The Impact of Network Coding on Mathematics

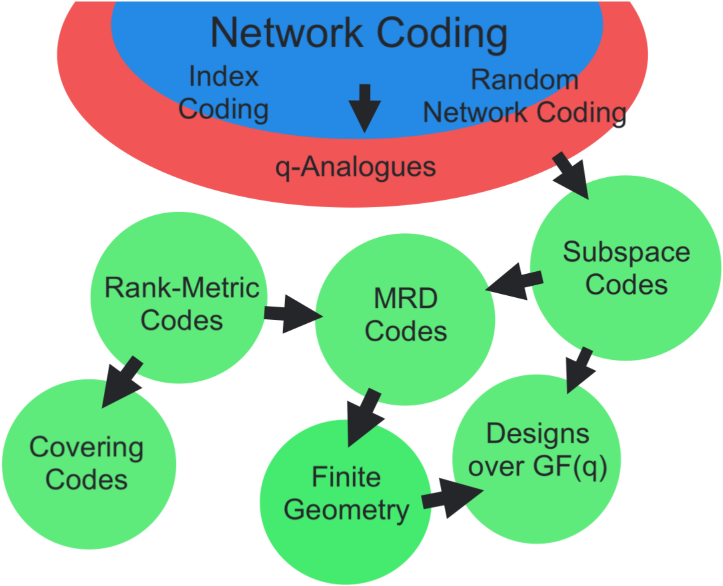
Eimear Byrne
University College Dublin

DIMACS Workshop on Network Coding: the Next 15 Years
Dec 15-17, 2015

Random Network Coding and Designs Over $GF(q)$

- COST Action IC1104: an EU-funded network
- Funding for workshops, meetings, short research visits
- Chairs: M. Greferath & M. Pavcević
- S. Blackburn, T. Etzion, A. Garcia-Vasquez, C. Hollanti, J. Rosenthal
- Network involving 28 participant countries
- Final meeting: *Network Coding and Designs*, Dubronvik, April 4-8, 2016.
- q-designs, subspace codes, rank-metric codes, distributed storage, cryptography, related combinatorial structures.

Some Impacts of Network Coding



Error-Correction in Network Coding

The following seminal papers stimulated a huge volume of work on subspace and rank-metric codes.

- Kötter, Kschischang, "Coding for Erasures and Errors in Random Network Coding," IEEE Trans. Inform. Th. (54), 8, 2008. (cited by: 292 (Scopus), 605 (Google))
- Silva, Kschischang, Kötter, "A Rank-Metric Approach to Error Control in Random Network Coding," IEEE Trans. Inform. Th. (54), 9, 2008. (cited by 195 (Scopus), 259 (Google))

Motivation: To provide a framework for error correction in networks without much knowledge of the network topology.

Constant Dimension Subspace Codes

A subspace code $\mathcal{C}$ is a set subspaces of $\mathbb{F}_q^n$, equipped with the subspace distance:

$$\begin{aligned} d_S(U,V) &= \dim(U+V) - \dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V). \end{aligned}$$

- If each codeword has dimension k then $\mathcal{C}$ is a constant dimension code and $d_S(U,V) = 2(k - \dim(U \cap V))$.
- Channel model: $U \longrightarrow V = \pi(U) \oplus W$.
- $\pi(U) < U$, formed by 'deletions', W formed by 'insertions'.
- Receiver decodes to unique codeword if

$$2(\dim U - \dim \pi(U) + \dim W) < d_S(\mathcal{C}).$$

- Matrix model: $X \in \mathbb{F}_q^{m \times n} \longrightarrow Y = AX + BZ$.

Rank-Metric Codes

A rank-metric code $\mathcal{C}$ is a subset of $\mathbb{F}_q^{m\times n}$, equipped with the rank distance:

$$d_{\mathrm{rk}}(F,G) \quad = \quad \mathrm{rk}(F-G)$$

$\mathcal{C}$ can be lifted to a (constant dimension) subspace code via:

$$\mathcal{I}(\mathcal{C}) := \{\langle X\rangle = \mathrm{rowspace}([I|x]) : x \in \mathcal{C}\}.$$

- $d_S(\langle X\rangle, \langle Y\rangle) = d_{\mathrm{rk}}(x-y)$
- Matrix model: $X \longrightarrow Y = AX + BZ$.
- Receiver decodes to unique codeword if

$$2(\mathrm{rk}X - \mathrm{rk}AX + \mathrm{rk}BZ) < d_{\mathrm{rk}}(\mathcal{C}).$$

Optimality

- $\mathcal{G}_q(n, k)$ = set of all k-dim'l subspaces of $\mathbb{F}_q^n$.
- What is the optimal size $A_q(n, d, k)$ of a constant dimension code in $\mathcal{G}_q(n, k)$ of minimum distance d?
- How do we construct such codes?

Example 1

Let $\mathcal{C} \subset \mathcal{G}(n, k)$ such that every t-dimensional subspace is contained in exactly one space of $\mathcal{C}$. So $\mathcal{C}$ is an $S_q(t, k, n)$ Steiner structure. Then $|\mathcal{C}| = A_q(n, 2(k - t + 1), k)$.

- A Steiner structure is a q-analogue of design theory. Steiner structures yield optimal subspace codes.

Examples of Steiner Structures

Theorem 2

There exists an $S_2(2,3,13)$. In fact there exist at least 401 non-isomorphic ones.

Braun, Etzion, Ostergard, Vardy, Wassermann, "Existence of q-Analogs of Steiner Systems," arXiv:1304.1462, 2012.

- This is the first known example of a non-trivial Steiner structure.
- It shows that $A_2(13,4,3) = \begin{bmatrix} 13 \\ 2 \end{bmatrix}_2 / \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 1,597,245.$
- Found by applying the Kramer-Mesner method.
- Prescribing an automorphism group of size $s = 13(2^{13}-1) = 106,483$ reduces from an exact-cover problem of size 1,597,245 to one of size $|S_2(2,3,13)|/s = 1,597,245/106,483 = 15.$

Steiner Structures

Problem 3

Is there an $S_2(2,3,13)$ *that is part of an infinite family of q-Steiner systems?*

Problem 4

Are there any other other examples?

Problem 5

Does there exist an $S_q(2,3,7)$*? This is the q-analogue of the Fano plane.*

- An $S_2(2,3,7)$ would have 381 of 11811 planes of $PG(6,\mathbb{F}_2)$.
- Currently known that $A_2(7,2,3) \geq 329$ (Braun & Reichelt).
- The automorphism group of any $S_2(2,3,7)$ is small (2,3 or 4).
- Computer search is infeasible at this time.

q-Fano plane

- Braun, Kiermaier, Nakić, "On the Automorphism Group of a Binary q-Analog of the Fano Plane," Eur. J. Comb. 51, 2016.
- Kiermaier, Honold, "On Putative q-Analogues of the Fano plane and Related Combinatorial Structures," arXiv: 1504.06688, 2015.
- Etzion, "A New Approach to Examine q-Steiner Systems," arXiv:1507.08503, 2015.
- Thomas, 1987: It is impossible to construct the q-Fano plane as a union of 3 orbits of a Singer group.

q-Analogues of Designs

Definition 6

$\mathcal{D} \subset G_q(n,k)$ is a $t-(n,k,\lambda;q)$ design (over $\mathbb{F}_q$) if every t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly λ subspaces of $\mathcal{D}$.

Existence: Fazeli, Lovett, Vardy, "Nontrivial t-Designs over Finite Fields Exist for all t", *J. Comb. Thy, A*, 127, 2014.

- Introduced by Cameron in 1974.
- Thomas gave an infinite family of $2-(n,3,7;2)$ designs for $n \equiv \pm 1 \mod 6$. "Designs Over Finite Fields" *Geometriae Dedicata*, 24, 1987.
- Suzuki (1992), Abe, Yoshiara (1993), Miyakawa, Munesmasa, Yoshiara (1995), Ito (1996), Braun (2005).
- No 4-designs over $\mathbb{F}_q$ are known.

q-Analogues of Designs

- Etzion, Vardy, "On q-Analogues of Steiner Systems and Covering Designs," Adv. Math. Comm. 2011.
- DISCRETAQ - a tool to construct q-analogs of combinatorial designs (Braun, 2005).
- Kiermaier, Pavĉević "Intersection Numbers for Subspace Designs," J. Comb. Designs 23, 11, 2015.
- Braun, Kiermaier, Kohnert, Laue, "Large Sets of Subspace Designs," arXiv: 1411.7181, 2014.

Maximum Rank Distance (MRD) Codes

- Delsarte, "Bilinear Forms over a Finite Field, with Applications to Coding Theory," J. Comb. Thy A, 25, 1978.
- Gabidulin, "Theory of Codes With Maximum Rank Distance," Probl. Inform. Trans., 1, 1985.

Theorem 7

A code $\mathcal{C} \subset \mathbb{F}_q^{m\times n}$ of minimum rank distance d satisfies

$$q^{m(d'-1)} \leq |\mathcal{C}| \leq q^{m(n-d+1)}.$$

Equality is achieved in either iff $d + d' - 2 = n$. If $\mathcal{C}$ is $\mathbb{F}_q$-linear then $d' = d_{\mathrm{rk}}(\mathcal{C}^{\perp})$.

- If $\mathcal{C}$ meets the upper bound it is called an MRD code
- If $\mathcal{C}$ is MRD and $\mathbb{F}_q$ linear we say it has parameters $[mn, mk, n-k+1]_q$.

Delsarte-Gabidulin Codes

Theorem 8 (Delsarte)

Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathbb{F}_{q^n}$ and let $\beta_1, \ldots, \beta_m \subset \mathbb{F}_{q^n}$ be linearly indep. over $\mathbb{F}_q$. The set

$$\mathcal{C} = \left\{ \left(\sum_{\ell=0}^{k-1} \operatorname{tr}\left(\omega_\ell \alpha_i^{q^\ell} \beta_i \right) \right)_{1 \le i \le n, 1 \le j \le m} : \omega_\ell \in \mathbb{F}_{q^n} \right\}$$

is an $\mathbb{F}_{q^n}$-linear $[mn, mk, n-k+1]_q$ MRD code.

Equivalent form: let $g_1, \ldots, g_m \subset \mathbb{F}_{q^n}$ be be linearly indep. over $\mathbb{F}_q$.

$$\mathcal{C} = \left\{ [x_1, \ldots, x_k] \begin{bmatrix} g_1 & g_2 & \cdots & g_m \\ g_1^q & g_2^q & \cdots & g_m^q \\ \vdots & & & \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_m^{q^{k-1}} \end{bmatrix} : x_i \in \mathbb{F}_{q^n} \right\} \subset \mathbb{F}_{q^n}^m$$

is an $\mathbb{F}_{q^n}$-linear $[mn, mk, n-k+1]_q$ MRD code.

MRD Codes

- If $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$ is $\mathbb{F}_q$-linear then $\mathcal{C}^\perp := \{Y \in \mathbb{F}_q^{m \times n} : \mathrm{Tr}(\mathrm{X}\mathrm{Y}^\mathrm{T}) = 0 \; \forall \; \mathrm{X} \in \mathcal{C}\}$.
- Mac Williams' duality theorem holds for rank-metric codes.
- Mac Williams' extension theorem does not hold for rank-metric codes.
- $\mathcal{C}$ is MRD iff $\mathcal{C}^\perp$ is MRD.
- If $\mathcal{C}$ is MRD then its weight distribution is determined.
- The covering radius of an MRD code is not determined.
- Not all MRD codes are Delsarte-Gabidulin codes.
- $[n^2, n, n]_q$ MRD codes are spread-sets in finite geometry.
- Delsarte-Gabidulin MRD codes can be decoded using Gabidulin's algorithm with quadratic complexity.

MRD Codes

There are many papers on decoding rank-metric codes. Recently there has been much activity on the structure of MRD codes.

- Gadouleau, Yan, "Packing and Covering Properties of Rank Metric Codes," IEEE Trans. Inform. Theory, 54 (9) 2008.
- Morrison, "Equivalence for Rank-metric and Matrix Codes and Automorphism Groups of Gabidulin Codes," IEEE Trans. Inform. Theory 60 (11), 2014.
- de la Cruz, Gorla, Lopez, Ravagnani, "Rank Distribution of Delsarte Codes," arXiv: 1510.01008, 2015.
- Nebe, Willems, "On Self-Dual MRD Codes, arXiv: 1505.07237, 2015.
- de la Cruz, Kiermaier, Wassermann, Willems, "Algebraic Structures of MRD Codes," arXiv:1502.02711, 2015.

Quasi-MRD Codes

Definition 9

$\mathcal{C} \subset \mathbb{F}_q^{m \times n}$ is called quasi-MRD (QMRD) if $m \nmid \dim(\mathcal{C})$ and

$$d(\mathcal{C}) = n - \left\lceil \frac{\dim(\mathcal{C})}{m} \right\rceil + 1.$$

$\mathcal{C}$ is called dually QMRD if $\mathcal{C}^\perp$ is also QMRD.

de la Cruz, Gorla, Lopez, Ravagnani, "Rank Distribution of Delsarte Codes," arXiv: 1510.01008, 2015.

- An easy construction is by expurgating an MRD code.
- If $\mathcal{C}$ is QMRD is does **not** follow that $\mathcal{C}^\perp$ is QMRD.
- The weight distribution of a QMRD code is not determined.

MRD Codes as Spaces of Linearized Polynomials

For $m = n$ we construct a Delsarte-Gabidulin MRD code with parameters $[n^2, nk, n-k+1]$ as follows:

$$G_{n,k} := \{f = f_0 x + f_1 x^q + \cdots f_{k-1} x^{q^{k-1}} : f_i \in \mathbb{F}_{q^n}\}$$

- $f = f_0 x + f_1 x^q + \cdots f_{k-1} x^{q^{k-1}}$ is $\mathbb{F}_q$-linear (in fact is $\mathbb{F}_{q^n}$-linear) and so can be identified with a unique $n \times n$ matrix over $\mathbb{F}_q$.
- Matrix multiplication corresponds to composition mod $x^q - x$.
- $\dim_q \ker f \leq k-1$, so $\mathrm{rk}\, f \geq n-k+1$.

New Classes of MRD Codes

Theorem 10

Let $\nu \in \mathbb{F}_{q^n}$ satisfy $\nu^{\frac{q^n-1}{q-1}} \neq (-1)^{nk}$. Then

$$\mathcal{H}_k(\nu, h) := \{f_0 x + f_1 x^q + \cdots f_{k-1} x^{q^{k-1}} + \nu f_0^{q^h} x^{q^k} : f_i \in \mathbb{F}_{q^n}\}$$

is an $\mathbb{F}_q$-linear $[n^2, nk, n-k+1]$ MRD code.

Sheekey, "A New Family of Linear Maximum Rank Distance Codes," arXiv:1504.01581, 2015.

This is the most general known infinite family of MRD codes and includes Delsarte-Gabidulin codes. Other work:

- Horlemann-Trautmann, Marshall, "New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions," arXiv:1507.08641, 2015.
- Lunardon, Trombetti, Zhou, "Generalized Twisted Gabidulin Codes," arXiv:1507.07855, 2015.

Rank Metric Covering Radius

Definition 11

The rank covering radius of a code $\mathcal{C} \subset \mathbb{F}_q^{m\times n}$ is given by

$$\begin{aligned}
\rho(\mathcal{C}) &:= \max\{\min\{d_{\mathrm{rk}}(X, C) : C \in \mathcal{C}\} : X \in \mathbb{F}_q^{m\times n}\} \\
&:= \max\{d_{\mathrm{rk}}(X, \mathcal{C}) : X \in \mathbb{F}_q^{m\times n}\} \\
&:= \max\{\mathrm{rk}(X + \mathcal{C}) : X \in \mathbb{F}_q^{m\times n}\}
\end{aligned}$$

- $\mathbb{F}_q^{m\times n}$, $m \times n$ matrices over $\mathbb{F}_q$.
- $\rho(\mathcal{C})$ is the max rank weight over all translates of $\mathcal{C}$ in $\mathbb{F}_q^{m\times n}$.

Some Bounds on the Covering Radius

Theorem 12 (B., 2015)

Let $\mathcal{C} \subset \mathcal{C}' \subset \mathbb{F}_q^{m\times n}$. Then

- $\rho(\mathcal{C}) \geq \min\{r : V_q(m,n,r)|\mathcal{C}| \geq q^{mn}\}$.
- $\rho(\mathcal{C}) \geq$

  $$\max\{d_{\mathrm{rk}}(X,C) : X \in C'\} \geq \min\{d_{\mathrm{rk}}(X,C) : X \in \mathcal{C}'\backslash\mathcal{C}\} \geq d_{\mathrm{rk}}(\mathcal{C}').$$

- *If $\mathcal{C}, \mathcal{C}'$ are $\mathbb{F}_q$-linear, then $\rho(\mathcal{C}) \geq \min\{\mathrm{rk}(X) : X \in \mathcal{C}'\backslash\mathcal{C}\}$.*
- *If $\mathcal{C}$ is $\mathbb{F}_q$-linear then $\rho(\mathcal{C})$ is no greater than the number of non-zero weights of $\mathcal{C}^\perp$.*

Example 13

Let $n = rs$ and let $\mathcal{C} = \{\sum_{i=0}^{r-1} f_i x^{q^{si}} : f_i \in \mathbb{F}_{q^n}\}$. Then $\mathcal{C}$ has non-zero rank weights $\{s, 2s, ..., rs\}$ over $\mathbb{F}_q$, so that $\rho(\mathcal{C}^\perp) \leq r$.

Maximality

A code $\mathcal{C} \subset \mathbb{F}_q^{m\times n}$ is called maximal if $\mathcal{C}$ is not strictly contained in any code $\mathcal{C}' \subset \mathbb{F}_q^{m\times n}$ with the same minimum distance.

Theorem 14 (Maximal Codes)

$\mathcal{C} \subset \mathbb{F}_q^{m\times n}$ is maximal $\Leftrightarrow \rho(\mathcal{C}) \leq d_{\mathrm{rk}}(\mathcal{C}) - 1$.

Clearly any MRD code is maximal.

Example 15 (Gadouleau, 2008)

Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear $[mn, mk, n-k+1]$ Gabidulin MRD code. $\mathcal{C}$ is a maximal code and is contained in an $\mathbb{F}_q$-$[mn, m(k+1), n-k]$ Delsarte-Gabidulin code $\mathcal{C}'$. Then

$$n-k = d_{\mathrm{rk}}(\mathcal{C}') \leq \rho(\mathcal{C}) \leq d_{\mathrm{rk}}(\mathcal{C}) - 1 = n-k.$$

Maximality

Theorem 16 (Sheekey, 2015)

Let $\nu \in \mathbb{F}_{q^n}$ satisfy $\nu^{\frac{q^n-1}{q-1}} \neq (-1)^{nk}$. Then

$$\mathcal{H}_k(\nu, h) := \{f_0 x + f_1 x^q + \cdots f_{k-1} x^{q^{k-1}} + \nu f_0^{q^h} x^{q^k} : f_i \in \mathbb{F}_{q^n}\}$$

is an $\mathbb{F}_q$-linear $[n^2, nk, n-k+1]$ MRD code.

Example 17

$\mathcal{C} = \mathcal{H}_k(\nu, h)$ is maximal and $\mathcal{H}_k(\nu, h) \subset \mathcal{H}_{k+1}(0, h') = \mathcal{C}'$.
Therefore

$$n - k = d_{\mathrm{rk}}(\mathcal{C}') \leq \rho(\mathcal{C}) \leq d_{\mathrm{rk}}(\mathcal{C}') - 1 = n - k.$$

- The current known families of MRD code $\mathcal{C}$ all have covering radius $d_{\mathrm{rk}}(\mathcal{C}) - 1$.
- There are sporadic examples of MRD codes $\mathcal{C}$ such that $\rho(\mathcal{C}) < d_{\mathrm{rk}}(\mathcal{C}) - 1$.

Maximality of dually QMRD Codes

Theorem 18

Let $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$ be dually QMRD.

- $$\rho(\mathcal{C}) \leq \sigma^*(\mathcal{C}) = n - d_{\mathrm{rk}}(\mathcal{C}^\perp) + 1 = d_{\mathrm{rk}}(\mathcal{C}).$$
- *Then $\rho(\mathcal{C}) < d_{\mathrm{rk}}(\mathcal{C})$ if and only if $\mathcal{C}$ is maximal.*
- *If $\mathcal{C}$ is maximal then in particular it cannot be embedded in an $[mn, mk, d_{\mathrm{rk}}(\mathcal{C})]$ MRD code.*

Example 19

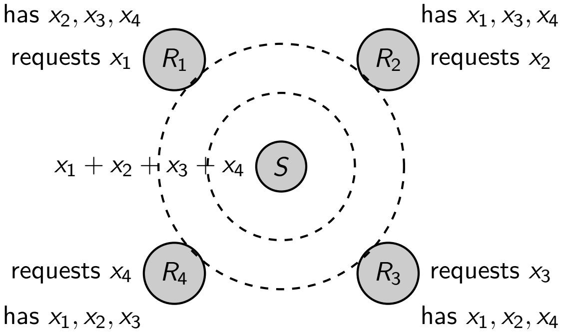
Let $\mathcal{C}$ be the $\mathbb{F}_2$-linear $[16, 3, 4]$ code generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

It can be checked that $\rho(\mathcal{C}) = 3 < d_{\mathrm{rk}}(\mathcal{C}) = 4$, so $\mathcal{C}$ is maximal.

Broadcasting With Coded-Side Information

- Index Coding
- Broadcast Relay Networks
- Coded Caching
- Network Coding



Broadcast with Coded-Side Information

- $X \in \mathbb{F}_q^{n \times t}$ is the raw data held by the sender for m users.
- User i wants the packet $R_i X \in \mathbb{F}_q^t$.
- User i has side information $(V^{(i)}, V^{(i)}X) \in \mathbb{F}_q^{d_i \times n} \times \mathbb{F}_q^{d_i \times t}$.
- The sender, after receiving each request R_i, transmits $Y = LX \in \mathbb{F}_q^{N \times t}$ for some $L \in \mathbb{F}_q^{N \times n}$, $N < n$.
- Each user decodes $R_i X$ by solving a linear system of equations in the received Y and its side-information.

Objective 1

The sender aims to find an encoding LX that minimizes N such that the demands of all users satisfied.

Dai, Shum, Sung, "Data Dissemination with Side Information and Feedback", IEEE Trans. Wireless Comm. (13) 9, 2014.

A Class of Codes for Coded-Caching

Now we consider codes of the form $\mathcal{C} = \mathcal{C}^{(1)} \oplus \cdots \oplus \mathcal{C}^{(m)}$ for some $\mathcal{C}^{(i)} < \mathbb{F}_q^n$ of dimension d_i. So $\mathcal{C}$ has the form:

$$\mathcal{C} = \left\{ \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{bmatrix} : X_i \in \mathcal{C}^{(i)} < \mathbb{F}_q^n \right\} \subset \mathbb{F}_q^{m \times n}.$$

- $\mathcal{C}$ with low covering radius are useful for coded-caching schemes.
- $\mathcal{C}^{\perp} = \mathcal{C}^{(1)\perp} \oplus \cdots \oplus \mathcal{C}^{(m)\perp}$.

A Class of Codes for Coded-Caching

Theorem 20 (B., Calderini, 2015)

Let $\mathcal{C} = \oplus_{i\in[m]}\mathcal{C}^{(i)}$.

- $\rho(\mathcal{C}) \leq \sigma^*(\mathcal{C}) = \max \mathrm{rk}(\mathcal{C}^\perp)$
  $= \max\{\dim\langle b_1, ..., b_m\rangle : b_i \in \mathcal{C}^{i\perp}\}$.
- $\rho(\mathcal{C}) \leq \max\{n - d_i : i \in [m]\}$, *if* $|\{\mathcal{C}^{(i)} : i \in [m]\}| \leq q$.
- $\rho(\mathcal{C}) \leq \min\{n - d_i : i \in [m]\} + \ell - 1$ *if* $|\{\mathcal{C}^{(i)} : i \in [m]\}| \leq q^{\ell t}/(q^t - 1), t > 1$.

Example 21

Let $\mathcal{C} = \mathcal{C}^{(1)} \oplus \cdots \oplus \mathcal{C}^{(m)}$, each $\mathcal{C}^{(i)} < \mathbb{F}_q^n$ of dimension d. Suppose that each $\mathcal{C}^{(i)}$ is systematic on the same set of coordinates, say $\{1, 2, ..., d\}$. Then given any $x \in \mathbb{F}_q^{m\times n}$, there exists $y \in \mathcal{C}$ such that $x - y = [0_d|z]$. So $\rho(\mathcal{C}) \leq n - d$.

Broadcast With Coded-Side Information

1. Dai, Shum, Sung, "Data Dissemination with Side Information and Feedback", IEEE Trans. Wireless Comm. (13) 9, 2014.
2. Shanmugam, Dimakis, Langberg, "Graph Theory versus Minimum Rank for Index Coding," arXiv:1402.3898

Results of [2] can be extended based on setting in [1] (joint with Calderini, 2015).

- clique: $C \subset [m]$ such that $\{v : R_i \in \langle v \rangle + \mathcal{C}^i; \forall i \in C\} \neq \emptyset$
- clique/local clique/fractional local clique covering number
- partitioned multicast/fractional partition multicast number
- partitioned local clique covering number
- there exist achievable schemes based on these

Other Impacts on Mathematics

- Semi/quasifields
- Linearized Polynomials
- Graph theory
- Matroids
- Lattices

The End

Thanks for your attention!