Linear-algebraic pseudorandomness: Subspace Designs & Dimension Expanders

Venkatesan Guruswami

Carnegie Mellon University

Simons workshop on "Proving and Using Pseudorandomness"
March 8, 2017

Based on a body of work, with
Chaoping Xing, Swastik Kopparty, Michael Forbes, Chen Yuan

Linear-algebraic pseudorandomness

Aim to understand the linear-algebraic analogs of fundamental Boolean pseudorandom objects, with *rank of subspaces playing the role of size of subsets.*

Examples

Rank-metric codes, Dimension expanders, subspace-evasive sets, rank-preserving condensers, subspace designs, etc.

Linear-algebraic pseudorandomness

Aim to understand the linear-algebraic analogs of fundamental Boolean pseudorandom objects, with *rank of subspaces playing the role of size of subsets.*

Examples

Rank-metric codes, Dimension expanders, subspace-evasive sets, rank-preserving condensers, subspace designs, etc.

Motivation: Intrinsic interest + diverse applications (to Ramsey graphs, list decoding, affine extractors, polynomial identity testing, network coding, space-time codes, ...)

Dimension expanders

Defined by [Barak-Impagliazzo-Shpilka-Wigderson'04] as a linear-algebraic analog of (vertex) expansion in graphs.

Dimension expanders

Defined by [Barak-Impagliazzo-Shpilka-Wigderson'04] as a linear-algebraic analog of (vertex) expansion in graphs.

Fix a vector space $\mathbb{F}^n$ over a field $\mathbb{F}$.

Dimension expanders

A collection of d linear maps $A_1, A_2, \ldots, A_d : \mathbb{F}^n \to \mathbb{F}^n$ is said to be an (b, α)-dimension expander if for all subspaces V of $\mathbb{F}^n$ of dimension $\leqslant b$,

$$\dim(\textstyle\sum_{i=1}^{d} A_i(V)) \geqslant (1 + \alpha) \dim(V).$$

- d is the "degree" of the dim. expander, and α the "expansion factor."

Constructing dimension expanders

(b, α)-dimension expander: $\forall V$, $\dim(V) \leqslant b$,
$\dim(\sum_{i=1}^{d} A_i(V)) \geqslant (1+\alpha)\dim(V)$.

Random constructions

Easy to construct probabilistically. For large n, w.h.p.

- A collection of 10 random maps is an $(\frac{n}{2}, \frac{1}{2})$-dim. expander.
- A collection of d random maps is an $(\frac{n}{2d}, d - O(1))$-dim. expander with high probability ("lossless" expansion).

Constructing dimension expanders

(b, α)-dimension expander: $\forall V$, $\dim(V) \leqslant b$,
$\dim(\sum_{i=1}^{d} A_i(V)) \geqslant (1+\alpha)\dim(V)$.

Random constructions

Easy to construct probabilistically. For large n, w.h.p.

- A collection of 10 random maps is an $(\frac{n}{2}, \frac{1}{2})$-dim. expander.
- A collection of d random maps is an $(\frac{n}{2d}, d - O(1))$-dim. expander with high probability ("lossless" expansion).

Challenge

Explicit constructions (i.e., deterministic poly(n) time construction of the maps A_i).

- Say of $O(1)$ degree $(\Omega(n), \Omega(1))$-dimension expanders.

We'll return to dimension expanders, but let's first talk about "subspace designs," our main topic.

Plan

Subspace designs:

- Why we defined them?
- Definition
- How to construct them?
- Applications in linear-algebraic pseudorandomness

Subspace designs: Original Motivation

Reducing the output list size in list decoding algorithms for (variants of) Reed-Solomon and Algebraic-Geometric codes.

Subspace designs: Original Motivation

Reducing the output list size in list decoding algorithms for (variants of) Reed-Solomon and Algebraic-Geometric codes.

Reed-Solomon codes

(mapping k symbols to n symbols over field $\mathbb{F}$, $|\mathbb{F}| \geqslant n$):

$$f \in \mathbb{F}[X]_{<k} \mapsto (f(a_1), f(a_2), \ldots, f(a_n)),$$

for n *distinct* elements $a_i \in \mathbb{F}$.

Subspace designs: Original Motivation

Reducing the output list size in list decoding algorithms for (variants of) Reed-Solomon and Algebraic-Geometric codes.

Reed-Solomon codes

(mapping k symbols to n symbols over field $\mathbb{F}$, $|\mathbb{F}| \geqslant n$):

$$f \in \mathbb{F}[X]_{<k} \mapsto (f(a_1), f(a_2), \ldots, f(a_n)),$$

for n *distinct* elements $a_i \in \mathbb{F}$.

Distance of the code $= n - k + 1 \implies$ even if $(n-k)/2$ worst-case errors occur, one can recover the original polynomial unambiguously.

- Plus, efficient algorithms to do this [Peterson'60,Berlekamp'68,Massey'69,...,Welch-Berlekamp'85,...]

For larger number of errors, can resort to **list decoding**.

List decoding RS codes

Reed-Solomon codes can be list decoded up to $n - \sqrt{kn}$ errors, which always exceeds $(n-k)/2$ [G.-Sudan'99]

List decoding RS codes

Reed-Solomon codes can be list decoded up to $n - \sqrt{kn}$ errors, which always exceeds $(n-k)/2$ [G.-Sudan'99]

Random codes (over sufficient large alphabet), allow decoding up to $(1-\varepsilon)(n-k)$ errors, for any fixed $\varepsilon > 0$ of one's choice

- 2x improvement over unambiguous decoding.

List decoding RS codes

Reed-Solomon codes can be list decoded up to $n - \sqrt{kn}$ errors, which always exceeds $(n-k)/2$ [G.-Sudan'99]

Random codes (over sufficient large alphabet), allow decoding up to $(1-\varepsilon)(n-k)$ errors, for any fixed $\varepsilon > 0$ of one's choice

- 2x improvement over unambiguous decoding.

Explicit such codes are also known

- Folded Reed-Solomon codes of [G.-Rudra'08] and follow-ups.
- Couple of such explicit code families motivated definition of **subspace designs**

Reed-Solomon codes with evaluation points in a sub-field

Code maps

$$f \in \mathbb{F}_{q^m}[X]_{<k} \mapsto (f(a_1), f(a_2), \ldots, f(a_n)) \in (\mathbb{F}_{q^m})^n,$$

for n distinct $a_i \in \mathbb{F}_q$.

Reed-Solomon codes with evaluation points in a sub-field

Code maps

$$f \in \mathbb{F}_{q^m}[X]_{<k} \mapsto (f(a_1), f(a_2), \ldots, f(a_n)) \in (\mathbb{F}_{q^m})^n,$$

for n distinct $a_i \in \mathbb{F}_q$.

Theorem (G.-Xing'13)

Linear-algebraic algorithm that given $r \in (\mathbb{F}_{q^m})^n$, list decodes it up to radius $\frac{s}{s+1}(n-k)$, pinning down all candidate message polynomials $f(X) = f_0 + f_1 X + \cdots + f_{k-1}X^{k-1}$ to an $\mathbb{F}_q$-subspace of form:

$$f_i \in W + A_i(f_0, \ldots, f_{i-1}), \qquad i = 0, 1, \ldots, k-1,$$

for some $\mathbb{F}_q$-subspace $W \subset \mathbb{F}_{q^m}$ of dim. $s-1$, and $\mathbb{F}_q$-affine fns A_i.

Reed-Solomon codes with evaluation points in a sub-field

Code maps

$$f \in \mathbb{F}_{q^m}[X]_{<k} \mapsto (f(a_1), f(a_2), \ldots, f(a_n)) \in (\mathbb{F}_{q^m})^n,$$

for n distinct $a_i \in \mathbb{F}_q$.

Theorem (G.-Xing'13)

Linear-algebraic algorithm that given $r \in (\mathbb{F}_{q^m})^n$, list decodes it up to radius $\frac{s}{s+1}(n-k)$, pinning down all candidate message polynomials $f(X) = f_0 + f_1 X + \cdots + f_{k-1}X^{k-1}$ to an $\mathbb{F}_q$-subspace of form:

$$f_i \in W + A_i(f_0, \ldots, f_{i-1}), \qquad i = 0, 1, \ldots, k-1,$$

for some $\mathbb{F}_q$-subspace $W \subset \mathbb{F}_{q^m}$ of dim. $s-1$, and $\mathbb{F}_q$-affine fns A_i.

- Each f_i belongs to affine shift of the *same* $(s-1)$-dimensional W
- $\#$ solutions $= q^{(s-1)k} \ll q^{mk}$; exponential unless $s = 1$ (unique decoding)
- Trade-off between decoding radius and list size by increasing s.

Pruning the list

We have $f_i \in W + A_i(f_0, f_1, \ldots, f_{i-1})$, $i = 0, 1, \ldots, k-1$. (*)

Pruning via "subspace design"

- Suppose we pre-code messages so that $f_i \in H_i$, where the H_i's are $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$.

Pruning the list

We have $f_i \in W + A_i(f_0, f_1, \ldots, f_{i-1})$, $i = 0, 1, \ldots, k-1$. (*)

Pruning via "subspace design"

- Suppose we pre-code messages so that $f_i \in H_i$, where the H_i's are $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$.
- Dimension of solutions to (*) and $f_i \in H_i$, $\forall i$, becomes $\sum_{i=0}^{k-1} \dim(W \cap H_i)$.
- Insist this is small (so in particular W intersects few H_i non-trivially), and also $\dim(H_i) = (1-\varepsilon)m$ to incur only minor loss in rate.

Subspace Designs

Fix a vector space $\mathbb{F}_q^m$, and desired co-dimension εm of subspaces.

Definition

A collection of subspaces $H_1, H_2, \ldots, H_M \subseteq \mathbb{F}_q^m$ (each of co-dimension εm) is said to be an (s, ℓ)-**subspace design** if for every s-dimensional subspace W of $\mathbb{F}_q^m$,

$$\sum_{j=1}^{M} \dim(W \cap H_j) \leqslant \ell.$$

Subspace Designs

Fix a vector space $\mathbb{F}_q^m$, and desired co-dimension εm of subspaces.

Definition

A collection of subspaces $H_1, H_2, \ldots, H_M \subseteq \mathbb{F}_q^m$ (each of co-dimension εm) is said to be an (s, ℓ)-**subspace design** if for every s-dimensional subspace W of $\mathbb{F}_q^m$,

$$\sum_{j=1}^{M} \dim(W \cap H_j) \leqslant \ell.$$

- Implies $W \cap H_i \neq \{0\}$ for at most ℓ subspaces: (s, ℓ)-*weak subspace design*.
- Would like a large collection with small intersection bound ℓ

Existence of subspace designs

Theorem (Probabilistic method)

For all fields $\mathbb{F}_q$ and $s \leqslant \varepsilon m/2$, there is an $(s, 2s/\varepsilon)$-subspace design with $q^{\Omega(\varepsilon m)}$ subspaces of $\mathbb{F}_q^m$ of co-dimension εm. (A random collection has the subspace design property w.h.p.)

Both s and $1/\varepsilon$ are easy lower bounds on ℓ for (s, ℓ)-subspace design.

Existence of subspace designs

Theorem (Probabilistic method)

For all fields $\mathbb{F}_q$ and $s \leqslant \varepsilon m/2$, there is an $(s, 2s/\varepsilon)$-subspace design with $q^{\Omega(\varepsilon m)}$ subspaces of $\mathbb{F}_q^m$ of co-dimension εm. (A random collection has the subspace design property w.h.p.)

Both s and $1/\varepsilon$ are easy lower bounds on ℓ for (s, ℓ)-subspace design.

List decoding application: Using such a subspace design for pre-coding will reduce dimension of solution space to $O(1/\varepsilon^2)$ for list decoding up to radius $(1-\varepsilon)(n-k)$.

Existence of subspace designs

Theorem (Probabilistic method)

For all fields $\mathbb{F}_q$ and $s \leqslant \varepsilon m/2$, there is an $(s, 2s/\varepsilon)$-subspace design with $q^{\Omega(\varepsilon m)}$ subspaces of $\mathbb{F}_q^m$ of co-dimension εm. (A random collection has the subspace design property w.h.p.)

Both s and $1/\varepsilon$ are easy lower bounds on ℓ for (s, ℓ)-subspace design.

List decoding application: Using such a subspace design for pre-coding will reduce dimension of solution space to $O(1/\varepsilon^2)$ for list decoding up to radius $(1-\varepsilon)(n-k)$.

Goal

Explicit construction of subspace designs with similar parameters.

Explicit subspace designs

Theorem (Polynomials based construction (G.-Kopparty'13))

For $s \leqslant \varepsilon m/4$ and $q > m$, an explicit collection of $q^{\Omega(\varepsilon m/s)}$ subspaces of co-dimension εm that form an $(s, \frac{2s}{\varepsilon})$-subspace design.

Almost matches probabilistic construction for **large fields**.

Explicit subspace designs

Theorem (Polynomials based construction (G.-Kopparty'13))

For $s \leqslant \varepsilon m/4$ and $q > m$, an explicit collection of $q^{\Omega(\varepsilon m/s)}$ subspaces of co-dimension εm that form an $(s, \frac{2s}{\varepsilon})$-subspace design.

Almost matches probabilistic construction for **large fields**.

Using extension fields and an $\mathbb{F}_q$-linear map to express elements of $\mathbb{F}_{q^r}$ as vectors in $\mathbb{F}_q^r$, can get construction of $(s, 2s/\varepsilon)$-**weak subspace design** for *all* fields $\mathbb{F}_q$.

Explicit subspace designs

Theorem (Polynomials based construction (G.-Kopparty'13))

For $s \leqslant \varepsilon m/4$ and $q > m$, an explicit collection of $q^{\Omega(\varepsilon m/s)}$ subspaces of co-dimension εm that form an $(s, \frac{2s}{\varepsilon})$-subspace design.

Almost matches probabilistic construction for **large fields**.

Using extension fields and an $\mathbb{F}_q$-linear map to express elements of $\mathbb{F}_{q^r}$ as vectors in $\mathbb{F}_q^r$, can get construction of $(s, 2s/\varepsilon)$-**weak subspace design** for *all* fields $\mathbb{F}_q$.

$\Rightarrow$ These results give explicit optimal rate codes for list decoding over fixed alphabets and in the rank metric [G.-Xing'13, G.-Wang-Xing'15]. (The large collection is more important than strongness of subspace design for these applications.)

Small field construction

The strongness of subspace design is, however, crucial for its application to dimension expanders (coming later).

Cyclotomic function field based const. [G.-Xing-Yuan'16]

For $s \leqslant \varepsilon m/4$, an explicit collection of $q^{\Omega(\varepsilon m/s)}$ subspaces of co-dimension εm that form an $(s, \frac{2s\lceil \log_q m \rceil}{\varepsilon})$-subspace design.

(Leads to *logarithmic degree* dimension expanders for all fields.)

Small field construction

The strongness of subspace design is, however, crucial for its application to dimension expanders (coming later).

Cyclotomic function field based const. [G.-Xing-Yuan'16]

For $s \leqslant \varepsilon m/4$, an explicit collection of $q^{\Omega(\varepsilon m/s)}$ subspaces of co-dimension εm that form an $(s, \frac{2s\lceil \log_q m \rceil}{\varepsilon})$-subspace design.

(Leads to *logarithmic degree* dimension expanders for all fields.)

Open

Explicit $\omega(1)$-sized $(s, O(s))$-subspace design of dimension $m/2$ subspaces over any field $\mathbb{F}_q$.

(Would yield explicit *constant degree* dimension expanders.)

Polynomial based subspace design construction

Theorem

For parameters satisfying $s < t < m < q$, a construction of $\Omega(q^r/r)$ subspaces of $\mathbb{F}_q^m$ of co-dimension rt that form an $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$-subspace design.

Polynomial based subspace design construction

Theorem

For parameters satisfying $s < t < m < q$, a construction of $\Omega(q^r/r)$ subspaces of $\mathbb{F}_q^m$ of co-dimension rt that form an $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$-subspace design.

Taking $t = 2s$ and $r = \frac{\varepsilon m}{2s}$ yields $(s, 2s/\varepsilon)$-subspace design of co-dimension εm subspaces.

Polynomial based subspace design construction

Theorem

For parameters satisfying $s < t < m < q$, a construction of $\Omega(q^r/r)$ subspaces of $\mathbb{F}_q^m$ of co-dimension rt that form an $\left(s, \frac{(m-1)s}{r(t-s+1)}\right)$-subspace design.

Taking $t = 2s$ and $r = \frac{\varepsilon m}{2s}$ yields $(s, 2s/\varepsilon)$-subspace design of co-dimension εm subspaces.

Illustrate above theorem with 3 simplifications:

1. Fix $r = 1$
2. Show weak subspace design property
3. Assume $\text{char}(\mathbb{F}_q) > m$

Theorem (Polynomial based subspace design, simplified)

Explicit $(s, \frac{(m-1)s}{t-s+1})$*-weak subspace design with* q *co-dimension* t *subspaces of* $\mathbb{F}_q^m$*, when* $char(\mathbb{F}_q) > m$.

Theorem (Polynomial based subspace design, simplified)

Explicit $(s, \frac{(m-1)s}{t-s+1})$*-weak subspace design with* q *co-dimension* t *subspaces of* $\mathbb{F}_q^m$*, when* $char(\mathbb{F}_q) > m$*.*

Warm-up: $s = 1$ case

Further let $t = 1$. Want q subspaces of $\mathbb{F}_q^m$ of co-dimension 1 s.t. each nonzero $p \in \mathbb{F}_q^m$ is in at most $m - 1$ of the subspaces.

- Identify $\mathbb{F}_q^m$ with $\mathbb{F}_q[X]_{<m}$.

Theorem (Polynomial based subspace design, simplified)

Explicit $(s, \frac{(m-1)s}{t-s+1})$-weak subspace design with q co-dimension t subspaces of $\mathbb{F}_q^m$, when $char(\mathbb{F}_q) > m$.

Warm-up: $s = 1$ case

Further let $t = 1$. Want q subspaces of $\mathbb{F}_q^m$ of co-dimension 1 s.t. each nonzero $p \in \mathbb{F}_q^m$ is in at most $m - 1$ of the subspaces.

- Identify $\mathbb{F}_q^m$ with $\mathbb{F}_q[X]_{<m}$.
- For $\alpha \in \mathbb{F}_q$, define $H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = 0\}$.

Theorem (Polynomial based subspace design, simplified)

Explicit $(s, \frac{(m-1)s}{t-s+1})$*-weak subspace design with* q *co-dimension* t *subspaces of* $\mathbb{F}_q^m$*, when char*$(\mathbb{F}_q) > m$*.*

Warm-up: $s = 1$ case

Further let $t = 1$. Want q subspaces of $\mathbb{F}_q^m$ of co-dimension 1 s.t. each nonzero $p \in \mathbb{F}_q^m$ is in at most $m-1$ of the subspaces.

- Identify $\mathbb{F}_q^m$ with $\mathbb{F}_q[X]_{<m}$.
- For $\alpha \in \mathbb{F}_q$, define $H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = 0\}$.
- Each nonzero polynomial p of degree $< m$ has at most $m-1$ roots $\alpha \in \mathbb{F}_q$.

Theorem (Polynomial based subspace design, simplified)

Explicit $(s, \frac{(m-1)s}{t-s+1})$-weak subspace design with q co-dimension t subspaces of $\mathbb{F}_q^m$, when $char(\mathbb{F}_q) > m$.

Warm-up: $s = 1$ case

Further let $t = 1$. Want q subspaces of $\mathbb{F}_q^m$ of co-dimension 1 s.t. each nonzero $p \in \mathbb{F}_q^m$ is in at most $m - 1$ of the subspaces.

- Identify $\mathbb{F}_q^m$ with $\mathbb{F}_q[X]_{<m}$.
- For $\alpha \in \mathbb{F}_q$, define $H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = 0\}$.
- Each nonzero polynomial p of degree $< m$ has at most $m - 1$ roots $\alpha \in \mathbb{F}_q$.

$s = 1$, $t < m$ arbitrary:

Theorem (Polynomial based subspace design, simplified)

Explicit $\left(s, \frac{(m-1)s}{t-s+1}\right)$-weak subspace design with q co-dimension t subspaces of $\mathbb{F}_q^m$, when $char(\mathbb{F}_q) > m$.

Warm-up: $s = 1$ case

Further let $t = 1$. Want q subspaces of $\mathbb{F}_q^m$ of co-dimension 1 s.t. each nonzero $p \in \mathbb{F}_q^m$ is in at most $m - 1$ of the subspaces.

- Identify $\mathbb{F}_q^m$ with $\mathbb{F}_q[X]_{<m}$.
- For $\alpha \in \mathbb{F}_q$, define $H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = 0\}$.
- Each nonzero polynomial p of degree $< m$ has at most $m - 1$ roots $\alpha \in \mathbb{F}_q$.

$s = 1$, $t < m$ arbitrary:

- Define $H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid \text{mult}(p, \alpha) \geqslant t\}$.
- A nonzero degree $< m$ polynomial has at most $(m-1)/t$ roots with multiplicity t.

Polynomial based subspace design

Theorem

For $s < t < m < char(\mathbb{F}_q)$, the subspaces
$H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = p'(\alpha) = \cdots = p^{(t-1)}(\alpha) = 0\}$, $\alpha \in \mathbb{F}_q$,
form a $(s, \frac{(m-1)s}{t-s+1})$-weak subspace design.

Proof sketch on board.

Polynomial based subspace design

Theorem

For $s < t < m < char(\mathbb{F}_q)$, the subspaces
$H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = p'(\alpha) = \cdots = p^{(t-1)}(\alpha) = 0\}$, $\alpha \in \mathbb{F}_q$,
form a $(s, \frac{(m-1)s}{t-s+1})$*-weak subspace design.*

Proof sketch on board.

Removing the 3 simplifications:

1. General r: Pick root points $\alpha \in \mathbb{F}_{q^r}$. (Co-dimension becomes rt.)

Polynomial based subspace design

Theorem

For $s < t < m < char(\mathbb{F}_q)$, the subspaces
$H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = p'(\alpha) = \cdots = p^{(t-1)}(\alpha) = 0\}$, $\alpha \in \mathbb{F}_q$,
form a $(s, \frac{(m-1)s}{t-s+1})$-weak subspace design.

Proof sketch on board.

Removing the 3 simplifications:

1. General r: Pick root points $\alpha \in \mathbb{F}_{q^r}$. (Co-dimension becomes rt.)
2. Strong subspace design property: more careful analysis.

Polynomial based subspace design

Theorem

For $s < t < m < char(\mathbb{F}_q)$, the subspaces
$H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = p'(\alpha) = \cdots = p^{(t-1)}(\alpha) = 0\}$, $\alpha \in \mathbb{F}_q$,
form a $(s, \frac{(m-1)s}{t-s+1})$-weak subspace design.

Proof sketch on board.

Removing the 3 simplifications:

1. General r: Pick root points $\alpha \in \mathbb{F}_{q^r}$. (Co-dimension becomes rt.)
2. Strong subspace design property: more careful analysis.
3. Working with $q > m$ rather than $\text{char}(\mathbb{F}_q) > m$:
   - t structured roots instead of t multiple roots.
   - $H_\alpha = \{p \in \mathbb{F}_q[X]_{<m} \mid p(\alpha) = p(\alpha\gamma) = \cdots = p(\alpha\gamma^{t-1}) = 0\}$ (where γ is a primitive element of $\mathbb{F}_q$).

Plan

Subspace designs:

- Why we defined them?
- Definition
- How to construct them?
- Applications in linear-algebraic pseudorandomness

Subspace designs as rank condensers

Suppose $H_i = \ker(E_i)$ for condensing map $E_i : \mathbb{F}^m \to \mathbb{F}^{\varepsilon m}$.

- In our construction, the E_i's were polynomial evaluation maps (underlying folded Reed-Solomon/derivative codes).

Note $\dim(W \cap H_i) = \dim(W) - \dim(E_i W)$.

Subspace designs as rank condensers

Suppose $H_i = \ker(E_i)$ for condensing map $E_i : \mathbb{F}^m \to \mathbb{F}^{\varepsilon m}$.

- In our construction, the E_i's were polynomial evaluation maps (underlying folded Reed-Solomon/derivative codes).

Note $\dim(W \cap H_i) = \dim(W) - \dim(E_i W)$.

Lossless rank condenser

So (s, ℓ)-weak subspace design property $\Longrightarrow$ for every s-dimensional W, $\dim(E_i W) = \dim(W)$ for all but ℓ maps. (So if size of subspace design is $> \ell$, at least one map preserves rank.)

Subspace designs as rank condensers

Suppose $H_i = \ker(E_i)$ for condensing map $E_i : \mathbb{F}^m \to \mathbb{F}^{\varepsilon m}$.

- In our construction, the E_i's were polynomial evaluation maps (underlying folded Reed-Solomon/derivative codes).

Note $\dim(W \cap H_i) = \dim(W) - \dim(E_i W)$.

Lossless rank condenser

So (s, ℓ)-weak subspace design property $\Longrightarrow$ for every s-dimensional W, $\dim(E_i W) = \dim(W)$ for all but ℓ maps. (So if size of subspace design is $> \ell$, at least one map preserves rank.)

Lossy rank condenser

(s, ℓ)-subspace design property $\Longrightarrow$ for every s-dimensional W, $\dim(E_i W) < (1 - \delta) \dim(W)$ for less than $\frac{\ell}{\delta s}$ maps. (So if size of subspace design is $\geqslant \frac{\ell}{\delta s}$, at least one map preserves rank up to $(1 - \delta)$ factor.)

Dimension expander via subspace designs

Fix a vector space $\mathbb{F}^n$ over a field $\mathbb{F}$.

Dimension expanders

A collection of d linear maps $A_1, A_2, \ldots, A_d : \mathbb{F}^n \to \mathbb{F}^n$ is said to be an (b, α)-dimension expander if for all subspaces V of $\mathbb{F}^n$ of dimension $\leqslant b$,

$$\dim(\textstyle\sum_{i=1}^{d} A_i(V)) \geqslant (1 + \alpha) \dim(V).$$

- d is the "degree" of the dim. expander, and α the "expansion factor."

Dimension expander via subspace designs [Forbes-G.'15]

Idea: "Tensor-then-condense"

Dimension expander via subspace designs [Forbes-G.'15]

Idea: "Tensor-then-condense"

A specific instantation:

- $\mathbb{F}^n \xrightarrow{\text{tensor}} \mathbb{F}^n \otimes \mathbb{F}^2 = \mathbb{F}^{2n} \xrightarrow{\text{condense}} \mathbb{F}^n$
- Tensoring: let $T_1(v) = (v, 0)$ & $T_2(v) = (0, v)$ be maps from $\mathbb{F}^n \to \mathbb{F}^{2n}$. (These trivially double the rank using twice the ambient dimension.)

Dimension expander via subspace designs [Forbes-G.'15]

Idea: "Tensor-then-condense"

A specific instantation:

- $\mathbb{F}^n \xrightarrow{\text{tensor}} \mathbb{F}^n \otimes \mathbb{F}^2 = \mathbb{F}^{2n} \xrightarrow{\text{condense}} \mathbb{F}^n$
- Tensoring: let $T_1(v) = (v, 0)$ & $T_2(v) = (0, v)$ be maps from $\mathbb{F}^n \to \mathbb{F}^{2n}$. (These trivially double the rank using twice the ambient dimension.)
- Condensing: Let $m = 2n$, and take a subspace design of $\frac{m}{2}$-dimensional subspaces in $\mathbb{F}^m$ with associated maps $E_1, E_2, \ldots, E_M : \mathbb{F}^{2n} \to \mathbb{F}^n$.
- Use the $2M$ maps $E_j \circ T_i$ for dimension expansion.

Analysis

Tensor-then-condense: $\mathbb{F}^n \xrightarrow{\text{tensor}} \mathbb{F}^n \otimes \mathbb{F}^2 = \mathbb{F}^{2n} \xrightarrow{\text{condense}} \mathbb{F}^n$

- Suppose (kernels of) condensing maps $E_1, E_2, \ldots, E_M : \mathbb{F}^{2n} \to \mathbb{F}^n$ form a (s, cs)-subspace design.
- (Lossy condensing): If $M \geqslant 3c$, for any s-dimensional subspace of $\mathbb{F}^{2n}$, at least one E_j has output rank $\frac{2s}{3}$.
- Composition $E_j \circ T_i$ gives an $(\frac{s}{2}, \frac{1}{3})$-dim. expander of degree $6c$.

Analysis

Tensor-then-condense: $\mathbb{F}^n \xrightarrow{\text{tensor}} \mathbb{F}^n \otimes \mathbb{F}^2 = \mathbb{F}^{2n} \xrightarrow{\text{condense}} \mathbb{F}^n$

- Suppose (kernels of) condensing maps $E_1, E_2, \ldots, E_M : \mathbb{F}^{2n} \to \mathbb{F}^n$ form a (s, cs)-subspace design.
- (Lossy condensing): If $M \geqslant 3c$, for any s-dimensional subspace of $\mathbb{F}^{2n}$, at least one E_j has output rank $\frac{2s}{3}$.
- Composition $E_j \circ T_i$ gives an $(\frac{s}{2}, \frac{1}{3})$-dim. expander of degree $6c$.

Consequences

1. Polynomials based subspace design $\Rightarrow$ constant degree $(\Omega(n), \frac{1}{3})$-dimension expander over $\mathbb{F}_q$ when $q \geqslant \Omega(n)$.

Analysis

Tensor-then-condense: $\mathbb{F}^n \xrightarrow{\text{tensor}} \mathbb{F}^n \otimes \mathbb{F}^2 = \mathbb{F}^{2n} \xrightarrow{\text{condense}} \mathbb{F}^n$

- Suppose (kernels of) condensing maps $E_1, E_2, \ldots, E_M : \mathbb{F}^{2n} \to \mathbb{F}^n$ form a (s, cs)-subspace design.
- (Lossy condensing): If $M \geqslant 3c$, for any s-dimensional subspace of $\mathbb{F}^{2n}$, at least one E_j has output rank $\frac{2s}{3}$.
- Composition $E_j \circ T_i$ gives an $(\frac{s}{2}, \frac{1}{3})$-dim. expander of degree $6c$.

Consequences

1. Polynomials based subspace design $\Rightarrow$ constant degree $(\Omega(n), \frac{1}{3})$-dimension expander over $\mathbb{F}_q$ when $q \geqslant \Omega(n)$.
2. Cyclotomic function field based subspace design $\Rightarrow$ $O(\log n)$ degree $(\frac{n}{\log \log n}, \frac{1}{3})$-dim. expander over *arbitrary* finite fields.

Dimension expanders: Prior (better) constructions

All guarantee expansion of subspaces of dimension up to $\Omega(n)$.

1. [Lubotzky-Zelmanov'08] Construction for fields of characteristic zero (using property T of groups). Constant degree and expansion.

Dimension expanders: Prior (better) constructions

All guarantee expansion of subspaces of dimension up to $\Omega(n)$.

1. [Lubotzky-Zelmanov'08] Construction for fields of characteristic zero (using property T of groups). Constant degree and expansion.
2. [Dvir-Shpilka'11] Constant degree and $\Omega(1/\log n)$ expansion, or $O(\log n)$ degree and $\Omega(1)$ expansion.
   - Construction via *monotone expanders*.
3. [Dvir-Wigderson'10]: monotone expanders (and hence dimension expanders) of $\log^{(c)} n$ degree.

Dimension expanders: Prior (better) constructions

All guarantee expansion of subspaces of dimension up to $\Omega(n)$.

1. [Lubotzky-Zelmanov'08] Construction for fields of characteristic zero (using property T of groups). Constant degree and expansion.
2. [Dvir-Shpilka'11] Constant degree and $\Omega(1/\log n)$ expansion, or $O(\log n)$ degree and $\Omega(1)$ expansion.
   - Construction via *monotone expanders*.
3. [Dvir-Wigderson'10]: monotone expanders (and hence dimension expanders) of $\log^{(c)} n$ degree.
4. [Bourgain-Yehudayoff'13] Sophisticated construction of constant degree monotone expanders using expansion in $SL_2(\mathbb{R})$ (note: no other proof is known even for existence)

Dimension expanders: Prior (better) constructions

All guarantee expansion of subspaces of dimension up to $\Omega(n)$.

1. [Lubotzky-Zelmanov'08] Construction for fields of characteristic zero (using property T of groups). Constant degree and expansion.
2. [Dvir-Shpilka'11] Constant degree and $\Omega(1/\log n)$ expansion, or $O(\log n)$ degree and $\Omega(1)$ expansion.
    - Construction via *monotone expanders*.
3. [Dvir-Wigderson'10]: monotone expanders (and hence dimension expanders) of $\log^{(c)} n$ degree.
4. [Bourgain-Yehudayoff'13] Sophisticated construction of constant degree monotone expanders using expansion in $SL_2(\mathbb{R})$ (note: no other proof is known even for existence)

<u>Our construction:</u> Avoids reduction to monotone expanders; works entirely within linear-algebraic setting, where expansion should be easier rather than harder than graph vertex expansion.

Degree vs expansion

Lossless expansion: Probabilistic construction with d linear maps achieves dimension expansion factor $d - O(1)$.

This trade-off not addressed (and probably quite poor?) in monotone expander based work.

Degree vs expansion

Lossless expansion: Probabilistic construction with d linear maps achieves dimension expansion factor $d - O(1)$.

This trade-off not addressed (and probably quite poor?) in monotone expander based work.

Our construction: Expansion $\Omega(\sqrt{d})$ with degree d

- Tensoring step uses α maps for expansion α
- Condensing uses another $\approx \alpha$ maps to shrink $\mathbb{F}^{\alpha n} \to \mathbb{F}^n$, preserving dimension up to constant factor.

Degree vs expansion

Lossless expansion: Probabilistic construction with d linear maps achieves dimension expansion factor $d - O(1)$.

This trade-off not addressed (and probably quite poor?) in monotone expander based work.

Our construction: Expansion $\Omega(\sqrt{d})$ with degree d

- Tensoring step uses α maps for expansion α
- Condensing uses another $\approx \alpha$ maps to shrink $\mathbb{F}^{\alpha n} \to \mathbb{F}^n$, preserving dimension up to constant factor.

Challenge

Can one explicitly achieve dimension expansion $\Omega(d)$?
Or even lossless expansion of $(1 - \varepsilon)d$?

Two-source rank condensers [Forbes-G.'15]

Two-source condenser for rank r

We would like a (bilinear) map $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ such that for all subsets $A, B \subseteq \mathbb{F}^n$ with $\mathrm{rk}(A), \mathrm{rk}(B) \leqslant r$, $\mathrm{rk}(f(A \times B))$ is large:

Two-source rank condensers [Forbes-G.'15]

Two-source condenser for rank r

We would like a (bilinear) map $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ such that for all subsets $A, B \subseteq \mathbb{F}^n$ with $\mathrm{rk}(A), \mathrm{rk}(B) \leqslant r$, $\mathrm{rk}(f(A \times B))$ is large:

lossless : $\mathrm{rk}(f(A \times B)) = \mathrm{rk}(A) \cdot \mathrm{rk}(B)$

lossy : $\mathrm{rk}(f(A \times B)) \geqslant 0.9 \cdot \mathrm{rk}(A) \cdot \mathrm{rk}(B)$

Two-source rank condensers [Forbes-G.'15]

Two-source condenser for rank r

We would like a (bilinear) map $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ such that for all subsets $A, B \subseteq \mathbb{F}^n$ with $\mathrm{rk}(A), \mathrm{rk}(B) \leqslant r$, $\mathrm{rk}(f(A \times B))$ is large:

$$\text{lossless} : \mathrm{rk}(f(A \times B)) = \mathrm{rk}(A) \cdot \mathrm{rk}(B)$$

$$\text{lossy} : \mathrm{rk}(f(A \times B)) \geqslant 0.9 \cdot \mathrm{rk}(A) \cdot \mathrm{rk}(B)$$

Derandomizing tensor product

- $f(x, y) = x \otimes y$ is lossless with $m = n^2$.
- Would like smaller output.

Lossless two-source rank condenser

Lemma (Equivalence to rank-metric codes)

A bilinear map $f(x, y) = \langle x^T E_1 y, x^T E_2 y, \ldots, x^T E_m y \rangle$ *is a lossless two-source condenser for rank* r *if and only if* $\{M \in \mathbb{F}^{n \times n} \mid \langle E_i, M \rangle = 0 \ \forall i\}$ *has no non-zero matrix of rank* $\leqslant r$.

Lossless two-source rank condenser

Lemma (Equivalence to rank-metric codes)

A bilinear map $f(x, y) = \langle x^T E_1 y, x^T E_2 y, \ldots, x^T E_m y \rangle$ *is a lossless two-source condenser for rank* r *if and only if* $\{M \in \mathbb{F}^{n \times n} \mid \langle E_i, M \rangle = 0 \ \forall i\}$ *has no non-zero matrix of rank* $\leqslant r$.

Condensers with optimal output length

Gabidulin construction (analog of Reed-Solomon codes with linearized polynomials) gives distance $r + 1$ rank-metric codes with $m = nr$, and this is best possible (for finite fields).

Lossless two-source rank condenser

Lemma (Equivalence to rank-metric codes)

A bilinear map $f(x, y) = \langle x^T E_1 y, x^T E_2 y, \ldots, x^T E_m y\rangle$ *is a lossless two-source condenser for rank* r *if and only if* $\{M \in \mathbb{F}^{n\times n} \mid \langle E_i, M\rangle = 0\ \forall i\}$ *has no non-zero matrix of rank* $\leqslant r$*.*

Condensers with optimal output length

Gabidulin construction (analog of Reed-Solomon codes with linearized polynomials) gives distance $r + 1$ rank-metric codes with $m = nr$, and this is best possible (for finite fields).

Condense-then-tensor approach: Use subspace design to condense to $\mathbb{F}^{2r}$ while preserving rank, and then tensor. Naively leads to output length $O(nr^2)$, but can eliminate linear dependencies to achieve output length $m = O(nr)$.

Lossy two-source rank condensers

A random bilinear map $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ is a lossy 2-source condenser for rank r when $m = C \cdot (n + r^2)$ for sufficiently large constant C.

Lossy two-source rank condensers

A random bilinear map $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ is a lossy 2-source condenser for rank r when $m = C \cdot (n + r^2)$ for sufficiently large constant C.

Challenge

Give an explicit construction with $m = O(n)$ (for $r \ll \sqrt{n}$).

Condenser-then-tensor approach achieves $m = O(nr)$, which doesn't beat the bound for lossless condenser.

Summary

- Emerging theory of pseudorandom objects dealing with rank of subspaces
- Subpace design a useful construct in this web of connections.
- Original motivation from list decoding, and construction based on algebraic codes.

Summary

- Emerging theory of pseudorandom objects dealing with rank of subspaces
- Subpace design a useful construct in this web of connections.
- Original motivation from list decoding, and construction based on algebraic codes.

Many open questions, such as:

1. Better/optimal subspace designs over small fields; would lead to constant degree dimension expanders for all fields.
2. Explicit lossy two-source rank condensers
3. Construction of subspace evasive sets with polynomial intersection size.