The Density of Optimal Error-Correcting Codes in Various Metric Spaces

Anna-Lena Horlemann

University of St.Gallen, Switzerland

Finite Geometry - Sixth Irsee Conference
August 31st 2022

Joint work with Anina Gruica, Alberto Ravagnani and Nadja Willenborg.

Interest in Random Codes (Hamming Metric)

- For fixed rate and growing length a random code (linear or non-linear) gets arbitrarily close to channel capacity for BSC and BEC (Shannon '48, Elias '55).
- Analogous result for list-decoding capacity for BSC (Guruswami-Haastad-Kapparty '10)
- For fixed length/rate, but growing field size, a random linear code is MDS (folklore).

Interest in Random Codes (Hamming Metric)

- For fixed rate and growing length a random code (linear or non-linear) gets arbitrarily close to channel capacity for BSC and BEC (Shannon '48, Elias '55).
- Analogous result for list-decoding capacity for BSC (Guruswami-Haastad-Kapparty '10)
- For fixed length/rate, but growing field size, a random linear code is MDS (folklore).
- For LRCs the locality is not a generic property, but the optimality w.r.t. Hamming distance is. (Neri-H. '19)
- In code-based cryptography we need to estimate the minimum distance of a random linear code.
  $\rightarrow$ Random linear codes achieve Gilbert-Varshamov bound w.h.p.

Interest in Random Codes (Other Metrics)

- There exist many non-Gabidulin MRD codes, for growing field extension degree. (Neri-H.-Randrianarisoa-Rosenthal '17)
- Nonlinear and $\mathbb{F}_q$-linear MRD codes are sparse for growing field size. (Gluesing-Luerssen-Byrne, Gruica-Ravagnani '20-'22)
- Random linear codes in Lee and restricted error metric achieve GV bound for growing field size. (Weger-Battaglioni-Santini-H.-Persichetti '21)
- Random linear sum-rank-metric codes are MSRD w.r.t. field extension degree. (Ott-Puchinger-Bossert '21)
- Random good constant dimension codes (e.g. spreads) are sparse. (Gruica-Ravagnani '21)

Our Results

- General bounds on density of (linear, sub-linear, non-linear) codes in translation-invariant metric vector spaces.
- Asymptotic behavior in all parameters (length, field size, linearity degree).
- GV-bound achievement in general.
- Singleton-type bound achievement in Hamming, rank, sum-rank, injection/subspace metric. (Some new, some re-established.)

Relation to Finite Geometry I

Hamming metric:

$$d_H(u, v) := |\{i \mid u_i \neq v_i\}|$$

$$\text{MDS} \longleftrightarrow d_H(C) = n - \log_q(|C|) + 1$$

Theorem

- *Linear MDS codes in $\mathbb{F}_{q^m}^n$ correspond to n-arcs over $\mathbb{F}_{q^m}$.*
- *(Additive or) $\mathbb{F}_q$-linear MDS codes in $\mathbb{F}_{q^m}^n$ correspond to n-arcs of $(m-1)$-spaces.*

- For linear codes the columns of the generator matrix form the n-arc.
- For additive codes we extend columns row-wise over $\mathbb{F}_q$ and view them as $(m-1)$-spaces.

Relation to Finite Geometry II

Rank metric on $\mathbb{F}_{q^m}^n$:

$$d_R(u,v) := \dim_q \langle u_1 - v_1, \ldots, u_n - v_n \rangle$$

$$\text{MRD} \longleftrightarrow \log_q(|C|) = \max(m,n)(\min(m,n) - d_R(C) + 1)$$

Theorem

MRD codes in $\mathbb{F}_{q^n}^n$ of maximal rank distance $d = n$ are spreadsets.

- *MRD codes in $\mathbb{F}_{q^n}^n$ (containing the zero and identity matrix) with minimum distance n correspond to finite quasifields Q with $K \leq KerQ$ and $\dim_q Q = n$.*
- *Additive MRD codes in $\mathbb{F}_{q^n}^n$ (containing the identity matrix) with minimum distance n correspond to finite semifields S with $K \leq KerS$ and $\dim_q S = n$.*
- *$\mathbb{F}_q$-linear MRD codes in $\mathbb{F}_{q^n}^n$ (containing the identity matrix) with minimum distance n correspond to finite division algebras D over $\mathbb{F}_q$ where $\mathbb{F}_q \leq Z(D)$ and $\dim_q D = n$.*

Relation to Finite Geometry III

Subspace/injection metric on $\mathcal{G}_q(k,n)$:

$$d_S(U,V) := k - \dim(U \cap V)$$

Theorem

- *A subspace code in $C \subseteq \mathcal{G}_q(k,n)$ is a set of subspaces where the elements intersect pairwise in dimension at most $k - d_S(C)$.*
- *If $d_S(C) = k$ then these codes are spreads or partial spreads.*

Graph Theory Tools[1]

- Construct bipartite graph $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$, where
  - $\mathcal{V} = \Big\{\{x, y\} \subseteq \mathbb{F}_q^n : x \neq y,\, D(x, y) \leq d - 1\Big\}$,
  - $\mathcal{W}$ is the collection of codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| = S$, and
  - $(\{x, y\}, \mathcal{C}) \in \mathcal{E}$ if and only if $\{x, y\} \subseteq \mathcal{C}$.

[1] From A. Gruica and A. Ravagnani, *Common complements of linear subspaces and the sparseness of MRD codes*, SIAM Journal on Applied Algebra and Geometry 6 (2022).

Graph Theory Tools[1]

- Construct bipartite graph $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$, where
  - $\mathcal{V} = \Big\{\{x,y\} \subseteq \mathbb{F}_q^n : x \neq y,\, D(x,y) \leq d-1\Big\}$,
  - $\mathcal{W}$ is the collection of codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| = S$, and
  - $(\{x,y\}, \mathcal{C}) \in \mathcal{E}$ if and only if $\{x,y\} \subseteq \mathcal{C}$.
-

$$|\mathcal{V}| = \frac{1}{2} q^n \left(\mathbf{v}_q^D(\mathbb{F}_q^n, d-1) - 1\right), \quad |\mathcal{W}| = \binom{q^n}{S},$$

$$|\{\mathcal{C} \in \mathcal{W} : (\{x,y\}, \mathcal{C}) \in \mathcal{E}\}| = \binom{q^n - 2}{S-2}.$$

[1] From A. Gruica and A. Ravagnani, *Common complements of linear subspaces and the sparseness of MRD codes*, SIAM Journal on Applied Algebra and Geometry 6 (2022).

Graph Theory Tools[1]

- Construct bipartite graph $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$, where
  - $\mathcal{V} = \left\{\{x, y\} \subseteq \mathbb{F}_q^n : x \neq y,\, D(x, y) \leq d - 1\right\}$,
  - $\mathcal{W}$ is the collection of codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| = S$, and
  - $(\{x, y\}, \mathcal{C}) \in \mathcal{E}$ if and only if $\{x, y\} \subseteq \mathcal{C}$.
-

$$|\mathcal{V}| = \frac{1}{2} q^n \left(\mathbf{v}_q^D(\mathbb{F}_q^n, d-1) - 1 \right), \quad |\mathcal{W}| = \binom{q^n}{S},$$

$$|\{\mathcal{C} \in \mathcal{W} : (\{x, y\}, \mathcal{C}) \in \mathcal{E}\}| = \binom{q^n - 2}{S - 2}.$$

- Hence $\mathcal{B}$ is a left-regular graph of degree $\binom{q^n-2}{S-2}$. The isolated vertices are the codes of minimum distance d.
  $\rightarrow$ Bounds for number of such is known.

[1] From A. Gruica and A. Ravagnani, *Common complements of linear subspaces and the sparseness of MRD codes*, SIAM Journal on Applied Algebra and Geometry 6 (2022).

Density of Non-Linear Codes

Metric space $(\mathbb{F}_q^n, D)$, volume of ball $\mathbf{v}_q^D(...)$, density $\delta_q^D(...)$

Theorem

The density of codes in $\mathbb{F}_q^n$ with minimum distance d among all codes of cardinality S is bounded by

$$1 - \frac{(\boldsymbol{v}_q^D(\mathbb{F}_q^n, d-1) - 1)S(S-1)}{2\,(q^n - 1)} \leq \delta_q^D(\mathbb{F}_q^n, S, 0, d),$$

$$\delta_q^D(\mathbb{F}_q^n, S, 0, d) \leq 1 - \frac{(\boldsymbol{v}_q^D(\mathbb{F}_q^n, d-1) - 1)S(S-1)}{2\Theta(q^n - 1)},$$

where

$$\Theta = 1 + \frac{(2\boldsymbol{v}_q^D(\mathbb{F}_q^n, d-1) - 4)(q^n - 3) + (\frac{1}{2}q^n(\boldsymbol{v}_q^D(\mathbb{F}_q^n, d-1) - 1) - 2\boldsymbol{v}_q^D(\mathbb{F}_q^n, d-1) + 3)(S-3)}{(S-2)^{-1}(q^n-2)(q^n-3)}.$$

Density of (Sub-)Linear Codes

Theorem

The density of $\mathbb{F}_{q^\ell}$-linear codes in $\mathbb{F}_{q^m}^n$ $(m = s\ell)$ of cardinality S with minimum distance d is bounded by

$$1 - \frac{\left(\boldsymbol{v}_q^D(\mathbb{F}_{q^m}^n, d-1) - 1\right)\begin{bmatrix} ns-1 \\ k-1 \end{bmatrix}_{q^\ell}}{(q^\ell - 1)\begin{bmatrix} ns \\ k \end{bmatrix}_{q^\ell}} \leq \delta_q^D(\mathbb{F}_{q^m}^n, q^{\ell k}, \ell, d)$$

$$\delta_q^D(\mathbb{F}_{q^m}^n, q^{\ell k}, \ell, d) \leq 1 - \frac{\left(\boldsymbol{v}_q^D(\mathbb{F}_{q^m}^n, d-1) - 1\right)\begin{bmatrix} ns-1 \\ k-1 \end{bmatrix}_{q^\ell}}{\bar{\Theta}(q^\ell - 1)\begin{bmatrix} ns \\ k \end{bmatrix}_{q^\ell}},$$

where $\bar{\Theta} = 1 + \begin{bmatrix} ns-1 \\ k-1 \end{bmatrix}_{q^\ell}^{-1} \left(\frac{\boldsymbol{v}_q^D(\mathbb{F}_{q^m}^n, d-1) - 1}{q^\ell - 1} - 1\right)\begin{bmatrix} ns-2 \\ k-2 \end{bmatrix}_{q^\ell}.$

Asymptotic Density of Non-Linear Codes

$a_n \in o(f_n) \iff \lim a_n/f_n = 0 \quad , \quad a_n \in \omega(f_n) \iff \lim f_n/a_n = 0$

Theorem

$$\lim \delta_q^D(\mathbb{F}_q^n, S_q, 0, d) = \begin{cases} 1 & \text{if } \mathbf{v}_q^D(\mathbb{F}_q^n, d-1) \in o(q^n S_q^{-2}) \\ 0 & \text{if } \mathbf{v}_q^D(\mathbb{F}_q^n, d-1) \in \omega(q^n S_q^{-2}) \end{cases}$$

as q *or* $n \to +\infty$.

Asymptotic Density of Non-Linear Codes

$$a_n \in o(f_n) \iff \lim a_n/f_n = 0 \quad , \quad a_n \in \omega(f_n) \iff \lim f_n/a_n = 0$$

Theorem

$$\lim \delta_q^D(\mathbb{F}_q^n, S_q, 0, d) = \begin{cases} 1 & \text{if } \mathbf{v}_q^D(\mathbb{F}_q^n, d-1) \in o(q^n S_q^{-2}) \\ 0 & \text{if } \mathbf{v}_q^D(\mathbb{F}_q^n, d-1) \in \omega(q^n S_q^{-2}) \end{cases}$$

as q or $n \to +\infty$.

GV-bound:

$$S_{[n,q,d]} \geq \frac{q^n}{\mathbf{v}_q^D(\mathbb{F}_q^n, d-1)}$$

Corollary

Non-linear codes achieving the Gilbert-Varshamov bound are asymptotically sparse with respect to q or n.

Asymptotic Density of (Sub-)Linear Codes II

Remember: $m = s\ell$

Theorem

$$\lim_{q\to+\infty} \delta_q^D(\mathbb{F}_{q^m}^n, q^{\ell k}, \ell, d) = \begin{cases} 1 & \text{if } \mathbf{v}_q^D(\mathbb{F}_{q^m}^n, d-1) \in o(q^{\ell(ns+1-k)}), \\ 0 & \text{if } \mathbf{v}_q^D(\mathbb{F}_{q^m}^n, d-1) \in \omega(q^{\ell(ns+1-k)}), \end{cases}$$

as q, n, s *or* $\ell \to +\infty$.

Asymptotic Density of (Sub-)Linear Codes II

Remember: $m = s\ell$

Theorem

$$\lim_{q\to+\infty} \delta_q^D(\mathbb{F}_{q^m}^n, q^{\ell k}, \ell, d) = \begin{cases} 1 & \text{if } \mathbf{v}_q^D(\mathbb{F}_{q^m}^n, d-1) \in o(q^{\ell(ns+1-k)}), \\ 0 & \text{if } \mathbf{v}_q^D(\mathbb{F}_{q^m}^n, d-1) \in \omega(q^{\ell(ns+1-k)}), \end{cases}$$

as q, n, s or $\ell \to +\infty$.

Corollary

1. *(Sub-)linear codes achieving the Gilbert-Varshamov bound are asymptotically dense with respect to q or ℓ.*
2. *The asymptotic density of (sub-)linear codes achieving the Gilbert-Varshamov bound is upper bounded by $q^\ell/(q^\ell+1)$, with respect to n or s.*

Hamming Metric

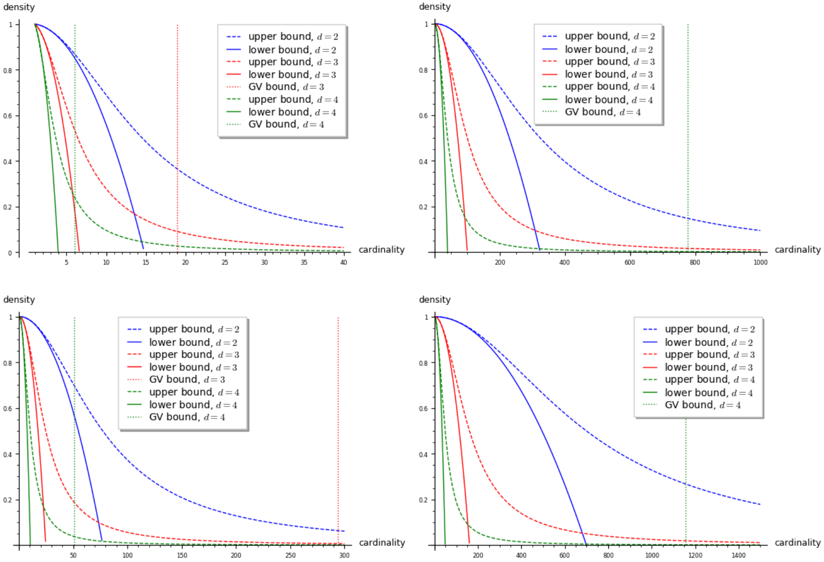
Singleton bound (MDS):

$$k \leq n - d + 1$$

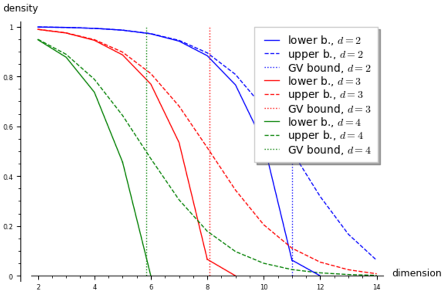
Volume of balls:

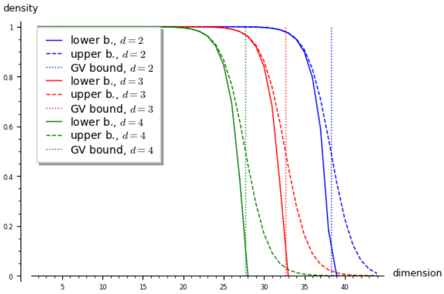
$$\mathbf{v}_q^{\mathrm{H}}(\mathbb{F}_{q^m}^n, r) = \sum_{i=0}^{r} \binom{n}{i} (q^m - 1)^i \sim \begin{cases} \binom{n}{r} q^{rm} & \text{as } q \to +\infty \\ \binom{n}{r} q^{rm} & \text{as } m \to +\infty \\ \binom{n}{r} (q^m - 1)^r & \text{as } n \to +\infty \end{cases}$$

Bounds for nonlinear codes and $(q, n) = (2, 10), (2, 20), (3, 10), (5, 10)$



Bounds for sublinear codes and $(q, m, n, l) = (2, 1, 15, 1), (2, 3, 15, 1)$





Hamming Metric Asymptotics

$$\mathbf{v}_q^{\mathrm{H}}(\mathbb{F}_{q^m}^n, r) = \sum_{i=0}^{r} \binom{n}{i} (q^m - 1)^i \sim \begin{cases} \binom{n}{r} q^{rm} & \text{as } q \to +\infty \\ \binom{n}{r} q^{rm} & \text{as } m \to +\infty \\ \binom{n}{r} (q^m - 1)^r & \text{as } n \to +\infty \end{cases}$$

Theorem

- *Non-linear MDS codes are sparse:*

$$\lim_{q,n \to +\infty} \delta_q^H(\mathbb{F}_q^n, q^{n-d+1}, 0, d) = 0$$

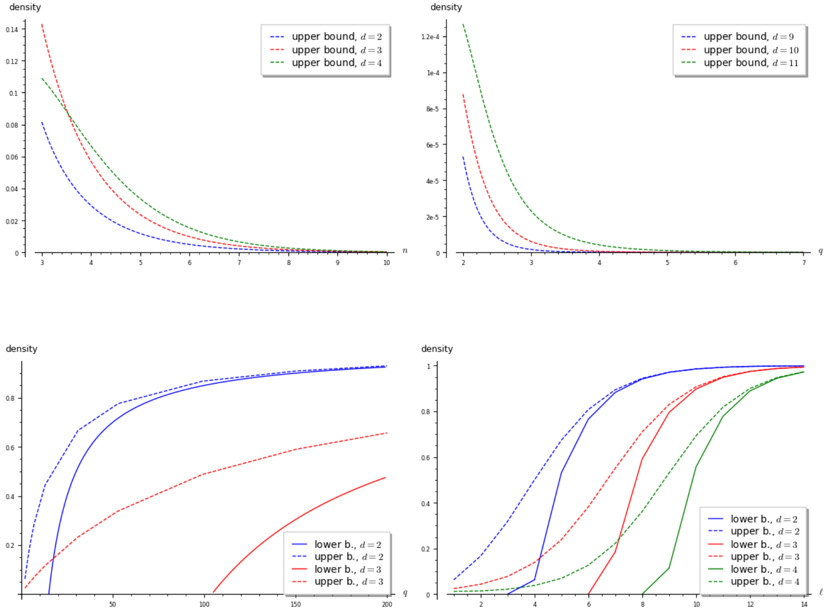
- *Dense sub-linear MDS codes:*

$$\lim_{q,\ell \to +\infty} \delta_q^H(\mathbb{F}_{q^m}^n, q^{m(n-d+1)}, \ell, d) = 1$$

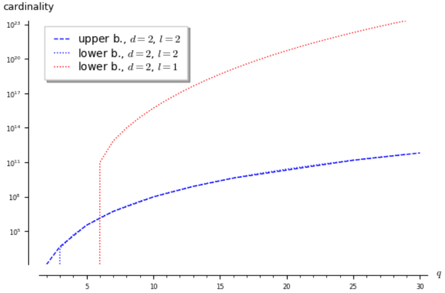
- *Sparse sub-linear MDS codes ($s = m/\ell$):*

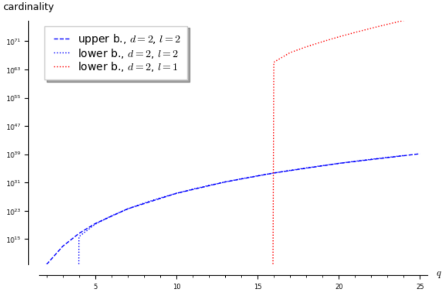
$$\lim_{n,s \to +\infty} \delta_q^H(\mathbb{F}_{q^m}^n, q^{m(n-d+1)}, \ell, d) = 0$$

Non- and sublinear MDS codes for $q = 2, n = 15$; and $m = \ell$



Quantum-MDS codes for $m = 2, \ell = 1$ and $n = 5, 15$





$\Longrightarrow$ Existence of $\mathbb{F}_q$-linear MDS codes that are not $\mathbb{F}_{q^2}$-linear!

Probability of Arcs

Theorem

1. *The probability that n randomly chosen points in $PG(k-1,q)$ form an n-arc goes to 1 for growing q.*
2. *The probability that n randomly chosen points in $PG(k-1,q)$ form an n-arc goes to 0 for growing n.*
3. *The probability that n randomly chosen $(m-1)$-spaces in $PG(mk-1,q)$ form an n-arc of $(m-1)$-spaces goes to 1 for growing q.*
4. *The probability that n randomly chosen $(m-1)$-spaces in $PG(mk-1,q)$ form an n-arc of $(m-1)$-spaces goes to 0 for growing n or m.*

Rank Metric

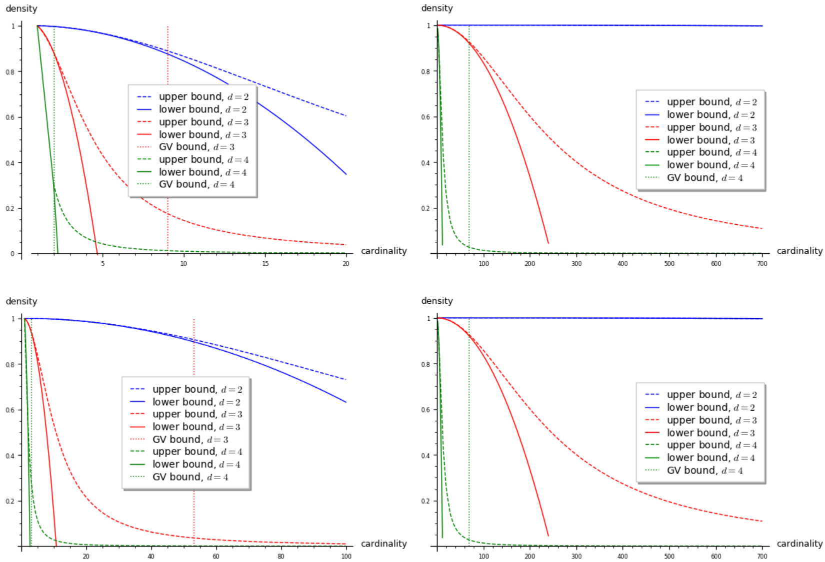
Singleton bound (MRD):

$$k \leq \max(m, n)(\min(m, n) - d + 1)$$

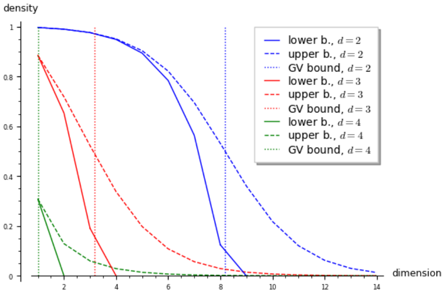
Volume of balls:

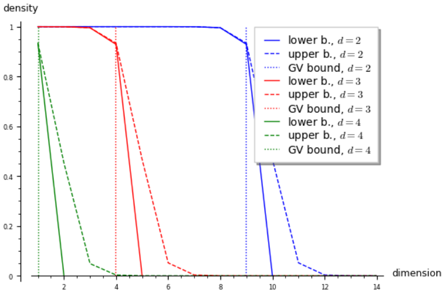
$$\mathbf{v}_q^{\mathrm{rk}}(\mathbb{F}_{q^m}^n, r) = \sum_{i=0}^{r} \begin{bmatrix} n \\ i \end{bmatrix}_q \prod_{j=0}^{i-1} (q^m - q^j) \sim \begin{cases} q^{r(m+n-r)} & \text{as } q \to +\infty \\ \begin{bmatrix} n \\ r \end{bmatrix}_q q^{rm} & \text{as } m \to +\infty \\ \begin{bmatrix} m \\ r \end{bmatrix}_q q^{rn} & \text{as } n \to +\infty \end{cases}$$

Bounds for nonlinear codes and $(q, m, n) = (2,4,4), (2,4,10), (3,4,4), (3,4,10)$



Bounds for sublinear codes and $(q, m, n, l) = (2, 4, 4, 1), (16, 4, 4, 1)$





Rank Metric Asymptotics

Theorem

- *Non-linear MRD codes are sparse:*

$$\lim_{q,n,m\to+\infty} \delta_q^{\mathrm{rk}}(\mathbb{F}_{q^m}^n, q^{\max\{n,m\}(\min\{n,m\}-d+1)}, 0, d) = 0.$$

- *Sub-linear (quasi-)MRD codes depend on the linearity degree:*

$\ell s \geq n$:

$$\lim_{q\to+\infty} \delta_q^{rk}(\mathbb{F}_{q^{\ell s}}^n, q^{\ell s(n-d+1)}, \ell, d) = \begin{cases} 1 & \textit{if } \ell > (d-1)(n-d+1), \\ 0 & \textit{if } \ell < (d-1)(n-d+1). \end{cases}$$

$\ell s < n$:

$$\lim_{q\to+\infty} \delta_q^{rk}(\mathbb{F}_{q^{\ell s}}^n, q^{\ell k}, \ell, d) = \begin{cases} 1 & \textit{if } \ell > (d-1)(\ell s-d+1)+r, \\ 0 & \textit{if } \ell < (d-1)(\ell s-d+1)+r. \end{cases}$$

where $k := \lfloor n(\ell s-d+1)/\ell \rfloor$ *and* $r := n(d-1) - \ell\lceil n(d-1)/\ell \rceil$.

Rank Metric Asymptotics II

Theorem

- *Density for growing linearity degree:*

$$\lim_{\ell \to +\infty} \delta_q^{rk}(\mathbb{F}_{q^{\ell s}}^n, q^{\ell s(n-d+1)}, \ell, d) = 1,$$

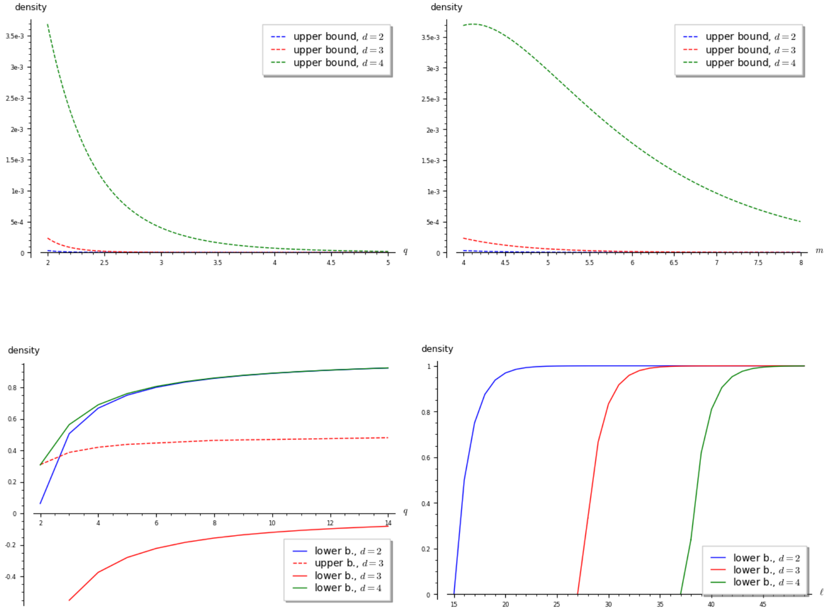
- *Bound for growing length:*

$$\limsup_{n \to +\infty} \delta_q^{rk}(\mathbb{F}_{q^{\ell s}}^n, q^{\ell \lfloor n(\ell s - d+1)/\ell \rfloor}, \ell, d) \leq \frac{1}{1 + \begin{bmatrix} m \\ d-1 \end{bmatrix}_q q^{-2\ell}} < 1,$$

- *Bound for growing extension degree:*

$$\limsup_{s \to +\infty} \delta_q^{rk}(\mathbb{F}_{q^{\ell s}}^n, q^{\ell s(n-d+1)}, \ell, d) \leq \frac{q^\ell}{q^\ell + \begin{bmatrix} n \\ d-1 \end{bmatrix}_q} < 1.$$

Non- and sublinear MRD codes for $q = 2, n = 4$ and $m = 4$ (and $n = 15$)



Probability of Spreadsets

Theorem

- *The probability that randomly chosen square matrices in* $\mathbb{F}_q^{n\times n}$ *form a spreadset goes to* 0 *for growing growing* q *or* n.
- *The probability that the* $\mathbb{F}_q$*-linear span of randomly chosen square matrices in* $\mathbb{F}_q^{n\times n}$ *form a spreadset goes to* 0 *for growing growing* q *or* n.
- *The probability that the* $\mathbb{F}_{q^m}$*-linear span of randomly chosen vectors in* $\mathbb{F}_{q^n}^n$ *form a spreadset goes to* 1 *for growing growing* q *or* n.

($\rightarrow$ connection to quasifields, semifields, division algebras)

Sum-Rank Metric

Ambient space ($n = t\eta$):

$$C \subseteq (\mathbb{F}_{q^m}^{\eta})^t$$

Singleton-type bound:

$$k \leq \max\{m, \eta\}(t \min\{m, \eta\} - d + 1)$$

$$\mathbf{v}_q^{\mathrm{sr,t}}(\mathbb{F}_{q^m}^n, r) = \sum_{h=0}^{r} \sum_{u \in U_h} \prod_{i=1}^{t} \begin{bmatrix} \eta \\ u_i \end{bmatrix}_q \prod_{j=0}^{u_i - 1} (q^m - q^j) \sim \binom{t}{\tilde{z}} q^{\frac{\tilde{z}^2}{t} - \tilde{z} + r(m + \eta - \frac{r}{t})}$$

as $q \to +\infty$, where $\tilde{z} \equiv r \pmod{t}$.

Sum-Rank Metric

Ambient space ($n = t\eta$):

$$C \subseteq (\mathbb{F}_{q^m}^{\eta})^t$$

Singleton-type bound:

$$k \leq \max\{m,\eta\}(t\min\{m,\eta\} - d + 1)$$

$$\mathbf{v}_q^{\mathrm{sr,t}}(\mathbb{F}_{q^m}^n, r) = \sum_{h=0}^{r} \sum_{u \in U_h} \prod_{i=1}^{t} \begin{bmatrix} \eta \\ u_i \end{bmatrix}_q \prod_{j=0}^{u_i - 1} (q^m - q^j) \sim \binom{t}{\tilde{z}} q^{\frac{\tilde{z}^2}{t} - \tilde{z} + r(m+\eta-\frac{r}{t})}$$

as $q \to +\infty$, where $\tilde{z} \equiv r \pmod t$.

Theorem

Non-linear MSRD codes are sparse:

$$\lim_{q\to+\infty} \delta_q^{\mathrm{sr,t}}(\mathbb{F}_{q^m}^n, q^{\max\{m,\eta\}(t\min\{m,\eta\}-d+1)}, 0, d) = 0$$

Sum-Rank Metric II

Theorem

Let $\theta := (d-1)\left(\min\{m,\eta\} - \frac{d-1}{t}\right) + \frac{\tilde{z}^2}{t} - \tilde{z}$.

- *If* $m \geq \eta$, *then:*

$$\lim_{q\to+\infty} \delta_q^{sr,t}(\mathbb{F}_{q^m}^n, q^{m(n-d+1)}, \ell, d) = \begin{cases} 1 & \text{if } \theta < \ell, \\ 0 & \text{if } \theta > \ell \end{cases}$$

- *If* $\eta > m$, *then:*

$$\lim_{q\to+\infty} \delta_q^{sr,t}(\mathbb{F}_{q^m}^n, q^{\ell k}, \ell, d) = \begin{cases} 1 & \text{if } \theta - r < \ell, \\ 0 & \text{if } \theta - r > \ell, \end{cases}$$

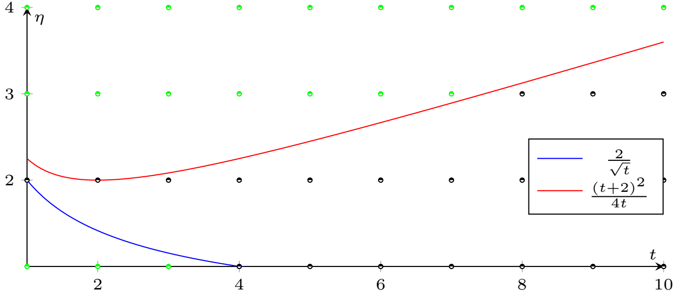
where $k = \left\lfloor \frac{\eta(mt-d+1)}{\ell} \right\rfloor$ *and* $r = \ell\left(\left\lceil \frac{\eta(d-1)}{\ell} \right\rceil - \frac{\eta(d-1)}{\ell}\right)$.

Sum-Rank Metric III

Corollary

Let $m \geq \eta$ and $2 \leq d \leq n$ be integers. We have

$$\lim_{q \to +\infty} \delta_q^{sr,t}(\mathbb{F}_{q^m}^n, q^{m(n-d+1)}, 1, d) = \begin{cases} 1 & \text{if } \eta < \frac{2}{\sqrt{t}} \\ 0 & \text{if } \eta > \frac{(t+2)^2}{4t}. \end{cases}$$



Density of Codes in the Grassmannian

Metric space $(\mathcal{G}_q(k,n), D)$, volume of ball $\mathbf{v}_q^D(...)$, density $\delta_q^D(...)$

Theorem

The density of codes in $\mathcal{G}_q(k,n)$ with minimum distance d among all codes of cardinality S is bounded by

$$1 - \frac{(\boldsymbol{v}_q^D(\mathcal{G}_q(k,n), d-1) - 1)S(S-1)}{2(\begin{bmatrix} n \\ k \end{bmatrix}_q - 1)} \leq \delta_q^D(\mathcal{G}_q(k,n), S, d),$$

$$\delta_q^D(\mathcal{G}_q(k,n), S, d) \leq 1 - \frac{(\boldsymbol{v}_q^D(\mathcal{G}_q(k,n), d-1) - 1)S(S-1)}{2\Theta(\begin{bmatrix} n \\ k \end{bmatrix}_q - 1)},$$

$$\Theta = 1 + 2\frac{(\boldsymbol{v}_q^D(d-1)-2)(S-2)}{bin(n,k,q)-2} + \frac{(\frac{1}{2}bin(n,k,q)(\boldsymbol{v}_q^D(d-1)-1)-2\boldsymbol{v}_q^D(d-1)+3)(S-2)(S-3)}{(bin(n,k,q)-2)(bin(n,k,q)-3)}.$$

Asymptotic Density

Theorem

$$\lim_{q,n\to\infty} \delta_q^D(\mathcal{G}_q(k,n), S_q, d) = \begin{cases} 1 & \text{if } \mathbf{v}_q^D(\mathcal{G}_q(k,n), d-1) \in o(\begin{bmatrix} n \\ k \end{bmatrix}_q S_q^{-2}) \\ 0 & \text{if } \mathbf{v}_q^D(\mathcal{G}_q(k,n), d-1) \in \omega(\begin{bmatrix} n \\ k \end{bmatrix}_q S_q^{-2}) \end{cases}$$

Asymptotic Density

Theorem

$$\lim_{q,n\to\infty} \delta_q^D(\mathcal{G}_q(k,n), S_q, d) = \begin{cases} 1 & \text{if } \mathbf{v}_q^D(\mathcal{G}_q(k,n), d-1) \in o(\begin{bmatrix} n \\ k \end{bmatrix}_q S_q^{-2}) \\ 0 & \text{if } \mathbf{v}_q^D(\mathcal{G}_q(k,n), d-1) \in \omega(\begin{bmatrix} n \\ k \end{bmatrix}_q S_q^{-2}) \end{cases}$$

GV-bound:

$$S_{[n,k,q,d]} \geq \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\mathbf{v}_q^D(\mathcal{G}_q(k,n), d-1)}$$

Corollary

Non-linear codes achieving the Gilbert-Varshamov bound are asymptotically sparse with respect to q or n.

Codes with the Subspace/Injection Distance[2]

$$d_I(U,V) := k - \dim(U \cap V)$$

$$|\mathbf{v}_q^I(\mathcal{G}_q(k,n),d)| = \sum_{i=0}^{d} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q$$

Singleton-type bound:

$$|C_{[n,k,d]}| \leq \begin{bmatrix} n-d+1 \\ \max(k,n-k) \end{bmatrix}_q$$

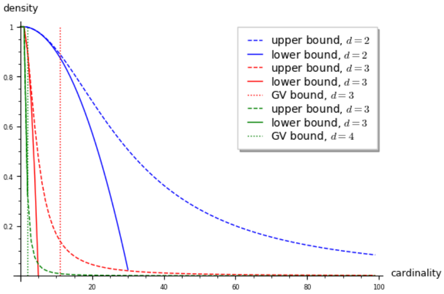
Theorem

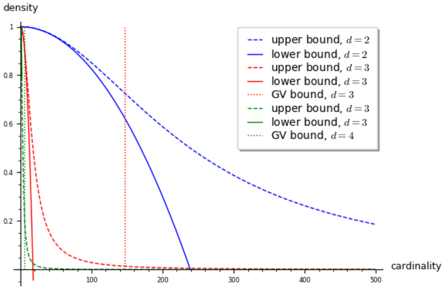
$$\lim_{q,n\to\infty} \delta_q^D(\mathcal{G}_q(k,n), \begin{bmatrix} n-d+1 \\ \max(k,n-k) \end{bmatrix}_q, d) = 0$$

($\to$ GV-bound is lower than Singleton-type bound)

[2] A. Gruica and A. Ravagnani, *The Typical Non-Linear Code over Large Alphabets*, IEEE Information Theory Workshop (ITW), 2021.

Bounds for $(q, k, n) = (2, 4, 8), (2, 4, 10)$





Geometric Interpretation

$$d_I(U,V) < d \iff \dim(U \cap V) > k - d$$

Theorem

Let $d \geq 2$. A set of

$$\frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\boldsymbol{v}_q^I(\mathcal{G}_q(k,n), d-1)} \leq \begin{bmatrix} n-d+1 \\ \max(k, n-k) \end{bmatrix}_q$$

randomly chosen k-dimensional subspaces in $\mathbb{F}_q^n$ contains a pair of elements which intersect in dimension at least $k-d+1$, with probability going to 1 for growing q or n.

Geometric Interpretation II

$$d_I(U,V) < d \iff \dim(U \cap V) > k - d$$

Theorem

Let $d \geq 2$. A set of

$$\left(\frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\boldsymbol{v}_q^I(\mathcal{G}_q(k,n), d-1)} \right)^{\frac{1}{2}}$$

randomly chosen k-dimensional subspaces in $\mathbb{F}_q^n$ intersect pairwise in dimension at most $k-d$, with probability going to 1 for growing q or n.

Summary and Conclusions

- General (asymptotic) bounds on densities in $(\mathbb{F}_{q^m}^n, D)$ and $(\mathcal{G}_q(k,n), D)$, D translation-invariant.

Summary and Conclusions

- General (asymptotic) bounds on densities in $(\mathbb{F}_{q^m}^n, D)$ and $(\mathcal{G}_q(k,n), D)$, D translation-invariant.
- Density/sparsity depends on relation of volume of balls to code cardinality.

Summary and Conclusions

- General (asymptotic) bounds on densities in $(\mathbb{F}_{q^m}^n, D)$ and $(\mathcal{G}_q(k,n), D)$, D translation-invariant.
- Density/sparsity depends on relation of volume of balls to code cardinality.
- All non-linear codes we considered are sparse (GV- or Singleton-achieving).

Summary and Conclusions

- General (asymptotic) bounds on densities in $(\mathbb{F}_{q^m}^n, D)$ and $(\mathcal{G}_q(k,n), D)$, D translation-invariant.
- Density/sparsity depends on relation of volume of balls to code cardinality.
- All non-linear codes we considered are sparse (GV- or Singleton-achieving).
- $\mathbb{F}_{q^\ell}$-linear codes always achieve GV-bound (with probability 1) for growing q or $\ell = m/s$.

Summary and Conclusions

- General (asymptotic) bounds on densities in $(\mathbb{F}_{q^m}^n, D)$ and $(\mathcal{G}_q(k,n), D)$, D translation-invariant.
- Density/sparsity depends on relation of volume of balls to code cardinality.
- All non-linear codes we considered are sparse (GV- or Singleton-achieving).
- $\mathbb{F}_{q^\ell}$-linear codes always achieve GV-bound (with probability 1) for growing q or $\ell = m/s$.
- For Singleton-type bound it depends on the metric and the linearity degree.

Summary and Conclusions

- General (asymptotic) bounds on densities in $(\mathbb{F}_{q^m}^n, D)$ and $(\mathcal{G}_q(k,n), D)$, D translation-invariant.
- Density/sparsity depends on relation of volume of balls to code cardinality.
- All non-linear codes we considered are sparse (GV- or Singleton-achieving).
- $\mathbb{F}_{q^\ell}$-linear codes always achieve GV-bound (with probability 1) for growing q or $\ell = m/s$.
- For Singleton-type bound it depends on the metric and the linearity degree.

Thank you for your attention!
Questions? – Comments?