.

2. For explicit (deterministic polynomial time) constructions, subcodes based on subspace-evasive sets of folded Reed-Solomon or multiplicity codes [8, 3], achieve constant list size of $(1/\varepsilon)^{O(1/\varepsilon)}$ and an alphabet size $n^{O(1/\varepsilon^2)}$. [1]

3. With a quasi-polynomial time construction, subcodes based on cascaded subspace designs of certain AG codes [10], achieve constant alphabet size (of $\exp(\tilde{O}(1/\varepsilon^2))$) and a near-constant list size of $\exp_{1/\varepsilon}\Big(\exp\big(O((\log^* n)^2)\big)\Big)$. (Here $\exp_a(x)$ denotes a^x.)

Plugging in our explicit subspace design into [10], we obtain a deterministic polynomial time construction of the subcodes mentioned in Part 3 above (we lose another exponent in the list size bound, but it remains a very slowly growing function):

Theorem 1. *For every $R \in (0, 1)$ and $\varepsilon > 0$, there is a deterministic polynomial time constructible family of error-correcting codes of rate R over an alphabet of size $(1/\varepsilon)^{O(1/\varepsilon^2)}$ that can be list decoded in $n^{O(1)}$ time from a fraction $(1-R-\varepsilon)$ of errors, outputting a list of size at most $\exp_{1/\varepsilon}\Big(\exp_{1/\varepsilon}\big(\exp(O(\log^* n))\big)\Big)$ where n is block length of the code.*

The above yields the *first deterministic* polynomial time construction of codes of rate R over constant-sized alphabets that can be list decoded in $n^{O(1)}$ time up to an error fraction $(1 - R - \varepsilon)$ with a list size that is nearly a constant (say, sub-logarithmic in the code length). We note that this result blends the better

[1] One can bring down the alphabet size to $\exp(\tilde{O}(1/\varepsilon^4))$ using expanders and code concatenation [7], but this would make the construction and decoding complexity $n^{\Omega(1/\varepsilon^2)}$, whereas we would like the complexity to be $O(n^c)$ for a fixed c independent of ε.

aspects of the parameters mentioned in Parts 1 and 2 above: it achieves constant alphabet size like 1, and a deterministic construction like 2, with a list size that only slightly super-constant.

Using our subspace designs in the Reed-Solomon based construction of [10], we can also get explicit subcodes of Reed-Solomon codes that can be list decoded up to a radius $1 - R - \varepsilon$. This result is stated in Section 6 where the applications of subspace designs to list decoding from [10] are described.

We conclude this discussion by noting that an *explicit* construction of codes for list decoding up to error fraction $1-R-\varepsilon$ with rate R in $n^{O(1)}$ time, that achieve alphabet size and list size *both* constants depending on ε, remains an open problem.

1.1 Techniques behind our subspace design construction and analysis

Suppose we are looking for an (s, A) subspace design $H_1, \dots, H_M \subseteq \mathbb{F}_q^m$ where each H_i has codimension εm. The probabilistic method guarantees the existence of such a subspace design with $M = q^{\Omega(\varepsilon m)}$ and $A = O(\frac{s}{\varepsilon})$ (and in fact these parameters are essentially optimal). Our main result gives explicit (s, A) subspace designs, with each subspace in the design having codimension εm, with $A = \frac{s}{\varepsilon}$ and $M = q^{\Omega(\varepsilon m/s)}$. Crucially, these constructions also work when $q = O(1)$, and this is what enables the application to list-decoding via [10].

We now give a brief overview of our constructions. The motivating example comes from the $s = 1$ case. Here the problem is to find a collection of subspaces such that no nonzero point of $\mathbb{F}_q^m$ is in too many of them. One well known construction for this problem is based on the moment curve: let $\alpha_1, \dots, \alpha_M$ be distinct elements of $\mathbb{F}_q$, and define

$$H_i = \{x \in \mathbb{F}_q^m \mid \langle x, v_{\alpha_i} \rangle = 0\},$$

where $v_\alpha \in \mathbb{F}_q^m$ equals $(1, \alpha, \dots, \alpha^{m-1})$. Then using the fact that a nonzero polynomial cannot have more roots than its degree, no nonzero point of $\mathbb{F}_q^m$ will lie $\geqslant m$ of these subspaces. Equivalently, this can be viewed as follows: we identify $\mathbb{F}_q^m$ with the space of all univariate $\mathbb{F}_q$ polynomials of degree $< m$; then H_i equals the space of all polynomials that vanish at the point α_i. Our constructions will be natural generalizations of this.

We present two algebraic constructions of subspace designs, both using only elementary properties of polynomials and finite fields. The constructions are closely related to certain algebraic error-correcting codes: folded Reed-Solomon codes, and multiplicity codes. Curiously enough, both these codes have very good list-decoding properties, but this seems to be a coincidence; as far as we know their list-decodability does not have any formal relation with the fact that subspace designs eventually get used in the construction of good (in fact, even better) list-decodable codes.

We describe the *simplest special cases* of our constructions below. The first of these constructions requires the underlying field to be large, while the second requires the field to have large characteristic. Later we will use a concatenation-like trick to transform constructions from big fields to small fields.

1. **Construction based on folded Reed-Solomon codes:** Identify $\mathbb{F}_q^m$ with the space of all polynomials $P(X)$ of degree $< m$. Let $\gamma \in \mathbb{F}_q^*$ be a generator. Define $t = \varepsilon m$. For $i \in \{0, 1, \dots, \frac{q}{t} - 1\}$, define:

$$H_i = \{P(X) \mid P(\gamma^{it+j}) = 0 \text{ for each } 0 \leqslant j < t\}.$$

2. **Construction based on multiplicity codes:** Identify $\mathbb{F}_q^m$ with the space of all polynomial $P(X)$ of degree $< m$. Define $t = \varepsilon m$. For $\alpha \in \mathbb{F}_q$, define:

$$H_\alpha = \{P(X) \mid P \text{ vanishes with multiplicity at least } t \text{ at } \alpha\}.$$

These construction both have the property that for every subspace $W \subseteq \mathbb{F}_q^m$ of dimension s, the number of subspaces H_i or H_α which intersect W is at most $O(\frac{s}{\varepsilon})$. While the above constructions have $\leqslant q$ spaces in them, both of them admit generalizations using extension fields of $\mathbb{F}_q$, and this gives exponentially large subspace designs.

The analyses of these constructions use the polynomial method/method of multiplicities. For every subspace $W \subseteq \mathbb{F}_q^m$ of dimension s we define a nonzero low-degree polynomial P_W. In the first construction, P_W which has the property that for every H_i in the subspace design that intersects W, P_W vanishes at all points in a large set S_i (where the S_i are all pairwise disjoint). This implies that there cannot be too many H_i in the first construction which intersect W. In fact, a more refined statement holds — P_W must vanish with multiplicity at least $\dim(W \cap H_i)$ at each point in S_i, yielding a "strong" subspace design (defined in Section 2). In the second construction, P_W has the property that for every H_α in the subspace design that intersects W, P_W vanishes at α with high multiplicity (here too, the multiplicity is proportional to $\dim(W \cap H_\alpha)$, giving a strong subspace design). This implies that there cannot be too many H_α in the second construction which intersect W.

The definition of the relevant P_W in the second construction uses a classical linear independence criterion for polynomials based on the Wronskian determinant. For the first construction, we use a different linear independence criterion, based on something which we call the folded Wronskian determinant.

We also would like to point out an interesting algebraic consequence of our results (in particular, the analysis of the second construction). Let $\mathbb{F}$ be a field (possibly infinite) with characteristic $> m$. Suppose we have a collection of polynomials $P_1(X), \ldots, P_s(X) \in \mathbb{F}[X]$ of degree at most m. For each $i \in [s]$, the number of points $\alpha \in \mathbb{F}$ at which $P_i(X)$ vanishes with multiplicity at least t is at most $\frac{m}{t}$. By a union bound, the number of points $\alpha \in \mathbb{F}$ at which some $P_i(X)$ vanishes with multiplicity at least t is at most $\frac{m}{t} \cdot s$. It is easy to see that this bound is tight. Now suppose we ask how many points α can there be such that some element of the *span* of $P_1(X), \ldots, P_s(X)$ vanishes with multiplicity at least t at α. A naive union bound would suggest that the answer is $|\mathbb{F}|^s \cdot \frac{m}{t}$. Our results imply that the number of such α is at most $\frac{m}{t-s+1} \cdot s$. Thus for $t \gg s$, the number of such points almost does not change when we include the full span of the polynomials $P_1(X), \ldots, P_s(X)$. This expresses some kind of linear independence of polynomials which have many disjoint high-multiplicity zeroes.

Remark: Our constructions are both of the following form: Fix a collection $R_1(X), \ldots, R_M(X)$ of pairwise relatively prime polynomials of degree εm. Define $H_i = \{P(X) \mid R_i(X) \text{ divides } P(X)\}$. One may be tempted to conjecture that any such collection is a $(s, O_{s,\varepsilon}(1))$ subspace design. This turns out to be false, and we give a counterexample in Appendix B. Note that any such collection of H_i is slightly design-like: no nonzero point of $\mathbb{F}_q^m$ is in more than $\frac{1}{\varepsilon}$ of these spaces. But the property of being a subspace design seems to lie deeper.

2 Subspace designs: Definitions and result statements

We being by formally defining weak and strong subspace designs. Both notions are very natural, and our basic constructions will be strong subspace designs. En route to constructing strong subspace designs over small fields (which is what is needed for the list-decoding application), our arguments will deal with weak subspace designs too.

Definition 2 (Weak subspace designs)**.** *A collection $\mathcal{H}$ of $\mathbb{F}_q$-subspaces $H_1, \dots, H_M \subseteq \mathbb{F}_q^m$ is called a (s, A) weak subspace design over $\mathbb{F}_q$, if for every $\mathbb{F}_q$-linear space $W \subset \mathbb{F}_q^m$ of dimension s, the number of $i \in \{1, 2, \dots, M\}$ for which $\dim_{\mathbb{F}_q}(H_i \cap W) > 0$ is at most A.*

Definition 3 (Strong subspace designs)**.** *A collection $\mathcal{H}$ of $\mathbb{F}_q$-subspaces $H_1, \dots, H_M \subseteq \mathbb{F}_q^m$ is called a (s, A) strong subspace design over $\mathbb{F}_q$, if for every $\mathbb{F}_q$-linear space $W \subset \mathbb{F}_q^m$ of dimension s, we have*

$$\sum_{i=1}^{M} \dim_{\mathbb{F}_q}(H_i \cap W) \leqslant A \, .$$

Strong and weak subspace designs have following (trivial) relations:

- Every (s, A) strong subspace design over $\mathbb{F}_q$ is also an (s, A) weak subspace design over $\mathbb{F}_q$.
- Every (s, A) weak subspace design over $\mathbb{F}_q$ is also an (s, sA) strong subspace design over $\mathbb{F}_q$.

We will be focusing on subspace designs consisting of subspaces of codimension εm for some constant $\varepsilon > 0$. Using the probabilistic method one can show the existence of exponentially large strong (and hence weak) subspace designs consisting of subspaces of codimension εm.

Lemma 4 (Probabilistic construction of subspace designs [10])**.** *Let $\varepsilon > 0$ and q be a prime power. Let s, m be integers such that $m \geqslant 8/\varepsilon$ and $s \leqslant \varepsilon m/2$. Consider a collection $\mathcal{H}$ of subspaces of $\mathbb{F}_q^m$ obtained by picking, independently at random, $q^{\varepsilon m/8}$ subspaces of $\mathbb{F}_q^m$ of dimension $(1 - \varepsilon)m$ each. Then, with probability at least $1 - q^{-ms}$, $\mathcal{H}$ is an $(s, 8s/\varepsilon)$ strong subspace desifn.*

We will be interested in explicit constructions of subspace designs. For this we need to talk about sequences $(q_j, m_j, \mathcal{H}_j)$, where $\mathcal{H}_j$ is a collection of M_j subspaces of $\mathbb{F}_{q_j}^{m_j}$ which forms a (s_j, A_j) subspace design. We say a sequence of subspace designs is *explicit* if there is an algorithm which given j, produces bases for all spaces in $\mathcal{H}_j$ in time $\mathrm{poly}(q_j, m_j, M_j)$.

We now state our main theorems on the explicit construction of subspace designs. The first theorem gives an explicit construction of exponentially large strong subspace designs over growing fields. The second theorem gives an explicit construction of exponentially large weak subspace designs over significantly smaller fields (in particular, this theorem is interesting even for fields of size 2 or $O(1)$, and will be useful for the main list-decoding application).

Theorem 5 (Explicit strong subspace designs)**.** *For every $\varepsilon \in (0, 1)$, positive integers s, m with $s \leqslant \varepsilon m/4$, and a prime power $q > m$, there exists an explicit collection of $M = q^{\Omega(\varepsilon m/s)}$ subspaces in $\mathbb{F}_q^m$, each of codimension at most εm, which form a $(s, \frac{2s}{\varepsilon})$ strong subspace design.*

Theorem 6 (Explicit weak subspace designs)**.** *For every $\varepsilon \in (0, 1)$, positive integers s, m with $s \leqslant \varepsilon m/4$, and a prime power q satisfying $\frac{2s}{\varepsilon} < q^{\varepsilon m/(2s)}$, there exists an explicit collection of $M \geqslant q^{\Omega(\varepsilon m/s)}/(2s)$ subspaces in $\mathbb{F}_q^m$, each of codimension at most εm, which form a $(s, \frac{s}{\varepsilon})$ weak subspace design.*

These theorems will all be based on our main technical theorem, stated below.

Theorem 7 (Main). *For all positive integers s, r, t, m and prime powers q satisfying $s \leqslant t \leqslant m < q$, there is an explicit collection of $M = \Omega(\frac{q^r}{rt})$ spaces $H_1, \ldots, H_M \subseteq \mathbb{F}_q^m$, each of codimension rt, which forms a $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$ strong subspace design.*

Proof of Theorem 5: Using $t = 2s$ and $r = \lfloor \frac{\varepsilon m}{2s} \rfloor$, we get an explicit collection of $M \geqslant q^{\Omega(\varepsilon m/s)}/(\varepsilon m)$ subspaces, each of codimension at most εm, which forms a $(s, \frac{2s}{\varepsilon})$ strong subspace design. □

To get our weak subspace design, we use the following lemma which shows that subspace designs over an extension field can be used to construct a *weak* subspace design over the base field. Unfortunately this conversion need not preserve the strong subspace design property.

Lemma 8. *Suppose $G_1, \ldots, G_M \subseteq \mathbb{F}_{q^r}^m$ are $\mathbb{F}_{q^r}$-linear spaces, each of codimension t, which form an (s, A) weak subspace design over $\mathbb{F}_{q^r}$.*

Pick any $\mathbb{F}_q$-linear isomorphism $\varphi : \mathbb{F}_{q^r}^m \to \mathbb{F}_q^{rm}$. Via this isomorphism, we get a collection of $\mathbb{F}_q$-linear spaces $H_1 = \varphi(G_1), \ldots, H_M = \varphi(G_M) \subseteq \mathbb{F}_q^{rm}$, each of codimension rt.

This collection forms an (s, A) weak subspace design over $\mathbb{F}_q$.

Proof. Let $W \subseteq \mathbb{F}_q^{rm}$ be a subspace of dimension s. Let W' equal the $\mathbb{F}_{q^r}$-span of $\varphi^{-1}(W)$. If $P_1, \ldots, P_s$ form an $\mathbb{F}_q$-basis for W, then $\varphi^{-1}(P_1), \ldots, \varphi^{-1}(P_s)$ will $\mathbb{F}_{q^r}$-span W', and so W' will have dimension at most s. Thus the number of G_i which intersect W' nontrivially is at most A.

We now claim that $\dim_{\mathbb{F}_q}(H_i \cap W) > 0$ implies that $\dim_{\mathbb{F}_{q^r}}(G_i \cap W') > 0$ (which would complete the proof). Equivalently, we claim that if there is a nonzero element in $H_i \cap W$, then there is a nonzero element in $G_i \cap W'$. But this is obvious, since

$$\{0\} \subsetneq \varphi^{-1}(H_i \cap W) = \varphi^{-1}(H_i) \cap \varphi^{-1}(W) = G_i \cap \varphi^{-1}(W) \subseteq G_i \cap W' \ . \qquad \square$$

Proof of Theorem 6: The plan is as follows. We will first construct a strong subspace design over a large field $\mathbb{F}_{q^a}$ via Theorem 7. This is automatically a weak subspace design over $\mathbb{F}_{q^a}$. Then via the above lemma, we will get a weak subspace design over $\mathbb{F}_q$.

Let $a = \lfloor \frac{\varepsilon m}{2s} \rfloor$. Let $q' = q^a$, $r' = 1$, $m' = \lfloor \frac{2s}{\varepsilon} \rfloor$, $t' = 2s$, $s' = s$. Note that $m' < q'$. By Theorem 7 (applied with parameters $q', \varepsilon', r', m', s', t'$), we get a collection of $M = \Omega(q'/t')$ many $\mathbb{F}_{q'}$-subspaces $G_1, \ldots, G_M \subseteq \mathbb{F}_{q'}^{m'}$, each of codimension t', which forms a $(s, \frac{m's'}{r'(t'-s'+1)} = m')$ strong, and hence weak, subspace design over $\mathbb{F}_{q'}$.

By the above lemma, this gives us a collection of $M \geqslant q^{\Omega(\varepsilon m/s)}/(2s)$ many $\mathbb{F}_q$-subspaces $H_1, \ldots, H_M \subseteq \mathbb{F}_q^{m'a} \subseteq \mathbb{F}_q^m$, each of codimension $\leqslant \varepsilon m$, which forms a $(s, \frac{2s}{\varepsilon})$ weak subspace design. This completes the proof of Theorem 6. □

Organization of this paper. Towards the task of proving Theorem 7, we present two families of related constructions, one based on Folded Reed-Solomon codes, and another based on Multiplicity codes. The multiplicity code constructions are strictly weaker; they can only prove Theorem 7 when the field size condition $|\mathbb{F}_q| > m$ is replaced by the characteristic condition $\mathrm{char}(\mathbb{F}_q) > m$. Theorem 7 as stated follows from Theorem 14 in Section 4.2.

The next section discusses some preliminaries on polynomials, derivatives, multiplicities and Wronskians. We then describe our constructions in Sections 4 and 5. The consequence of our constructions for list decoding of subcodes of Reed-Solomon and algebraic-geometric codes is described in Section 6.

3 Preliminaries

For a field $\mathbb{F}$, let $\mathbb{F}[X]$ denote the ring of polynomials in the variable X over $\mathbb{F}$, and let $\mathbb{F}[X]^{<m}$ denote the $\mathbb{F}$-linear space of polynomials of degree $< m$.

We will use some simple properties of derivatives and multiplicities of univariate polynomials. For a polynomial $P(X) \in \mathbb{F}[X]$, we define its i^{th} (Hasse) derivative $P^{(i)}(X) \in \mathbb{F}[X]$ by the equation:

$$P(X+Z) = \sum_{i=0}^{\infty} P^{(i)}(X) Z^i.$$

This notion of derivative is closely related to the i^{th} iterated usual formal derivative, but behaves better over fields of small characteristic.

We define the multiplicity of vanishing of P at a point $\alpha \in \mathbb{F}$, $\mathsf{mult}(P, \alpha)$ to be the smallest $i \geqslant 0$ such that $P^{(i)}(\alpha) \neq 0$. The key fact that we need about multiplicities is that low degree polynomials cannot have too many zeroes, counting multiplicity:

$$\sum_{\alpha \in \mathbb{F}} \mathsf{mult}(P, \alpha) \leqslant \deg(P).$$

For a discussion of the basic properties of the Hasse derivative, see [2, Section 2].

Our proofs will use the fact that linear independence of polynomials can be captured by a polynomial. We now describe two such linear independence criteria.

Definition 9 (Classical Wronskian)**.** *Let* $P_1(X), \ldots, P_s(X) \in \mathbb{F}[X]$.
We define their Wronskian*,* $W(P_1, \ldots, P_s)(X) \in \mathbb{F}[X]$*, by:*

$$W(P_1, \ldots, P_s)(X) \stackrel{\text{def}}{=} \begin{pmatrix} P_1(X) & \cdots & P_s(X) \\ P_1^{(1)}(X) & \cdots & P_s^{(1)}(X) \\ \vdots & \ddots & \vdots \\ P_1^{(s-1)}(X) & \cdots & P_s^{(s-1)}(X) \end{pmatrix}$$

Lemma 10 (Wronskian criterion for linear independence)**.** *Let* $m < \operatorname{char}(\mathbb{F})$*, and let* $P_1(X), \ldots, P_s(X) \in \mathbb{F}[X]^{<m}$*. Then* $P_1(X), \ldots, P_s(X)$ *are linearly independent over* $\mathbb{F}$ *if and only if the Wronskian determinant* $\det(W(P_1, \ldots, P_s)(X)) \neq 0$.

This dates back to the 19th century [14]. See [5, 1] for some recent variations and proofs. The switch between usual derivatives and Hasse derivatives multiplies the Wronskian determinant by a constant, which is nonzero as long as $m < \operatorname{char}(\mathbb{F})$, and thus this criterion works with both notions.

We will actually require a linear independence criterion over fields of small characteristic. The following definition is an analogue of the classical Wronskian which serves this purpose.

Definition 11 (Folded Wronskian)**.** *Let* $P_1(X), \ldots, P_s(X) \in \mathbb{F}[X]$*. Let* $\gamma \in \mathbb{F}^*$*. We define their* γ-folded Wronskian*,* $W_\gamma(P_1, \ldots, P_s)(X) \in \mathbb{F}[X]$*, by:*

$$W_\gamma(P_1, \ldots, P_s)(X) \stackrel{\text{def}}{=} \begin{pmatrix} P_1(X) & \cdots & P_s(X) \\ P_1(\gamma X) & \cdots & P_s(\gamma X) \\ \vdots & \ddots & \vdots \\ P_1(\gamma^{s-1} X) & \cdots & P_s(\gamma^{s-1} X) \end{pmatrix}$$

Lemma 12 (Folded Wronskian criterion for linear independence)**.** *Let $m < |\mathbb{F}| = q$, let $\gamma \in \mathbb{F}^*$ be a generator, and let $P_1(X), \ldots, P_s(X) \in \mathbb{F}_q[X]^{<m}$. Then $P_1(X), \ldots, P_s(X)$ are linearly independent over $\mathbb{F}_q$ if and only if the Folded Wronskian determinant* $\det W_\gamma(P_1, \ldots, P_s)(X) \neq 0$.

This lemma is implicit in the work of Guruswami-Wang [8] and Forbes-Shpilka [4]. Since this is not explicitly stated in this form, and it is quite short, we give a proof in Appendix A.

The above linear independence criteria are in terms of the determinant of a matrix of univariate polynomials. Let $M(X)$ be an $s \times s$ matrix with each entry $M_{jk}(X)$ being a polynomial in the variable X. Let $L(X) = \det(M(X))$. We will be using the following formula for the derivatives of $L(X)$:

$$L^{(\ell)}(X) = \sum_{i_1,\ldots,i_s \geqslant 0 | \sum_{c=1}^{s} i_c = \ell} \det(M^{(i_1,\ldots,i_s)}(X)),$$

where $M^{(i_1,\ldots,i_s)}(X)$ is the matrix whose j,k entry equals $M_{jk}^{(i_j)}(X)$ (in words: $M^{(i_1,\ldots,i_s)}(X)$ is the matrix obtained from $M(X)$ by taking i_j^{th} derivative of the j'th row, for each j).

4 Constructions from Folded Reed-Solomon Codes

In this section we describe our constructions based on folded Reed-Solomon codes.

4.1 The basic construction

To illustrate the main ideas in a simple setting, we begin with a basic construction that corresponds to the $r = 1$ case of Theorem 7 (and further we will only show the weak subspace design property even though the strong property also holds, see Section 4.2). Let $s \leqslant t \leqslant m < q$ be integer parameters, with q being a prime power. Let $V = \mathbb{F}_q^m = \mathbb{F}_q[X]^{<m}$ be the $\mathbb{F}_q$-vector space of polynomials of degree $< m$. Let γ be a generator of $\mathbb{F}_q^*$.

Let $\mathcal{F} = \{\gamma^{jt} \mid j \in \{0, 1, \ldots, \lfloor q/t \rfloor\}$. For each $\alpha \in \mathcal{F}$, consider the subspace

$$H_\alpha = \{P(X) \in V \mid P(\alpha \cdot \gamma^i) = 0 \text{ for each } i \in \{0, 1, \ldots, t-1\}\} .$$

Note that H_α has codimension exactly t in V.

The final construction in the next subsection will work by picking α from an extension field $\mathbb{F}_{q^r}$.

Theorem 13. *The collection of subspace $(H_\alpha)_{\alpha \in \mathcal{F}}$ is a $\left(s, \frac{(m-1)s}{t-s+1}\right)$ weak subspace design.*

Proof. Let $W \subseteq \mathbb{F}_q^m$ be a subspace of dimension s. Let $P_1, \ldots, P_s \in \mathbb{F}_q[X]$ be a basis for W.

Define the $t \times s$ matrix of polynomials

$$M(X) \stackrel{\text{def}}{=} \begin{pmatrix} P_1(X) & \cdots & P_s(X) \\ P_1(\gamma X) & \cdots & P_s(\gamma X) \\ \vdots & \ddots & \vdots \\ P_1(\gamma^{t-1} X) & \cdots & P_s(\gamma^{t-1} X) \end{pmatrix} \tag{1}$$

Let $A(X)$ be the top $s \times s$ submatrix of $M(X)$. Notice that this is precisely the folded Wronskian $W_\gamma(P_1, \dots, P_s)(X)$. Now let $L(X) \in \mathbb{F}_q[X]$ be the determinant of $A(X)$, which we know is a nonzero polynomial by Lemma 12 (here we use that $q > m$).

Suppose $\alpha \in \mathcal{F}$ is such that $\dim_{\mathbb{F}_q}(W \cap H_\alpha) > 0$. This means that the columns of $M(\alpha)$ are linearly dependent over $\mathbb{F}_q$. Therefore, $\operatorname{rank}(A(\alpha)) \leqslant \operatorname{rank}(M(\alpha)) < s$, implying that $L(\alpha) = 0$. Further, for $0 \leqslant i \leqslant t-s$, $A(\alpha \cdot \gamma^i)$ is a submatrix of $M(\alpha)$ for $i < t-s+1$, so that $\operatorname{rank}(A(\alpha \cdot \gamma^i)) \leqslant \operatorname{rank}(M(\alpha)) < s$. Thus $L(\alpha \cdot \gamma^i) = 0$ for $0 \leqslant i \leqslant t-s$. Thus each α such that $\dim_{\mathbb{F}_q}(W \cap H_\alpha) > 0$ gives $t-s+1$ distinct roots in $\mathbb{F}_q$ for $L \in \mathbb{F}_q[X]$ which is a nonzero polynomial of degree at most $(m-1)s$. Hence there can be at most $\frac{(m-1)s}{t-s+1}$ choices of $\alpha \in \mathcal{F}$ for which $W \cap H_\alpha$ is non-trivial. □

4.2 An improved construction

Let s, t, r, q, m be parameters. Let $s \leqslant t \leqslant m < q$. Let $V = \mathbb{F}_q^m = \mathbb{F}_q[X]^{<m}$.

Let $\gamma \in \mathbb{F}_q$ be a generator of $\mathbb{F}_q^*$. For $\alpha \in \mathbb{F}_{q^r}$, let $S_\alpha \subseteq \mathbb{F}_{q^r}$ be given by:

$$S_\alpha = \{\alpha^{q^j}\gamma^i \mid 0 \leqslant j < r, 0 \leqslant i < t\}.$$

Also define

$$S'_\alpha = \{\alpha^{q^j}\gamma^i \mid 0 \leqslant j < r, 0 \leqslant i < t-s+1\}.$$

Let $\mathcal{F} \subseteq \mathbb{F}_{q^r}$ be a large set such that:

- Each $\alpha \in \mathcal{F}$ is such that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$.
- For distinct $\alpha, \beta \in \mathcal{F}$, the sets S_α and S_β are disjoint.
- Each S_α has cardinality rt.

We may take $\mathcal{F}$ to be of size $\Omega(\frac{q^r}{rt})$. (In the next subsection 4.3 we discuss how to choose such an $\mathcal{F}$ efficiently.) Note that for $\alpha \in \mathcal{F}$, each S'_α has cardinality $r(t-s+1)$, and the S'_α are all pairwise disjoint.

For each $\alpha \in \mathcal{F}$, consider the subspace

$$H_\alpha = \{P(X) \in V \mid P(\alpha \cdot \gamma^j) = 0 \text{ for each } j \in \{0, 1, \dots, t-1\}\}.$$

Note that H_α has codimension exactly rt in V. Therefore, Theorem 7 follows from the result below.

Theorem 14. *The collection of subspace $(H_\alpha)_{\alpha \in \mathcal{F}}$ is a $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$ strong subspace design.*

Proof. Let $W \subseteq \mathbb{F}_q^m$ be a subspace of dimension s. Let $P_1, \dots, P_s \in \mathbb{F}_q[X]$ be a basis for W. Recall the matrix of polynomials $M(X)$ defined in (1). We have the following claim relating the $\mathbb{F}_q$-dimension of $W \cap H_\alpha$ to the rank of the matrix $M(\alpha)$.

Claim 15. *The matrix $M(\alpha) \in \mathbb{F}_{q^r}^{t \times s}$ satisfies*

$$\operatorname{rank}(M(\alpha)) \leqslant s - \dim_{\mathbb{F}_q}(W \cap H_\alpha).$$

Proof. This follows easily from the equalities:

$$\begin{aligned}
\dim_{\mathbb{F}_q}(W \cap H_\alpha) &= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid \forall i \in \{0, 1, \ldots, t-1\}, \sum_{j=1}^{s} a_j P_j(\alpha\gamma^i) = 0\}) \\
&= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid M(\alpha) \cdot a = 0\}) \\
&= \dim_{\mathbb{F}_q}(\ker_{\mathbb{F}_{q^r}}(M(\alpha)) \cap \mathbb{F}_q^s) \\
&\leqslant \dim_{\mathbb{F}_{q^r}}(\ker(M(\alpha))) \\
&= s - \operatorname{rank}(M(\alpha)).
\end{aligned}$$

Above, in the last but one step we used the fact that for any $\mathbb{F}_{q^r}$-linear space $S \subseteq \mathbb{F}_{q^r}^s$, we have $\dim_{\mathbb{F}_q}(S \cap \mathbb{F}_q^s) \leqslant \dim_{\mathbb{F}_{q^r}}(S)$; this fact follows easily after putting a basis for S in echelon form. □

As before, let $A(X)$ be the top $s \times s$ submatrix of $M(X)$, and $L \in \mathbb{F}_q[X]$ be the determinant of $A(X)$. We know that $L \neq 0$ (by virtue of Lemma 12 and the assumption $q > m$) and $\deg(L) \leqslant (m-1) \cdot s$.

Next we show that L vanishes with multiplicity proportional to $\dim(W \cap H_\alpha)$ at each $\beta \in S'_\alpha$.

Claim 16. *For each $\beta \in S'_\alpha$,*

$$\mathsf{mult}(L, \beta) \geqslant \dim(W \cap H_\alpha).$$

Proof. Since $L \in \mathbb{F}_q[X]$, we have $\mathsf{mult}(L, \beta) = \mathsf{mult}(L, \beta^q)$. Therefore, it suffices to prove the claim for β of the form $\alpha\gamma^i$ for $i < t - s + 1$. For each $\ell < \dim(W \cap H_\alpha)$, we will show that the ℓ'th derivative $L^{(\ell)}$ of L vanishes at β. This will prove the claim.

Note that $\operatorname{rank}(A(\beta)) = \operatorname{rank}(A(\alpha\gamma^i)) \leqslant \operatorname{rank}(M(\alpha))$ since $A(\alpha\gamma^i)$ is a submatrix of $M(\alpha)$ when $i < t - s + 1$. Furthermore, $\operatorname{rank}(M(\alpha)) \leqslant s - \dim(W \cap H_\alpha)$ (by Claim 15). Any matrix which has at least $s - \ell$ rows in common with $A(\beta)$ has rank $\leqslant s - \dim(W \cap H_\alpha) + \ell < s$, and therefore has determinant 0.

Now $L^{(\ell)}(X)$ is a sum of determinants, each of which has at least $s - \ell$ rows in common with $A(X)$. By the above discussion, each determinant in the expansion of $L^{(\ell)}(\beta)$ equals 0, and so $L^{(\ell)}(\beta) = 0$, as desired. □

Putting everything together, we get that:

$$(m-1)s \geqslant \sum_{\beta \in \bigcup_{\alpha \in \mathcal{F}} S'_\alpha} \mathsf{mult}(L, \beta) \geqslant \sum_{\alpha \in \mathcal{F}} \sum_{\beta \in S'_\alpha} \dim(W \cap H_\alpha) = r \cdot (t - s + 1) \cdot \sum_{\alpha \in \mathcal{F}} \dim(W \cap H_\alpha),$$

which completes the proof of Theorem 14. □

4.3 Explicitness

We want to produce bases for all the H_i in time $\operatorname{poly}(q^r)$. In $\operatorname{poly}(q, r)$ time we can construct a presentation of the finite field $\mathbb{F}_{q^r}$. Then in $\operatorname{poly}(q^r)$ time we can construct a large $\mathcal{F}$ as follows: greedily include into $\mathcal{F}$ elements $\alpha \in \mathbb{F}_{q^r}$ with $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$ such that $S(\alpha)$ is disjoint from $S(\beta)$ for every β already included in $\mathcal{F}$.

In fact, one can generate a suitable $\mathcal{F}$ in $\mathrm{poly}(q, r)$ space and $\mathrm{poly}(q^r)$ time. For simplicity we will describe it when r is prime, so that every element $\alpha \in \mathbb{F}_{q^r} \setminus \mathbb{F}_q$ satisfies $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$. It suffices to give a procedure, which when given $\alpha \in \mathbb{F}_{q^r}$, can decide in time $\mathrm{poly}(q, r)$ whether α should be included in $\mathcal{F}$.

For $\alpha, \beta \in \mathbb{F}_{q^r} \setminus \mathbb{F}_q$, say that α is equivalent to β if $\beta \in \alpha^{q^j}\mathbb{F}_q$ for some $0 \leqslant j < r$. This is an equivalence relation. Given α, we can in time $\mathrm{poly}(q, r)$ enumerate all the elements equivalent to α. Then we may choose the lexicographically smallest element of this equivalence class α_0. We decide to include $\alpha \in \mathcal{F}$ as follows: Suppose $\alpha = \alpha_0^{q^j} \cdot \gamma^a$, where $0 \leqslant j < r$ and $0 \leqslant a \leqslant q - 2$. Then we include $\alpha \in \mathcal{F}$ if and only if $j = 0$ and a is of the form it, with $i \leqslant \frac{(q-1)}{t} - 1$. It is easy to see that this procedure generates a valid $\mathcal{F}$.

Once we have constructed $\mathcal{F}$, the spaces H_α are specified completely, and we can easily get bases for them.

5 Constructions based on multiplicity codes

In this section we describe our constructions based on univariate multiplicity codes. As mentioned earlier, these constructions work only in fields of large characteristic.

5.1 The basic construction

Let s, t, q, m be parameters. Let $s \leqslant t \leqslant m < \mathrm{char}(\mathbb{F}_q)$. Let $V = \mathbb{F}_q^m = \mathbb{F}_q[X]^{<m}$.

For each $\alpha \in \mathbb{F}_q$ consider the subspace $H_\alpha = \{P(X) \in V \mid \mathsf{mult}(P, \alpha) \geqslant t\}$. Note that H_α has codimension exactly t in V.

Theorem 17. *For every $\mathbb{F}_q$-subspace $W \subseteq V$ with $\dim(W) = s$, we have*

$$\sum_{\alpha \in \mathbb{F}_q} \dim(H_\alpha \cap W) \leqslant \frac{(m-1)s}{(t-s+1)}.$$

Proof. Let $P_1, \ldots, P_s \in \mathbb{F}_q[X]$ be a basis for W. For a nonnegative integer i, $v_i(X)$ be the row vector $(P_1^{(i)}(X), P_2^{(i)}(X), \ldots, P_s^{(i)}(X))$ consisting of the i'th derivations of $P_1, \ldots, P_s$. For a tuple $(i_1, \ldots, i_k)$ of nonnegative integers, let $M_{(i_1,\ldots,i_k)}(X)$ be the $k \times s$ matrix with whose j^{th} row equals $v_{i_j}(X)$. Finally, let $M(X)$ be the $t \times s$ matrix $M_{(0,1,\ldots,t-1)}(X)$, i.e.,

$$M(X) \stackrel{\text{def}}{=} \begin{pmatrix} P_1(X) & \cdots & P_s(X) \\ P_1'(X) & \cdots & P_s'(X) \\ \vdots & \ddots & \vdots \\ P_1^{(t-1)}(X) & \cdots & P_s^{(t-1)}(X) \end{pmatrix} \tag{2}$$

If $W \cap H_\alpha$ is nontrivial, then there exists a nonzero linear combination of the columns of $M(X)$ that vanishes at α. In other words, the matrix $M(\alpha) \in \mathbb{F}_q^{t \times s}$ is singular. The following claim shows that $\dim_{\mathbb{F}_q}(W \cap H_\alpha)$ precisely equals the dimension of the null space of $M(\alpha)$ over $\mathbb{F}_q$.

Claim 18. $\mathrm{rank}(M(\alpha)) = s - \dim_{\mathbb{F}_q}(W \cap H_\alpha)$.

Proof. This follows easily from the equalities:

$$\begin{aligned}\dim_{\mathbb{F}_q}(W \cap H_\alpha) &= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid \mathsf{mult}(\sum_j a_j P_j, \alpha) \geqslant t\}) \\ &= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid \forall i < t, \sum_{j=1}^{s} a_j P_j^{(i)}(\alpha) = 0\}) \\ &= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid M(\alpha) \cdot a = 0\}) \\ &= \dim(\ker_{\mathbb{F}_q}(M(\alpha))) \\ &= s - \operatorname{rank}(M(\alpha))\ . \end{aligned}$$

□

Now let $L(X) \in \mathbb{F}_q[X]$ be the determinant of the top $s \times s$ submatrix of $M(X)$. Notice that this submatrix is in fact the Wronskian of $P_1, \ldots, P_s$. Since the characteristic of $\mathbb{F}_q$ is larger than m, the Wronskian criterion for linear independence implies that $L(X)$ is a nonzero polynomial. Also, clearly $\deg(L) \leqslant (m-1) \cdot s$.

Next we show that L vanishes with multiplicity proportional to $\dim(H_\alpha \cap W)$ at each $\alpha \in \mathbb{F}_q$.

Claim 19.

$$\mathsf{mult}(L, \alpha) \geqslant (t - s + 1) \cdot \dim(W \cap H_\alpha).$$

Proof. For each $\ell < (t - s + 1) \cdot \dim(W \cap H_\alpha)$, we will show that $L^{(\ell)}(\alpha) = 0$. This will prove the claim. We have:

$$L^{(\ell)}(X) = \sum_{i_0 + i_1 + \ldots + i_{s-1} = \ell} \det(M_{(i_0, 1+i_1, 2+i_2, \ldots, (s-1)+i_{s-1})}(X)). \tag{3}$$

Since $\ell < (t - s + 1) \cdot \dim(W \cap H_\alpha)$, we know that for every $i_0, \ldots, i_{s-1}$ with $\sum i_j = \ell$, there are less than $\dim(W \cap H_\alpha)$ values of $j \in \{0, 1, \ldots, s-1\}$ such that $j + i_j \geqslant t$. Hence, the matrix $M_{(i_0, 1+i_1, 2+i_2, \ldots, (s-1)+i_{s-1})}(\alpha)$ has more than $s - \dim(W \cap H_\alpha)$ rows in common with $M(\alpha)$, and so by Claim 18 it does not have full rank. It follows that each term in the expansion (3) of $L^{(\ell)}(\alpha)$ equals 0, and so $L^{(\ell)}(\alpha) = 0$. □

Putting everything together, we get that:

$$(m-1)s \geqslant \deg(L) \geqslant \sum_{\alpha \in \mathbb{F}_q} \mathsf{mult}(L, \alpha) \geqslant (t - s + 1) \cdot \sum_{\alpha \in \mathcal{F}} \dim(W \cap H_\alpha),$$

as desired. □

5.2 An improved construction

Let s, t, q, m, r be parameters as in the previous section. We assume $s \leqslant t \leqslant m < \operatorname{char}(\mathbb{F}_q)$. Let $V = \mathbb{F}_q^m = \mathbb{F}_q[X]^{<m}$.

We now obtain a collection of many more subspaces compared to Section 5.1 by picking α from an extension field $\mathbb{F}_{q^r}$.

Let $\mathcal{F}_0$ be the subset of $\mathbb{F}_{q^r}$ consisting of elements α such that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$. Note that $|\mathcal{F}_0| \approx q^r(1 - o(1))$. The elements of $\mathcal{F}_0$ can be partitioned into sets of cardinality r, each set consisting of mutual conjugates over $\mathbb{F}_q$. Let $\mathcal{F}$ be a set formed by choosing exactly one element from each of these sets. Thus $|\mathcal{F}| \approx \frac{q^r}{r}$. The construction of $\mathcal{F}$ here is simpler than in Section 4.2 and discussed in Section 5.3. For each $\alpha \in \mathcal{F}$ consider the subspace $H_\alpha = \{P(X) \in V \mid \mathsf{mult}(P, \alpha) \geqslant t\}$. Note that H_α has codimension exactly tr in V.

Theorem 20. *For every $\mathbb{F}_q$-subspace $W \subseteq V$ with $\dim(W) = s$, we have*

$$\sum_{\alpha \in \mathcal{F}} \dim(H_\alpha \cap W) \leqslant \frac{(m-1)s}{r(t-s+1)}.$$

Proof. Let $P_1, \ldots, P_s \in \mathbb{F}_q[X]$ be a basis for W. We define the matrix $M(X)$ as in (2).

Similarly to Claim 18, we show that the dimension of $W \cap H_\alpha$ is *upper bounded* by the dimension of the null space of $M(\alpha)$.

Claim 21. *For each $\alpha \in \mathcal{F}$,*

$$\operatorname{rank}(M(\alpha)) \leqslant s - \dim_{\mathbb{F}_q}(W \cap H_\alpha)\ .$$

Proof. This follows easily from the equalities:

$$\begin{aligned}
\dim_{\mathbb{F}_q}(W \cap H_\alpha) &= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid \forall i < t, \sum_{j=1}^{s} a_j P_j^{(i)}(\alpha) = 0\}) \\
&= \dim_{\mathbb{F}_q}(\{(a_1, \ldots, a_s) \in \mathbb{F}_q^s \mid M(\alpha) \cdot a = 0\}) \\
&= \dim_{\mathbb{F}_q}(\ker_{\mathbb{F}_{q^r}}(M(\alpha)) \cap \mathbb{F}_q^s) \\
&\leqslant \dim_{\mathbb{F}_{q^r}}(\ker(M(\alpha))) \\
&= s - \operatorname{rank}(M(\alpha)).
\end{aligned}$$

(Here we used the fact that for any $\mathbb{F}_{q^r}$-linear space $S \subseteq \mathbb{F}_{q^r}^s$, we have $\dim_{\mathbb{F}_q}(S \cap \mathbb{F}_q^s) \leqslant \dim_{\mathbb{F}_{q^r}}(S)$; this fact follows easily after putting a basis for S in echelon form). □

Defining $L \in \mathbb{F}_q[X]$ be the determinant of the top $s \times s$ submatrix of $M(X)$, i.e., the Wronskian of $P_1, \ldots, P_s$, we have that L is a nonzero polynomial of degree at most $(m-1)s$.

The following claim is *exactly* similar to Claim 19.

Claim 22. *For $\alpha \in \mathcal{F}$, we have*

$$\mathsf{mult}(L, \alpha) \geqslant (t - s + 1) \cdot \dim(W \cap H_\alpha)\ .$$

Finally, we notice that as $L \in \mathbb{F}_q[X]$, L vanishes with the same multiplicity at all the other $r - 1$ conjugates of α too. Putting everything together, we get that:

$$(m-1)s \geqslant \sum_{\alpha \in \mathcal{F}_0} \mathsf{mult}(L, \alpha) = \sum_{\alpha \in \mathcal{F}} r \cdot \mathsf{mult}(L, \alpha) \geqslant r \cdot (t - s + 1) \cdot \sum_{\alpha \in \mathcal{F}} \dim(W \cap H_\alpha),$$

which completes the proof of Theorem 20. □

5.3 Explicitness

Here the explicitness is even easier. In time $\mathrm{poly}(q, r)$ we can construct a presentation for the finite field $\mathbb{F}_{q^r}$. Then for each element α, we compute its r conjugates α^{q^j} with $0 \leqslant j < r$, and we include α in $\mathcal{F}$ if and only if it is lexicographically smallest amongst its conjugates.

Once we have constructed $\mathcal{F}$, the spaces H_α are specified completely, and we can easily get bases for them.

6 Consequences for list decoding via [10]

In this section, we briefly recall the connection of subspace designs to algebraic list decoding from [10]. There are two such results in [10], one for Reed-Solomon codes and another for algebraic-geometric codes. In each case, subspace designs are used to pick subcodes of these codes that enable reducing the size of the list output by the decoder.

Reed-Solomon subcodes. Let us discuss the simpler application to Reed-Solomon (RS) codes. Consider the RS code of length q over $\mathbb{F}_{q^m}$ consisting of evaluations of polynomials $f(X) = f_0 + f_1 X + \cdots + f_{k-1} X^{k-1} \in \mathbb{F}_{q^m}[X]$ of degree $< k \leqslant q$ at points in $\mathbb{F}_q$. Thus the encoding only consists of evaluations of the polynomial on a subfield. The construction in [10] picks a subcode where the coefficients of the polynomials are restricted to subspaces from a subspace design. Formally, they show that if $f_i \in H_i$ for $\mathbb{F}_q$-subspaces $H_0, H_1, \ldots, H_{k-1}$ that form an (s, A) strong subspace design, then the subcode can be list decoded by a linear-algebraic algorithm from up to $\frac{s}{s+1}(q - k)$ errors, pinning down messages to an $\mathbb{F}_q$-subspace of dimension A. If $\dim(H_i) = (1 - \varepsilon)m$ for each i, then the rate of the subcode is $(1 - \varepsilon)k/q$. So the error fraction list decoded is $\frac{s}{s+1}\left(1 - \frac{R}{1-\varepsilon}\right)$ which is at least $1 - R - O(\varepsilon)$ if one picks $s = O(1/\varepsilon)$.

If we pick $m = \Omega(s/\varepsilon)$, then we can apply Theorem 5 and find explicit subspaces $H_0, H_1, \ldots, H_{k-1}$ (note that $k \leqslant q$) which form an $(s, O(s/\varepsilon))$ strong subspace design. When combined with the abovementioned reslt from [10], we will get the following:

Theorem 23. *For all $R \in (0, 1)$, $\varepsilon > 0$, and all prime powers $q \geqslant \Omega(1/\varepsilon^2)$, there are* explicit *$\mathbb{F}_q$-linear subcodes of RS codes over $\mathbb{F}_{q^{O(1/\varepsilon^2)}}$ that have rate R and block length q, and that are list decodable from error fraction $(1 - R - \varepsilon)$ pinning down messages to a $\mathbb{F}_q$-subspace of dimension $O(1/\varepsilon^2)$. Here explicit means that the code can be constructed in $(q/\varepsilon)^{O(1)}$ time.*

In [10] this subcode was constructed probabilistically via a random subspace design, or deterministically via a derandomization using conditional expectations, which led to a large construction time of $q^{\mathrm{poly}(1/\varepsilon)}$.

Algebraic-geometric subcodes. The algebraic-geometric codes considered in [10] consist of the evaluations of functions from a Riemann-Roch vector space over $\mathbb{F}_{q^m}$ at a set of N $\mathbb{F}_q$-rational points of an algebraic curve. The connection to subspace designs can be described modularly, by abstracting away the specifics of the construction. As in the Reed-Solomon case, the messages can be specified by a k-tuple $(f_0, f_1, \ldots, f_{k-1}) \in (\mathbb{F}_q^m)^k$, and subspace designs are used to pick an $\mathbb{F}_q$-subspace of these tuples. However, in the AG case, the code dimension k will be much bigger than q^m (this is in fact the big draw of AG codes, that they can be much longer than the alphabet size). Due to this, one cannot have a non-trivial subspace design that has k subspaces of $\mathbb{F}_q^m$.

The idea in [10] is to employ a multilevel construction of cascaded subspace designs where one restricts blocks of coefficients, of rapidly increasing sizes, to belong to subspace designs over correspondingly larger dimensions. Let us explain the construction more formally. Assume that $k = n_1 n_2 \ldots n_l$ for positive integers $n_1 \leqslant n_2 \leqslant \ldots \leqslant n_l$ (this is only for notational convenience below; a general value of k can be handled by padding with a small proportion of 0's). This means that for each $i = 1, 2, \ldots, l$, the coefficients $f_0, f_1, \ldots, f_{k-1}$ can be broken into successive blocks of size $N_i \stackrel{\Delta}{=} n_1 n_2 \cdots n_i$. We restrict the coefficients in each such block to belong to subspaces from a subspace design with n_i subspaces of $\mathbb{F}_q^{mN_{i-1}}$ (we define $N_0 = 1$). Formally, let $m_1 = m$, and for $2 \leqslant i \leqslant l$, define $m_i = m_{i-1} n_{i-1}$. For $i = 1, 2, \ldots, l$, let $H_0^{(i)}, H_1^{(i)}, \ldots, H_{n_i-1}^{(i)} \subset \mathbb{F}_q^{m_i}$ be $\mathbb{F}_q$-subspaces of dimension $(1 - \zeta_i) m_i$ that form an (r_{i-1}, r_i)-strong subspace design (for some sequence of positive integers $r_0 \leqslant r_1 \leqslant \ldots \leqslant r_l$).

Given these subspace designs, the coefficients are restricted as follows. At the first level, $f_j \in H^{(1)}_{j \bmod n_1}$ for $0 \leqslant j < k$. At the next level,we will impose the linear constraints

$$(f_{jn_1}, f_{jn_1+1}, \ldots, f_{(j+1)n_1-1}) \in H^{(2)}_{j \bmod n_2} \text{ for } 0 \leqslant j < k/n_1.$$

In general, for $1 \leqslant i \leqslant l$, we will restrict

$$(f_{jN_{i-1}}, f_{jN_{i-1}+1}, \ldots, f_{(j+1)N_{i-1}-1}) \in H^{(i)}_{j \bmod n_i} \quad \text{for } 0 \leqslant j < k/N_{i-1}\ .$$

These pose a total of at most $\left(\sum_{i=1}^{l} \zeta_i\right) mk$ $\mathbb{F}_q$-linear constraints, so the dimension of the $\mathbb{F}_q$-subspace U consisting of those $(f_0, f_1, \ldots, f_{k-1}) \in \mathbb{F}_q^{mk}$ satisfying these constraints is at least $\left(1 - \sum_{i=1}^{l} \zeta_i\right) mk$.

In [10], a linear-algebraic list decoding algorithm is given for subcodes of the AG codes formed by restricting the coefficients to this subspace U. This algorithm corrects an error fraction $\tau \approx \frac{s}{s+1}(1 - (k + 3g)/N)$ where g is the genus of the function field, and outputs a subspace of dimension r_l that contains all candidate messages, when $r_0 = s - 1$. (Recall that the i'th subspace design above was a (r_{i-1}, r_i)-strong subspace design.) If we pick a function field so that $g/N \ll \varepsilon$, and pick $\zeta_i = \varepsilon/2^i$, the dimension of the subspace U is at least $(1 - \varepsilon)mk$, and the error fraction $\tau \approx \frac{s}{s+1}(1 - R - \varepsilon)$ where R is rate of the subcode. Taking $s \approx 1/\varepsilon$, the list decodable error fraction is at least $1 - R - O(\varepsilon)$.

In [10], by using a probabilistic construction the authors achieved (r_{i-1}, r_i)-strong subspace designs at the i'th level (consisting of subspaces of $\mathbb{F}_q^{m_i}$) of size $n_i \geqslant q^{\sqrt{m_i}}$ and $r_i = O(r_{i-1}/\zeta_i)$. Plugging in $\zeta_i = \varepsilon/2^i$ and $r_0 < s$, leads to the bound

$$r_l \leqslant s \cdot (1/\varepsilon)^{O(\log^*(km))} \cdot 2^{O((\log^*(km))^2)}\ . \tag{4}$$

This is because the lengths n_i grow exponentially in each step, and therefore we will reach a length exceeding mk in at most $\log^*(mk)$ iterations. The construction can also be derandomized in quasi-polynomial time.

Using our explicit construction from Theorem 6, we can explicitly construct a subspace design of size $n_i \geqslant q^{\sqrt{m_i}}$ at the i'th level as in [10], and achieve a slightly weaker guarantee $r_i \leqslant O(r_{i-1}^2/\zeta_i)$ (the quadratic dependence on r_{i-1} is due to the conversion from a weak subspace design guaranteed by Theorem 6 to a strong subspace design). Recalling $r_0 \leqslant s$ and $\zeta_i = \varepsilon/2^i$, this recurrence yields the upper bound $r_l \leqslant O(s/\varepsilon)^{2^l}$. As $l \leqslant \log^*(mk)$, and $s \approx 1/\varepsilon$ for list decoding up to error fraction $(1 - R - O(\varepsilon))$, the bound on the dimension of the space of solutions output by the list decoding algorithm is at most $(1/\varepsilon)^{O(2^{\log^*(mk)})}$. This is exponentially worse than the bound (4) achieved via random constructions in [10], but as $\log^*$ is a very slowly growing function, the list size is "almost" constant. The trade-offs achieved by these codes were formally stated as Theorem 1 in the introduction.

Thus the combination of our subspace design constructions with the methods of [10] yields the first deterministic polynomial time construction of codes of rate R over constant-sized alphabets that can be list decoded up to an error fraction $(1 - R - \varepsilon)$ with a list size that is nearly a constant (say, sub-logarithmic in the code length).

7 Open questions

We conclude with some open questions.

1. Construct $(s, O(s/\varepsilon))$ subspace designs of size $q^{\Omega(\varepsilon m)}$ to match the probabilistic construction of Lemma 4.
2. Over small fields, we only get weak $(s, s/\varepsilon)$ subspace designs, which translate into strong $(s, \frac{s^2}{\varepsilon})$ subspace designs. It would be interesting to get strong $(s, \frac{s}{\varepsilon})$ subspace designs over small fields (the probabilistic construction achieves this).
3. Spreads are a collection of subspaces $H_1, H_2, \ldots, H_M$ of $\mathbb{F}_q^m$ which cover every nonzero point of $\mathbb{F}_q^m$ exactly once. Spreads are classic objects that have found several applications, with recent ones in random network coding [13] and self-repairing codes [15]. Subspace designs are a natural relaxation of the notion of spreads and it will be interesting to find other applications of the concept.
4. Finally, we mention again the question of getting deterministic constructions of codes over constant size alphabet, with rate R, which are list-decodable from $1 - R - \varepsilon$ fraction errors with constant list size in $n^{O(1)}$ time.

Acknowledgments

This work began when we were attending a workshop on complexity theory at Oberwolfach. We thank the organizers for the opportunity to attend the workshop, and acknowledge the hospitality and stimulating environment provided by the Mathematisches Forschungsinstitut Oberwolfach. Many thanks also to Chaoping Xing for useful discussions.

References

[1] Alin Bostan and Philippe Dumas. Wronskians and linear independence. *American Mathematical Monthly*, 117(8):722–727, 2010. 7

[2] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and Mergers. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 181–190. IEEE Computer Society, 2009. 7

[3] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In *Proceedings of the 44th ACM Symposium on Theory of Computing*, pages 351–358, 2012. 2

[4] Michael A. Forbes and Amir Shpilka. On identity testing of tensors, low-rank recovery and compressed sensing. In *Proceedings of the 44th Symposium on Theory of Computing Conference*, pages 163–172, 2012. 8, 18

[5] Arnaldo Garcia and Jose Felipe Voloch. Wronskians and linear independence in fields of prime characteristic. *Manuscripta Mathematica*, 59(4):457–469, 1987. 7

[6] Venkatesan Guruswami. Cyclotomic function fields, Artin-Frobenius automorphisms, and list error-correction with optimal rate. *Algebra and Number Theory*, 4(4):433–463, 2010. 2

[7] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008. 2, 18

[8] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:73, 2012. To appear in IEEE Trans. Info. Theory, 2013. 2, 8, 18

[9] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In *Proceedings of the 44th ACM Symposium on Theory of Computing*, pages 339–350, 2012. 2

[10] Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:146, 2012. Extended abstract to appear in the *Proceedings of the 2013 ACM Symposium on Theory of Computing*. 2, 3, 5, 14, 15, 16

[11] Venkatesan Guruswami and Chaoping Xing. Optimal rate algebraic list decoding using narrow ray class fields. *CoRR*, arXiv:1302.6660 [math.NT], 2013. 2

[12] Swastik Kopparty. List-decoding multiplicity codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:44, 2012. 2

[13] Felice Manganiello, Elisa Gorla, and Joachim Rosenthal. Spread codes and spread decoding in network coding. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 881–885, 2008. 16

[14] Thomas Muir. *A Treatise on the theory of determinants*. Dover books on advanced mathematics. Dover Publications, 1882. 7

[15] Frédérique E. Oggier and Anwitaman Datta. Self-repairing codes for distributed storage - a projective geometric construction. *CoRR*, abs/1105.0379, 2011. 16

[16] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 285–294, 2005. 2

A The Folded Wronskian criterion for linear independence

In this section we give a proof of Lemma 12 (which is implicit in [8] and [4]) using the method of [7].

Proof. First suppose the P_i are linearly dependent over $\mathbb{F}_q$. If $\sum_{i=1}^s a_i P_i(X) = 0$, then for all j, $\sum_{i=1}^s a_i P_i(\gamma^j X) = 0$, and so $W_\gamma(P_1, \ldots, P_s)(X) \cdot \mathbf{a} = 0$. This implies that $\det(W_\gamma(P_1, \ldots, P_s)(X)) = 0$.

Conversely, suppose $\det(W_\gamma(P_1, \ldots, P_s)(X)) = 0$. Then there exist polynomials $A_i(X)$ such that for each $j \in [s]$:

$$\sum_{i=0}^{s-1} A_i(X) P_j(\gamma^i X) = 0.$$

Without loss of generality, we may assume the A_i do not all share a common factor. Now consider the polynomial $E(X) = X^{q-1} - \gamma$, which happens to be irreducible. We have $X^q = \gamma X \mod E(X)$, and so for each $j \in [s]$:

$$\sum_{i=0}^{s-1} A_i(X) P_j(X^{q^j}) = 0 \mod E(X).$$

Because $P_j(X) \in \mathbb{F}_q[X]$, we have $P_j(X^{q^j}) = P_j(X)^{q^j}$. Thus for each $j \in [s]$:

$$\sum_{i=0}^{s-1} A_i(X) P_j(X)^{q^j} = 0 \mod E(X).$$

In fact, we have that for each $P(X) \in \mathrm{span}_{\mathbb{F}_q}(P_1(X), \ldots, P_s(X))$ (i.e., the span of the P_i's over $\mathbb{F}_q$),

$$\sum_{i=0}^{s-1} A_i(X) P(X)^{q^j} = 0 \mod E(X).$$

Now $\mathbb{F}_q[X]/\langle E(X) \rangle \equiv \mathbb{F}_{q^{q-1}}$. Let $A_i(X) \mod E(X) = \alpha_i \in \mathbb{F}_{q^{q-1}}$, and note that not all $\alpha_i = 0$. For $P(X) \in \mathrm{span}_{\mathbb{F}_q}(P_1(X), \ldots, P_s(X))$, let $P(X) \mod E(X) = \beta_P \in \mathbb{F}_{q^{q-1}}$. Since $\deg(P) < m \leqslant q - 1$ and $\deg(E) = q - 1$, all the β_P are distinct. Defining $Q(Y) \in \mathbb{F}_{q^{q-1}}[Y]$ by:

$$Q(Y) = \sum_{i=0}^{s-1} \alpha_i Y^{q^i}.$$

Then $Q(Y)$ is a nonzero polynomial of degree $\leqslant q^{s-1}$ such that for every $P(X) \in \mathrm{span}_{\mathbb{F}_q}(P_1(X), \ldots, P_s(X))$, we have $Q(\beta_P) = 0$. Thus $\mathrm{span}_{\mathbb{F}_q}(P_1(X), \ldots, P_s(X))$ must have size at most q^{s-1}, and so $P_1, \ldots, P_s$ must be linearly dependent over $\mathbb{F}_q$. □

B A counterexample

In this appendix we give an example of a collection of subspaces, very closely related to our constructions of subspace designs, that is not a good subspace design.

As in our constructions, identify $\mathbb{F}_q^{m+1}$ with $\mathbb{F}_q[X]^{\leqslant m}$. Let $t = \varepsilon m$. Let $R_1(X), \ldots, R_M(X)$ be all the irreducible polynomials of degree t. Define

$$H_i = \{P(X) \in \mathbb{F}_q[X]^{\leqslant m} \mid R_i(X) \text{ divides } P(X)\} . \tag{5}$$

Note that each H_i has codimension εm.

Note that our constructions have this general form, though the R_i's are not irreducible. In our basic construction using folded RS codes (Section 4.1), we had $R_\alpha = \prod_{i=0}^{t-1}(X - \alpha\gamma^i)$. In the basic construction using multiplicity codes (Section 5.1), we had $R_\alpha = (X - \alpha)^t$.

We will now show that the above construction (5) need not even be a $(2, c_\varepsilon)$ weak subspace design.

Let us choose the integer m and the prime power q, such that:

1. $(m, q-1) = 1$,
2. $m < q$,
3. $\mathrm{ord}_m(q) = d \approx \varepsilon m$.

Such m, q can be chosen arbitrarily large as follows. First let $r \approx \frac{1}{\varepsilon}$ be an integer. Choose a large prime $m \equiv 1 \mod r$ (such a prime m exists by Dirichlet's theorem). Now we have $r' = (m-1)/r \approx \varepsilon m$, with r' being an integer. Let $a \in \mathbb{Z}_m^*$ be such that the order of a equals r' (such an a exists because r' divides $m-1$). Now choose a large prime $q \equiv a \mod m$ (again, such a prime q exists by Dirichlet's theorem). We then have the desired relation between q and m.

Now let $W = \mathrm{span}\{X^m, 1\}$, which has dimension 2. We will show that there exist at least q spaces H_i which intersect W nontrivially.

For each $\alpha \in \mathbb{F}_q$, the polynomial $X^m - \alpha$ is in W. We will find an $i \in [M]$ for which H_i contains $X^m - \alpha$. Since the $X^m - \alpha$ are pairwise relatively prime, this will complete the proof.

Let $\beta \in \mathbb{F}_q$ be such that $\beta^m = \alpha$ (such a β exists and is unique since $(m, q-1) = 1$, and so the map $x \to x^m$ is a permutation of $\mathbb{F}_q$).

Let ω be a primitive m^{th}-root of unity in the algebraic closure of $\mathbb{F}_q$. Since $\mathrm{ord}_m(q) = d$, we have that ω lies in $\mathbb{F}_{q^d}$.

Now consider the d elements $\beta{\cdot}\omega, \beta{\cdot}\omega^q, \beta{\cdot}\omega^{q^2}, \ldots, \beta{\cdot}\omega^{q^{d-1}}$. They are a complete set of conjugates over $\mathbb{F}_q$, and distinct, and so there is an irreducible polynomial of degree d which has exactly these d elements as roots. Let $R_i(X)$ be that irreducible polynomial. All the d roots of $R_i(X)$ are m^{th} roots of α, and so $R_i(X)$ divides $X^m - \alpha$, and thus H_i contains $X^m - \alpha$, as desired.