Subspace Designs Based on Algebraic Function Fields*

Venkatesan Guruswami[†1], **Chaoping Xing**[‡2], **and Chen Yuan**[3]

1 **Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA**
guruswami@cmu.edu

2 **School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore**
xingcp@ntu.edu.sg

3 **School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore**
yuan0064@e.ntu.edu.sg

Abstract

Subspace designs are a (large) collection of high-dimensional subspaces $\{H_i\}$ of $\mathbb{F}_q^m$ such that for any low-dimensional subspace W, only a small number of subspaces from the collection have non-trivial intersection with W; more precisely, the sum of dimensions of $W \cap H_i$ is at most some parameter L. The notion was put forth by Guruswami and Xing (STOC'13) with applications to list decoding variants of Reed-Solomon and algebraic-geometric codes, and later also used for explicit rank-metric codes with optimal list decoding radius.

Guruswami and Kopparty (FOCS'13, Combinatorica'16) gave an explicit construction of subspace designs with near-optimal parameters. This construction was based on polynomials and has close connections to folded Reed-Solomon codes, and required large field size (specifically $q \geqslant m$). Forbes and Guruswami (RANDOM'15) used this construction to give explicit constant degree "dimension expanders" over large fields, and noted that subspace designs are a powerful tool in linear-algebraic pseudorandomness.

Here, we construct subspace designs over any field, at the expense of a modest worsening of the bound L on total intersection dimension. Our approach is based on a (non-trivial) extension of the polynomial-based construction to algebraic function fields, and instantiating the approach with cyclotomic function fields. Plugging in our new subspace designs in the construction of Forbes and Guruswami yields dimension expanders over $\mathbb{F}^n$ for any field $\mathbb{F}$, with logarithmic degree and expansion guarantee for subspaces of dimension $\Omega(n/(\log\log n))$.

1998 ACM Subject Classification F.2.1 Numerical Algorithms and Problems, F.2.2 Nonnumerical Algorithms and Problems, G.1.3 Numerical Linear Algebra

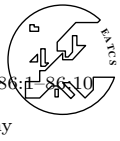
Keywords and phrases Pseudorandomness, algebraic codes, explicit constructions, expanders, linear algebra

Digital Object Identifier 10.4230/LIPIcs.ICALP.2017.86

* A full version of the paper is available at https://arxiv.org/abs/1704.05992.

† Research supported in part by NSF CCF-1422045.

‡ Research supported in part by the Singapore MoE Tier 1 grants RG20/13 and RG25/16.



1 Introduction

An emerging theory of "linear-algebraic pseudorandomness" studies the linear-algebraic analogs of fundamental Boolean pseudorandom objects where the rank of subspaces plays the role of the size of subsets. A recent work [4] studied the interrelationships between several such algebraic objects such as subspace designs, dimension expanders, rank condensers, and rank-metric codes, and highlighted the fundamental unifying role played by *subspace designs* in this web of connections.

Informally, a subspace design is a collection of subspaces of a vector space $\mathbb{F}_q^m$ (throughout we denote by $\mathbb{F}_q$ the finite field with q elements) such that any low-dimensional subspace W intersects only a small number of subspaces from the collection. More precisely:

▶ **Definition 1.** A collection $H_1, H_2, \ldots, H_M$ of b-dimensional subspaces of $\mathbb{F}_q^m$ form an (s, L)-(strong) subspace design, if for every s-dimensional subspace $W \subset \mathbb{F}_q^m$, $\sum_{i=1}^{M} \dim(W \cap H_i) \leqslant L$.

In particular, this implies that at most L subspaces H_i have non-trivial intersection with W. A collection meeting this weaker requirement is called a *weak* subspace design; unless we mention otherwise, by subspace design we always mean a strong subspace design in this paper. One would like the dimension b of each subspace in the subspace design to be large, typically $\Omega(m)$ for applications of interest, L to be small, and the number of subspaces M to be large.

Subspace designs were introduced by the first two authors in [11], where they used them to improve the list size and efficiency of list decoding algorithms for algebraic-geometric codes, yielding efficiently list-decodable codes with optimal redundancy over fixed alphabets and small output list size. A standard probabilistic argument shows that a random collection of subspaces forms a good subspace design with high probability. Subsequently, Guruswami and Kopparty [7] gave an explicit construction of subspace designs, nearly matching the parameters of random constructions, albeit over large fields.

Intriguingly, the construction in [7] was based on algebraic list-decodable codes (specifically folded Reed-Solomon codes). Recall that improving the list-decodability of such codes was the motivation for the formulation of subspace designs in the first place! This is yet another compelling example of the heavily intertwined nature of error-correcting codes and other pseudorandom objects. The following states one of the main trade-offs achieved by the construction in [7].

▶ **Theorem 2** (Folded Reed-Solomon based construction [7]). *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*[1] *collection of $M = q^{\Omega(\varepsilon m/s)}$ subspaces in $\mathbb{F}_q^m$, each of dimension at least $(1 - \varepsilon)m$, which form a $(s, \frac{2s}{\varepsilon})$-(strong) subspace design.*

Note the requirement of the field size q being larger than the ambient dimension m in their construction. To construct subspace designs over small fields, they use a construction over a large extension field $\mathbb{F}_{q^r}$, and view b-dimensional subspaces of $\mathbb{F}_{q^r}^{m'}$ as br-dimensional subspaces of $\mathbb{F}_q^{rm'}$. However, this transformation need not preserve the "strongness" of the subspace design, and an (s, L)-subspace design over the extension field only yields an (s, L)-weak subspace design over $\mathbb{F}_q$.

[1] By explicit, we mean a deterministic construction that runs in time $\text{poly}(q, m, M)$ and outputs a basis for each of the subspaces in the subspace design.

The strongness property is crucial for all the applications of subspace designs in [4]. In particular, the strongness is what drives the construction of dimension expanders (defined below) of low degree. The weak subspace design property does *not* suffice for these applications.

▶ **Definition 3.** A collection of linear maps $A_1, A_2, \ldots, A_d : \mathbb{F}^n \to \mathbb{F}^n$ is said to be a (b, α)-dimension expander if for every subspace V of $\mathbb{F}^n$ of dimension at most b, $\dim(\sum_{i=1}^{d} A_i(V)) \geqslant (1+\alpha)\cdot\dim(V)$. The number of maps d is the "degree" of the expander, and α is the expansion factor.

Using the subspace designs constructed in Theorem 2 in a black-box fashion, Forbes and Guruswami [4] gave explicit $(\Omega(n), \Omega(1))$-dimension expanders of $O(1)$ degree when $|\mathbb{F}| \geqslant \text{poly}(n)$. Here explicit means that the maps A_i are specified explicitly, say by the matrix representing their action with respect to some fixed basis. Extending Theorem 2 to smaller fields will yield constant-degree $(\Omega(n), \Omega(1))$-dimension expanders over all fields. The only known constructions of such dimension expanders over finite fields rely on monotone expanders [3, 2], a rather complicated (and remarkable) form of bipartite vertex expanders whose neighborhood maps are monotone. Even the existence of constant-degree monotone expanders does not follow from standard probabilistic methods, and the only known explicit construction is a sophisticated one using the group $\text{SL}_2(\mathbb{R})$ by Bourgain and Yehudayoff [1]. (Earlier, Dvir and Shpilka [2] constructed monotone expanders of logarithmic degree using Cayley graphs over the cyclic group, yielding logarithmic degree $(\Omega(n), \Omega(1))$-dimension expanders.)

In light of this, it is a very interesting question to remove the field size restriction in Theorem 2 above, as it will yield an arguably simpler construction of constant-degree dimension expanders over every field, and which might also offer a quantitatively better trade-off between the degree and expansion factor. We note that probabilistic constructions achieve similar parameters (in fact a slightly larger sized collection with $q^{\Omega(\varepsilon m)}$ subspaces) with no restriction on the field size (one can even take $q = 2$).

Our construction. The large field size in Theorem 2 was inherited from Reed-Solomon codes, which are defined over a field of size at least the code length. Our main contribution in this work is a construction of subspace designs based on algebraic function fields, which permits us to construct subspace designs over small fields. By instantiating this approach with a construction based on cyclotomic function fields, we are able to prove the following main result in this work:

▶ **Theorem 4** (Main Theorem). *For every $\varepsilon \in (0, 1)$, a prime power q and positive integers s, m such that $s \leq \varepsilon m/4$, there exists an explicit construction of $M = \Omega(q^{\lfloor \varepsilon m/(2s) \rfloor}/\varepsilon)$ subspaces in $\mathbb{F}_q^m$, each of dimension at least $(1-\varepsilon)m$, which form an $\left(s', \frac{2s'\lceil \log_q(m) \rceil}{\varepsilon}\right)$-strong subspace design for all $s' \leqslant s$.*

Note that we state a slightly stronger property that the bound on intersection size improves for subspaces of lower dimension $s' \leqslant s$. This property also holds for Theorem 2 and in fact is important for the dimension expander construction in [4], and so we make it explicit.

The bound on intersection size we guarantee above is worse than the one from the random construction by a factor of $\log_q m$. The result of Theorem 2 can be viewed as a special case of Theorem 4 since $\log_q m \leqslant 1$ when $q > m$. The factor $\log_q m$ comes out as a trade-off of the explicit construction vs the random construction given in [11]. The extension field based construction using Theorem 2 would yield an $(s, O(s^2/\varepsilon))$-subspace design (since an

(s, L)-weak subspace design is trivially an (s, sL)-(strong) subspace design). The bound we achieve is better for all $s = \Omega(\log_q m)$. In the use of subspace designs in the dimension expander construction of [4], s governs the dimension of the subspaces which are guaranteed to expand, which we would like to be large (and ideally $\Omega(m)$). The application of subspace designs to list decoding [11, 9] employs the parameter choice $m = O(s)$ in order keep the alphabet size q^m small. Therefore, our improvement applies to a meaningful setting of parameters that is important for the known applications of (strong) subspace designs.

Application to dimension expanders over small fields. By plugging in the subspace designs of Theorem 4 into the dimension expander construction of [4], we can get the following:

▶ **Theorem 5.** *For every prime power q and positive integer $n \geqslant q$, there exists an explicit construction of a $\left(b = \Omega\left(\frac{n}{\log_q \log_q n}\right), 1/3\right)$-dimension expander with $O(\log_q n)$ degree.*

For completeness, let us very quickly recap how such dimension expanders may be obtained from the subspace designs of Theorem 4, using the "tensor-then-condense" approach in [4]. We begin with linear maps $T_1, T_2 : \mathbb{F}^n \to \mathbb{F}^{2n}$, where $T_1(v) = (v; 0)$ and $T_2(v) = (0; v)$ – these trivially achieve expansion factor 2 by doubling the ambient dimension. Then we take the subspace design of Theorem 4 with $m = 2n$, $\varepsilon = 1/2$, $s = 2b$, and $M = 12\lceil \log_q m \rceil$ subspaces H_i (if $b = \beta n/(\log_q \log_q n)$ for small enough absolute constant $\beta > 0$, Theorem 4 guarantees these many subspaces). Let $E_i : \mathbb{F}^{2n} \to \mathbb{F}^n$ be linear maps such that $H_i = \ker(E_i)$. The dimension expander consists of the $2M$ composed maps $E_i \circ T_j$ for $i = 1, 2, \ldots, M$ and $j = 1, 2$. Briefly, the analysis of the expansion in dimension proceeds as follows. Let V be a subspace of $\mathbb{F}^n$ with $\dim(V) = \ell \leqslant b$, and let $W = T_1(V) + T_2(V)$ be the 2ℓ-dimensional subspace of $\mathbb{F}^{2n}$ after the tensoring step. The strong subspace design property implies that the number of maps E_i for which $\dim(E_i W) < 4\ell/3$ – which is equivalent to $\dim(W \cap H_i) > 2\ell/3$ – is less than $12\lceil \log_q m \rceil = M$. So there must be an i for which $\dim(E_i W) \geqslant 4\ell/3$, and this E_i when composed with T_1 and T_2 will expand V to a subspace of dimension at least $\frac{4}{3}\dim(V)$.

By using a method akin to the conversion of Reed-Solomon codes over extension fields to BCH codes over the base field, applied to the large field subspace designs of Theorem 2, Forbes and Guruswami [4] constructed $(\Omega(n/\log n), \Omega(1))$-dimension expanders of $O(\log n)$ degree. In contrast, our construction here guarantees expansion for dimension up to $\Omega(n/(\log \log n))$. The parameters offered by Theorem 5 are, however, weaker than both the construction given in [2], which has logarithmic degree but expands subspaces of dimension $\Omega(n)$, as well as the one in [1], which further gets constant degree. However, we do not go through monotone expanders which are harder to construct than vertex expanders, and our construction works fully within the linear-algebraic setting. We hope that the ideas in this work pave the way for a subspace design similar to Theorem 2 over small fields, and the consequent construction of constant-degree $(\Omega(n), \Omega(1))$-dimension expanders over all fields. In fact, all that is required for this is an $(s, O(s))$-subspace design with a sufficiently large constant number of subspaces, each of dimension $\Omega(m)$.

Construction approach. The generalization of the polynomials-based subspace design from [7] to take advantage of more general algebraic function fields is not straightforward. The natural approach would be to replace the space of low-degree polynomials by a Riemann-Roch space consisting of functions of bounded pole order ℓ at some place. We prove that such a construction can work, provided the degree ℓ is less than the degree of the field extension (and some other mild condition is met). However, this degree restriction is a severe one, and the dimension of the associated Riemann-Roch space will typically be too small (as

the "genus" of the function field, which measures the degree minus dimension "defect," will be large), unless the field size is large. Therefore, we don't know an instantiation of this approach that yields a family of good subspace designs over a fixed size field.

Let us now sketch the algebraic crux of the polynomial based construction in [7], and the associated challenges in extending it to other function fields. The core property of a dimension s subspace W of polynomials underlying the construction of Theorem 2 is the following: If $f_1, f_2, \ldots, f_s \in \mathbb{F}_q[X]$ of degree less than $q-1$ are linearly independent over $\mathbb{F}_q$ (these s polynomials being a basis of the subspace W), then the "folded Wronskian," which is the determinant of the matrix $M(f_1, f_2, \ldots, f_s)$ whose i,j'th entry is $f_j(\gamma^{i-1}X)$, is a *nonzero* polynomial in $\mathbb{F}_q[X]$. Here γ is an arbitrary primitive element of $\mathbb{F}_q$. One might compare this with the classical Wronskian criterion for linear dependence over characteristic zero fields (and also holds when characteristic is bigger than the degree of the f_i's), based on the singularity of the $s \times s$ matrix whose i,j'th entry is $\frac{d^{i-1} f_j}{dX^{i-1}}$.

One approach is to prove this claim about the folded Wronskian is via a "list size" bound from list decoding: one can prove that for any $A_1, \ldots, A_s \in \mathbb{F}_q[X]$, not all 0, the space of solutions $f \in \mathbb{F}_q[X]_{<(q-1)}$ to

$$A_1(X)f(X) + A_2(X)f(\gamma X) + \cdots + A_s(X)f(\gamma^{s-1}X) = 0 \tag{1}$$

has dimension at most $s-1$. (This was the basis of the linear-algebraic list decoding algorithm for folded Reed-Solomon codes [6, 8].) Stating the contrapositive, if $f_1, f_2, \ldots, f_s$ are linearly independent over $\mathbb{F}_q[X]$, then the rows of the matrix $M(f_1, f_2, \ldots, f_s)$ are linearly independent, and therefore its determinant, the folded Wronskian, is a nonzero polynomial. On the other hand, being the determinant of an $s \times s$ matrix whose entries are degree m polynomials, the folded Wronskian has degree at most ms. To prove the subspace design property, one then establishes that for each subspace H_i in the collection that intersects $W = \mathrm{span}(f_1, \ldots, f_s)$, the determinant picks up a number of distinct roots each with $\dim(W \cap H_i)$ multiplicity, the set of roots for different intersecting H_i being disjoint from each other. The total intersection bound then follows because the folded Wronskian has at most ms roots, counting multiplicities.

One can try to mimic the above approach for folded algebraic-geometric (AG) codes, with f^σ for some suitable automorphism σ playing the role of the shifted polynomial $f(\gamma X)$. This, however, runs into significant trouble, as the bound on number of solutions f to the functional equation analogous to (1), $A_1 f + A_2 f^\sigma + \cdots + A_s f^{\sigma^{s-1}} = 0$, is much higher. The list of solutions is either exponentially large and needs pruning via pre-coding the folded AG codes with subspace-evasive sets [10], or it is much bigger than q^{s-1} in the constructions based on cyclotomic function fields and narrow ray class fields where the folded AG codes work directly [5, 12].

Let F/K be a function field where the extension is Galois with Galois group generated by an automorphism σ. We choose the m-dimensional ambient space $\mathcal{V} \cong \mathbb{F}_q^m$ to be a carefully chosen subspace of a Riemann-Roch space in F of degree $\ell \gg m$ (specifically, we require $\ell \geqslant m + 2\mathfrak{g}$ where $\mathfrak{g}$ is the genus). We then establish that if $f_1, f_2, \ldots, f_s \in \mathcal{V}$ are linearly independent over $\mathbb{F}_q$, a certain "automorphism Moore matrix" $M_\sigma(f_1, f_2, \ldots, f_s)$ is non-singular. The determinant of this Moore matrix is thus a non-zero function in F, and this generalizes the folded Wronskian criterion for polynomials mentioned above.

This non-singularity result is proved in two steps. First, we show that for functions in $\mathcal{V}$, linear independence over $\mathbb{F}_q$ implies linear independence over K. Then we show that for any $f_1, \ldots, f_s \in F$ that are linearly independent over $K = F^\sigma$, the automorphism Moore matrix associated with σ is non-singular. With our hands on the non-zero function

$\Delta = \mathsf{det}(M_\sigma(f_1, f_2, \ldots, f_s))$, we can proceed as in the folded Reed-Solomon case – the part about Δ picking up many zeroes whenever a subspace in the collection intersects $\mathrm{span}(f_1, \ldots, f_s)$ also generalizes. The pole order of Δ, however, is now ℓs instead of ms in the polynomial-based construction. This is the cause for the worse bound on total intersection dimension in our Theorem 4. The detailed analysis of the above function field generalization will be presented in a full version of this paper. In the current version, we present only constructions without proof and hence "automorphism Moore matrix" is not introduced.

Organization. We begin with a quick review of background on algebraic function fields in general and cyclotomic function fields in particular in Section 2. We presentour constructions of subspace designs from function fields in Section 3 In Section 4, we instantiate our construction with specific cyclotomic function fields and derive our main consequence for subspace designs and establish Theorem 4.

2 Preliminaries on function fields

Background on function fields. Throughout this paper, $\mathbb{F}_q$ denotes the finite field of q elements. A function field F over $\mathbb{F}_q$ is a field extension over $\mathbb{F}_q$ in which there exists an element z of F that is transcendental over $\mathbb{F}_q$ such that $F/\mathbb{F}_q(z)$ is a finite extension. $\mathbb{F}_q$ is called the full constant field of F if the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself. In this paper, we always assume that $\mathbb{F}_q$ is the full constant field of F, denoted by $F/\mathbb{F}_q$.

Each discrete valuation ν from F to $\mathbb{Z} \cup \{\infty\}$ defines a local ring $O = \{f \in F : \nu(f) \geqslant 0\}$. The maximal ideal P of O is called a *place*. We denote the valuation ν and the local ring O corresponding to P by ν_P and O_P, respectively. The residue class field O_P/P, denoted by F_P, is a finite extension of $\mathbb{F}_q$. The extension degree $[F_P : \mathbb{F}_q]$ is called *degree* of P, denoted by $\deg(P)$.

Let $\mathbb{P}_F$ denote the set of places of F. A divisor D of F is a formal sum $\sum_{P \in \mathbb{P}_F} m_P P$, where $m_P \in \mathbb{Z}$ are equal to 0 except for finitely many P. The degree of D is defined to be $\deg(D) = \sum_{P \in \mathbb{P}_F} m_P \deg(P)$. We say that D is positive, denoted by $D \geqslant 0$, if $m_P \geqslant 0$ for all $P \in \mathbb{P}_F$. For a nonzero function f, the principal divisor (f) is defined to be $\sum_{P \in \mathbb{P}_F} \nu_P(f) P$. Then the degree of the principal divisor (f) is 0. The Riemann-Roch space associated with a divisor D, denoted by $\mathcal{L}(D)$, is defined by

$$\mathcal{L}(D) := \{f \in F \setminus \{0\} : (f) + D \geqslant 0\} \cup \{0\}. \tag{2}$$

Then $\mathcal{L}(D)$ is a finite dimensional space over $\mathbb{F}_q$. By the Riemann-Roch theorem [15], the dimension of $\mathcal{L}(D)$, denoted by $\dim_{\mathbb{F}_q}(D)$, is lower bounded by $\deg(D) - \mathfrak{g} + 1$, i.e., $\dim_{\mathbb{F}_q}(D) \geqslant \deg(D) - \mathfrak{g} + 1$, where $\mathfrak{g}$ is the genus of F. Furthermore, $\dim_{\mathbb{F}_q}(D) = \deg(D) - \mathfrak{g} + 1$ if $\deg(D) \geqslant 2\mathfrak{g} - 1$. In addition, we have the following results [15, Lemma 1.4.8 and Corollary 1.4.12(b)]:

- **(i)** If $\deg(D) < 0$, then $\dim_{\mathbb{F}_q}(D) = 0$;
- **(ii)** For a positive divisor G, we have $\dim_{\mathbb{F}_q}(D) - \dim_{\mathbb{F}_q}(D - G) \leqslant \deg(G)$, i.e., $\dim_{\mathbb{F}_q}(D - G) \geqslant \dim_{\mathbb{F}_q}(D) - \deg(G)$.

Let $\mathrm{Aut}(F/\mathbb{F}_q)$ denote the set of automorphisms of F that fix every element of $\mathbb{F}_q$, i.e.,

$$\mathrm{Aut}(F/\mathbb{F}_q) = \{\tau : \tau \text{ is an automorphism of } F \text{ and } \alpha^\tau = \alpha \text{ for all } \alpha \in \mathbb{F}_q\}.$$

For a place $P \in \mathbb{P}_F$ and an automorphism $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$, we denote by P^σ the set $\{f^\sigma : f \in P\}$. Then P^σ is a place and moreover we have $\deg(P^\sigma) = \deg(P)$. The place P^σ is called a conjugate place of P. σ also induces an automorphsim of $\mathrm{Aut}(\mathbb{F}_P/\mathbb{F}_q)$. This

implies that there exists an integer $e \geqslant 0$ such that $\alpha^\sigma = \alpha^{q^e}$ for all $\alpha \in F_P$. σ is called the *Frobenius* of P if $e = 1$, i.e., $\alpha^\sigma = \alpha^q$ for all $\alpha \in F_P$. For a place P and a function $f \in O_P$, we denote by $f(P)$ the residue class of f in F_P. Thus, we have $(f(P))^{q^e} = (f(P))^\sigma = f^\sigma(P^\sigma)$.

Background on cyclotomic function fields. Let x be a transcendental element over $\mathbb{F}_q$ and denote by K the rational function field $\mathbb{F}_q(x)$. Let K^{ac} be an algebraic closure of K. Denote by $\mathbb{F}_q[x]$ the polynomial ring $\mathbb{F}_q[x]$. Let $\mathrm{End}(K^{ac})$ be the ring of homomorphisms from K^{ac} to K^{ac}. We define $\rho_x(z) = z^q + xz$ for all $z \in K^{ac}$. For $i \geqslant 2$, we define $\rho_{x^i}(z) = \rho_x(\rho_{x^{i-1}}(z))$. For a polynomial $p(x) = \sum_{i=0}^n a_i x^i \in \mathbb{F}_q[x]$, we define $\rho_{p(x)}(z) = \sum_{i=0}^n a_i \rho_{x^i}(z)$. For simplicity, we denote $\rho_{p(x)}(z)$ by $z^{p(x)}$. It is easy to see that $z^{p(x)} \in \mathbb{F}_q[x][z]$ is a q-linearized polynomial in z of degree q^d, where $d = \deg(p(x))$.

For a polynomial $p(x) \in \mathbb{F}_q[x]$ of degree d, define the set

$$\Lambda_{p(x)} := \{\alpha \in K^{ac} : \alpha^{p(x)} = 0\}. \tag{3}$$

Then $\Lambda_{p(x)} \simeq \mathbb{F}_q[x]/(p(x))$ is an $\mathbb{F}_q[x]$-module and it has exactly q^d elements. Furthermore, $\Lambda_{p(x)}$ is a cyclic $\mathbb{F}_q[x]$-module. For any generator λ of $\Lambda_{p(x)}$, one has $\Lambda_{p(x)} = \{\lambda^A : A \in \mathbb{F}_q[x]/(p(x))\}$ and λ^A is a generator of $\Lambda_{p(x)}$ if and only if $\gcd(A, p(x)) = 1$. The extension $K(\lambda) = K(\Lambda_{p(x)})$ is a Galois extension over K with $\mathrm{Gal}(K(\Lambda_{p(x)})/K) \simeq (\mathbb{F}_q[x]/p(x))^*$, where $(\mathbb{F}_q[x]/p(x))^*$ is the unit group of the ring $\mathbb{F}_q[x]/(p(x))$. We use σ_A to denote the automorphism of $\mathrm{Aut}(K(\lambda)/K)$ corresponding to A, i.e., $\lambda^{\sigma_A} = \lambda^A$. The size of $(\mathbb{F}_q[x]/p(x))^*$ is denoted by $\Phi(p(x))$. If $p(x)$ is an irreducible polynomial of degree d over $\mathbb{F}_q$, we have $\Phi(p(x)) = q^d - 1$. In this case, the extension $K(\Lambda_{p(x)})/K$ is cyclic and $\mathrm{Gal}(K(\Lambda_{p(x)})/K) \simeq (\mathbb{F}_q[x]/p(x))^* \simeq \mathbb{F}_{q^d}^*$.

3 Construction of subspace design

Let $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ be an automorphism of a finite order. Denote by F^σ the fixed field by $\langle\sigma\rangle$, i.e., $F^\sigma = \{x \in F : x^\sigma = x\}$. By the Galois theory, F/F^σ is a Galois extension and $\mathrm{Gal}(F/F^\sigma) = \langle\sigma\rangle$. Let D be a divisor of F such that $D^\sigma = D$. Assume that Q' is a place of F lying above a rational place Q of F^σ and $Q' \notin \mathrm{supp}(D)$. Furthermore, assume that $\mathcal{V}$ is an $\mathbb{F}_q$-subspace of $\mathcal{L}(D)$ such that $\mathcal{V} \cap \mathcal{L}(D - Q') = \{0\}$.

For each place $P \in \mathbb{P}_F$ such that $P \notin \mathrm{supp}(D)$ and $P, P^{\sigma^{-1}}, \ldots, P^{\sigma^{-(t-1)}}$ are distinct, we define the subspace $\mathcal{H}_P$:

$$\mathcal{H}_P = \{f \in \mathcal{V} : f(P^{\sigma^{-i}}) = 0 \text{ for each } i \in \{0, \ldots, t-1\}\} = \mathcal{V} \cap \mathcal{L}\left(D - \sum_{i=0}^{t-1} P^{\sigma^{-i}}\right). \tag{4}$$

Recall that $f(P)$ is defined to be the residue class of f in the residue field O_P/P. Hence, it is clear that

$$\dim_{\mathbb{F}_q}(\mathcal{H}_P) \geqslant \dim_{\mathbb{F}_q}(\mathcal{V}) + \dim_{\mathbb{F}_q}\left(D - \sum_{i=0}^{t-1} P^{\sigma^{-i}}\right) - \dim_{\mathbb{F}_q}(D) \geqslant \dim_{\mathbb{F}_q}(\mathcal{V}) - t\deg(P).$$

Let $f(P)^\sigma = f(P)^{q^e}$ for some integer $e \geqslant 0$. Thus, we have $f^{\sigma^i}(P^{\sigma^i}) = f(P)^{\sigma^i} = f(P)^{q^{ei}}$ for all integers $i \geqslant 0$.

Define $S_P = \{P^{\sigma^{-i}} : i \in \{0, \ldots, t-1\}\}$, and denote by $\mathcal{F}_r$ a set of places P with degree r such that S_P are disjoint and $|S_P| = t$.

▶ **Theorem 6.** *For any integers s, t with $1 \leqslant s \leqslant t$, the collection $(\mathcal{H}_P)_{P \in \mathcal{F}_r}$ of subspaces of $\mathcal{V}$, each of codimension at most rt, is an $\left(s, \frac{\ell s}{r(t-s+1)}\right)$ strong subspace design, where $\ell = \deg(D)$.*

In the above construction, there is no upper bound on the degree of the divisor D. This makes it possible to compute the dimension of the Riemann-Roch space $\mathcal{L}(D)$. The next construction is for the case when the degree of D is upper bounded by $[F : F^\sigma]$. This construction works for function fields of small genus.

Suppose that there exists a rational place Q in F^σ such that there is only one place Q' of F lying above Q. Let D be a positive divisor of F with $Q' \notin \mathrm{supp}(D)$ and $\deg(D) < n$. For each place $P \in \mathbb{P}_F$ such that $P \notin \mathrm{supp}(D)$ and $P, P^{\sigma^{-1}}, \ldots, P^{\sigma^{-(t-1)}}$ are distinct, we define the subspace $\mathcal{I}_P$:

$$\mathcal{I}_P = \{f \in \mathcal{L}(D) : f(P^{\sigma^{-i}}) = 0 \text{ for each } i \in \{0, \ldots, t-1\}\}. \tag{5}$$

▶ **Theorem 7.** *For any integers s, t with $1 \leqslant s \leqslant t$, the collection $(\mathcal{I}_P)_{P \in \mathcal{F}_r}$ of subspaces of $\mathcal{L}(D)$, each of codimension at most rt, is an $\left(s, \frac{\ell s}{r(t-s+1)}\right)$ strong subspace design, where $\ell = \deg(D)$.*

4 Subspace design from cyclotomic function fields

In this section, we will present subspace design from the construction given in Section 3 by applying cyclotomic function fields. We start with the subspace design in an ambient space of smaller dimension.

The small dimension case. If $\deg(D)$ is smaller than $n = [F : F^\sigma]$ and n is smaller than the genus $\mathfrak{g}(F)$ of F, in general it is hard to compute dimension of the Riemann-Roch space $\mathcal{L}(D)$. Therefore, we cannot use the construction given in Theorem 7. In this subsection, we apply Theorem 7 to the case where we can estimate the dimension of $\mathcal{L}(D)$.

Let F be the rational function field $\mathbb{F}_q(x)$. Let $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ be given by $x \mapsto \gamma x$, where γ is a primitive element of $\mathbb{F}_q^*$. By Theorem 7, one can obtain the subspace design given in [7]. Below we show that the subspace design given in [7] can be realized by using cyclotomic function fields.

Put $K = \mathbb{F}_q(x)$. Let $p_1(x)$ be a monic linear polynomial. For instance, we can simply take $p_1(x) = x$. Then the cyclotomic function field $F_1 := K(\Lambda_{p_1})$ is a cyclic extension over K with $\mathrm{Gal}(F_1/K) \simeq \mathbb{F}_q^*$. In fact, $F_1 = K(\lambda) = \mathbb{F}_q(\lambda)$ with λ satisfying $\lambda^{q-1} + x = 0$. Thus, $K = \mathbb{F}_q(\lambda^{q-1})$. Let γ be a primitive root of $\mathbb{F}_q$ and let $\sigma \in \mathrm{Gal}(F/K)$ be defined by $\lambda^\sigma = \lambda^\gamma = \gamma\lambda$. This gives the exactly the same function fields and automorphism σ as in [7]. Therefore, we conclude that this cyclotomic function field also realizes the subspace design given in [7].

Next we consider a monic *primitive* quadratic polynomial $p_2(x) = x^2 + \alpha x + \beta$ with $\alpha, \beta \in \mathbb{F}_q$. Then the cyclotomic function field $F_2 := K(\Lambda_{p_2})$ is a cyclic extension over K with $\mathrm{Gal}(F_2/K) \simeq (\mathbb{F}_q[x]/(p_2)^*$. In fact, $F_2 = K(\lambda)$ with λ satisfying $\lambda^{q^2-1} + \lambda^{q-1}(x^q + x + \alpha) + x^2 + \alpha x + \beta = 0$. (see [14]). Let σ be a generator of $\mathrm{Gal}(F_2/K)$. Then by the Galois theory, the fixed field F_2^σ is the rational function field $K = \mathbb{F}_q(x)$. The genus of the function field F_2 is $\mathfrak{g}(F_2) = \frac{(q-2)(q+1)}{2}$ [13, 14].

The zero of $p_2(x)$ is the unique ramified place in $\mathbb{F}_q(x)$ and it is totally ramified. Let P' be the unique place of F_2 that lies over the zero of $p_2(x)$. Let ℓ be an even positive integer with $\ell < q^2 - 1$ and let $D = (\ell/2)P'$. Then $\deg(D) = \ell$ and $D^\sigma = D$. Furthermore, we know

that the the zero of $(x-\alpha)$ is fully inert in F_2/K. By Theorem 7, we have the following result.

▶ **Theorem 8.** *For all positive integers s, r, t, m and prime powers q satisfying $s \le t \le m = \zeta q^2$ for some $\zeta \in (0, 1/2]$, the above construction yields a collection of $M = \Omega(\frac{q^r}{rt})$ spaces $\mathcal{I}_1, \ldots, \mathcal{I}_M \subset \mathbb{F}_q^m$, each of codimension rt, which forms an $\left(s', \frac{(1+1/(2\zeta))ms'}{r(t-s'+1)}\right)$ strong subspace design for all $s' \leqslant s$.*

Proof. Choose ℓ such that the dimension of $\mathcal{L}((\ell/2)P')$ is $m = \zeta q^2$. By the Riemman-Roch Theorem, we have $\zeta q^2 \geqslant \deg((\ell/2)P') - \mathfrak{g}(F_2) + 1$, i.e., $\ell \le \zeta q^2 + g - 1 \le (1/2 + \zeta)q^2$. The desired result follows from Theorem 7. ◀

The large dimension case. In this subsection, we will make use of Theorem 6 due to large genus. Let $p(x) \in \mathbb{F}_q[x]$ be a monic primitive polynomial of degree $d \geqslant 2$. Consider the cyclotomic function field $F := K(\Lambda_{p(x)})$, where K is the rational function field $\mathbb{F}_q(x)$. Then F/K is a Galois extension with $\mathrm{Gal}(F/K) \simeq (\mathbb{F}_q[x]/(p(x)))^*$. Thus, $\mathrm{Gal}(F/K)$ is a cyclic group of order $q^d - 1$. Let σ be a generator of this group. Then by the Galois theory, the fixed field F^σ is the rational function field $\mathbb{F}_q(x)$.

The zero of $p(x)$ is the unique ramified place in $\mathbb{F}_q(x)$ and it is totally ramified. Let P' be the unique place of F lying over the zero of $p(x)$. Let Q' be the unique place of F that lies over the zero of x. Since Q' is totally inert, we have $\deg(Q') = [F : F^\sigma] = q^d - 1 := m$.

The genus of the function field F is $\mathfrak{g} = \frac{1}{2}\left(d - 2 + \frac{q-2}{q-1}\right)(q^d - 1) + 1$. Put $D = \left\lceil \frac{2\mathfrak{g}+m-1}{d} \right\rceil P'$. Then $\ell = \deg(D) \geqslant 2\mathfrak{g} + m$ and hence, $\dim_{\mathbb{F}_q}(D - Q') = \deg(D - Q') - \mathfrak{g} + 1$. Choose $\mathcal{V} \subseteq \mathcal{L}(D)$ such that $\mathcal{V}$ and $\mathcal{L}(D - Q')$ are a direct sum of $\mathcal{L}(D)$. Thus, we have $\mathcal{V} \cap \mathcal{L}(D - Q') = \{0\}$ and $\dim_{\mathbb{F}_q}(\mathcal{V}) = \dim_{\mathbb{F}_q}(D) - \dim_{\mathbb{F}_q}(D - Q') = q^d - 1 = m$.

By Theorem 6, we have the following.

▶ **Theorem 9.** *For all positive integers s, r, t, d, m and prime powers q satisfying $\gcd(r, m) = 1$ and $s \le t \le m/r = (q^d - 1)/r$, there is an explicit collection of $M = \Omega(\frac{m \cdot q^r}{rt})$ spaces $\mathcal{H}_1, \ldots, \mathcal{H}_M \subset \mathbb{F}_q^m$, each of codimension at most rt, which forms an $(s', \frac{(d-1/(q-1))ms'}{r(t-s'+1)})$-strong subspace design for all $s' \leqslant s$. Furthermore, the subspace design can be constructed in $\mathrm{poly}(q, m, r)$ time.*

Proof. The subspace design property follows from Theorem 6 since $\ell = \deg(D) \leqslant (d - 1/(q-1))m$. The construction of the subspace design mainly involves finding a basis of $\mathcal{V}$ and evaluations of functions at places of degree r which can be computed in $\mathrm{poly}(q, m, r)$. We can enumerate over all degree r irreducible polynomials $R \in \mathbb{F}_q[x]$ by brute-force in $q^{O(r)}$ time. None of these places are ramified, and each of these places R splits completely into m places of degree r, say $\{P^{\sigma^{i-1}} \mid 1 \leqslant i \leqslant m\}$, in F. So we can pick $b = \lfloor \frac{m}{t} \rfloor$ of these places $P, P^{\sigma^t}, \ldots, P^{\sigma^{(b-1)t}}$, and define a particular subspace of co-dimension rt associated with each of them as in (4). ◀

By setting $t \approx 2s$ and $r \approx \lfloor \frac{\varepsilon m}{2s} \rfloor$ in Theorem 9, we obtain the Main Theorem 4.

References

1 Jean Bourgain and Amir Yehudayoff. Expansion in $\mathrm{SL}_2(\mathbb{R})$ and monotone expanders. *Geometric and Functional Analysis*, 23(1):1–41, 2013. doi:10.1007/s00039-012-0200-9.

2 Zeev Dvir and Amir Shpilka. Towards dimension expanders over finite fields. *Combinatorica*, 31(3):305–320, 2011. doi:10.1007/s00493-011-2540-8.

3 Zeev Dvir and Avi Wigderson. Monotone expanders: Constructions and applications. *Theory of Computing*, 6(12):291–308, 2010. doi:10.4086/toc.2010.v006a012.

4 Michael A. Forbes and Venkatesan Guruswami. Dimension expanders via rank condensers. In *Proceedings of the 19th International Workshop on Randomization and Computation (RANDOM)*, pages 800–814, 2015. Extended full version available as ECCC Technical Report TR14-162.

5 Venkatesan Guruswami. Cyclotomic function fields, Artin-Frobenius automorphisms, and list error-correction with optimal rate. *Algebra and Number Theory*, 4(4):433–463, 2010. Preliminary version in STOC 2009.

6 Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *Proceedings of the 26th IEEE Conference on Computational Complexity*, June 2011.

7 Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016. Preliminary version in FOCS 2013. doi:10.1007/s00493-014-3169-1.

8 Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013. doi:10.1109/TIT.2013.2246813.

9 Venkatesan Guruswami, Carol Wang, and Chaoping Xing. Explicit list-decodable rank-metric and subspace codes via subspace designs. *IEEE Trans. Information Theory*, 62(5):2707–2718, 2016. Preliminary versions in STOC 2013 and RANDOM 2014. doi:10.1109/TIT.2016.2544347.

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

11 Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound. In *Proceedings of the 45th ACM Symposium on Theory of Computing*, pages 843–852, June 2013. Extended version available as ECCC Technical Report TR12-146.

12 Venkatesan Guruswami and Chaoping Xing. Optimal rate algebraic list decoding using narrow ray class fields. *J. Comb. Theory, Ser. A*, 129:160–183, 2015. Preliminary version in SODA 2014 under slightly different title.

13 David R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, March 1974.

14 Liming Ma, Chaoping Xing, and Sze Ling Yeo. On automorphism groups of cyclotomic function fields over finite fields. *Journal of Number Theory*, 169:406–419, 2016. doi:10.1016/j.jnt.2016.05.026.

15 Henning Stichtenoth. *Algebraic function fields and codes*. GMT 254, Springer-Verlag, Berlin, 2008.