Linear independence of rank 1 matrices and the dimension of $*$-products of codes

Hugues Randriambololona

Telecom ParisTech & LTCI CNRS

ISIT Hong-Kong
2015-06-15

Let V be a finite dimensional vector space, and $X \subseteq V$ an arbitrary subset.

Definition

Say X is in (linearly) general position if, for any finite $S \subseteq X$,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

This means: no "unexpected" linear relation between elements of X.

Example: $V = \mathbb{F}_q^k$, $X \subseteq V$, $n = |X|$, $C = [n,k]_q$-code with generating matrix whose columns are X. Then: X in general position $\iff$ C MDS.

Let V be a finite dimensional vector space, and $X \subseteq V$ an arbitrary subset.

Definition

Say X is in (linearly) general position if, for any finite $S \subseteq X$,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

This means: no "unexpected" linear relation between elements of X.

Example: $V = \mathbb{F}_q^k$, $X \subseteq V$, $n = |X|$, $C = [n,k]_q$-code with generating matrix whose columns are X. Then: X in general position $\iff$ C MDS.

Weaker variants? Measure of failure?

Let V be a finite dimensional vector space, and $X \subseteq V$ an arbitrary subset.

Definition

Say X is in (linearly) general position if, for any finite $S \subseteq X$,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

This means: no "unexpected" linear relation between elements of X.

Example: $V = \mathbb{F}_q^k$, $X \subseteq V$, $n = |X|$, $C = [n,k]_q$-code with generating matrix whose columns are X. Then: X in general position $\iff$ C MDS.

Weaker variants? Measure of failure?

Assume X equipped with a probability distribution $\mathscr{L}$.

Estimate the "error probability"

$$\mathbb{P}(n) = \mathbb{P}[\dim\langle \mathbf{u}_1, \ldots, \mathbf{u}_n\rangle < \min(n, \dim V)]$$

for random $\mathbf{u}_1, \ldots, \mathbf{u}_n \in X$.

In this work: $V = \mathbb{F}_q^{k\times l}$ matrix space, $X \subseteq V$ set of matrices of rank 1.

In this work: $V = \mathbb{F}_q^{k \times l}$ matrix space, $X \subseteq V$ set of matrices of rank 1.

Linked with the theory of products of codes.
Componentwise multiplication: $\mathbf{c} = (c_1, \dots, c_n), \mathbf{c}' = (c'_1, \dots, c'_n) \in \mathbb{F}_q^n$

$$\mathbf{c} * \mathbf{c}' = (c_1 c'_1, \dots, c_n c'_n) \in \mathbb{F}_q^n.$$

Pass to the linear span: $C, C' \subseteq \mathbb{F}_q^n$

$$C * C' = \langle \mathbf{c} * \mathbf{c}' \rangle_{\mathbf{c} \in C, \mathbf{c}' \in C'} \subseteq \mathbb{F}_q^n$$

$\rightarrow$ square $C^{\langle 2 \rangle} = C * C$, higher powers $C^{\langle s \rangle}$.

In this work: $V = \mathbb{F}_q^{k \times l}$ matrix space, $X \subseteq V$ set of matrices of rank 1.

Linked with the theory of products of codes.
Componentwise multiplication: $\mathbf{c} = (c_1, \dots, c_n), \mathbf{c}' = (c'_1, \dots, c'_n) \in \mathbb{F}_q^n$

$$\mathbf{c} * \mathbf{c}' = (c_1 c'_1, \dots, c_n c'_n) \in \mathbb{F}_q^n.$$

Pass to the linear span: $C, C' \subseteq \mathbb{F}_q^n$

$$C * C' = \langle \mathbf{c} * \mathbf{c}' \rangle_{\mathbf{c} \in C, \mathbf{c}' \in C'} \subseteq \mathbb{F}_q^n$$

$\rightarrow$ square $C^{\langle 2 \rangle} = C * C$, higher powers $C^{\langle s \rangle}$.

Many recent (and less recent) applications:

- bilinear algorithms & arithmetic secret sharing systems
- analysis of McEliece-type cryptosystems
- algebraic decoding (error-correcting pairs, power decoding, ...)
- construction of lattices, oblivious transfer, quantum codes, ...

Bilinear algorithms

Over $\mathbb{F}_q$, given a bilinear map B (example: $E = E' = F = \mathbb{F}_{q^r}$, $B =$ field multiplication)

$$E \times E' \xrightarrow{B} F$$

Bilinear algorithms

Over $\mathbb{F}_q$, given a bilinear map B (example: $E = E' = F = \mathbb{F}_{q^r}$, $B =$ field multiplication) we want linear maps $\varphi, \varphi', \theta$ and a diagram

$$\begin{array}{ccc} E \times E' & \xrightarrow{B} & F \\ {\scriptstyle \varphi\times\varphi'}\big\downarrow & & \big\uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

so $B(x, x') = \theta(\varphi(x) * \varphi'(x'))$ for $x \in E, x' \in E'$.

Bilinear algorithms

Over $\mathbb{F}_q$, given a bilinear map B (example: $E = E' = F = \mathbb{F}_{q^r}$, $B =$ field multiplication) we want linear maps $\varphi, \varphi', \theta$ and a diagram

$$\begin{array}{ccc} E \times E' & \xrightarrow{B} & F \\ {\scriptstyle \varphi\times\varphi'}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

so $B(x, x') = \theta(\varphi(x) * \varphi'(x'))$ for $x \in E, x' \in E'$.

Observe $\varphi(x) * \varphi'(x') \in C * C'$ where $C = \varphi(E), C' = \varphi'(E')$.
Possible objectives: minimize n, maximize d and/or $d^\perp$ of $C, C', C * C'$...

Bilinear algorithms

Over $\mathbb{F}_q$, given a bilinear map B (example: $E = E' = F = \mathbb{F}_{q^r}$, $B =$ field multiplication) we want linear maps $\varphi, \varphi', \theta$ and a diagram

$$\begin{tikzcd} E \times E' \arrow[r, "B"] \arrow[d, "\varphi\times\varphi'"'] & F \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n \arrow[r, "*"] & (\mathbb{F}_q)^n \arrow[u, "\theta"'] \end{tikzcd}$$

so $B(x, x') = \theta(\varphi(x) * \varphi'(x'))$ for $x \in E, x' \in E'$.

Observe $\varphi(x) * \varphi'(x') \in C * C'$ where $C = \varphi(E), C' = \varphi'(E')$.
Possible objectives: minimize n, maximize d and/or $d^\perp$ of $C, C', C * C'$...

Choose bases, set $k = \dim E$, $l = \dim E'$, $f = \dim F$.
Then: $B \iff$ collection of matrices $\mathbf{B}_1, \ldots, \mathbf{B}_f \in \mathbb{F}_q^{k\times l}$,
our diagram $\iff$ $\mathbf{u}_1, \ldots, \mathbf{u}_n$ of rank 1 whose span contains $\mathbf{B}_1, \ldots, \mathbf{B}_f$.

McEliece-type cryptosystems

Secret key: $\mathbf{G}$ with an efficient decoding algorithm, $\mathbf{S}, \mathbf{P}$ “masks”.
Public key: $\widetilde{\mathbf{G}} = \mathbf{SGP}$ hard to decode (NP-hard if $\widetilde{\mathbf{G}}$ were really random).

McEliece-type cryptosystems

Secret key: $\mathbf{G}$ with an efficient decoding algorithm, $\mathbf{S}, \mathbf{P}$ “masks”.
Public key: $\widetilde{\mathbf{G}} = \mathbf{SGP}$ hard to decode (NP-hard if $\widetilde{\mathbf{G}}$ were really random).

Attacks:

- distinguish $\widetilde{\mathbf{G}}$ from a random matrix
- recover its hidden algebraic structure.

McEliece-type cryptosystems

Secret key: $\mathbf{G}$ with an efficient decoding algorithm, $\mathbf{S}, \mathbf{P}$ "masks".
Public key: $\widetilde{\mathbf{G}} = \mathbf{SGP}$ hard to decode (NP-hard if $\widetilde{\mathbf{G}}$ were really random).

Attacks:

- distinguish $\widetilde{\mathbf{G}}$ from a random matrix
- recover its hidden algebraic structure.

Heuristic: for $k = \dim C$, $l = \dim C'$, both of length n,

$$\dim C * C' \leq \min(n, kl)$$

(proof: $C = \langle \mathbf{c}_i \rangle_{i \in [k]}$, $C' = \langle \mathbf{c}'_j \rangle_{j \in [l]} \implies C * C' = \langle \mathbf{c}_i * \mathbf{c}'_j \rangle_{i \in [k], j \in [l]}$).
Expects equality for random C, C'.
Strict inequality means (bilinear) algebraic relations between C, C'
(example: $C = [n, k]_q$-RS, $C' = [n, l]_q$-RS $\rightarrow C * C' = [n, k + l - 1]_q$-RS).

McEliece-type cryptosystems

Secret key: $\mathbf{G}$ with an efficient decoding algorithm, $\mathbf{S}, \mathbf{P}$ "masks".
Public key: $\widetilde{\mathbf{G}} = \mathbf{SGP}$ hard to decode (NP-hard if $\widetilde{\mathbf{G}}$ were really random).

Attacks:

- distinguish $\widetilde{\mathbf{G}}$ from a random matrix
- recover its hidden algebraic structure.

Heuristic: for $k = \dim C$, $l = \dim C'$, both of length n,

$$\dim C * C' \leq \min(n, kl)$$

(proof: $C = \langle \mathbf{c}_i \rangle_{i \in [k]}$, $C' = \langle \mathbf{c}'_j \rangle_{j \in [l]} \implies C * C' = \langle \mathbf{c}_i * \mathbf{c}'_j \rangle_{i \in [k], j \in [l]}$).
Expects equality for random C, C'.
Strict inequality means (bilinear) algebraic relations between C, C'
(example: $C = [n,k]_q$-RS, $C' = [n,l]_q$-RS $\rightarrow C * C' = [n, k+l-1]_q$-RS).

$\rightarrow$ Apply this to $C, C' =$ subcodes of the row span code of $\widetilde{\mathbf{G}}$.

Row view vs. column view

Let $C = [n,k]_q$-code with $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ and $C' = [n,l]_q$-code with $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$.
From these we deduce a generating matrix $\widetilde{\mathbf{G}}$ for $C * C'$ (remark: we allow redundant rows).

Row view vs. column view

Let $C = [n,k]_q$-code with $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ and $C' = [n,l]_q$-code with $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$. From these we deduce a generating matrix $\widetilde{\mathbf{G}}$ for $C * C'$ (remark: we allow redundant rows).

Row view: As we just saw, $\{\mathbf{c}_i\}_{i\in[k]}$ rows of $\mathbf{G}$, $\{\mathbf{c}'_j\}_{j\in[l]}$ rows of $\mathbf{G}'$,
$\rightarrow$ $\{\mathbf{c}_i * \mathbf{c}'_j\}_{i\in[k],j\in[l]}$ rows of $\widetilde{\mathbf{G}}$.

Row view vs. column view

Let $C = [n,k]_q$-code with $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ and $C' = [n,l]_q$-code with $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$. From these we deduce a generating matrix $\widetilde{\mathbf{G}}$ for $C * C'$ (remark: we allow redundant rows).

Row view: As we just saw, $\{\mathbf{c}_i\}_{i\in[k]}$ rows of $\mathbf{G}$, $\{\mathbf{c}'_j\}_{j\in[l]}$ rows of $\mathbf{G}'$,
$\rightarrow \{\mathbf{c}_i * \mathbf{c}'_j\}_{i\in[k],j\in[l]}$ rows of $\widetilde{\mathbf{G}}$.

Column view: Identify $\mathbb{F}_q^{kl}$ with matrix space $\mathbb{F}_q^{k\times l}$.
Set $\mathbf{p}_1,\dots,\mathbf{p}_n \in \mathbb{F}_q^k$ columns of $\mathbf{G}$, $\mathbf{q}_1,\dots,\mathbf{q}_n \in \mathbb{F}_q^l$ columns of $\mathbf{G}'$,

$$\longrightarrow \quad \mathbf{u}_i = \mathbf{p}_i\mathbf{q}_i^T \in \mathbb{F}_q^{k\times l} \text{ of rank } (\leq)1.$$

Then $\mathbf{u}_1,\dots,\mathbf{u}_n$ are the columns of $\widetilde{\mathbf{G}}$.

Row view vs. column view

Let $C = [n,k]_q$-code with $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ and $C' = [n,l]_q$-code with $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$.
From these we deduce a generating matrix $\widetilde{\mathbf{G}}$ for $C * C'$ (remark: we allow redundant rows).

Row view: As we just saw, $\{\mathbf{c}_i\}_{i\in[k]}$ rows of $\mathbf{G}$, $\{\mathbf{c}'_j\}_{j\in[l]}$ rows of $\mathbf{G}'$,
$\rightarrow \{\mathbf{c}_i * \mathbf{c}'_j\}_{i\in[k],j\in[l]}$ rows of $\widetilde{\mathbf{G}}$.

Column view: Identify $\mathbb{F}_q^{kl}$ with matrix space $\mathbb{F}_q^{k\times l}$.
Set $\mathbf{p}_1,\dots,\mathbf{p}_n \in \mathbb{F}_q^k$ columns of $\mathbf{G}$, $\mathbf{q}_1,\dots,\mathbf{q}_n \in \mathbb{F}_q^l$ columns of $\mathbf{G}'$,

$$\longrightarrow \quad \mathbf{u}_i = \mathbf{p}_i\mathbf{q}_i^T \in \mathbb{F}_q^{k\times l} \text{ of rank } (\leq)1.$$

Then $\mathbf{u}_1,\dots,\mathbf{u}_n$ are the columns of $\widetilde{\mathbf{G}}$.

Row rank = column rank!

$$\dim C * C' = \dim\langle \mathbf{u}_1,\dots,\mathbf{u}_n\rangle$$

The setting

- $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l \times n}$ random with uniform distribution
- $C, C' \subseteq \mathbb{F}_q^n$ their respective row spans
- $\mathbf{p}_1, \dots, \mathbf{p}_n \in \mathbb{F}_q^k$, $\mathbf{q}_1, \dots, \mathbf{q}_n \in \mathbb{F}_q^l$ their columns, resp. ($\rightarrow$ uniform)
- $\mathbf{u}_i = \mathbf{p}_i \mathbf{q}_i^T \in \mathbb{F}_q^{k \times l}$.

The setting

- $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$ random with uniform distribution
- $C, C' \subseteq \mathbb{F}_q^n$ their respective row spans
- $\mathbf{p}_1, \ldots, \mathbf{p}_n \in \mathbb{F}_q^k$, $\mathbf{q}_1, \ldots, \mathbf{q}_n \in \mathbb{F}_q^l$ their columns, resp. ($\rightarrow$ uniform)
- $\mathbf{u}_i = \mathbf{p}_i \mathbf{q}_i^T \in \mathbb{F}_q^{k\times l}$.

We are interested in

$$\begin{aligned}\mathbb{P}(n) &= \mathbb{P}[\dim C * C' < \min(n, kl)] \\ &= \mathbb{P}[\dim\langle \mathbf{u}_1, \ldots, \mathbf{u}_n\rangle < \min(n, kl)].\end{aligned}$$

The setting

- $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$ random with uniform distribution
- $C, C' \subseteq \mathbb{F}_q^n$ their respective row spans
- $\mathbf{p}_1, \dots, \mathbf{p}_n \in \mathbb{F}_q^k$, $\mathbf{q}_1, \dots, \mathbf{q}_n \in \mathbb{F}_q^l$ their columns, resp. ($\rightarrow$ uniform)
- $\mathbf{u}_i = \mathbf{p}_i \mathbf{q}_i^T \in \mathbb{F}_q^{k\times l}$.

We are interested in

$$\begin{aligned}\mathbb{P}(n) &= \mathbb{P}[\dim C * C' < \min(n, kl)] \\ &= \mathbb{P}[\dim\langle \mathbf{u}_1, \dots, \mathbf{u}_n\rangle < \min(n, kl)].\end{aligned}$$

Possible tweaks in the probabilistic model:

- $\mathbf{G}, \mathbf{G}'$ may have zero columns, so $\mathrm{rk}(\mathbf{u}_i) \leq 1$ (with 0 allowed) $\rightarrow$ distribution $\mathscr{L}$ on the set X of $\mathrm{rk} \leq 1$ matrices.
  However $\mathbf{u}_i = b_i \widetilde{\mathbf{u}}_i$ with $b_i \in \{0, 1\}$ Bernoulli($(1 - q^{-k})(1 - q^{-l})$), and $\mathrm{rk}\, \widetilde{\mathbf{u}}_i = 1$, uniform.
- Likewise $\dim C \leq k, \dim C' \leq l$, strict inequality allowed...

Set $C_q = \prod_{j\geq 1}(1-q^{-j})^{-1} \leq C_2 \approx 3.463$, and parameter domain

$$\mathcal{P}(\varepsilon,\kappa) = \left\{(k,l);\ 2 \leq k \leq l \leq \frac{\varepsilon q^{\kappa k}}{(q-1)k}\right\} \qquad (0<\varepsilon<1,\ \kappa>0).$$

Set $C_q = \prod_{j\geq 1}(1-q^{-j})^{-1} \leq C_2 \approx 3.463$, and parameter domain

$$\mathcal{P}(\varepsilon,\kappa) = \left\{(k,l);\ 2\leq k\leq l\leq \frac{\varepsilon q^{\kappa k}}{(q-1)k}\right\} \qquad (0<\varepsilon<1,\ \kappa>0).$$

Theorem 16

Suppose κ small enough, so $q^{(1-\kappa)^2} \geq 1+\frac{q-1}{q}$ (ex: $\kappa = 0.23$).
Then for $(k,l)\in\mathcal{P}(\varepsilon,\kappa)$ and $n\geq kl$, we have

$$\mathbb{P}(n) = \mathbb{P}[\dim C * C' < kl] \leq c''\rho^{n-kl}$$

with $\rho = \frac{1}{q}\left(1+\frac{q-1}{q}\right) < 1$ and $c'' = \frac{qC_q}{(q-1)^2}\left(1+\frac{1}{1-\varepsilon}\right)$.

Theorem 17

For $(k,l)\in\mathcal{P}(\varepsilon,\frac{1}{2})$ and $n\leq kl$, we have

$$\mathbb{P}(n) = \mathbb{P}[\dim C * C' < n] \leq \frac{qC_q}{(q-1)^2}\left(\frac{2\varepsilon}{1-\varepsilon} + q^{-(kl-n)}\right).$$

Proof of Theorem 16 ($n \geq kl$): Union bound + independence give

$$\mathbb{P}(n) \leq \sum_H \mathbb{P}[\mathbf{u}_1, \ldots, \mathbf{u}_n \in H] = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^n \leq c' \rho^{n-kl}$$

where $\rho = \max_H \mathbb{P}[\mathbf{u}_1 \in H]$, $c' = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^{kl}$, and H ranges over hyperplanes of $V = \mathbb{F}_q^{k \times l}$.
Conclude with estimate on $c' \iff$ count bilinear forms of given rank and the pairs of vectors on which they vanish.

Proof of Theorem 16 ($n \geq kl$): Union bound + independence give

$$\mathbb{P}(n) \leq \sum\nolimits_H \mathbb{P}[\mathbf{u}_1, \ldots, \mathbf{u}_n \in H] = \sum\nolimits_H \mathbb{P}[\mathbf{u}_1 \in H]^n \leq c' \rho^{n-kl}$$

where $\rho = \max_H \mathbb{P}[\mathbf{u}_1 \in H]$, $c' = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^{kl}$, and H ranges over hyperplanes of $V = \mathbb{F}_q^{k \times l}$.
Conclude with estimate on $c' \iff$ count bilinear forms of given rank and the pairs of vectors on which they vanish.

Proof of Theorem 17 ($n \leq kl$): Set $\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j \in V$.
Then for $\mathbf{z} \in \mathbb{F}_q^n$, $\mathrm{wt}(\mathbf{z}) = w$, we have

$$\mathbb{P}[\mathbf{z} \text{ is a lin. rel. for } \mathbf{u}_1, \ldots, \mathbf{u}_n] = \mathbb{P}[\mathbf{s}_w = 0].$$

And then

$$\mathbf{s}_w = 0 \quad \iff \quad \langle \mathbf{x}_1, \ldots, \mathbf{x}_k \rangle \perp \langle \mathbf{y}_1, \ldots, \mathbf{y}_l \rangle \text{ in } \mathbb{F}_q^w$$

where $\mathbf{x}_1, \ldots, \mathbf{x}_k$ and $\mathbf{y}_1, \ldots, \mathbf{y}_l$ are the punctured rows of $\mathbf{G}, \mathbf{G}'$.

Proof of Theorem 16 ($n \geq kl$): Union bound + independence give

$$\mathbb{P}(n) \leq \sum\nolimits_H \mathbb{P}[\mathbf{u}_1, \dots, \mathbf{u}_n \in H] = \sum\nolimits_H \mathbb{P}[\mathbf{u}_1 \in H]^n \leq c' \rho^{n-kl}$$

where $\rho = \max_H \mathbb{P}[\mathbf{u}_1 \in H]$, $c' = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^{kl}$, and H ranges over hyperplanes of $V = \mathbb{F}_q^{k \times l}$.
Conclude with estimate on c' $\iff$ count bilinear forms of given rank and the pairs of vectors on which they vanish.

Proof of Theorem 17 ($n \leq kl$): Set $\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j \in V$.
Then for $\mathbf{z} \in \mathbb{F}_q^n$, $\mathrm{wt}(\mathbf{z}) = w$, we have

$$\mathbb{P}[\mathbf{z} \text{ is a lin. rel. for } \mathbf{u}_1, \dots, \mathbf{u}_n] \;=\; \mathbb{P}[\mathbf{s}_w = 0].$$

And then

$$\mathbf{s}_w = 0 \quad \iff \quad \langle \mathbf{x}_1, \dots, \mathbf{x}_k \rangle \perp \langle \mathbf{y}_1, \dots, \mathbf{y}_l \rangle \text{ in } \mathbb{F}_q^w$$

where $\mathbf{x}_1, \dots, \mathbf{x}_k$ and $\mathbf{y}_1, \dots, \mathbf{y}_l$ are the punctured rows of $\mathbf{G}, \mathbf{G}'$.

Note: some of these ingredients are generic and work for arbitrary $V, X, \mathscr{L}$.

Get rid of the $\mathcal{P}(\varepsilon,\kappa)$ conditions?

- In fact these were introduced only to get explicit constants.
  E.g. (for $n \geq kl$) by the generic approach, $\mathbb{P}(n) \geq c'\rho^{n-kl}$, so case $n \gg kl$ seems tractable, but new ideas needed for n close to kl.
- Also perhaps coming from our probabilistic model.
  Otherwise, restricting $\mathbf{G}, \mathbf{G}'$ to have full rank, and/or to have no zero column, should only lead to stronger bounds!

Get rid of the $\mathcal{P}(\varepsilon, \kappa)$ conditions?

- In fact these were introduced only to get explicit constants. E.g. (for $n \geq kl$) by the generic approach, $\mathbb{P}(n) \geq c' \rho^{n-kl}$, so case $n \gg kl$ seems tractable, but new ideas needed for n close to kl.
- Also perhaps coming from our probabilistic model. Otherwise, restricting $\mathbf{G}, \mathbf{G}'$ to have full rank, and/or to have no zero column, should only lead to stronger bounds!

Still in our model we can derive an interesting unconditional result:

Theorem 18

For any (k, l), and $k + l \leq n \leq kl$, we have

$$\mathbb{P}[\mathrm{d}_{\max}(C * C')^{\perp} \geq k + l] \leq \frac{qC_q}{(q-1)^2} q^{-(kl-n)}.$$

(Proof: included in that of Theorem 17!)

So with high probability $(C * C')^{\perp}$ has small $\mathrm{d}_{\max}$. This is a very strong restriction. It forces $(C * C')^{\perp}$ small, hence $C * C'$ large, as expected.

Squares and higher powers

For any $[n,k]_q$-code C we have

$$\dim C^{\langle 2\rangle} \leq \min(n, \tfrac{k(k+1)}{2})$$

(proof: $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
Expects equality for random C.

Squares and higher powers

For any $[n,k]_q$-code C we have

$$\dim C^{\langle 2\rangle} \leq \min(n, \tfrac{k(k+1)}{2})$$

(proof: $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).

Expects equality for random C.

And indeed, Cascudo-Cramer-Mirandola-Zémor gave an upper bound on $\mathbb{P}[\dim C^{\langle 2\rangle} < \min(n, \frac{k(k+1)}{2})]$.

Squares and higher powers

For any $[n,k]_q$-code C we have

$$\dim C^{\langle 2\rangle} \leq \min(n, \tfrac{k(k+1)}{2})$$

(proof: $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
Expects equality for random C.
And indeed, Cascudo-Cramer-Mirandola-Zémor gave an upper bound on $\mathbb{P}[\dim C^{\langle 2\rangle} < \min(n, \frac{k(k+1)}{2})]$.

Likewise for any $s \geq 2$,

$$\dim C^{\langle s\rangle} \leq \min(n, \tbinom{k+s-1}{s}).$$

Squares and higher powers

For any $[n,k]_q$-code C we have

$$\dim C^{\langle 2\rangle} \leq \min(n, \tfrac{k(k+1)}{2})$$

(proof: $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).

Expects equality for random C.

And indeed, Cascudo-Cramer-Mirandola-Zémor gave an upper bound on $\mathbb{P}[\dim C^{\langle 2\rangle} < \min(n, \tfrac{k(k+1)}{2})]$.

Likewise for any $s \geq 2$,

$$\dim C^{\langle s\rangle} \leq \min(n, \tbinom{k+s-1}{s}).$$

Warning!

For $s > q$, we have: $\dim C^{\langle s\rangle} < \binom{k+s-1}{s}$ always strict.

Squares and higher powers

For any $[n,k]_q$-code C we have

$$\dim C^{\langle 2\rangle} \leq \min(n, \tfrac{k(k+1)}{2})$$

(proof: $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
Expects equality for random C.
And indeed, Cascudo-Cramer-Mirandola-Zémor gave an upper bound on $\mathbb{P}[\dim C^{\langle 2\rangle} < \min(n, \frac{k(k+1)}{2})]$.

Likewise for any $s \geq 2$,

$$\dim C^{\langle s\rangle} \leq \min(n, \tbinom{k+s-1}{s}).$$

Warning!

For $s > q$, we have: $\dim C^{\langle s\rangle} < \binom{k+s-1}{s}$ always strict.

Reason: $C^s \xrightarrow{*} C^{\langle s\rangle}$ is Frobenius-symmetric. Hence

$$\dim C^{\langle s\rangle} \leq \min(n, \chi_q(k,s))$$

where $\chi_q(k,s) = \dim(\mathbb{F}_q[t_1,\dots,t_k]/(t_i^q t_j - t_i t_j^q))_s < \binom{k+s-1}{s}$.

Miscellanea

- In the proof of Theorem 17, we introduced

$$\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j.$$

This defines a random walk in $\mathbb{F}_q^{k \times l}$ (or $\mathbb{F}_q^k \otimes \mathbb{F}_q^l$) whose steps are rank 1 matrices (or elementary tensors).

Miscellanea

- In the proof of Theorem 17, we introduced

$$\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j.$$

This defines a random walk in $\mathbb{F}_q^{k\times l}$ (or $\mathbb{F}_q^k \otimes \mathbb{F}_q^l$) whose steps are rank 1 matrices (or elementary tensors).

Very natural object, with nice algebraic properties.

Same for the associated $r_j = \mathrm{rk}\,\mathbf{s}_j$, Markov chain with values in $[k]$.

$\rightarrow$ Work in progress, joint with D. Madore et al.

Miscellanea

- In the proof of Theorem 17, we introduced

$$\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j.$$

This defines a random walk in $\mathbb{F}_q^{k \times l}$ (or $\mathbb{F}_q^k \otimes \mathbb{F}_q^l$) whose steps are rank 1 matrices (or elementary tensors).
Very natural object, with nice algebraic properties.
Same for the associated $r_j = \mathrm{rk}\, \mathbf{s}_j$, Markov chain with values in $[k]$.
$\rightarrow$ Work in progress, joint with D. Madore et al.

- So far we considered only dimension of products.

More challenging: consider dimension together with minimum distance.

Miscellanea

- In the proof of Theorem 17, we introduced

$$\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j.$$

This defines a random walk in $\mathbb{F}_q^{k\times l}$ (or $\mathbb{F}_q^k \otimes \mathbb{F}_q^l$) whose steps are rank 1 matrices (or elementary tensors).
Very natural object, with nice algebraic properties.
Same for the associated $r_j = \operatorname{rk} \mathbf{s}_j$, Markov chain with values in $[k]$.
$\rightarrow$ Work in progress, joint with D. Madore et al.

- So far we considered only dimension of products.

More challenging: consider dimension together with minimum distance.

Do products of random codes, or squares of random codes, typically form asymptotically good families?

Miscellanea

- In the proof of Theorem 17, we introduced

$$\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j.$$

This defines a random walk in $\mathbb{F}_q^{k \times l}$ (or $\mathbb{F}_q^k \otimes \mathbb{F}_q^l$) whose steps are rank 1 matrices (or elementary tensors).
Very natural object, with nice algebraic properties.
Same for the associated $r_j = \mathrm{rk}\, \mathbf{s}_j$, Markov chain with values in $[k]$.
$\rightarrow$ Work in progress, joint with D. Madore et al.

- So far we considered only dimension of products.

More challenging: consider dimension together with minimum distance.

Do products of random codes, or squares of random codes, typically form asymptotically good families?

Do they lie on the Gilbert-Varshamov bound?

(Observe the answer is negative if we replace $*$-product with tensor product.)