Electronic Colloquium on Computational Complexity, Report No. 17 (2018)

Lossless dimension expanders via linearized polynomials and subspace designs*

Venkatesan Guruswami[†] Nicolas Resch[‡] Chaoping Xing[§]

Abstract

For a vector space $\mathbb{F}^n$ over a field $\mathbb{F}$, an (η, β)-dimension expander of degree d is a collection of d linear maps $\Gamma_j : \mathbb{F}^n \to \mathbb{F}^n$ such that for every subspace U of $\mathbb{F}^n$ of dimension at most ηn, the image of U under all the maps, $\sum_{j=1}^{d} \Gamma_j(U)$, has dimension at least $\beta \dim(U)$. Over a finite field, a random collection of $d = O(1)$ maps Γ_j offers excellent "lossless" expansion whp: $\beta \approx d$ for $\eta \geq \Omega(1/d)$. When it comes to a family of *explicit constructions* (for growing n), however, achieving even modest expansion factor $\beta = 1 + \varepsilon$ with constant degree is a non-trivial goal.

We present an explicit construction of dimension expanders over finite fields based on linearized polynomials and subspace designs, drawing inspiration from recent progress on list decoding in the rank-metric. Our approach yields the following:

- *Lossless* expansion over large fields; more precisely $\beta \geq (1 - \varepsilon)d$ and $\eta \geq \frac{1-\varepsilon}{d}$ with $d = O_\varepsilon(1)$, when $|\mathbb{F}| \geq \Omega(n)$.
- Optimal up to constant factors expansion over fields of arbitrarily small polynomial size; more precisely $\beta \geq \Omega(\delta d)$ and $\eta \geq \Omega(1/(\delta d))$ with $d = O_\delta(1)$, when $|\mathbb{F}| \geq n^\delta$.

Previously, an approach reducing to monotone expanders (a form of vertex expansion that is highly non-trivial to establish) gave $(\Omega(1), 1 + \Omega(1))$-dimension expanders of constant degree over all fields. An approach based on "rank condensing via subspace designs" led to dimension expanders with $\beta \gtrsim \sqrt{d}$ over large finite fields. Ours is the first construction to achieve lossless dimension expansion, or even expansion proportional to the degree.

*Research supported in part by NSF grant CCF-1422045 and NSERC grant CGSD2-502898. Some of this work was done when the first author was visiting the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

[†] Computer Science Department, Carnegie Mellon University. venkatg@cs.cmu.edu

[‡] Computer Science Department, Carnegie Mellon University. nresch@cs.cmu.edu

[§] School of Physical and Mathematical Sciences, Nanyang Technological University. xingcp@ntu.edu.sg

ISSN 1433-8092

1 Introduction

The field of *pseudorandomness* is concerned with efficiently constructing objects that share desirable properties with random objects while using no or little randomness. The ideas developed in pseudorandomness have found broad applications in areas such as complexity theory, derandomizaton, coding theory, cryptography, high-dimensional geometry, graph theory, and additive combinatorics. Due to much effort on the part of many researchers, nontrivial constructions of expander graphs, randomness extractors and condensers, Ramsey graphs, list-decodable codes, compressed sensing matrices, Euclidean sections, and pseudorandom generators and functions have been presented. Interestingly, while these problems may appear superficially to be unrelated, many of the techniques developed in one context have been useful in others, and the deep connections uncovered between these pseudorandom objects have led to a unified theory of "Boolean pseudoranomness". (See for instance this survey by Vadhan [Vad12] for more discussion of this phenomenon.)

More recently, there is a developing theory of "algebraic pseudorandomness," wherein the pseudorandom objects of interest now have "algebraic structure" rather than a purely combinatorial structure. In these scenarios, instead of studying the size of subsets or min-entropy, we consider the dimension of subspaces. Many analogs of classical pseudorandom objects have been defined, such as dimension expanders, subspace-evasive sets, subspace designs, rank-preserving condensers, and list-decodable rank-metric codes. Beyond being interesting in their own rights, these algebraic pseudorandom objects have found many applications: for example, subspace-evasive sets have been used in the construction of Ramsey graphs [PR04] and list-decodable codes [GX12, GW14]; subspace designs have been used to list-decode codes over the Hamming metric and the rank-metric [GX13, GW14]; and rank-preserving condensers have been used in affine extractors [Gab11] and polynomial identity testing [KS11, FS12].

In this work, we focus upon providing explicit constructions of *dimension expanders* over finite fields. A dimension expander is a collection of d linear maps $\Gamma_j : \mathbb{F}^n \to \mathbb{F}^n$ such that, for any subspace $U \subseteq \mathbb{F}^n$ of sufficiently small small dimension, the sum of the images of U under all the maps $\Gamma_1(U)+\cdots+\Gamma_d(U)$ has dimension which is a constant factor larger than $\dim U$. As suggested by their name, dimension expanders may be viewed as a linear-algebraic analog of expander graphs. Indeed, one can imagine creating a graph with vertex set $\mathbb{F}^n$, and then we add an edge from a vertex $u \in \mathbb{F}^n$ to the vertices $\Gamma_j(u)$.[1]. Alternatively, one may consider the bipartite graph with left and right partition given by $\mathbb{F}^n$, and we attach a vertex $u \in \mathbb{F}^n$ in the left partition to $\Gamma_j(u)$ in the right partition for each j. For this reason, d is referred to as the *degree* of the dimension expander. The property of being a dimension expander then says that, given any (sufficiently small) *subspace*, the span of the neighborhood will have appreciably larger dimension. Indeed, we use the notation Γ_j for the linear maps in analogy with the "neighborhood function" of a graph. Just as with expander graphs, we seek dimension expanders with constant degree, and moreover we would like to be able expand subspaces of dimension at most ηn by a multiplicative factor of β, where $\eta = \Omega(1)$ and $\beta = 1+\Omega(1)$. We refer to such an object as an (η, β)-dimension expander. If $\beta = \Omega(d)$, we deem the dimension expander *degree-proportional.* If moreover $\beta = (1-\varepsilon)d$, we deem the dimension expander *lossless.* Via a probabilistic argument, it is a simple exercise to show that constant-degree lossless dimension expanders exist over every field.

Finally, we indicate that *unbalanced* bipartite expander graphs play a key role in constructions of extractors and other Boolean pseudorandom objects. In this scenario, the left partition is significantly larger than the right partition, but we still have that sufficiently small subsets U

[1] In general, this yields a directed graph. However, we may assume the maps Γ_j are invertible and then add the maps Γ_j^{-1} to the collection, which makes the graph undirected.

of the left partition expand significantly, with $(1-\varepsilon)d|U|$ neighbors in the right partition in the lossless case. Such unbalanced expanders are closely related to *randomness condensers*, which preserve all or most of the min-entropy of a source while compressing its length. The improved min-entropy *rate* at the output makes subsequent *extraction* of near-uniformly random bits easier. Indeed, the extractors in [GUV09] were obtained via this paradigm, once lossless expanders based on list-decodable codes were constructed. Inspired by this, we consider the challenge of constructing *unbalanced* dimension expanders: for N and n not necessarily equal, we would like a collection of maps $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}^N \to \mathbb{F}^n$ that expand sufficiently small subspaces by a factor of $\approx d$. We quantify the "unbalancedness" of the dimension expander by $b = \frac{N}{n}$, and we refer to it as a *b-unbalanced dimension expander in $\mathbb{F}^n$*. Again, if the expansion factor is $\Omega(d)$ we deem the unbalanced dimension expander *degree-proportional*, while if the expansion factor is $(1-\varepsilon)d$ we deem it *lossless*.

1.1 Our results

We provide various explicit constructions of dimension expanders. More precisely, we have a family of sets of matrices $\{\{\Gamma_1^{(n_k)}, \ldots, \Gamma_d^{(n_k)}\}\}_{k\in\mathbb{N}}$ for an infinite sequence of integers $n_1 < n_2 < \cdots$, where each $\Gamma_j^{(n_k)}$ is an $n_k \times n_k$ matrix (or $n_k \times bn_k$ matrix in the case of b-unbalanced expanders). The family is *explicit* if there is an algorithm outputting the list of matrices $\Gamma_1^{(n_k)}, \ldots, \Gamma_d^{(n_k)}$ in $\mathsf{poly}(n_k)$ field operations.

First of all, we provide the first explicit construction of a lossless dimension expander. Moreover we emphasize that the η parameter is optimal as well, as one cannot hope to expand subspaces of dimension more than $\frac{n}{d}$ by a factor of $\approx d$.

Theorem 1.1 (Informal Statement; cf. Theorem 5.2)**.** *For all $\varepsilon > 0$ constant, there exists an integer $d = d(\varepsilon)$ sufficiently large such that there is an explicit family of $(\frac{1-\varepsilon}{d}, (1-\varepsilon)d)$-dimension expanders of degree d over $\mathbb{F}^n$ when $|\mathbb{F}| \geq \Omega(n)$.*

The main drawback of the above result is the constraint on the field size. Our next result allows for smaller field sizes, but we are only able to guarantee degree-proportional expansion. We remark that prior to this work, no explicit constructions of degree-proportional dimension expanders were known.

Theorem 1.2 (Informal Statement; cf. Theorem 5.1)**.** *For all $\delta > 0$ constant, there exists an integer $d = d(\delta)$ sufficiently large such that there is an explicit family of $\left(\Omega\left(\frac{1}{\delta d}\right), \Omega(\delta d)\right)$-dimension expanders of degree d over $\mathbb{F}^n$ when $|\mathbb{F}| \geq n^\delta$.*

Moreover, our paradigm is flexible enough to allow for the construction of unbalanced dimension expanders. We remark that while the results of Forbes and Guruswami [FG15] could be adapted to obtain nontrivial constructions of unbalanced expanders, our work is the first to explicitly state this. Furthermore, our work is the first to achieve lossless expansion, or even degree-proportionality. Recall that we view unbalanced dimension expanders as mapping $\mathbb{F}^N \to \mathbb{F}^n$ and we call it b-unbalanced dimension expander over $\mathbb{F}^n$ where $b = \frac{N}{n}$.

First, we provide a construction of a lossless unbalanced dimension expander, again over fields of linear size.

Theorem 1.3 (Informal Statement; cf. Theorem 6.7)**.** *For all $\varepsilon > 0$ and integer $b \geq 1$, there exists an integer $d = d(\varepsilon, b)$ sufficiently large such that there is an explicit family of b-unbalanced $(\frac{1-\varepsilon}{db}, (1-\varepsilon)d)$-dimension expanders of degree d over $\mathbb{F}^n$ when $|\mathbb{F}| \geq \Omega(n)$.*

This result is again complemented by a construction of degree-proportional unbalanced dimension expanders over fields of arbitrarily small polynomial size.

Theorem 1.4 (Informal Statement; cf Theorem 6.6)**.** *For all $\delta > 0$ and integer $b \geq 1$, there exists an integer $d = d(\delta, b)$ sufficiently large such that there is an explicit family of b-unbalanced $\left(\Omega\left(\frac{1}{\delta b d}\right), \Omega(\delta d)\right)$-dimension expanders of degree d over $\mathbb{F}^n$ when $|\mathbb{F}| \geq n^\delta$.*

Our final contribution is to define *subspace evasive subspaces*, and observe that they yield degree-proportional dimension expanders. Informally, a subspace evasive subspace H is an $\mathbb{F}_q$-subspace that has small intersection with any subspace of bounded dimension defined over an *extension field.* (To properly define this notion, it is best to identify $\mathbb{F}_q^n$ with $\mathbb{F}_{q^n}$, and then consider $\mathbb{F}_{q^d}$-subspaces of $\mathbb{F}_{q^n}$ for $d|n$.)

Theorem 1.5 (Informal Statement; cf. Proposition A.4)**.** *Suppose there exists an explicit construction of a subspace evasive subspace H with parameters approximately matching those achievable by a random subspace. Then, there is an explicit construction of a degree-proportional dimension expander.*

1.2 Our approach

Our approach for constructing dimension expanders uses ideas recently developed in the context of list-decoding rank-metric codes. A *rank-metric code* is a set of matrices $\mathcal{C} \subseteq \mathbb{F}^{m\times n}$ with $m \geq n$, and we define the *rank-distance* between matrices A, B to be $d_R(A, B) = \mathsf{rank}(A - B)$. A code $\mathcal{C}$ is said to be (ρ, L)-*list-decodable* if, for any $Y \in \mathbb{F}^{m\times n}$, the number of matrices in $\mathcal{C}$ at rank-distance at most ρn from Y is at most L. A line of work [GWX16] succeeded in constructing high-rate rank-metric codes which are list-decodable up to the Singleton bound.[2] The code may also readily be seen to be *list-recoverable* in the following sense: given vector spaces $V_1, \dots, V_n \subseteq \mathbb{F}^m$ of bounded dimension, the number of matrices in $A \in \mathcal{C}$ with $A_i \in V_i$ for all $i \in [n]$ is bounded, where A_i denotes the ith column of A. The code constructed in [GWX16] is a carefully selected subcode of the Gabidulin code [Gab85], which is based on the evaluation of low degree *linearized* polynomials and is the analog of Reed-Solomon codes for the rank metric. Briefly, the Gabidulin code $G[n, m, k, q]$ is obtained by evaluating linearized polynomials $f(X) = \sum_{i=0}^{k-1} f_i X^{q^i} \in \mathbb{F}_{q^m}[X]$ at the $\mathbb{F}_q$-linearly independent points $\alpha_1, \dots, \alpha_n \in \mathbb{F}_{q^m}$, and then identifying the vector $(f(\alpha_1), \dots, f(\alpha_n))$ with the matrix in $\mathbb{F}_q^{m\times n}$ obtained by expressing $f(\alpha_j) \in \mathbb{F}_{q^m}$ as an element of $\mathbb{F}_q^m$ by fixing a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The *q-degree* of $f = \sum_{i=0}^{k-1} f_i X^{q^i}$ is the maximal i such that $f_i \neq 0$.

In the case of Boolean pseudorandomness, not long after the construction of Parvaresh-Vardy codes and folded Reed-Solomon codes [PV05, GR08], the techniques used to prove list-decodability of these codes were adapted to show lossless expansion properties of unbalanced expanders built from these codes [GUV09]. Our approach is strongly inspired by the connection between list recovery and expansion that drives [GUV09] and its instantiation with algebraic codes shown to achieve optimal redundancy for list decoding. Indeed, our methodology can be viewed as an adaption of the GUV approach to the "linearized world". Various challenges arise in attempting to adapt the approach of the GUV framework to the setting of Gabidulin-like codes. For instance, we are no longer able to "append the seed" (in our context, the field element α_j) to the output of the neighborhood functions as is done in [GUV09], as that will prevent the maps from being linear.[3] More significantly, we also need to perform a careful "pruning" of subspaces which arise

[2] The Singleton bound from coding theory over the Hamming metric possesses a natural analog in the rank-metric case.

[3] One could instead try tensoring the output with the seed, but it is unclear to us how to make this approach work without suffering a significant hit in the expansion factor.

in the analysis by exploiting the extra structure possessed by these subspaces. In turn this calls for better "subspace designs" which we construct. Broadly speaking, our approach necessitates the use of more sophisticated ideas from linear-algebraic list-decoding than were present in [GUV09].

We now describe our approach in more detail. Let $\mathbb{F}_{q^n}[X;(\cdot)^q]_{<k}$ denote the space of all linearized polynomials of q-degree less than k. We fix a subspace $\mathcal{F} \subseteq \mathbb{F}_{q^n}[X;(\cdot)^q]_{<k}$ of dimension n over $\mathbb{F}_q$, and then each Γ_j is simply the evaluation of $f \in \mathcal{F}$ at a point $\alpha_j \in \mathbb{F}_{q^n}$, i.e., $\Gamma_j(f) = f(\alpha_j)$. We will in fact choose $\alpha_1, \dots, \alpha_d$ to span a degree d field extension $\mathbb{F}_h$ over $\mathbb{F}_q$.

The analysis of this construction mirrors the proof of the list-decodability of the codes from [GWX16] and we sketch it here. In contrapositive, the dimension expander property amounts to showing that for every subspace $V \subseteq \mathbb{F}_{q^n}$ of bounded dimension, the space of $f \in \mathcal{F}$ such that $f(\alpha_j) \in V \; \forall j \in [d]$ has dimension about a factor d smaller. So we study the structure of the space of polynomials $f \in \mathbb{F}_{q^n}[X,(\cdot)^q]_{<k}$ which, for some fixed subspace V, have $f(\alpha_j) \in V$ for all $j \in [d]$, and show that it forms a *periodic subspace* (cf. Definition 2.7). Thus, the challenge at this point is to find an appropriate subspace $\mathcal{F} \subseteq \mathbb{F}_{q^n}[X;(\cdot)^q]_{<k}$ that has small intersection with *every* periodic subspace.

We accomplish this by using an appropriate construction of a *subspace design* (cf. Definition 2.6). Subspace designs were originally formulated for applications to algebraic list-decoding, where they led to optimal redundancy list-decodable codes over small alphabets [GX13] and over the rank-metric [GWX16]. Briefly, subspace designs are collections of subspaces $\{H_i\}_{i=1}^k$ such that, for any subspace W of bounded dimension, the total intersection dimension $\sum_{i=1}^k \dim(H_i \cap W)$ is small. In fact, we will be interested in a slightly more general object: we are only required to have small intersection with $\mathbb{F}_h$-subspaces W, where we recall that $\mathbb{F}_h$ is an extension field of $\mathbb{F}_q$. Once we have a good subspace design, it will suffice to define $\mathcal{F} = \left\{ f(X) = \sum_{i=0}^{k-1} f_i X^{q^i} : f_i \in H_{i+1} \right\}$.

Thus, we have reduced the task of constructing dimension expanders to the task of constructing subspace designs. We provide two constructions, yielding our two claimed constructions of dimension expanders. Both use an explicit subspace design given in [GK16] as a black box (cf. Lemma 4.1). We remark that in this work the authors only considered the $d = 1$ case, i.e., the H_i's were required to have small intersection with all $\mathbb{F}_q$-subspaces, and not just $\mathbb{F}_h$-subspaces. Thus, our task is easier in the sense that we only require intersection with $\mathbb{F}_h$-subspaces to be small. However, for our purposes, we will require a better bound on the total intersection dimension than that which is guaranteed by [GK16]. We also remark that this construction requires linear-sized fields which prevents us from obtaining dimension expanders over fields of subpolynomial size.

The subspace design which yields our degree-proportional expander is more elementary so we describe it first. Essentially, we take the subspace design of [GK16] and define it over an "intermediate field" $\mathbb{F}_\ell$, i.e., $\mathbb{F}_q \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_h$. By appropriately choosing the degree of the extension we are able to guarantee smaller intersections with $\mathbb{F}_h$-subspaces and also allow q to be smaller (as it is now only ℓ that must be linear in n, and we can take $\ell \approx q^{1/\delta}$).

Our construction which yields lossless dimension expanders is more involved. We take the construction of [GK16] and now view it as lying in $\mathbb{F}_q[Y]_{<\delta n}$ (for an appropriately chosen constant $\delta > 0$), where $\mathbb{F}_q[Y]_{<\delta n}$ denotes the $\mathbb{F}_q$-vector space of polynomials of degree $< \delta n$. We then map each of the subspaces into $\mathbb{F}_h^{n/d}$ by evaluating the polynomials at a tuple of correlated degree d places (recall that $h = q^d$). Identifying $\mathbb{F}_h^{n/d}$ with $\mathbb{F}_{q^n}$ completes the construction. Ideas similar to the linear algebraic list-decoding of folded Reed-Solomon codes [Gur11, GW13] are used to prove the final bound on intersection dimension, which with a careful choice of parameters is good enough to guarantee lossless expansion. For technical reasons, in order to explicitly construct the degree d place we require $n = q - 1$.

Lastly, while we are able to use explicit constructions of subspace designs to obtain degree-proportional dimension expanders, we observe that with high probability a random $\mathbb{F}_q$-subspace H of dimension n/k will have small intersection with every $\mathbb{F}_h$-subspace W of bounded dimension. We refer to such an H as a *subspace evasive subspace* (cf. Definition A.1). Then, instantiating our approach with $\mathcal{F} = \left\{ f(X) = \sum_{i=0}^{k-1} f_i X^{q^i} : f_i \in H \right\}$ will provide a *degree-proportional* dimension expander. Thus, an explicit construction of a subspace evasive subspace with parameters matching the probabilistic construction would yield an explicit degree-proportional dimension expander. We leave the construction of such an H, which seems like an interesting object in its own right, for future work.

1.3 Previous work

We now survey previous work on dimension expanders. Previous constructions have followed one of three main approaches: the first uses Cayley graphs of groups satisfying Kazhdan's property T, the second uses monotone expanders, and the third uses rank condensers.

Property T. The problem of constructing dimension expanders was originally proposed by Wigderson [Wig04, BISW04]. Along with the definition, he conjectured that dimension expanders could be constructed with Cayley graphs. This is in analogy with expander graphs, where such approaches have been very successful. To construct an expanding Cayley graph, one uses a group G with generating set S satisfying *Kazhdan's property T*. Wigderson conjectured (see Dvir and Wigderson [DW10], Conjecture 7.1) that an expanding Cayley graph would automatically yield a dimension expander. More precisely, if one takes any irreducible representation $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ of the group G, then $\rho(S)$ would provide a dimension expander.

In characteristic zero, Lubotzky and Zelmanov [LZ08] succeeded in proving Wigderson's conjecture. Unfortunately, their approach intrinsically uses the notion of unitarity which does not possess a meaningful definition over positive characteristic. They also provided an example of an expanding group whose linear representation over a finite field does *not* yield a dimension expander, although in the example the characteristic of the field divides the order of the group. In an independent work, Harrow [Har08] proved the same result in the context of *quantum expanders*, which imply dimension expanders in characteristic zero. The following theorem summarizes this discussion.

Theorem 1.6 ([LZ08, Har08]). *Let $\mathbb{F}$ be a field of characteristic zero, $n \geq 1$ an integer. There exists an explicit $(1/2, 1 + \Omega(1))$-dimension expander over $\mathbb{F}^n$ of constant degree.*

Unfortunately, this approach is inherently unable to construct unbalanced dimension expanders. Moreover, it is unclear to us if it is possible to obtain expansion proportional to the degree via this strategy.

Monotone expanders. Consider a bipartite graph G with left and right partition given by $[n]$, and let $\Gamma_1, \ldots, \Gamma_d : [n] \to [n]$ denote the neighbor (partial)[4] functions of the graph, i.e., each left vertex $i \in [n]$ is connected to $\Gamma_j(i)$ whenever it's defined. One can then define the linear maps $\Gamma_1', \ldots, \Gamma_d'$ which map $e_i \mapsto e_{\Gamma_j(i)}$ whenever $\Gamma_j(i)$ is defined and then extending linearly, where the e_i are the standard basis vectors. It is easily seen that if G is an expander, the corresponding collection $\{\Gamma_j'\}_{j=1}^d$ will expand subspaces of the form $\mathrm{span}\{e_i : i \in S\}$ for $S \subseteq [n]$. To expand all subspaces (and hence obtain dimension expanders), Dvir and Shpilka [DS11] implicitly observed that it is sufficient for the maps Γ_j to be *monotone* (this observation is made explicit in [DW10]).

[4] That is, Γ_j need only be defined on a *subset* of $[n]$.

Note that the matrices Γ'_j have entires in $\{0,1\}$, and they form a dimension expander over *every* field.

Thus, in order to construct dimension expanders, it suffices to construct monotone expander graphs. Unfortunately, constructing monotone expander graphs is a *highly* non-trivial task: indeed, the standard probabilistic arguments seem insufficient to even prove the *existence* of monotone expanders (see [DW10, BY13]). Nonetheless, Dvir and Shpilka [DS07] succeeded in constructing monotone expanders with logarithmic degree, as well as constant-degree expanders with inverse-logarithmic expansion. Later, using the zig-zag product of Reingold, Vadhan and Wigderson [RVW02], Dvir and Wigderson [DW10] constructed monotone expanders of degree $\log^{(c)} n$ (the c-th iterated logarithm) for any constant c. Moreover, given any constant-degree monotone expander as a starting point (which is not known to exist via the probabilistic method), their method is capable of constructing a constant degree monotone expander graph. Lastly, by a sophisticated analysis of expansion in the group $\mathrm{SL}_2(\mathbb{R})$, Bourgain and Yehudayoff [BY13] were able to construct explicit monotone expanders of constant degree. Thus, we have the following theorem.

Theorem 1.7 ([BY13])**.** *Let $n \geq 1$ be an integer. There exists an explicit $(1/2, 1+\Omega(1))$-dimension expander of degree $O(1)$ over $\mathbb{F}^n$, for every field $\mathbb{F}$.*

Unfortunately, just as with the previous approach, it is unclear to us if this argument could be adapted to yield degree-proportional dimension expanders.

Rank condensers. This final approach to constructing dimension expanders, developed by Forbes and the first author [FG15], uses *rank condensers.* Unlike the constructions of the previous sections, it inherently uses properties of finite fields and ideas from algebraic pseudorandomness more broadly, and thus is most in the spirit of our work. The construction proceeds in two steps. First, one "trivially" expands the subspaces by a factor of d by defining $T_j : \mathbb{F}^n \to \mathbb{F}^n \otimes \mathbb{F}^d$ mapping $v \mapsto v \otimes e_j$. The challenge is then to map $\mathbb{F}^n \otimes \mathbb{F}^d \cong \mathbb{F}^{nd}$ back to $\mathbb{F}^n$ such that subspaces do not decrease in dimension too much. This is precisely the problem of *lossy rank condensing*, namely, of constructing a small collection of linear maps $S_k : \mathbb{F}^{nd} \to \mathbb{F}^n$ such that, for any subspace U of bounded degree, there exists some S_k such that $\dim S_k(U) \geq (1-\varepsilon)\dim U$. To complete the construction, one takes the set of all $S_k T_j$ for all k, j. We remark that the construction of the rank condenser from this work used the subspace designs of [GK16], providing more evidence for the interrelatedness of the objects studied in algebraic pseudorandomness. Unfortunately, the construction of subspace designs used in this work require polynomially large fields. The authors are able to decrease the field size using techniques reminiscent of code-concatenation at the cost of certain logarithmic penalties.

The following theorem was obtained.

Theorem 1.8 ([FG15])**.**

1. *Let $n, d \geq 1$. Assume $|\mathbb{F}| \geq \Omega(n^2)$. There exists an explicit $(\Omega(1/\sqrt{d}), \Omega(\sqrt{d}))$-dimension expander in $\mathbb{F}^n$ of degree d.*
2. *Let $\mathbb{F}_q$ be a finite field, $n, d \geq 1$. There exists an explicit $(\Omega(1/d\log_q(dn)), \Omega(d))$-dimension expander in $\mathbb{F}_q^n$ of degree $O(d^2\log_q(dn))$.*

In order to improve the dependence on the field size, improved subspace designs over small fields were constructed by Guruswami, Xing and Yuan [GXY17]. These subspace designs yield a family of explicit $(\Omega(1/\log_q \log_q n), 1+\Omega(1))$-dimension expander of degree $O(\log_q n)$ over $\mathbb{F}_q^n$.

1.4 Organization

In Section 2 we set notation and define the various pseudorandom objects that we use in our construction. We also provide probabilistic arguments ascertaining the existence of good dimension expanders in order to set expectations. In Section 3 we prove that the problem of constructing dimension expanders can be reduced to that of constructing appropriate subspace designs, which is the task we address in Section 4. In Section 5, we put all of the pieces together to deduce our main theorems for balanced dimension expanders. In Section 6 we show that all our results readily adapt to the case of unbalanced expanders. Finally we summarize our work and list open problems in Section 7, while Appendix A contains a discussion of subspace evasive subspaces. On a first reading, we recommend the reader skim the definitions in Section 2, and then focus on the core of the paper, which is contained in Sections 3 and 4.

2 Background

Notation. First, we briefly summarize the notation that we will use regularly (other notation will be introduced as needed). $\mathbb{F}$ will always refer to an arbitrary field, q always denotes a prime power, and $\mathbb{F}_q$ denotes the finite field with q elements. We denote $[n] := \{1, \ldots, n\}$. We write $a|b$ to assert that the integer a divides the integer b without remainder.

Given a subspace $U \subseteq \mathbb{F}^n$ and a linear map $T : \mathbb{F}^n \to \mathbb{F}^m$, $T(U) = \{Tu : u \in U\}$ denotes the image of the subspace U under the map T. Given two subspaces $U, V \subseteq \mathbb{F}^n$, $U + V = \{u + v : u \in U, v \in V\}$ denotes their sum, which is also a subspace.

The finite field with q^n elements, i.e., $\mathbb{F}_{q^n}$, has the structure of a vector space over $\mathbb{F}_q$ of dimension n. Thus, we often identify $\mathbb{F}_{q^n}$ with $\mathbb{F}_q^n$. Moreover, if $h = q^d$ is a power of q and $d|n$, so $\mathbb{F}_h \subseteq \mathbb{F}_{q^n}$, the field $\mathbb{F}_{q^n}$ also has the structure of a vector space over $\mathbb{F}_h$ of dimension n/d. Throughout this work, we will always assume $d|n$ and write $n = md$.

We will sometimes have subspaces of $W \subseteq \mathbb{F}_{q^n}$ that are linear over $\mathbb{F}_h$, i.e., for all $w \in W$ and $\alpha \in \mathbb{F}_h$ we have $\alpha w \in W$. When we wish to emphasize this, we will say that W is an $\mathbb{F}_h$-subspace. Moreover, we will write $\dim_{\mathbb{F}_q} W$ or $\dim_{\mathbb{F}_h} W$ if we need to emphasize that the dimension is computed when viewing W as an $\mathbb{F}_q$-subspace or as an $\mathbb{F}_h$-subspace, respectively.

A *q-linearized polynomial* f is a polynomial of the form $f(X) = \sum_{i=0}^{k-1} f_i X^{q^i}$. We denote the space of q-linearized polynomials with coefficients in $\mathbb{F}_{q^n}$ as $\mathbb{F}_{q^n}[X; (\cdot)^q]$. The *$q$-degree* of a linearized polynomial $f(X) = \sum_{i=0}^{k-1} f_i X^{q^i}$ is the maximum i such that $f_i \neq 0$, and is denoted $\deg_q f$. We denote $\mathbb{F}_{q^n}[X; (\cdot)^q]_{<k} = \left\{ f \in \mathbb{F}_{q^n}[X; (\cdot)^q] : \deg_q f < k \right\}$, which we remark is a k-dimensional vector space over $\mathbb{F}_{q^n}$.

Note that if $\alpha, \beta \in \mathbb{F}_{q^n}$ and $a, b \in \mathbb{F}_q$ then for any $f \in \mathbb{F}_{q^n}[X; (\cdot)^q]$, $f(a\alpha + b\beta) = af(\alpha) + bf(\beta)$, i.e., f gives an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. Moreover, the space of roots of such an f is an $\mathbb{F}_q$-subspace of dimension at most $\deg_q f$ (assuming $f \neq 0$).

2.1 Dimension expanders

We now formally define dimension expanders and provide an alternate characterization that we find easier to reason about.

Definition 2.1 (Dimension expander)**.** Let $n, d \geq 1$ be an integer, $\eta > 0$ and $\beta > 1$. Let $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}^n \to \mathbb{F}^n$ be linear maps. The collection $\{\Gamma_j\}_{j=1}^d$ forms a (η, β)-*dimension expander* if for all

Figure 1: Regularly used parameters and notations

Parameter	Meaning	Comments
n	the dimension of the expander	growing
q	a prime power	expanders will be $\mathbb{F}_q$-linear
d	the degree of the expander	$d\|n$
h	a power of q	evaluation points span $\mathbb{F}_h/\mathbb{F}_q$; $h = q^d$
k	q-degree bound for linearized polynomials	$1 \leq k \leq d$, $k\|d$
$\mathbb{F}_{q^n}[X, (\cdot)^q]_{<k}$	q-linearized polynomials of q-degree $< k$	domain of expanders is a subspace
$\mathbb{F}_{q^n}$	degree n extension of $\mathbb{F}_q$	image space of expander
m	degree of $\mathbb{F}_{q^n}/\mathbb{F}_h$	$m = \frac{n}{d}$
N	dimension of domain for unbalanced expanders	$k\|N$
b	the "unbalancedness"; assume $\in \mathbb{Z}$	$b = \frac{N}{n}$

subspaces $U \subseteq \mathbb{F}^n$ of dimension at most ηn,

$$\dim\left(\sum_{j=1}^{d} \Gamma_j(U)\right) \geq \beta \dim U \ .$$

The *degree* of the dimension expander is d.

When clear from context we refer to a dimension expander just as an *expander*. The following proposition follows easily from the definitions.

Proposition 2.2 (Contrapositive characterization)**.** *Let $n \geq 1$ be an integer, $\eta > 0$ and $\beta > 1$. Let $\Gamma_1, \dots, \Gamma_d : \mathbb{F}^n \to \mathbb{F}^n$ be linear maps. Suppose that for all $V \subseteq \mathbb{F}^n$ of dimension at most ηn,*

$$\dim\{u \in \mathbb{F}^n : \Gamma_j(u) \in V \quad \forall j \in [d]\} \leq \frac{1}{\beta}\dim V \ .$$

Then $\{\Gamma_j\}_{j=1}^d$ forms an $(\frac{\eta}{\beta}, \beta)$-dimension expander.

Proof. Let $U \subseteq \mathbb{F}^n$ be a subspace of dimension at most $(\eta/\beta)n$ and put $V = \sum_{j=1}^d \Gamma_j(U)$. If $\dim(V) > \eta n$ then we are done, so assume $\dim(V) \leq \eta n$. By the assumption of the proposition, this tells us that

$$\dim\{u \in \mathbb{F}^n : \Gamma_j(u) \in V \quad \forall j \in [d]\} \leq \frac{1}{\beta}\dim V \ .$$

Since $U \subseteq \{u \in \mathbb{F}^n : \Gamma_j(u) \in V \quad \forall j \in [d]\}$, we have $\dim U \leq \frac{1}{\beta}\dim V$. Rearranging this yields $\dim V \geq \beta \dim U$, as was to be shown. □

Next, we define a slight generalization of dimension expanders, wherein the domain and codomain may no longer have the same dimension. That is, the linear maps Γ_j now map $\mathbb{F}^N \to \mathbb{F}^n$, where N, n may not be equal. We parametrize the "unbalancedness" of the dimension expander by $b = \frac{N}{n}$. In our construction we will assume for simplicity that $b \in \mathbb{Z}$, although we note that this is not a fundamental restriction. The formal definition is as follows.

Definition 2.3 (Unbalanced dimension expanders)**.** Let $N, n, d \geq 1$ be integers, $\eta > 0$ and $\beta > 1$. Let $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}^N \to \mathbb{F}^n$ be linear maps. Set $b = \frac{N}{n}$. The collection $\{\Gamma_j\}_{j=1}^d$ forms a *b-unbalanced* (η, β)*-dimension expander* if for all subspaces $U \subseteq \mathbb{F}^N$ of dimension at most ηN,

$$\dim \left(\sum_{j=1}^{d} \Gamma_j(U) \right) \geq \beta \dim U \ .$$

The *degree* of the unbalanced dimension expander is d.

The appropriate generalization of Proposition 2.2 is as follows. As the proof is a very simple adaptation of the proof of Proposition 2.2 we omit it.

Proposition 2.4 (Contrapositive characterization)**.** *Let $N, n \geq 1$ be integers, $\eta > 0$ and $\beta > 1$. Put $b = \frac{N}{n}$. Let $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}^N \to \mathbb{F}^n$ be linear maps. Suppose that for all $V \subseteq \mathbb{F}^n$ of dimension at most ηN,*

$$\dim \left\{ u \in \mathbb{F}^N : \Gamma_j(u) \in V \quad \forall j \in [d] \right\} \leq \frac{1}{\beta} \dim V \ .$$

Then $\{\Gamma_j\}_{j=1}^d$ forms a b-unbalanced $(\frac{\eta}{\beta}, \beta)$-dimension expander.

We now quote the parameters achievable by a random construction of unbalanced dimension expanders. This sets the stage and ultimate target to aim for with explicit constructions. We prove this proposition in Appendix D, and we remark that our argument is completely analogous to that given in Section C.3 of [FG15].

Proposition 2.5 (Simple generalization of Proposition C.10 of [FG15])**.** *Let $\mathbb{F}_q$ be a finite field, N, n positive integers and put $b := \frac{N}{n}$. Let $\beta > 1$ and $\eta \in (0, \frac{1}{b\beta})$. Then, assuming*

$$d \geq \beta + \frac{b}{1 - b\beta\eta} + \log_q 16 \ ,$$

there exists a collection of linear maps $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}_q^N \to \mathbb{F}_q^n$ forming a (η, β)-unbalanced dimension expander.

Thus, for $b = 1$, if we wish to have $\beta = (1 - \varepsilon)d$ and $\eta = \frac{1-\varepsilon}{d}$ we may take $d = O(1/\varepsilon^2)$. We remark that in Theorem 5.2, we obtain $d = O(1/\varepsilon^3)$. Similarly, for the b-unbalanced case, if we would like $\beta = (1 - \varepsilon)d$ and $\eta = \frac{1-\varepsilon}{bd}$ we may take $d = O(b/\varepsilon^2)$, while in Theorem 6.7 we obtain $d = O(b/\varepsilon^3)$.

2.2 Subspace design

A crucial ingredient in our construction of dimension expanders are subspace designs. They were originally introduced by two of the authors [GX13] in order to obtain algebraic codes list-decodable up to the Singleton bound. As in [GWX16], we will be concerned with a slight weakening of this notion, where we are only concerned with having small intersection with subspaces which are linear over an extension of the base field, although we will also require the intersection dimension to be smaller.

Definition 2.6. Let V be a $\mathbb{F}_{q^d}$-vector space. A collection $H_1, \ldots, H_k \subseteq V$ of $\mathbb{F}_q$-subspaces is called a (s, A, d)*-subspace design in V* if for every $\mathbb{F}_{q^d}$-subspace $W \subseteq V$ of $\mathbb{F}_{q^d}$-dimension s,

$$\sum_{i=1}^{k} \dim_{\mathbb{F}_q}(H_i \cap W) \leq As \ .$$

We call a subspace design *explicit* if there is an algorithm outputting $\mathbb{F}_q$-bases for each subspace H_i in $\mathsf{poly}(n)$ field operations.

Remark. In previous works, what we have termed a (s, A, d)-subspace design would have been called a (s, As, d)-subspace design. We find it more convenient in this work to remove the multiplicative factor of s from the parameter in the definition.

2.3 Periodic subspaces

We now abstract the kind of structure that will be found in the subspace of $\mathbb{F}_q^n$ which is mapped entirely into a low-dimensional subspace of $\mathbb{F}_q^n$ by the d linear transformations in our dimension expander construction. We note that our definition here is slightly different in form and notation than earlier ones in [GX13, GWX16].

Definition 2.7 (Periodic subspaces)**.** For positive integers n, k, s, d with $d|n$, an $\mathbb{F}_q$-subspace T of $\mathbb{F}_{q^n}^k$ is said to be (s, d)*-periodic* if there exists an $\mathbb{F}_{q^d}$-subspace $W \subseteq \mathbb{F}_{q^n}$ of dimension at most s such that for all j, $1 \le j \le k$, and all $\xi_1, \xi_2, \ldots, \xi_{j-1} \in \mathbb{F}_{q^n}$, the $\mathbb{F}_q$-affine subspace

$$\{\xi_j : \exists v \in T \text{ with } v_\iota = \xi_\iota \text{ for } 1 \le \iota \le j\} \subseteq \mathbb{F}_{q^n}$$

belongs to a coset of W. In other words, for every *prefix* $(\xi_1, \ldots, \xi_{j-1})$, the possible extensions ξ_j to the j'th symbol that can belong to a vector in T are contained in a coset of W.

An important property of periodic subspaces is that they have small intersection with subspace designs. This is captured by the following proposition.

Proposition 2.8 ([GWX16], Proposition 3.9)**.** *Let T be a (s, d)-periodic $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^k$, and $H_1, \ldots, H_k \subseteq \mathbb{F}_{q^n}$ be $\mathbb{F}_q$-subspaces forming a (s, A, d) subspace design in $\mathbb{F}_{q^n}$. Then $T \cap (H_1 \times \cdots \times H_k)$ is an $\mathbb{F}_q$-subspace of dimension at most As.*

For completeness, we provide the proof in Appendix B.

3 Dimension expander construction

As discussed in the introduction (Section 1), the construction of our dimension expander is inspired by recent constructions of variants of Gabidulin codes for list decoding in the rank metric. Indeed, the analysis of our dimension expander proceeds similarly to the analysis of list-decodability of the rank-metric codes presented in [GWX16]. The presentation here is self-contained algebraically, and does not refer to any coding-theoretic context or language.

Construction. Our dimension expanders map $\mathbb{F}_q^n \to \mathbb{F}_q^n$. We view the domain as

$$\mathcal{F} := \left\{ f(X) = \sum_{i=0}^{k-1} f_i X^{q^i} : f_i \in H_i,\ i = 0, \ldots, k-1 \right\}$$

where $H_0, \ldots, H_{k-1}$ give a collection of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$, each of $\mathbb{F}_q$-dimension $\frac{n}{k}$ (thus, we assume $k|n$). We will choose $H_1, H_2, \ldots, H_k$ forming a subspace design. We view the image space as $\mathbb{F}_{q^n}$. Let $h = q^d$, and let $\alpha_1, \ldots, \alpha_d$ give a basis for $\mathbb{F}_h$ over $\mathbb{F}_q$. We assume $d|n$ and write $md = n$. For $j = 1, \ldots, d$, we define

$$\Gamma_j : \mathcal{F} \to \mathbb{F}_{q^n} \quad \text{by} \quad f \mapsto f(\alpha_j)\ . \tag{1}$$

That is, each $\Gamma_j(f)$ is just the evaluation of f at the basis element α_j. These maps are clearly linear over $\mathbb{F}_q$.

Analysis. We now prove that the collection $\{\Gamma_j\}_{j=1}^d$ forms a dimension expander.

For a positive integers D, s with $s \leq m$, we define $\mathcal{L}_{D,s}$ to be the space of polynomials $Q \in \mathbb{F}_{q^n}[Z_0, \dots, Z_{s-1}]$ of the form $Q(Z_0, \dots, Z_{s-1}) = A_0(Z_0) + \cdots + A_{s-1}(Z_{s-1})$ with each $A_i \in \mathbb{F}_{q^n}[X; (\cdot)^q]_{<D}$, i.e., each A_i is a q-linearized polynomial of q-degree at most $D-1$.

Lemma 3.1. *Let $V \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-subspace of dimension B. If $Ds > B$, there exists a nonzero polynomial $Q \in \mathcal{L}_{D,s}$ such that*

$$\forall v \in V, \quad Q(v, v^h, \dots, v^{h^{s-1}}) = 0 \ . \tag{2}$$

Proof. Let $v_1, \dots, v_B$ give a basis for V over $\mathbb{F}_q$. Then, since $\gamma \mapsto \gamma^h = \gamma^{q^d}$ is a linear operation over $\mathbb{F}_q$, so long as $Q(v_i, v_i^h, \dots, v_i^{h^{s-1}}) = 0$ for all $i \in [B]$ we have $Q(v, v^h, \dots, v^{h^{s-1}}) = 0$ for all $v \in V$. Thus, finding such a Q amounts to solving a homogeneous linear system over $\mathbb{F}_{q^n}$ with B constraints. Since the $\mathbb{F}_{q^n}$-dimension of $\mathcal{L}_{D,s}$ is $Ds > B$, a nonzero $Q \in \mathcal{L}_{D,s}$ meeting Condition (2) must exist. □

Given a polynomial $g(X) = g_0 + g_1X + \cdots + g_rX^r$ and an automorphism τ of $\mathbb{F}_{q^n}$, we write g^τ for the polynomial $g^\tau(X) = \tau(g_0) + \tau(g_1)X + \cdots + \tau(g_r)X^r$, and let $g^{\tau^i} = (g^{\tau^{i-1}})^\tau$. We let $\sigma : \gamma \mapsto \gamma^h$, i.e., σ is the Frobenius automorphism of $\mathbb{F}_{h^m} = \mathbb{F}_{q^n}$ over $\mathbb{F}_h$.

Lemma 3.2. *Let $f \in \mathbb{F}_{q^n}[X]$ be a q-linearized polynomial with q-degree at most $k-1$. Let $V \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-subspace, and $Q \in \mathcal{L}_{D,s}$ a polynomial satisfying* (2)*. Suppose that $f(\alpha) \in V$ for all $\alpha \in \mathbb{F}_h = \mathbb{F}_{q^d}$ and that $D \leq d-k+1$. Then*

$$A_0(f(X)) + A_1(f^\sigma(X)) + \cdots + A_{s-1}(f^{\sigma^{s-1}}(X)) = Q(f(X), f^\sigma(X), \dots, f^{\sigma^{s-1}}(X)) = 0 \ . \tag{3}$$

Proof. Let $\alpha \in \mathbb{F}_h$. Since $f(\alpha) \in V$ by assumption, we have

$$Q(f(\alpha), f(\alpha)^h, \dots, f(\alpha)^{h^{s-1}}) = 0$$

as we have assumed Q satisfies Equation (2). Now, since $\alpha \in \mathbb{F}_h$, we have $\alpha^h = \alpha$, so

$$f(\alpha)^h = \left(\sum_{i=0}^{k-1} f_i \alpha^{q^i} \right)^h = \sum_{i=0}^{k-1} f_i^h (\alpha^{q^i})^h = \sum_{i=1}^{k-1} f_i^h \alpha^{q^i} = f^\sigma(\alpha) \ ,$$

and by iterating we have $f(\alpha)^{h^i} = f^{\sigma^i}(\alpha)$ for all $i = 0, \dots, s-1$. Thus, we find that for all $\alpha \in \mathbb{F}_h$,

$$Q(f(\alpha), f^\sigma(\alpha), \dots, f^{\sigma^{s-1}}(\alpha)) = 0 \ .$$

Now, the univariate polynomial $R_f(X) := Q(f(X), f^\sigma(X), \dots, f^{\sigma^{s-1}}(X)) \in \mathbb{F}_{q^n}[X]$ has q-degree at most $(D-1) + (k-1) = D + k - 2$. Thus, if $D \leq d - k + 1$, the q-degree of $R_f(X)$ is at most $d-1$. Since it vanishes on $\mathbb{F}_h$, an $\mathbb{F}_q$-subspace of dimension d, we conclude that $R_f(X)$ must be the 0 polynomial. □

Lemma 3.3. *The set of solutions to Equation* (3)*, for any nonzero $Q \in \mathcal{L}_{D,s}$ (for arbitrary D), is an $(s-1, d)$-periodic subspace.*

Proof. First, by replacing $A_0, \dots, A_{s-1}$ with $A_0^{q^j}, \dots, A_{s-1}^{q^j}$ for an appropriate j and identifying X^{q^n} with X (which is valid since we only ever evaluate the polynomials on elements of $\mathbb{F}_{q^n}$), we may assume that there exists an $i^* \in \{0, \dots, s-1\}$ such that A_{i^*} has a nonzero coefficient on X. (Of course, this might increase the q-degree of the A_i.)

Write $A_\iota(X) = a_{\iota,0}X + a_{\iota,1}X^q + a_{\iota,2}X^{q^2} + \cdots$ for $\iota = 0,\dots,s-1$. Then, for $\ell = 0,1,\dots,k-1$, we define

$$B_\ell(X) := a_{0,\ell}X + a_{1,\ell}X^h + \cdots + a_{s-1,\ell}X^{h^{s-1}} \ .$$

Since $a_{i^*,0} \neq 0$, we see that $B_0 \neq 0$. Since $s-1 \leq m-1$, if $W = \ker(B_0)$, we find that W is an $\mathbb{F}_h$-subspace of $\mathbb{F}_{q^n} = \mathbb{F}_{h^m}$ of dimension at most $s-1$.

The condition (3) informs us that

$$A_0(f(X)) + A_1(f^\sigma(X)) + \cdots + A_{s-1}(f^{\sigma^{s-1}}(X)) = 0 \ . \tag{4}$$

The coefficient of X in the left hand size of (4) is $B_0(f_0)$; upon equating it to 0, we see $f_0 \in W$.

Now, fix an $i \in \{1,\dots,k-1\}$. The coefficient of X^{q^i} in the left hand side of (4) is

$$B_i(f_0^{q^i}) + B_{i-1}(f_1^{q^{i-1}}) + \cdots + B_1(f_{i-1}^q) + B_0(f_i) \ .$$

Upon equating this coefficient to 0, we see that $f_i \in W + \theta_i$, where $\theta_i \in \mathbb{F}_{q^n}$ is determined by $f_0, f_1, \dots, f_{i-1}$. Explicitly, we can take $\theta_i = -B_i(f_0^{q^i}) - B_{i-1}(f_1^{q^{i-1}}) - \cdots - B_1(f_{i-1}^q)$. Therefore, for each choice of $(f_0, f_1, \dots, f_{i-1})$, f_i must belong to a coset of the subspace W. This shows that the solutions lie in a $(s-1,d)$-periodic subspace. □

Equipped with these lemmas, we are in position to deduce our main theorem for this section.

Theorem 3.4. *Let $\{H_i\}_{i=0}^{k-1}$ give a (s,A,d)-subspace design for all $s \leq \mu n$ for some $0 < \mu < 1/d$. Then $\{\Gamma_j\}_{j=1}^d$ is a $(\mu A, \frac{d-k+1}{A})$-dimension expander. Moreover if the subspace design is explicit then the dimension expander is explicit.*

Proof. We will appeal to Proposition 2.2. Let $V \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-subspace of dimension $B \leq (d-k+1)\mu n$. Let

$$U := \{f \in \mathcal{F} : \Gamma_j(f) \in V \ \ \forall j \in [d]\}.$$

By the $\mathbb{F}_q$-linearity of the polynomials f and the fact that $\alpha_1,\dots,\alpha_d$ gives a basis for $\mathbb{F}_h$ over $\mathbb{F}_q$, we may rewrite this as

$$U = \{f \in \mathcal{F} : f(\alpha) \in V \ \ \forall \alpha \in \mathbb{F}_h\} \ .$$

Let $D = d-k+1$ and choose the integer s such that $\frac{B}{D} < s \leq \frac{B}{D} + 1 \leq \mu n + 1$. As $\mu < 1/d$, we have $s \leq n/d = m$. By Lemma 3.1, we have a nonzero $Q \in \mathcal{L}_{D,s}$ such that $Q(v, v^h, \dots, v^{h^{s-1}}) = 0$ for all $v \in V$. We then have that every $f \in \mathcal{F}$ satisfies (3), so we conclude that U is contained in a $(s-1,d)$-periodic subspace. Since $s-1 \leq \mu n$, our assumption on $\{H_i\}_{i=0}^{k-1}$ combined with Proposition 2.8 tells us that U is contained in an affine subspace over $\mathbb{F}_q$ of dimension at most $A(s-1)$. In particular, $\dim_{\mathbb{F}_q} U \leq A(s-1)$. Recalling $s-1 \leq \frac{B}{D}$,

$$\dim_{\mathbb{F}_q} U \leq A\frac{B}{D} = \frac{A}{D}\dim_{\mathbb{F}_q} V \ .$$

Applying Proposition 2.2 with $\eta = D\mu$ and $\beta = \frac{D}{A}$, we conclude that $\{\Gamma_j\}_{j=1}^d$ gives a $(\mu A, \frac{D}{A})$-dimension expander, as was to be shown.

Finally, as for the explicitness, suppose that $H_1,\dots,H_k$ are explicit. Thus, in $\mathsf{poly}(n)$ field operations we may output $\mathbb{F}_q$-bases $\mathcal{B}_1,\dots,\mathcal{B}_k$ for $H_1,\dots,H_k$. Then, the we construct the basis $\mathcal{B} = \{f = \sum_{i=0}^{k-1} f_i X^{q^i} : f_i \in \mathcal{B}_i, i \in [k]\}$, and enumerate $\mathcal{B} = \{g_1,\dots,g_n\}$. Finally, for $j \in [d]$ we output the matrix Γ_j obtained by evaluating $g_1(\alpha_j),\dots,g_n(\alpha_j)$, writing each $g_i(\alpha_j)$ in an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$, and then putting $g_i(\alpha_j)$ as the i-th column of Γ_j. □

Intuitively, we have that subspaces of dimension As are expanded to subspaces of dimension $(d-k+1)s/A$. This informs what we should hope for from our subspace designs. In particular, obtaining $A = O(1)$ is enough to obtain a degree proportional expander (by setting $k = \Theta(d)$), while if $A \approx 1+\varepsilon$ and $k \approx \varepsilon d$ we can obtain a *lossless* expander. With these goals in mind, we turn our attention to constructing subspace designs.

4 Constructions of subspace designs

For the case of $d = 1$, explicit constructions of subspace designs have been given in previous works. The first explicit construction was given in [GK16], using ideas which had been developed in constructions of list-decodable codes. This construction was subsequently improved over fields of small size in [GXY17].

A previous construction of a subspace design for $d > 1$ was given in [GWX16]. In this work, a subspace design over the base field (i.e., for $d = 1$) was intersected with a *subspace evasive set* from [DL12]. However, for our purposes, the size of the intersection dimension (i.e., the product As) of this construction is too large. In that work, the authors were more concerned with ensuring that the H_i's had large dimension; however, we only require that the H_i's have dimension n/k.

We provide two constructions of subspace designs in this work, yielding our two constructions of dimension expanders. The first construction yields a *degree-proportional* dimension expander over fields of size n^δ (for arbitrarily small constant δ). The next yields a *lossless* dimension expander. The only drawback is that it requires a field of size linear in n (for technical reasons, we take $q-1 = n$). We present our first construction in Section 4.1 and our second construction in Section 4.2.

Both of our constructions use as a black box a subspace design provided in [GK16]. Specifically, by taking $r = 2$ in Theorem 7 of [GK16], we obtain a subspace design with the following parameters.

Lemma 4.1. *For all positive integers s, t, m and prime powers ℓ satisfying $s \le t \le m < \ell$, there is an explicit collection of $M \ge \frac{\ell^2}{4t}$ $\mathbb{F}_\ell$-spaces $V_1, V_2, \ldots, V_M \subseteq \mathbb{F}_\ell^m$, each of codimension $2t$, which forms an $(s, \frac{m-1}{2(t-s+1)}, 1)$ subspace design in $\mathbb{F}_\ell^m$.*

4.1 Subspace designs via an intermediate field

This first construction takes the subspace design of Lemma 4.1 defined over an intermediate field $\mathbb{F}_\ell$. That is, we fix an integer $1 < c < d$ such that $c|d$ so that, for $\ell = q^c$, $\mathbb{F}_q \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_h$. Then, if $\omega_1, \ldots, \omega_m$ gives a basis for $\mathbb{F}_{h^m}/\mathbb{F}_h$, define

$$L = \left\{ \sum_{i=1}^{m} a_i \omega_i : a_i \in \mathbb{F}_\ell \right\} .$$

This is an $\mathbb{F}_\ell$-subspace of $\mathbb{F}_{h^m} = \mathbb{F}_{q^n}$ of $\mathbb{F}_\ell$-dimension m, as $\omega_1, \ldots, \omega_m$ are linearly independent over $\mathbb{F}_h$ and so *a fortiori* are linearly independent over the subfield $\mathbb{F}_\ell$. Thus, $L \simeq \mathbb{F}_\ell^m$, and we fix an $\mathbb{F}_\ell$-linear isomorphism $\psi : \mathbb{F}_\ell^m \to L$. Note that an $\mathbb{F}_\ell$-linear map is automatically $\mathbb{F}_q$-linear, so, in particular, the dimension of $\mathbb{F}_q$-subspaces in $\mathbb{F}_\ell^m$ are preserved by ψ. Then, if $V_1, \ldots, V_k$ give the subspace design from Lemma 4.1, we define $H_i := \psi(V_i)$ for $i = 1, \ldots, k$.

Our analysis of the subspace design makes use of the following lemma, whose proof is provided in Appendix C.

Lemma 4.2. *Let W be an $\mathbb{F}_h$-subspace of $\mathbb{F}_{q^n}$ and let $U := W \cap L$. Then U is an $\mathbb{F}_\ell$-subspace of L and $\dim_{\mathbb{F}_\ell} U \le \dim_{\mathbb{F}_h} W$.*

With this lemma we are in a position to prove our main proposition for this section.

Proposition 4.3. *Let $\ell = q^c$ with $c = \frac{d}{k} \cdot \frac{m}{m-2t}$, where $1 \le k < d$. For all $1 \le s < t < \ell$ and $1 \le k < d$ such that $\ell^2 \ge 4kt$, $k|d$, $m|k(m-2t)$ and $k(m-2t)|n$, there is an explicit construction of $\{H_i\}_{i=1}^k$ that forms a $(s, \frac{d}{k} \cdot \frac{m-1}{m-2t} \cdot \frac{m}{2(t-s)}, d)$-subspace design in $\mathbb{F}_{q^n}$. Furthermore $\dim_{\mathbb{F}_q} H_i = \frac{n}{k}$ for all $i = 1, \dots, k$.*

Proof. The condition that $k|d$ implies $k|n$, so $\frac{n}{k} \in \mathbb{Z}$. The condition that $k(m-2t)|n$ implies that $c \in \mathbb{Z}$. Finally, the condition that $m|k(m-2t)$ implies $c|d$ and so $\mathbb{F}_\ell \subseteq \mathbb{F}_h \subseteq \mathbb{F}_{q^n}$. We take the first k subspaces $\{V_i\}_{i=1}^k$ given in Lemma 4.1 (which is valid since $\ell^2/(4t) \ge k$) and define $H_i = \psi(V_i)$ for $i = 1, \dots, k$. For any $\mathbb{F}_\ell$-subspace $U \subseteq L$ of $\mathbb{F}_\ell$-dimension $u < t$, we have

$$\sum_{i=1}^k \dim_{\mathbb{F}_\ell}(U \cap H_i) = \sum_{i=1}^k \dim_{\mathbb{F}_\ell}(\psi^{-1}(U) \cap V_i) \le \frac{(m-1)u}{2(t-u+1)} \ .$$

Now for any $\mathbb{F}_h$-subspace $W \subseteq \mathbb{F}_{q^n}$, Lemma 4.2 tells us that the intersection $U := W \cap L$ is an $\mathbb{F}_\ell$-subspace in L of dimension at most s. Let $u \le s$ be the $\mathbb{F}_\ell$-dimension of U. As $W \cap H_i = U \cap H_i$ (since $H_i \subseteq L$), we have

$$\sum_{i=1}^k \dim_{\mathbb{F}_q}(W \cap H_i) = c \sum_{i=1}^k \dim_{\mathbb{F}_\ell}(U \cap H_i) \le \frac{d}{k} \cdot \frac{m-1}{m-2t} \cdot \frac{m}{2(t-u)} u \le \frac{d}{k} \cdot \frac{m-1}{m-2t} \cdot \frac{m}{2(t-s)} s \ .$$

Note that each H_i has $\mathbb{F}_\ell$ dimension $m-2t$, i.e, it has $\mathbb{F}_q$-dimension $c(m-2t) = \frac{n}{k}$ by our choice of parameters.

As for the explicitness, we compute the bases $\mathcal{B}_1, \dots, \mathcal{B}_k$ for $V_1, \dots, V_k$ and then we obtain bases for $H_1, \dots, H_k$ by applying ψ to each element of the corresponding basis. Thus, assuming the basis for V_i can be computed in $\mathsf{poly}(m)$ field operations we may also compute a basis for H_i is $\mathsf{poly}(m) = \mathsf{poly}(n)$ field operations. □

We now fix parameters in such a way to show that we can obtain a subspace design over fields of size n^δ for any constant $\delta > 0$.

Corollary 4.4. *Let $\delta > 0$ be given and choose an integer r such that $\frac{1}{2\delta} < r \le \frac{1}{\delta}$. Let k, d be integers such that $d = 2k$ and $r|k$. Assume moreover that $2r|m$. Then, assuming $q \ge n^\delta$, there exists an explicit construction of $\{H_i\}_{i=1}^k$ that forms a $(s, \frac{8}{\delta}, d)$-subspace design in $\mathbb{F}_{q^n}$ for all $s \le \frac{1-2\delta}{4d} n$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{n}{k}$ for all $i = 1, \dots, k$.*

Proof. Put $t = \frac{1}{2}(1 - \frac{1}{r})m$, so $m - 2t = \frac{m}{r}$. Our assumptions on m imply that $t \in \mathbb{Z}$. Moreover, $k(m-2t) = km/r$, and so $m|k(m-2t)$ as we assumed $r|k$. We also have $k(m-2t) = km/r|md$ as $k|d$ and $(m/r)|m$. Thus, all the divisibility conditions of Proposition 4.3 are satisfied, so let $H_1, \dots, H_k \subseteq \mathbb{F}_{q^n}$ denote the explicit subspace design promised by the proposition, each satisfying $\dim_{\mathbb{F}_q} H_i = \frac{n}{k}$.

Defining c as in Proposition 4.3, we have

$$c = \frac{d}{k} \cdot \frac{m}{m-2t} = 2 \cdot \frac{m}{m/r} = 2r \ .$$

Next, assuming $s \le t/2 = \frac{1}{4}(1 - \frac{1}{r})m$, we have the bound

$$\frac{d}{k} \cdot \frac{m-1}{m-2t} \cdot \frac{m}{2(t-s)} \le 2r \cdot \frac{m}{\frac{1}{2}(1-\frac{1}{r})m} = \frac{4r}{1-\frac{1}{r}} \le 8r \le \frac{8}{\delta} \ ,$$

where the second to last inequality is valid assuming $r \geq 2$ (which is valid assuming δ is sufficiently small). Note further that $\frac{1}{4}(1-\frac{1}{r}) \geq \frac{1}{4}(1-2\delta)$. Thus, we conclude that $H_1, \ldots, H_k$ forms a $(s, \frac{8}{\delta}, d)$-subspace design in $\mathbb{F}_{q^n}$ for all $s \leq \frac{1-2\delta}{4d}n$, as was to be shown.

Lastly, note that $c = 2r > 1/\delta$. To satisfy the conditions of Proposition 4.3 we require $\ell = q^c > t = \frac{1}{2}(1-\frac{1}{r})m$ and $\ell^2 \geq 4kt = 2k(1-\frac{1}{r})m$; note that the first condition implies the second for m large. Thus, we just require $q > t^{1/c}$, which is implied by $q \geq n^\delta$ as $t^{1/c} < n^\delta$. □

4.2 Construction via correlated high-degree places

This next construction utilizes techniques developed in the context of linear algebraic list-decoding of folded Reed-Solomon codes [Gur11, GW13]. Briefly, we take a subspace design in the space of polynomials of bounded degree, and then map it into $\mathbb{F}_h^m$ in a manner reminiscent of the encoding map of the folded Reed-Solomon code. As we are concerned with bounding the intersection dimension with $\mathbb{F}_h$-linear spaces, we in fact evaluate the polynomial at degree d places. The details follow.

Let ζ be a primitive root of the finite field $\mathbb{F}_q$. Choose a real $\delta \in (0,1)$ such that $\delta > \frac{1}{k}$ and $\delta n < q-1$, where we recall $0 < k < d$ and $n = md$. Denote by σ the automorphism of the function field $\mathbb{F}_q(Y)$ sending Y to ζY. The order of σ is $q-1 \geq m$. Given $g \in \mathbb{F}_q(Y)$, we abbreviate $g^\sigma := \sigma(g(Y)) = g(\zeta Y)$.[5]

Denote by $\mathbb{F}_q[Y]_{<\delta n}$ the set of polynomials of degree less than δn. By Lemma 4.1, there exist $V_1, V_2, \ldots, V_k$ of $\mathbb{F}_q[Y]_{<\delta n}$, each of codimension $\delta n - \frac{n}{k}$, which forms a $(r, \frac{\delta n - 1}{\delta n - \frac{n}{k} - 2r + 2}, 1)$ subspace design.

Let $P(Y)$ be an irreducible polynomial of degree d such that $P, P^\sigma, \ldots, P^{\sigma^{m-1}}$ are pairwise coprime. Consider the map

$$\pi : \mathbb{F}_q[Y]_{<\delta n} \to \mathbb{F}_{q^d}^m, \quad f \mapsto (f(P), f(P^\sigma), \ldots, f(P^{\sigma^{m-1}})) \ ,$$

where $f(P^{\sigma^j})$ is viewed as the residue of f in the residue field $\mathbb{F}_q[Y]/(P^{\sigma^j}) \cong \mathbb{F}_{q^d} = \mathbb{F}_h$. The Chinese Remainder Theorem guarantees that π is injective. We define

$$\widetilde{H}_i = \pi(V_i) = \left\{ (f(P), f(P^\sigma), \ldots, f(P^{\sigma^{m-1}})) : f \in V_i \right\} \subseteq \mathbb{F}_h^m \tag{5}$$

for $i = 1, 2, \ldots, k$.

We remark that this π is reminiscent the encoding map of the folded Reed-Solomon code (recall that $P^\sigma = P(\zeta Y)$), although in this case we evaluate f at the high-degree place P.

Proposition 4.5. *If $s < (1-\delta)m = (1-\delta)\frac{n}{d}$, then the subspaces $\widetilde{H}_1, \widetilde{H}_2, \ldots, \widetilde{H}_k$ defined above is an $(s, \frac{\delta}{1-\delta} \cdot \frac{m}{(\delta - \frac{1}{k})m - \frac{2s}{d(1-\delta)}}, d)$-subspace design in $\mathbb{F}_h^m$. Moreover $\dim_{\mathbb{F}_q} \widetilde{H}_i = \frac{n}{k}$ for all $i = 1, \ldots, k$.*

Lastly, when $n = q-1$, the subspace design can be constructed explicitly.

Proof. The claim about the $\mathbb{F}_q$-dimension of the $\widetilde{H}_i$'s follows from the fact that each V_i has $\mathbb{F}_q$-dimension $\frac{n}{k}$ and the injectivity of π.

Let W be an $\mathbb{F}_h$-subspace of $\mathbb{F}_h^m$ of dimension s and let $\{\mathbf{w}_i = (w_{i1}, \ldots, w_{im})\}_{i=1}^s$ be an $\mathbb{F}_h$-basis of W. Put $r = \lfloor \frac{s}{1-\delta} \rfloor$ and $D = \lfloor \frac{sd(m-r+1)}{r} \rfloor$. Then one can verify that

$$D + \delta dm < d(m-r+1) \ . \tag{6}$$

[5] Note that in Section 3 we wrote g^σ to denote the polynomial obtained by applying σ to the coefficients of g. We hope that this notation does not cause any confusion.

Consider the interpolation polynomial

$$R(X, Z_1, \ldots, Z_r) := A_0(X)Z_1 + A_1(X)Z_2 + \cdots + A_{r-1}(X)Z_r \ ,$$

where each $A_i(X) \in \mathbb{F}_q[X]$ has degree at most D. Consider the homogeneous equation system with coefficients of $A_i(X)$ as variables

$$A_0(P^{\sigma^j})w_{i,j+1} + A_1(P^{\sigma^j})w_{i,j+2} + \cdots + A_{r-1}(P^{\sigma^j})w_{i,j+r} = 0 \tag{7}$$

for $i = 1, 2, \ldots, s$ and $j = 0, 1, \ldots, m - r$. There are $s(m - r + 1)$ equations in $\mathbb{F}_h = \mathbb{F}_{q^d}$ and $r(D + 1)$ coefficients of $A_i(X)$ in $\mathbb{F}_q$ in total. Since $r(D + 1) > sd(m - r + 1)$, we can find polynomials $A_0, A_1, \ldots, A_{r-1} \in \mathbb{F}_q[X]$ of degree at most D that are not all zero such that the identities (7) hold.

For any $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in W$, we write $\mathbf{w} = \sum_{i=1}^{s} a_i \mathbf{w}_i$ for some $a_i \in \mathbb{F}_h$. By (7) we have

$$\begin{aligned} &A_0(P^{\sigma^j})w_{j+1} + A_1(P^{\sigma^j})w_{j+2} + \cdots + A_{r-1}(P^{\sigma^j})w_{j+r} \\ &= \sum_{i=1}^{s} a_i(A_0(P^{\sigma^j})w_{i,j+1} + A_1(P^{\sigma^j})w_{i,j+2} + \cdots + A_{r-1}(P^{\sigma^j})w_{i,j+r}) = 0 \end{aligned} \tag{8}$$

for $j = 0, 1, \ldots, m - r$.

Now for any element $(w_1, w_2, \ldots, w_m) \in W \cap \widetilde{H}_i$, there exists a function $f \in V_i$ such that $(f(P), f(P^\sigma), \ldots, f(P^{\sigma^{m-1}})) = (w_1, w_2, \ldots, w_m)$. By the identities (8), we have

$$A_0(P^{\sigma^j})f(P^{\sigma^j}) + A_1(P^{\sigma^j})f(P^{\sigma^{j+1}}) + \cdots + A_{r-1}(P^{\sigma^j})f(P^{\sigma^{j+r-1}}) = 0$$

for $j = 0, 1, \ldots, m - r$. This gives

$$(A_0 f + A_1 f^{\sigma^{-1}} + \cdots + A_{r-1} f^{\sigma^{-r+1}})(P^{\sigma^j}) = 0$$

for $j = 0, 1, \ldots, m - r$. As the polynomial $A_0 f + A_1 f^{\sigma^{-1}} + \cdots + A_{r-1} f^{\sigma^{-r-1}}$ has degree at most $D + \delta dm$ and it has $m - r + 1$ zeros at irreducible polynomials of degree d, by (6) we must have

$$A_0 f + A_1 f^{\sigma^{-1}} + \cdots + A_{r-1} f^{\sigma^{-r+1}} = 0 \ .$$

Recalling the definition of σ, we have

$$A_0(Y)f(Y) + A_1(Y)f(\zeta Y) + \cdots + A_{r-1}(Y)f(\zeta^{r-1}Y) = 0 \ . \tag{9}$$

Observe that the solutions $f \in \mathbb{F}_q[Y]_{<\delta n}$ to (9) form an $\mathbb{F}_q$-linear space; denote it by U. Our task now is to bound the dimension of U. This is essentially the content of Lemma 6 in [GW13], although we include the argument for completeness' sake. Write $f(Y) = f_0 + f_1 Y + \cdots + f_{k-1}Y^{k-1}$.

By factoring out common powers of Y we may assume that there exists $i^* \in \{0, 1, \ldots, r-1\}$ such that A_{i^*} has a nonzero constant term. Write $A_i(Y) = a_{i,0} + a_{i,1}Y + \cdots + a_{i,D}Y^D$ for $i = 0, 1, \ldots, r-1$, and define the polynomials

$$B_j(Y) := a_{0,j} + a_{1,j}Y + \cdots + a_{r-1,j}Y^{r-1}$$

for $j = 0, 1, \ldots, k - 1$. Note that our assumption on A_{i^*} states that $a_{i^*,0} \neq 0$, so B_0 is a nonzero polynomial of degree $\leq r - 1$. Let $\Lambda(Y) := A_0(Y)f(Y) + A_1(Y)f(\zeta Y) + \cdots + A_{r-1}(Y)f(\zeta^{r-1}Y)$, which is the 0 polynomial by the identity 9.

Note that the constant term of Λ is $a_{0,0}f_0 + a_{1,0}f_0 + \cdots + a_{r-1}f_0 = B_0(1)f_0$. Thus, assuming $B_0(1) \neq 0$ we find that $f_0 = 0$; otherwise f_0 can take an arbitrary value in $\mathbb{F}_q$.

Now fix an $\ell \in \{1, 2, \ldots, k-1\}$. The coefficient on Y^ℓ in $\Lambda(Y)$ may be expressed as $f_\ell B_0(\zeta^\ell) + f_{\ell-1}B_1(\zeta^{\ell-1}) + \cdots + f_1 B_{\ell-1}(\zeta) + f_0 B_\ell(1)$. As $\Lambda \equiv 0$, this linear form must equal 0. The crucial observation is that, assuming $B_0(\zeta^\ell) \neq 0$, once $f_0, \ldots, f_{\ell-1}$ are fixed there is a unique choice for $f_\ell \in \mathbb{F}_q$ such that this linear form is 0 (otherwise $f_\ell \in \mathbb{F}_q$ is unconstrained). We therefore obtain that the dimension of U is at most the number of $0 \leq \ell \leq k-1$ for which $B_0(\zeta^\ell) = 0$. As ζ is primitive and $k \leq q$, the elements ζ^ℓ for $\ell = 0, 1, \ldots, k-1$ are distinct. As B_0 is a nonzero polynomial of degree $\leq r-1$ we find that there can be at most $r-1$ values of ℓ such that $B_0(\zeta^\ell) = 0$. This implies that $\dim_{\mathbb{F}_q} U \leq r-1$.

Finally it is clear that $\pi^{-1}(W \cap \widetilde{H}_i) \subseteq U \cap V_i$ for $i = 1, 2, \ldots, k$. Thus, we have

$$\sum_{i=1}^{k} \dim_{\mathbb{F}_q}(\widetilde{H}_i \cap W) \leq \sum_{i=1}^{k} \dim_{\mathbb{F}_q}(V_i \cap U) \leq \frac{r(\delta dm - 1)}{\delta dm - \frac{dm}{k} - 2r + 2} \leq \frac{\delta}{1-\delta} \cdot \frac{m}{(\delta - \frac{1}{k})m - \frac{2s}{d(1-\delta)}} \cdot s \ .$$

This demonstrates that $\widetilde{H}_1, \ldots, \widetilde{H}_k$ form a subspace design as claimed.

Establishing the explicitness of this construction is a bit nontrivial, as there is no known deterministic algorithm to find irreducible polynomials of a given input degree. However, a simple approach is to assume $n = q-1$ and take the polynomial $P(Y) = Y^d - \zeta^{-1}$, where we recall that ζ^{-1} is a primitive root of $\mathbb{F}_q$. Note that finding such a primitive root can be done in $\mathsf{poly}(q)$ time by brute force. That $P(Y)$ is irreducible follows from the following proposition.

Proposition 4.6 ([LN94], Chapter 3). *Let $d \geq 2$ be an integer and $\alpha \in \mathbb{F}_q \backslash \{0\}$. Then the binomial $X^d - \alpha$ is irreducible in $\mathbb{F}_q[X]$ iff the following conditions hold:*

1. *Each prime factor of d divides $\mathrm{ord}_{\mathbb{F}_q}(\alpha)$ and $\gcd(d, \frac{q-1}{\mathrm{ord}_{\mathbb{F}_q}(\alpha)}) = 1$;*

2. *$q \equiv 1 \pmod 4$ if $d \equiv 0 \pmod 4$.*

Moreover the polynomials $P(Y^{\sigma^j}) = P(\zeta^j Y) = \zeta^j Y - \zeta^{-1} = \zeta^j(Y - \zeta^{-(j+1)})$ are also irreducible and pairwise coprime (as $j < m < n = q-1$). Finally evaluating a polynomial f at the place P^{σ^j}, which amounts to reducing the polynomial modulo $Y^d - \zeta^{-(j+1)}$, can be done in $\mathsf{poly}(n)$ field operations. Thus, given bases $\mathcal{B}_1, \ldots, \mathcal{B}_k$ for $V_1, \ldots, V_k$, we obtain the bases for $\widetilde{H}_i$ by evaluating π on each element of $\mathcal{B}_i$, respectively. □

Setting parameters. By choosing k, d and appropriately we obtain the following corollary.

Corollary 4.7. *Let $\delta > 0$ be such that $1/\delta \in \mathbb{Z}$ and put $k = 1/\delta^2$, $d = 1/\delta^3$. Assume that $q - 1 = n$. There exist $H_1, \ldots, H_k$ which form an explicit $(s, \frac{1}{1-2\delta-\delta^2+2\delta^3}, d)$-subspace design in $\mathbb{F}_{q^n}$ for all $s \leq \frac{1-2\delta}{d}n$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{n}{k}$ for all $i = 1, \ldots, k$.*

Proof. Fix an $\mathbb{F}_h$-linear isomorphism $\varphi : \mathbb{F}_h^m \to \mathbb{F}_{q^n}$ and define $H_i = \varphi(\widetilde{H}_i)$ for $i = 1, 2, \ldots, k$, where $\widetilde{H}_1, \widetilde{H}_2, \ldots, \widetilde{H}_k \subseteq \mathbb{F}_h^m$ form the subspace design promised in Proposition 4.5. Since φ is also $\mathbb{F}_q$-linear, the dimensions of $\mathbb{F}_q$-subspaces are also preserved by φ. Then, if $W \subseteq \mathbb{F}_{q^n}$ is an $\mathbb{F}_h$-subspace,

$$\sum_{i=1}^{k} \dim_{\mathbb{F}_q}(H_i \cap W) = \sum_{i=1}^{k} \dim_{\mathbb{F}_q}(\widetilde{H}_i \cap \varphi^{-1}(W))$$

so $H_1, \ldots, H_k$ forms a subspace design in $\mathbb{F}_{q^n}$ with the same parameters as $\widetilde{H}_1, \ldots, \widetilde{H}_k$. That $H_1, \ldots, H_k$ are explicit follows easily from the explicitness of $\widetilde{H}_1, \ldots, \widetilde{H}_k$.

Assuming $s \leq \frac{1-2\delta}{d} n < (1-\delta)m$, we find

$$\frac{\delta}{1-\delta} \cdot \frac{m}{(\delta - \frac{1}{k})m - \frac{2s}{d(1-\delta)}} \leq \frac{\delta}{1-\delta} \cdot \frac{m}{\delta(1-\delta)m - \frac{2(1-\delta)\delta^3 m}{1-\delta}}$$
$$= \frac{1}{(1-\delta)^2} \cdot \frac{1}{1 - \frac{2\delta^2}{1-\delta}} = \frac{1}{(1-\delta)^2 - 2\delta^2(1-\delta)} = \frac{1}{1 - 2\delta - \delta^2 + 2\delta^3} \ .$$

The result now follows from Proposition 4.5. □

5 Explicit instantiations of dimension expanders

As outlined in Section 3, our approach for obtaining explicit constructions of dimension expanders is by reducing to the construction of subspace designs. Specifically, we will will apply Theorem 3.4 with the constructions of Section 4. These results yield Theorems 1.2 and 1.1, respectively.

First, using the subspace design constructed in Corollary 4.4, we obtain a degree-proportional dimension expander over fields of arbitrarily small polynomial size.

Theorem 5.1. *Let $\delta > 0$ be given and assume $|\mathbb{F}_q| \geq n^\delta$. Let r be an integer satisfying $\frac{1}{2\delta} \leq r < \frac{1}{\delta}$, let k be a multiple of r, and let $d = 2k$. There exists an explicit construction of a (η, β)-dimension expander of degree d over $\mathbb{F}_q^n$ whenever $2dr|n$, where $\eta = \Omega\left(\frac{1}{\delta d}\right)$ and $\beta = \Omega(\delta d)$.*

Proof. Using Corollary 4.4, we have an explicit (s, A, d)-subspace design $\{H_i\}_{i=1}^k$ for all $s \leq \mu n$, where $\mu = \frac{1-2\delta}{4d}$ and $A = \frac{8}{\delta}$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{n}{k}$ for all $i = 1, \ldots, k$. Recall that $d = 2k$, so $d - k + 1 \geq d/2$. Thus, Theorem 3.4 implies that we have an explicit (η, β)-dimension expander for

$$\eta = \mu A = \frac{1-2\delta}{4d} \cdot \frac{8}{\delta} = 2(1-2\delta) \cdot \frac{1}{\delta d} = \Omega\left(\tfrac{1}{\delta d}\right)$$

and

$$\beta = \frac{d-k+1}{A} \geq \frac{d/2}{8/\delta} = \frac{1}{16} \cdot \delta d = \Omega(\delta d) \ .$$ □

Next, we use the subspace design constructed in Corollary 4.7 to obtain an explicit construction of a lossless dimension expander.

Theorem 5.2. *Fix $\varepsilon > 0$, and choose $\delta = \Theta(\varepsilon)$ sufficiently small and such that $1/\delta \in \mathbb{Z}$. Let $d = 1/\delta^3$ and $k = 1/\delta^2$ and assume that $q-1 = n$ and $d|n$. Then there exists an explicit construction of a $(\frac{1-\varepsilon}{d}, (1-\varepsilon)d)$-dimension expander with degree d over $\mathbb{F}_q^n$.*

Proof. Using Corollary 4.7, there exists a collection $\{H_i\}_{i=1}^k$ forming a (s, A, d) subspace design for all $s \leq (1-2\delta)m = \frac{1-2\delta}{d} n$, where

$$A = \frac{1}{1 - 2\delta - \delta^2 + 2\delta^3} \ .$$

Hence, by Theorem 3.4, using the fact that $d - k \geq d(1-\delta)$ we obtain the expansion factor

$$\beta = \frac{d-k+1}{A} \geq d(1-\delta)(1 - 2\delta - \delta^2 + 2\delta^3) \ .$$

By assuming $\delta \leq \varepsilon/4$, this is $\geq (1-\varepsilon)d$, as desired. The lower bound on η is obtained by plugging in $(1-2\delta)/d$ for μ in Theorem 3.4:

$$\eta = \mu A \geq \mu = \frac{1-2\delta}{d} \geq \frac{1-\varepsilon}{d} \ .$$ □

We remark that this construction has degree $d = O(1/\varepsilon^3)$. Recalling Proposition 2.5, we know that one could hope for $d = O(1/\varepsilon^2)$ when $\eta = \frac{1-\varepsilon}{d}$ and $\beta = (1-\varepsilon)d$. Hence, the dependence of the degree on ε is just a factor of ε away from the probabilistic construction.

6 Unbalanced expanders

For clarity's sake, we have presented all our results in the context of balanced dimension expanders. However, as remarked earlier, our techniques are flexible enough to produce *unbalanced* dimension expanders. In this section, we state the appropriate generalizations of our results that are required to construct unbalanced dimension expanders. As the proofs are extremely similar to those given before, we do not provide full proofs, but merely indicate the details that need to be changed.

We recall Definition 2.3: a b-unbalanced (η, β)-dimension expander of degree d is a collection $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}^N \to \mathbb{F}^n$ of linear maps such that for any $V \subseteq \mathbb{F}^N$ of dimension at most ηN, $\dim \sum_j \Gamma_j(V) \geq \beta \dim V$. We also recall that $b = \frac{N}{n}$, which we assume to be an integer.

6.1 Unbalanced dimension expander construction

In this subsection, we provide the appropriate generalizations of the results of Section 3.

Construction. Recall that the dimension expanders map $\mathbb{F}_q^N \to \mathbb{F}_q^n$. We view the domain as

$$\mathcal{F} = \left\{ f(X) = \sum_{i=0}^{k-1} f_i X^{q^i} : f_i \in H_i,\ i = 0, \ldots, k-1 \right\}$$

where $H_0, \ldots, H_{k-1}$ give a collection of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$, each of $\mathbb{F}_q$-dimension $\frac{N}{k}$. Thus, we now require $k|N$. As before, $H_0, \ldots, H_{k-1}$ will form a subspace design. We view the image space as $\mathbb{F}_{q^n}$. Again $h = q^d$ and $\alpha_1, \ldots, \alpha_d$ gives a basis for $\mathbb{F}_h/\mathbb{F}_q$. The definition of Γ_j is just as before:

$$\Gamma_j : \mathcal{F} \to \mathbb{F}_{q^n}; \quad f \mapsto f(\alpha_j) \ .$$

Analysis. We remark that the statements of Lemmas 3.1, 3.2 and 3.3 remain valid as stated. We are then able to conclude the following theorem:

Theorem 6.1. *Let $\{H_i\}_{i=0}^{k-1}$ give a (s, A, d)-subspace design in $\mathbb{F}_{q^n}$ for all $s \leq \mu N$ for some $\mu \in (0, \frac{1}{bd})$. Then $\{\Gamma_j\}_{j=1}^d$ is a b-unbalanced $(\mu A, \frac{d-k+1}{A})$-dimension expander.*

The only detail which has changed from Theorem 3.4 is that now $\mu < \frac{1}{bd}$, rather than just $\mu < \frac{1}{d}$. Asides from this, the proof proceeds identically to before, appealing now to Proposition 2.4 instead of Proposition 2.2.

6.2 Higher-dimensional subspace designs

In this section we construct subspace designs $H_1, \ldots, H_k \subseteq \mathbb{F}_{q^n}$, where the H_i's now have $\mathbb{F}_q$-dimension $\frac{N}{k}$.

6.2.1 Subspace designs via an intermediate field

First, we note that the proof of Proposition 4.3 still applies in this scenario. Essentially, we just need to redefine the t parameter in order to ensure that the subspaces have dimension $\frac{N}{k}$.

Proposition 6.2. *Let $\ell = q^c$ with $c = \frac{d}{k} \cdot \frac{bm}{m-2t}$, where $1 \leq k < d$. For all $1 \leq s < t < \ell$ such that $\ell^2 \geq 4kt$, $k|d$, $mb|(m-2t)k$ and $k(m-2t)|N$, there is an explicit construction of $\{H_i\}_{i=1}^k$ that forms a $(s, \frac{d}{k} \cdot \frac{bm}{m-2t} \cdot \frac{m-1}{2(t-s)}, d)$-subspace design in $\mathbb{F}_{q^n}$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{N}{k}$ for all $i = 1, \ldots, k$.*

We now fix the parameters to obtain our subspace designs over fields of arbitrarily small polynomial size.

Corollary 6.3. *Let $\delta > 0$ be given and choose an integer r such that $\frac{1}{2\delta} \leq r < \frac{1}{\delta}$. We assume $\delta > 0$ is sufficiently small so that $r \geq \max\{b, 2\}$. Let k, d be integers such that $d = 2k$ and $r|k$. Assume moreover that $2r|mb$. Then, assuming $q \geq n^\delta$, there exists an explicit construction of $\{H_i\}_{i=1}^k$ that forms a $(s, \frac{8}{\delta}, d)$-subspace design in $\mathbb{F}_{q^n}$ for all $s \leq \frac{1-2\delta b}{4bd}N$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{N}{k}$ for all $i = 1, \ldots, k$.*

The proof proceeds very similarly to the proof of Corollary 4.4; we just define the appropriate parameters. Set $t = \frac{1}{2}(1 - \frac{b}{r})m = \frac{1}{2db}(1 - \frac{b}{r})N$ and assume $s \leq t/2$. Thus we may take $\mu = \frac{1-2\delta b}{4db} \leq \frac{1-b/r}{4db}$ and A is bounded by

$$\frac{d}{k} \cdot \frac{bm}{m-2t} \cdot \frac{m}{2(t-s)} \leq 2r\frac{2}{1-\frac{1}{r}} \leq \frac{8}{\delta} .$$

6.2.2 Subspace designs via correlated high-degree places

The results in this section follow from the same arguments as those provided in Section 4.2, except now we will set $\delta = \sqrt{\frac{b}{k}}$ and insist that the $V_1, \ldots, V_k \subseteq \mathbb{F}_q[X]_{<\delta n}$ are chosen to have codimension $\delta n - \frac{N}{k}$.

Proposition 6.4. *Fix $\delta > 0$ such that $\delta > \frac{1}{bk}$ and $\delta n < q - 1$. If $s < (1-\delta)m = (1-\delta)\frac{N}{bd}$, there exists a collection $\{\widetilde{H}_i\}_{i=1}^k$ forming an $(s, \frac{\delta}{1-\delta} \cdot \frac{m}{(\delta - \frac{1}{bk})m - \frac{2s}{d(1-\delta)}}, d)$-subspace design in $\mathbb{F}_h^m$. Moreover $\dim_{\mathbb{F}_q} \widetilde{H}_i = \frac{N}{k}$ for all $i = 1, \ldots, k$.*

Lastly, when $n = q - 1$, the subspace design can be constructed explicitly.

Corollary 6.5. *Let $\delta > 0$ be such that $1/\delta \in \mathbb{Z}$ and put $k = b/\delta^2$, $d = b/\delta^3$. Assume that $n = q - 1$ and $d|n$. There exist $H_1, \ldots, H_k$ which form an explicit $(s, \frac{1}{1-2\delta-\delta^2+\delta^3}, d)$-subspace design in $\mathbb{F}_{q^n}$ for all $s \leq \frac{1-2\delta}{db}N$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{N}{k}$ for all $i = 1, \ldots, k$.*

6.3 Explicit instantiations

Finally, we provide the analogous results to those obtained in Section 5. These yield Theorems 1.4 and 1.3, respectively.

First, instantiating Theorem 6.1 with Corollary 6.3 yields

Theorem 6.6. *Let $\delta > 0$ (sufficiently small) be given and assume $q \geq n^\delta$. Let r be an integer in the range $(\frac{1}{2\delta}, \frac{1}{\delta})$, choose a multiple k of r, and let $d = 2k$. Let b be an integer. There exists an explicit construction of a b-unbalanced (η, β)-dimension expander of degree d over $\mathbb{F}_q^n$ whenever $2dr|nb$, where $\eta = \Omega\left(\frac{1}{\delta bd}\right)$ and $\beta = \Omega(\delta d)$.*

Then, appealing to Corollary 6.5 instead, we obtain the following.

Theorem 6.7. *Fix $\varepsilon > 0$ sufficiently small, and choose $\delta = \Theta(\varepsilon)$ sufficiently small and such that $1/\delta \in \mathbb{Z}$. Let $k = b/\delta^2$ and $d = b/\delta^3$. Suppose that $n = q - 1$ and $d|n$. Then there exists an explicit construction of a $(\frac{1-\varepsilon}{bd}, (1-\varepsilon)d)$-dimension expander of degree d over $\mathbb{F}_q$.*

As before, we remark that $d = O(b/\varepsilon^3)$, whereas the existential argument yields $d = O(b/\varepsilon^2)$. Moreover we once again emphasize that η is optimal: one cannot expand subspaces of dimension greater than $\frac{N}{bd} = \frac{n}{d}$ by a factor of $\approx d$.

7 Conclusion

In this work we provide the first explicit construction of a lossless dimension expander. Our construction uses ideas from recent constructions of list-recoverable rank-metric codes, which is in analogy with the approach taken by [GUV09] in the "Boolean" world. Our approach is sufficiently general to achieve lossless expansion even in the case that the expander is "unbalanced", i.e., when the codomain has dimension smaller than the domain.

The main open problem that remains is to achieve similar constructions over fields of smaller size. Our construction of lossless expanders requires fields of size $q > n$, whereas our construction of degree-proportional expanders requires fields of size n^δ for arbitrarily small (constant) δ. The constraints on the field size arise largely from the constructions of subspace designs that we employed. Thus, we believe that a fruitful avenue of attack on this problem would be to obtain constructions of subspace designs over smaller fields.[6]

The authors of [GXY17] addressed precisely this challenge. In this work the authors do manage to construct subspace designs over all fields, but the intersection size now grows with $\log_q n$. If $q = O(1)$, then instantiating our approach with these subspace designs only guarantees expansion if the degree is logarithmic. One could also have q grow polynomially with n and achieve degree-proportional expanders, but as this does not improve over the intermediate fields approach of Section 4.1 we have not included it.

Lastly, we recall that our construction of a $(\frac{1-\varepsilon}{d}, (1-\varepsilon)d)$-dimension expander had degree $d = \Theta(1/\varepsilon^3)$, while the probabilistic argument shows $d = O(1/\varepsilon^2)$ is sufficient. Moreover if one is satisfied with a $(\frac{1}{2d}, (1-\varepsilon)d)$-dimension expander then it is sufficient to have $d = O(1/\varepsilon)$. Thus, constructing lossless expanders whose degree has even better dependence on ε would also be interesting.

References

[BISW04] Boaz Barak, Russell Impagliazzo, Amir Shpilka, and Avi Wigderson. Personal Communication to Dvir-Shpilka [DS11], 2004.

[Bou09] Jean Bourgain. Expanders and dimensional expansion. *Comptes Rendus Mathematique*, 347(7-8):357–362, 2009.

[BY13] Jean Bourgain and Amir Yehudayoff. Expansion in $\mathrm{SL}_2(\mathbb{R})$ and monotone expanders. *Geometric and Functional Analysis*, 23(1):1–41, 2013. Preliminary version in the *44th Annual ACM Symposium on Theory of Computing (STOC 2012)*. This work is the full version of [**?**].

[6] In [GK16] there is also an "extension field" construction that allows for smaller field sizes, but only guarantees the existence of "weak" subspace designs, which does not suffice for the dimension expander application.

[DL12] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, pages 351–358. ACM, 2012.

[DS07] Zeev Dvir and Amir Shpilka. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM J. Comput.*, 36(5):1404–1434, 2007. Preliminary Version in the *37th Annual ACM Symposium on Theory of Computing (STOC 2005).*

[DS11] Zeev Dvir and Amir Shpilka. Towards dimension expanders over finite fields. *Combinatorica*, 31(3):305–320, 2011.

[DW10] Zeev Dvir and Avi Wigderson. Monotone expanders: Constructions and applications. *Theory of Computing*, 6(12):291–308, 2010.

[FG15] Michael A Forbes and Venkatesan Guruswami. Dimension expanders via rank condensers. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 800–814, 2015.

[FS12] Michael A Forbes and Amir Shpilka. On identity testing of tensors, low-rank recovery and compressed sensing. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 163–172. ACM, 2012.

[Gab85] Ernst M. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inform. Transm.*, 21(1):1–12, 1985.

[Gab11] Ariel Gabizon. Deterministic extractors for affine sources over large fields. In *Deterministic Extraction from Weak Random Sources*, pages 33–53. Springer, 2011.

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016.

[GR08] 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. Preliminary Version in the *38th Annual ACM Symposium on Theory of Computing (STOC 2006).*

[Gur11] Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity (CCC 2011)*, pages 77–85, 2011.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM (JACM)*, 56(4):20, 2009.

[GW13] 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.

[GW14] Venkatesan Guruswami and Carol Wang. Evading subspaces over large fields and explicit list-decodable rank-metric codes. In *Proceedings of the 18th International Workshop on Randomization and Computation (RANDOM 2014)*, pages 748–761, 2014. Full version at arXiv:1311.7084.

[GWX16] Venkatesan Guruswami, Carol Wang, and Chaoping Xing. Explicit list-decodable rank-metric and subspace codes via subspace designs. *IEEE Transactions on Information Theory*, 62(5):2707–2718, 2016.

[GX12] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC 2012)*, pages 339–350, 2012. Full version at arXiv:1204.4209.

[GX13] Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the Singleton bound. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC 2013)*, pages 843–852. ACM, 2013.

[GXY17] Venkatesan Guruswami, Chaoping Xing, and Chen Yuan. Subspace designs based on algebraic function fields. *Transactions of the AMS*, 2017. To appear. Available as arXiv:1704.05992.

[GY08] Maximilien Gadouleau and Zhiyuan Yan. On the decoder error probability of bounded rank-distance decoders for maximum rank-distance codes. *IEEE Transactions on Information Theory*, 54(7):3202–3206, 2008.

[Har08] Aram W. Harrow. Quantum expanders from any classical cayley graph expander. *Quantum Information & Computation*, 8(8–9):715–721, 2008.

[KS11] Zohar S. Karnin and Amir Shpilka. Black box polynomial identity testing of generalized depth-3 arithmetic circuits with bounded top fan-in. *Combinatorica*, 31(3):333–364, 2011.

[LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications.* Cambridge University Press, 1994.

[LZ08] Alexander Lubotzky and Efim Zelmanov. Dimension expanders. *Journal of Algebra*, 319(2):730–738, 2008.

[PR04] Pavel Pudlák and Vojtěch Rödl. Pseudorandom sets and explicit constructions of Ramsey graphs. In *Complexity of computations and proofs*, volume 13 of *Quad. Mat.*, pages 327–346. Dept. Math., Seconda Univ. Napoli, Caserta, 2004.

[PV05] 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 (FOCS)*, pages 285–294, 2005.

[RVW02] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Annals of Mathematics*, 155(1):157–187, 2002.

[Vad12] Salil P. Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012.

[Wig04] Avi Wigderson. Expanders: Old and new applications and problems. Lecture at the Institute for Pure and Applied Mathematics (IPAM), February 2004.

A Subspace evasive subspaces

Recall the discussion from Section 1.2: we wish to find a subspaces $H_1, \dots, H_k$ which have small total intersection with subspaces W which are linear over $\mathbb{F}_{q^d} =: \mathbb{F}_h$. While we have the freedom of choosing the H_i's to be distinct subspaces, we observe that there exists a single subspace that has small intersection with all such subspaces W! That is, it is possible to take $H_1 = \cdots = H_k =: H$, and still obtain a good subspace design. We call such an H a *subspace evasive subspace.*

Moreover, we show that by taking a subspace evasive subspace with parameters matching those achievable by a random subspace, we may obtain *degree-proportional* dimension expanders. We find this observation rather surprising, and also demonstrative of the efficiency of our reduction from dimension expanders to subspace designs.

We begin with the definition germane to this section.

Definition A.1 (Subspace evasive subspace)**.** An $\mathbb{F}_q$-subspace $H \subseteq \mathbb{F}_{q^n}$ is called a (s, A, d)-subspace evasive subspace if for every $\mathbb{F}_{q^d}$-linear subspace $W \subseteq \mathbb{F}_{q^n}$ of dimension s,

$$\dim_{\mathbb{F}_q}(H \cap W) \leq As \ .$$

We first observe that subspace evasive subspaces naturally yield subspace designs, although the A parameter degrades by a factor of k.

Observation A.2. *Suppose H is (s, A, d)-evasive. The tuple $(H, H, \dots, H)$, repeated k times, forms a (s, kA, d)-subspace design.*

The following proposition demonstrates that good subspace evasive subspaces exist.

Proposition A.3. *Let $k, d, n > 2$ be positive integers such that $q^{n/4} \geq m = n/d$ and $k < d$. Let H be a random $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n} \cong \mathbb{F}_q^n$ of dimension n/k. Then, with probability at least $1 - q^{-\Omega(n)}$, for every $\mathbb{F}_h$-subspace W of $\mathbb{F}_{q^n}$ with $\dim_{\mathbb{F}_h}(W) \leq \frac{m}{4} = \frac{n}{4d}$,*

$$\dim_{\mathbb{F}_q}(W \cap H) \leq \frac{\dim_{\mathbb{F}_h}(W)}{1 - 2/k} \ .$$

That is, H is $(s, \frac{1}{1-2/k}, d)$-evasive for all $s \leq \frac{m}{4} = \frac{n}{4d}$.

Proof. The probability that a fixed set of L vectors that are linearly independent over $\mathbb{F}_q$ belong to H is at most

$$\left(\frac{q^{n/k}}{q^n}\right)^L = q^{-n(1-1/k)L} \ .$$

By a union bound, the probability that some $\mathbb{F}_h$-subspace of dimension s has at least L such vectors belong to H is at most

$$h^{ms} \cdot h^{sL} \cdot q^{-n(1-1/k)L} = q^{sn} \cdot q^{-L(n(1-1/k)-sd)} \ . \tag{10}$$

Assuming $s \leq \frac{n}{4d}$ and taking $L \geq s/(1-2/k)$, recalling that $k \geq 3$, we have

$$q^{-L(n(1-1/k)-sd)} \leq q^{-\frac{s}{1-2/k}(n(1-1/k)-n/4)} \leq q^{-3s(2n/3-n/4)} = q^{-\frac{5}{4}ns} \ .$$

Thus, (10) is at most $q^{ns}q^{-\frac{5}{4}ns} = q^{-\frac{1}{4}ns}$. Summing up over all s, $1 \leq s \leq m/4$, we get that the desired claim holds for all subspaces $W \subseteq \mathbb{F}_{h^m}$ with $\dim_{\mathbb{F}_h}(W) \leq m/4$ except with probability at most $m \cdot q^{-n/4} \leq q^{-n/8} \leq q^{-\Omega(n)}$. □

We now set $k = 3$ and apply Theorem 3.4 with this H to obtain a degree-proportional dimension expander. We remark that we may even have $\eta \geq 1/d$.

Proposition A.4. *Let n, d be integers with $3|n$, $d|n$ and $3 < d$. Let H be the subspace evasive subspace promised by Proposition A.3, and let $\{\Gamma_j\}_{j=1}^d$ denote the dimension expander constructed in Section 3 with each $H_i = H$. Then $\{\Gamma_j\}_{j=1}^d$ forms a degree-proportional dimension expander.*

Proof. By combining Proposition A.3 and Observation A.2, we have that (H, H, H) forms a $(s, 3A, d)$-subspace design for all $s \leq \mu n$, for $A = 3$ and $\mu = \frac{1}{4d}$. Applying Theorem 3.4, this implies that $\Gamma_1, \dots, \Gamma_d$ form an (η, β)-dimension expander for $\eta = \mu \cdot 3 \cdot A = \frac{1}{4d} \cdot 3 \cdot 3 = \frac{9}{4d}$ and $\beta = \frac{d-k+1}{3A} = \frac{d-2}{9}$. □

B Proof of Proposition 2.8

In this section we provide a proof of Proposition 2.8, which we restate for convenience.

Proposition B.1 ([GWX16], Proposition 3.9)**.** *Let T be a (s, d)-periodic $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^k$, and $H_1, \dots, H_k \subseteq \mathbb{F}_{q^n}$ be $\mathbb{F}_q$-subspaces forming a (s, A, d) subspace design in $\mathbb{F}_{q^n}$. Then $T \cap (H_1 \times \cdots \times H_k)$ is an $\mathbb{F}_q$-subspace of dimension at most As.*

Proof. Let $h = q^d$ and let W be the $\mathbb{F}_h$-subspace associated to T as in Definition 2.7. For $1 \leq j \leq k$, let $T_j \subseteq \mathbb{F}_{q^n}^j$ denote the projection of T onto the first j coordinates. We will show by induction on j that

$$|T_j \cap (H_1 \times \cdots \times H_j)| \leq q^{\sum_{\iota=1}^{j} \dim_{\mathbb{F}_q}(W \cap H_\iota)} \ . \tag{11}$$

Once we've shown this, since T and $H_1 \times \cdots \times H_k$ are both $\mathbb{F}_q$-subspaces, we will be able to conclude

$$\dim_{\mathbb{F}_q}(T \cap (H_1 \times \cdots \times H_k)) \leq \sum_{\iota=1}^{k} \dim_{\mathbb{F}_q}(W \cap H_\iota) \leq As \ ,$$

where the last inequality follows from the fact that $H_1, \dots, H_k$ form a subspace design.

Hence, we turn our attention to establishing (11) by induction. For the base case of $j = 1$, we observe that $T_1 \subseteq W$, as T_1 is contained in an affine shift of W and T_1 contains the 0 vector. Hence, we have $T_1 \cap H_1 \subseteq W \cap H_1$, so *a fortiori* $|T_1 \cap H_1| \leq |W \cap H_1|$.

For the induction step, we fix an element $(\xi_1, \dots, \xi_{j-1}) \in T_{j-1} \cap (H_1 \times \cdots \times H_{j-1})$. As T is periodic, the set of choices of $\xi_j \in \mathbb{F}_{q^n}$ for which $(\xi_1, \dots, \xi_j) \in T_j$ is contained in a coset of W, say, $\theta_j + W$ for $\theta_j \in \mathbb{F}_{q^n}$. Thus, the choices of $\xi_j \in H_j$ for which $(\xi_1, \dots, \xi_j) \in T_j$ is contained in $H_j \cap (\theta_j + W)$: since H_j is a subspace, this set is contained in a coset of $H_j \cap W$. Hence, there are at most $|H_j \cap W|$ choices for ξ_j. By induction, $|T_{j-1} \cap (H_1 \times \cdots \times H_{j-1})| \leq q^{\sum_{\iota=1}^{j-1} \dim_{\mathbb{F}_q}(W \cap H_\iota)}$, so there are at most this many choices for the prefix $(\xi_1, \dots, \xi_{j-1}) \in T_{j-1} \cap (H_1 \times \cdots \times H_{j-1})$. We thus find that there are at most $\left(q^{\sum_{\iota=1}^{j-1} \dim_{\mathbb{F}_q}(W \cap H_\iota)}\right) \cdot q^{\dim_{\mathbb{F}_q}(W \cap H_j)} = q^{\sum_{\iota=1}^{j} \dim_{\mathbb{F}_q}(W \cap H_\iota)}$ choices for $(\xi_1, \dots, \xi_j) \in T_j \cap (H_1 \times \cdots \times H_j)$, as desired. □

C Proof of Lemma 4.2

In this section we provide a proof of Lemma 4.2, which we restate for convenience. Recall that $\ell = q^c$ and $c|d$, so $\mathbb{F}_q \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_h$. Also, $\omega_1, \dots, \omega_m$ denotes a basis for $\mathbb{F}_{h^m}/\mathbb{F}_h$ and we define

$$L := \left\{ \sum_{i=1}^{m} a_i \omega_i : a_1, \dots, a_m \in \mathbb{F}_\ell \right\} \ .$$

Lemma C.1. *Let W be an $\mathbb{F}_h$-subspace of $\mathbb{F}_{q^n}$ and let $U := W \cap L$. Then U is an $\mathbb{F}_\ell$-subspace of L and $\dim_{\mathbb{F}_\ell} U \leq \dim_{\mathbb{F}_h} W$.*

Proof. It is clear that U is an $\mathbb{F}_\ell$ subspace as $\mathbb{F}_h \supseteq \mathbb{F}_\ell$. Suppose $u_1, \ldots, u_t \in U$ are linearly independent over $\mathbb{F}_\ell$; we will show that they are also linearly independent over $\mathbb{F}_h$. Once we have shown this, the lemma follows.

Put $r = d/c$ and let $\gamma_1, \ldots, \gamma_r$ denote a basis for $\mathbb{F}_h/\mathbb{F}_\ell$. Suppose that $\sum_{k=1}^t a_k u_k = 0$ with $a_1, \ldots, a_t \in \mathbb{F}_h$; we want to show $a_1 = \cdots = a_t = 0$. Using our bases, we may write $a_k = \sum_{j=1}^r b_{jk}\gamma_j$ and $u_k = \sum_{i=1}^m c_{ki}\omega_i$ for $b_{jk}, c_{ki} \in \mathbb{F}_\ell$. Thus, we have

$$\sum_{k=1}^t \left(\sum_{j=1}^r b_{jk}\gamma_j\right)\left(\sum_{i=1}^m c_{ki}\omega_i\right) = 0$$

which, upon rearranging, becomes

$$\sum_{i=1}^m \left(\sum_{j=1}^r \left(\sum_{k=1}^t b_{jk}c_{ki}\right)\gamma_j\right)\omega_i = 0 \ .$$

Since $\omega_1, \ldots, \omega_m$ form a basis for $\mathbb{F}_{q^n}/\mathbb{F}_h$ and $\sum_{j=1}^r \left(\sum_{k=1}^t b_{jk}c_{ki}\right)\gamma_j \in \mathbb{F}_h$ for all $i \in [m]$, we deduce

$$\sum_{j=1}^r \left(\sum_{k=1}^t b_{jk}c_{ki}\right)\gamma_j = 0 \ \ \forall i \in [m] \ .$$

Next, since $\gamma_1, \ldots, \gamma_r$ form a basis for $\mathbb{F}_h/\mathbb{F}_\ell$ and $\sum_{k=1}^t b_{jk}c_{ki} \in \mathbb{F}_\ell$ for all $j \in [r]$, we deduce

$$\sum_{k=1}^t b_{jk}c_{ki} = 0 \ \ \forall i \in [m], \ j \in [r] \ .$$

Thus, defining the matrices $B = (b_{jk}) \in \mathbb{F}_\ell^{r \times t}$ and $C = (c_{ki}) \in \mathbb{F}_\ell^{t \times m}$, we find $BC = 0$ (where 0 denotes the $r \times m$ matrix of all zeroes). Moreover, since $u_1, \ldots, u_t$ are assumed to be $\mathbb{F}_\ell$-linearly independent it follows that the matrix C has full-rank, i.e., $\mathsf{rank}(C) = t$. We therefore have $0 = \mathsf{rank}(BC) = \mathsf{rank}(B)$, i.e., B must be the $r \times t$ matrix of zeroes. This shows that $a_1 = \cdots = a_t = 0$, as desired. □

D Random construction of unbalanced dimension expander

In this section, we show that good unbalanced lossless dimension expanders exist. Our argument is modeled after Section C.2 in [FG15], wherein it is shown that good (balanced) dimension expanders exist. As is standard in the theory of pseudorandomness, our existential argument uses the probabilistic method.

First, we state a lemma that bounds the probability that a random $n \times N$ matrix has low rank.

Lemma D.1. *Let M be a uniformly random matrix in $\mathbb{F}_q^{n \times N}$. The probability that $\mathsf{rank}(M) \leq r$ is at most*

$$4q^{-(N-r)(n-r)} \ .$$

Next, we quote a bound on the number of subspaces of a given dimension.

Lemma D.2. *The number of subspaces $V \subseteq \mathbb{F}_q^n$ of dimension k is at most*

$$4q^{k(n-k)} \ .$$

A proof of these lemmas can be found in [GY08].

Lemma D.3. *Let q be a prime power and assume $N, n \geq t \geq r \geq 1$. Let $\Gamma_1, \ldots, \Gamma_d$ be independent random matrices, uniformly distributed over $\mathbb{F}_q^{n \times N}$. Then with probability at least $1 - q^r$, for any subspace $V \subseteq \mathbb{F}_q^N$ of dimension r we have*

$$\dim \sum_{j=1}^{d} \Gamma_j(V) \geq t \ ,$$

assuming

$$d \geq \frac{t-1}{r} + \frac{N-r+1}{n-t+1} + \frac{\log_q 16}{r(n-t+1)} \ .$$

Proof. Fix a subspace $V \subseteq \mathbb{F}_q^N$ of dimension r, and let $M \in \mathbb{F}_q^{N \times r}$ be a matrix whose columns give a basis for V. Thus, $\mathsf{rank}(M) = r$ and the column span of M is V. In particular, $\dim \sum_j \Gamma_j(V) \geq t$ iff the $\mathbb{F}_q^{n \times rd}$ block matrix

$$A(V) := [\Gamma_1 M| \cdots |\Gamma_d M]$$

has rank at least t. As M is nonsingular and the Γ_j are uniformly random, the matrix $A(V)$ is a uniformly random matrix in $\mathbb{F}_q^{n \times rd}$. Thus, the probability it has rank at most $t-1$ is at most

$$4q^{-(rd-t+1)(n-t+1)} \ .$$

Then, taking a union bound over the choice of V, we see that the probability of failure is at most

$$16q^{r(N-r)-(rd-t+1)(n-t+1)} \ .$$

This is at most q^{-r} assuming

$$(n-t+1)(rd-t+1) \geq r(N-r+1) + \log_q 16 \ .$$

Dividing both sides by $r(n-t+1)$ and rearranging, the previous inequality is equivalent to

$$d \geq \frac{t-1}{r} + \frac{N-r+1}{n-t+1} + \frac{\log_q 16}{r(n-t+1)} \ . \qquad \square$$

The existential proof will be complete upon taking a union bound over the choice of r; the following proposition does exactly this.

Proposition D.4. *Let $\mathbb{F}_q$ be a finite field and assume $N, n \geq 1$ and put $b = \frac{N}{n}$. Let $\beta > 1$ and $\eta \in (0, \frac{1}{b\beta})$. Then there exists a collection of matrices $\{\Gamma_1, \ldots, \Gamma_d\} \subseteq \mathbb{F}_q^{n \times N}$ forming a (η, β)-dimension expander of degree d, assuming*

$$d \geq \beta + \frac{b}{1 - b\beta\eta} + \log_q 16 \ .$$

Proof. Fix any $r \leq \eta N$; we wish to show $\dim \sum_j \Gamma_j(V) \geq \beta \dim V$ for any $V \subseteq \mathbb{F}_q^N$ of dimension r; i.e., we wish to show $\dim \sum_j \Gamma_j(V) \geq \lceil \beta r \rceil$. For any fixed r, Lemma D.3 promises that this occurs with probability $\geq 1 - q^{-r}$ assuming

$$d \geq \frac{\lceil \beta r \rceil - 1}{r} + \frac{N - r + 1}{n - \lceil \beta r \rceil + 1} + \frac{\log_q 16}{r(n - r + 1)} \ .$$

As $\lceil \beta r \rceil - 1 \leq \beta r$ and $r(n - r + 1) \geq 1$, it actually suffices for

$$d \geq \beta + \frac{N}{n - \beta r} + \log_q 16 \ .$$

Recalling $r \leq \eta N = \eta b n$ and $b = \frac{N}{n}$, we see that it suffices to have

$$d \geq \beta + \frac{b}{1 - b\beta\eta} + \log_q 16 \ ,$$

as stated. Now, as $\sum_{r=1}^{\lceil \eta N \rceil} q^{-r} \leq \sum_{r=1}^{\infty} q^{-r} < 1$, we can take a union bound over the choice of r to conclude that $\{\Gamma_j\}_{j=1}^d$ indeed forms a (η, β)-dimension expander. □

E Random subspace design

We prove via the probabilistic method that good subspace designs exist. However, we note that the μ parameter is actually not as large as the μ parameter achieved constructively in Corollary 4.7!

Proposition E.1. *Let n, k, d be integers with $k|d$ and $d|n$. Let $\delta \in (0,1)$, and assume $k \geq 4/\delta$. There exists a collection $H_1, H_2, \ldots, H_k \subseteq \mathbb{F}_{q^n}$ of $\mathbb{F}_q$-subspaces, each of $\mathbb{F}_q$-dimension $\frac{n}{k}$, which forms a $(s, 1+\delta, d)$-subspace design for all $s \leq \frac{\delta}{4d} n$.*

Proof. We choose $H_1, \ldots, H_k$ independently and uniformly at random among all subspaces of dimension $\frac{n}{k}$ in $\mathbb{F}_{q^n}$. Let $W \subseteq \mathbb{F}_{q^n}$ be a $\mathbb{F}_{q^d}$-subspace of $\mathbb{F}_{q^d}$-dimension s (so it satisfies $\dim_{\mathbb{F}_q} W = ds$). For an integer a, the probability that $\dim_{\mathbb{F}_q}(H_i \cap W) \geq a$ is at most

$$q^{ads} \cdot q^{-(1-1/k)an} = q^{a(ds - n + n/k)} \leq q^{an(1-\delta/2)}$$

where the inequality follows from the assumptions $s \leq \frac{\delta}{4d} n$ and $k \geq 4/\delta$. Then, for any tuple $(a_1, \ldots, a_k)$ of integers summing to $\ell := \lceil (1+\delta)s \rceil$, since the H_i are selected independently the probability that each $\dim_{\mathbb{F}_q}(H_i \cap W) \geq a_i$ is at most

$$q^{-\ell n(1-\delta/2)} \leq q^{-ns(1+\delta)(1-\delta/2)} \leq q^{-ns(1+\delta/4)}$$

where the last inequality holds as $\delta < 1$. Taking a union bound over all at most q^{sn} choices for W and $\binom{\ell+k}{\ell} \leq k^{2\ell}$ choices for the tuple $(a_1, \ldots, a_k)$, the probability of failure is at most

$$q^{sn} k^{2\ell} q^{-ns(1+\delta/4)} = k^{2\ell} q^{-ns\delta/4} \leq q^{4(1+\delta)s \log_q k - ns\delta/4} = q^{-s(n\delta/4 - 4(1+\delta)\log_q k)} \ .$$

This probability is exponentially small in n. Thus, for n sufficiently large we can take a union bound over all $1 \leq s \leq \frac{\delta}{4d} n$ to conclude that the probability of failure is strictly less than 1. □

We now instantiate Theorem 3.4 with the subspace design from Proposition E.1 and observe that we obtain *lossless* dimension expanders. Of course, we have already demonstrated this constructively over fields of large size, but we still include the proof as it shows that our approach can work over smaller fields. However, we are only able to guarantee $\eta \geq \Omega\left(\frac{\varepsilon}{d}\right)$, although we know that we can have $\eta \geq \frac{1-\varepsilon}{d}$.

Theorem E.2. *Let $\varepsilon \in (0,1)$ be given. Let n, k, d be integers with $k|d$ and $d|n$. Let $\delta = \Theta(\varepsilon)$ be sufficiently small and assume $k \geq 4/\delta$. Let $H_1, H_2, \ldots, H_k$ be the subspace design from Proposition E.1. Finally, assumed $d \geq k/\delta$. Then, when Theorem 3.4 is instantiated with this subspace design, we obtain a $(\eta, (1-\varepsilon)d)$-dimension expander, where $\eta = \Omega(\varepsilon/d)$.*

Proof. The expansion factor that we can achieve is

$$\frac{d-k+1}{1+\delta} \geq \frac{1-\delta}{1+\delta} d \geq (1-\varepsilon)d$$

by choosing $\delta = \Theta(\varepsilon)$ sufficiently small (take, say, $\delta \approx \varepsilon/2$). The lower bound on η is obtained by observing

$$\frac{\delta}{4d}(1+\delta) = \Omega(\varepsilon/d) \ . \qquad \square$$