Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs

Venkatesan Guruswami[1]
Department of Computer Science, Carnegie Mellon University
5000 Forbes Ave, Pittsburgh, PA, USA, 15213
venkatg@cs.cmu.edu
https://orcid.org/0000-0001-7926-3396

Nicolas Resch[2]
Department of Carnegie Mellon University
5000 Forbes Ave, Pittsburgh, PA, USA, 15213
nresch@cs.cmu.edu

Chaoping Xing
School of Physical and Mathematical Sciences, Nanyang Technological University
21 Nanyang Link, Singapore 637371
xingcp@ntu.edu.sg
https://orcid.org/0000-0002-1257-1033

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 fields. Ours is the first construction to achieve lossless dimension expansion, or even expansion proportional to the degree.

2012 ACM Subject Classification Theory of computation → Randomness, geometry and discrete structures, Theory of computation → Pseudorandomness and derandomization, Theory of computation → Computational complexity and cryptography, Theory of computation → Algebraic complexity theory

Keywords and phrases Algebraic constructions, coding theory, linear algebra, list-decoding, polynomial method, pseudorandomness

[1] Research supported in part by NSF grants CCF-1422045 and CCF-1563742.
[2] Research supported in part by NSF grants CCF-1618280, CCF-1422045, NSF CAREER award CCF-1750808 and NSERC grant CGSD2-502898.

COMPUTATIONAL COMPLEXITY CONFERENCE
33rd Computational Complexity Conference (CCC 2018).
Editor: Rocco A. Servedio; Article No. 4; pp. 4:1–4:16
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Digital Object Identifier 10.4230/LIPIcs.CCC.2018.4

Related Version Full version available at `https://eccc.weizmann.ac.il/report/2018/017/`.

Acknowledgements Some of this work was done when the first author was visiting the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

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 [28] 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 [26] and list-decodable codes [19, 17]; subspace designs have been used to list-decode codes over the Hamming metric and the rank-metric [20, 17]; and rank-preserving condensers have been used in affine extractors [11] and polynomial identity testing [23, 9].

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 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 $\Gamma_j(u)$.[3]. 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

[3] 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.

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 (see)

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 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 [15] 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 [8] 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 $b = \frac{N}{n}$. Below we provide informal statements of our results; we refer to the full version for precise statements.

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

▶ **Theorem 1.3** (Informal Statement). *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). *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 $\left(\Omega\left(\frac{1}{\delta bd}\right), \Omega(\delta d)\right)$-dimension expanders of degree d over $\mathbb{F}^n$ when $|\mathbb{F}| \geq n^\delta$.*

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 [18] succeeded in constructing high-rate rank-metric codes which are list-decodable up to the Singleton bound.[4] The code may also readily be seen to be *list-recoverable* in the following sense: given vector spaces $V_1, \ldots, V_n \subseteq \mathbb{F}^m$ 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 [18] is a carefully selected subcode of the Gabidulin code [10], 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 $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$, and then identifying the vector $(f(\alpha_1), \ldots, f(\alpha_n))$ 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 [25, 14], the techniques used to prove list-decodability of these codes were adapted to show lossless expansion properties of unbalanced expanders built from these codes [15]. Our approach is strongly inspired by the connection between list recovery and expansion that drives [15] 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 [15], as that will prevent the maps from being linear.[5] More significantly, we also need to perform

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

[5] 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.

a careful "pruning" of subspaces which arise 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 [15].

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 $\alpha_1, \ldots, \alpha_d$ 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 [18] 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 2.6). 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 2.5). Subspace designs were originally formulated for applications to algebraic list-decoding, where they led to optimal redundancy list-decodable codes over small alphabets [20] and over the rank-metric [18]. 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 [13] 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 [13]. 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 [13] 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 [13] 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 [12, 16] 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 $n = q - 1$.

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.

1.3.1 Property T

The problem of constructing dimension expanders was originally proposed by Wigderson [29, 1]. 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 [7], 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 [24] 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 [22] proved the same result in the context of *quantum expanders*, which imply dimension expanders in characteristic zero. The following theorem summarizes this discussion.

▶ **Theorem 1.5** ([24, 22]). *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.

1.3.2 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)[6] 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 [6] implicitly observed that it is sufficient for the maps Γ_j to be *monotone* (this observation is made explicit in [7]). Note that the matrices Γ'_j have entires in $\{0, 1\}$, and they form a dimension expander over *every* field.

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

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 [7, 3]). Nonetheless, Dvir and Shpilka [5] 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 [27], Dvir and Wigderson [7] 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 [3] were able to construct explicit monotone expanders of constant degree. Thus, we have the following theorem.

▶ **Theorem 1.6** ([3]). *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.

1.3.3 Rank condensers

This final approach to constructing dimension expanders, developed by Forbes and the first author [8], uses *rank condensers*. Unlike the constructions of the previous sections, it inherently uses ideas from algebraic pseudorandomness 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 $S_k T_j$. We remark that the construction of the rank condenser from this work used the subspace designs of [13], 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 1.7** ([8]).

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 [21]. 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 (for our results on unbalanced dimension expanders, we refer to the full version of the paper). We summarize our work and list open problems in Section 6.

2 Background

2.1 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 $f \neq 0$).

2.2 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 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 $\Gamma_1, \ldots, \Gamma_d : \mathbb{F}^n \to \mathbb{F}^n$ be linear maps. Suppose that for all $V \subseteq \mathbb{F}^n$ of dimension at most $\eta\beta n$,*

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

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

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.

Lastly, we state the parameters achievable via the probabilistic method in order to set expectations.

▶ **Proposition 2.4** (Simple generalization of Proposition C.10 of [8]). *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 $d = O(1/\varepsilon^3)$.

2.3 Subspace design

A crucial ingredient in our construction of dimension expanders are subspace designs. They were originally introduced by two of the authors [20] in order to obtain algebraic codes list-decodable up to the Singleton bound. As in [18], 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 2.5.** 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.

2.4 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 [20, 18].

▶ **Definition 2.6** (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, $1 \leq j \leq k$, and all $\xi_1, \xi_2, \ldots, \xi_{j-1} \in \mathbb{F}_{q^n}$, the $\mathbb{F}_q$-affine subspace

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

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 2.7** ([18], 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.*

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 [18]. The presentation here is self-contained algebraically, and does not refer to any coding-theoretic context or language.

3.1 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 $H_0,\dots,H_{k-1}$ 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 $H_1,H_2,\dots,H_k$ forming a subspace design. We view the image space as $\mathbb{F}_{q^n}$. Let $h=q^d$, and let $\alpha_1,\dots,\alpha_d$ give a basis for $\mathbb{F}_h$ over $\mathbb{F}_q$. We assume $d|n$ and write $md=n$. For $j=1,\dots,d$, 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 $\mathbb{F}_q$.

3.2 Analysis

We now state the steps involved in showing that the collection $\{\Gamma_j\}_{j=1}^d$ forms a dimension expander. We have omitted the proofs; they can be found in the full version of the paper.

For a positive integers D,s with $s\le m$, 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 $Q(Z_0,\dots,Z_{s-1})=A_0(Z_0)+\dots+A_{s-1}(Z_{s-1})$ 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*

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

Given a polynomial $g(X)=g_0+g_1X+\dots+g_rX^r$ and an automorphism τ of $\mathbb{F}_{q^n}$, we write g^τ for the polynomial $g^\tau(X)=\tau(g_0)+\tau(g_1)X+\dots+\tau(g_r)X^r$, 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 $D\le d-k+1$. Then*

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

▶ **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.*

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 $s\le\mu n$ 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.*

Thus, 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 $A\approx1+\varepsilon$ 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 [13], using ideas which had been developed in constructions of list-decodable codes. This construction was subsequently improved over fields of small size in [21].

A previous construction of a subspace design for $d > 1$ was given in [18]. In this work, a subspace design over the base field (i.e., for $d = 1$) was intersected with a *subspace evasive set* from [4]. 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.[7] We present our first construction in Section 4.1 and our second construction in Section 4.2. The full version contains all of the proofs that we have removed from this section.

Both of our constructions use as a black box a subspace design provided in [13]. Specifically, by taking $r = 2$ in Theorem 7 of [13], 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 $i = 1, \ldots, k$.

▶ **Proposition 4.2.** *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 $i = 1, \ldots, k$.*

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 $\delta > 0$.

[7] In fact, in order to ensure our construction is algorithmically explicit, we take $q - 1 = n$.

▶ **Corollary 4.3.** *Let $\delta > 0$ be given and choose an integer r such that $\frac{1}{2\delta} < r \leq \frac{1}{\delta}$. Let k, d be integers such that $d = 2k$ and $r|k$. Assume moreover that $2r|m$. 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 $s \leq \frac{1-2\delta}{4d}n$. Moreover $\dim_{\mathbb{F}_q} H_i = \frac{n}{k}$ for all $i = 1, \ldots, k$.*

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 [12, 16]. 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 $g^{\sigma} := \sigma(g(Y)) = g(\zeta Y)$.[8]

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

$$\widetilde{H}_i = \pi(V_i) = \left\{(f(P), f(P^{\sigma}), \ldots, f(P^{\sigma^{m-1}})) : f \in V_i\right\} \subseteq \mathbb{F}_h^m \tag{4}$$

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

We remark that this π is reminiscent of 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 4.4.** *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.

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

▶ **Corollary 4.5.** *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 $i = 1, \ldots, k$.*

[8] 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.

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 4.3, 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 $\beta = \Omega(\delta d)$.*

Next, we use the subspace design constructed in Corollary 4.5 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 $\mathbb{F}_q^n$.*

We remark that this construction has degree $d = O(1/\varepsilon^3)$. Recalling Proposition 2.4, 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 randomized construction.

6 Conclusion

In this work we provide the first explicit construction of a lossless dimension expander. Our construction uses ideas from recent constructions of list-decodable rank-metric codes, which is in analogy with the approach taken by [15] 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.[9]

The authors of [21] 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

[9] In [13] 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.

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

1 Boaz Barak, Russell Impagliazzo, Amir Shpilka, and Avi Wigderson. Personal Communication to Dvir-Shpilka [6], 2004.

2 Jean Bourgain. Expanders and dimensional expansion. *Comptes Rendus Mathematique*, 347(7-8):357–362, 2009. doi:10.1016/j.crma.2009.02.009.

3 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 [2]. doi:10.1007/s00039-012-0200-9.

4 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.

5 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. doi:10.1137/05063605X.

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

7 Zeev Dvir and Avi Wigderson. Monotone expanders: Constructions and applications. *Theory of Computing*, 6(1):291–308, 2010. doi:10.4086/toc.2010.v006a012.

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

9 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.

10 Ernst M. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inform. Transm.*, 21(1):1–12, 1985. URL: http://www.mathnet.ru/eng/ppi967.

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

12 Venkatesan Guruswami. Linear-algebraic list decoding of folded reed-solomon codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, June 8-10, 2011*, pages 77–85. IEEE Computer Society, 2011. doi:10.1109/CCC.2011.22.

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

14 Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Trans. Information Theory*, 54(1):135–150, 2008. doi:10.1109/TIT.2007.911222.

15 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.

16 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.

17 Venkatesan Guruswami and Carol Wang. Evading subspaces over large fields and explicit list-decodable rank-metric codes. In Klaus Jansen, José D. P. Rolim, Nikhil R. Devanur, and Cristopher Moore, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2014, September 4-6, 2014,*

Barcelona, Spain, volume 28 of *LIPIcs*, pages 748–761. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2014. doi:10.4230/LIPIcs.APPROX-RANDOM.2014.748.

18 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.

19 Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In Howard J. Karloff and Toniann Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 339–350. ACM, 2012. doi:10.1145/2213977.2214009.

20 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.

21 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.

22 Aram W. Harrow. Quantum expanders from any classical cayley graph expander. *Quantum Information & Computation*, 8(8–9):715–721, 2008. URL: http://www.rintonpress.com/journals/qiconline.html#v8n89.

23 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.

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

25 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.

26 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.

27 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.

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

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