Subspace Codes for Network Coding

Frank R. Kschischang
Department of Electrical & Computer Engineering
University of Toronto

2011 Canadian Workshop on Information Theory
Kelowna, British Columbia

May 18, 2011

Joint work with:

Ralf Kötter, Danilo Silva, Azadeh Khaleghi.

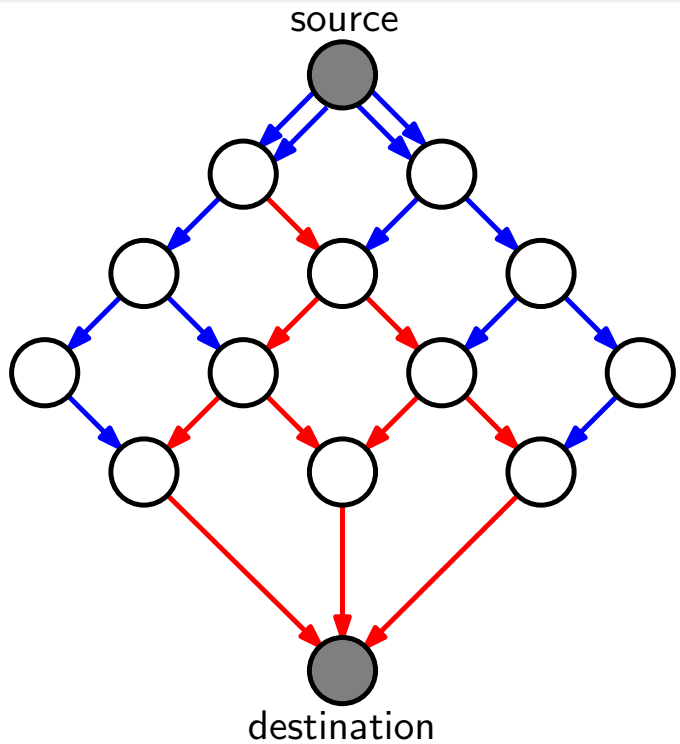
Acknowledgments:

Thank you to the organizers: Robert Schober and Julian Cheng

Thank you to CAPES (Brazil), NSERC (Canada) and DARPA (USA) for financial support.

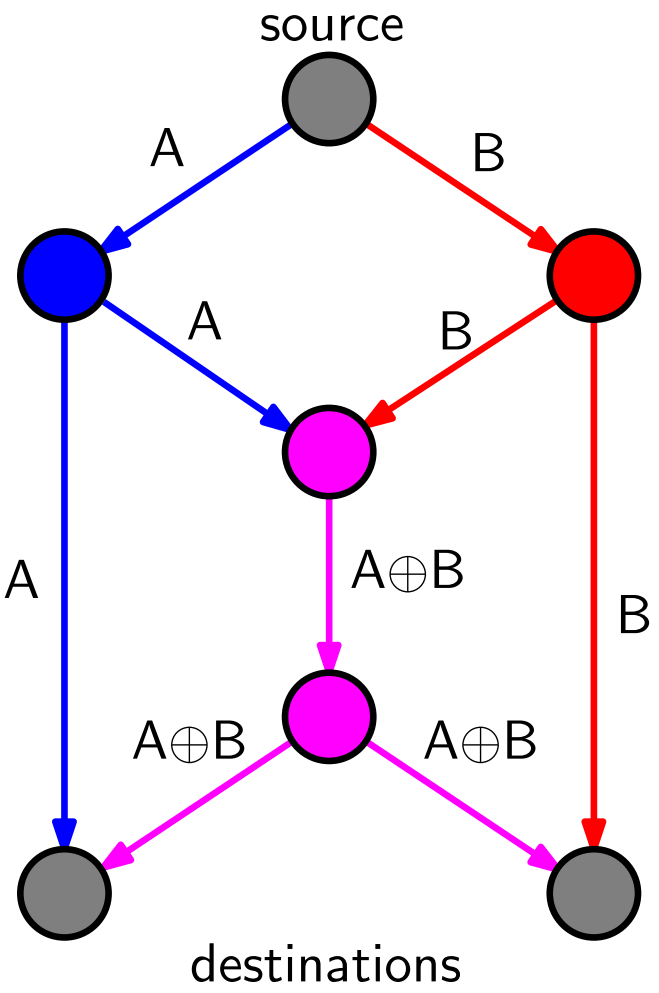
Part I

Error Control in Network Coding



Network Coding

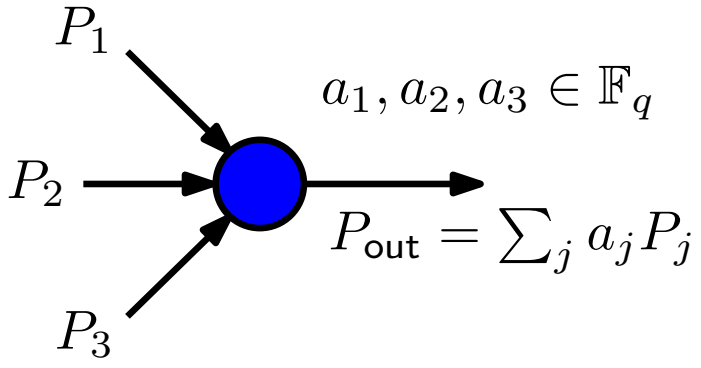
- A new approach to information dissemination over networks
- Essence: packets can be *mixed* with each other (rather than just routed or replicated)
- A higher throughput can be achieved



Linear Network Coding

- Packets are length-m vectors over a finite field $\mathbb{F}_q$
- Nodes create outgoing packets as $\mathbb{F}_q$-linear combinations of incoming packets
- Original packets can be recovered by solving a linear system of equations

$$X_i = \begin{bmatrix} X_{i1} & \cdots & X_{im} \end{bmatrix}$$



$$\begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix} = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix}$$

transfer matrix

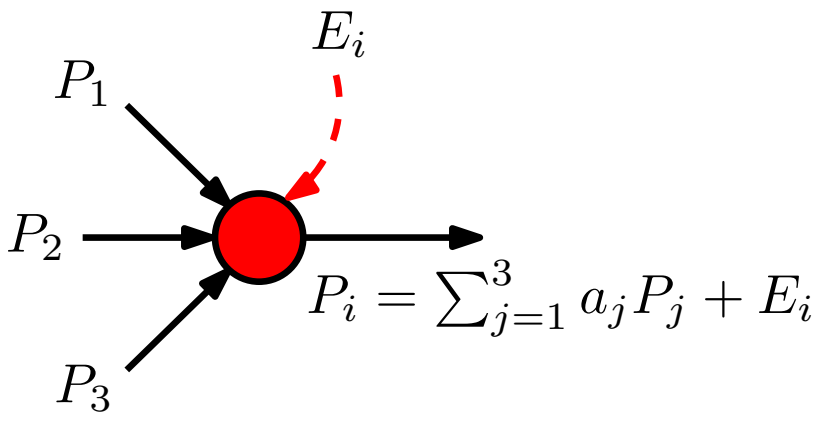
Random Linear Network Coding

- Nodes draw coding coefficients uniformly at random from $\mathbb{F}_q$
- The transfer matrix will be invertible with high probability if q is sufficiently large
- The transfer matrix can be recorded by appending a header to each original packet

$$\begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix} = \left[\begin{array}{ccc|c} 1 & \cdots & 0 & \boxed{\text{payload } 1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & \boxed{\text{payload } n} \end{array}\right]$$

Random Linear Network Coding with Errors

- A corrupt packet is modeled as the addition of an error packet to a genuine packet
- Assume that at most t error packets are injected



- The overall network can be viewed as a point-to-point channel

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix} \quad E = \begin{bmatrix} E_1 \\ \vdots \\ E_t \end{bmatrix} \quad Y = AX + BE \quad Y = \begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix}$$

network coding channel

Why Consider Errors?

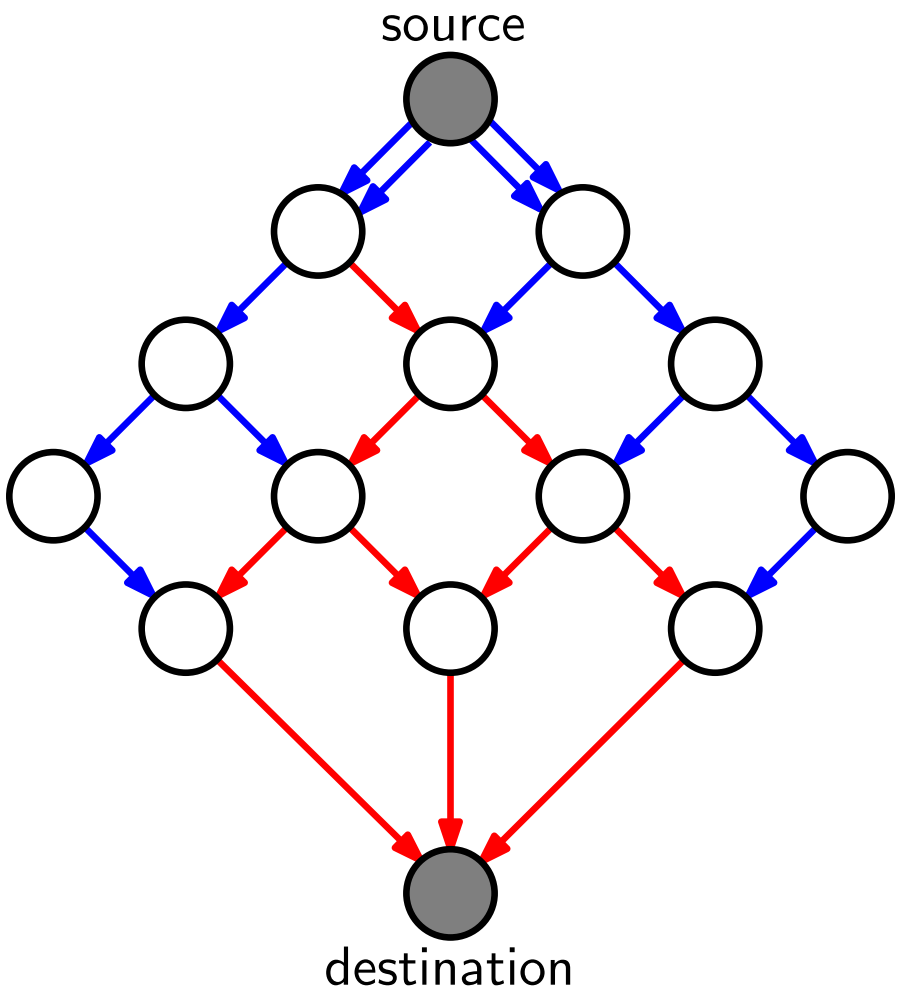
Possible error sources:

- Random errors that could not be detected at the physical layer
- Corrupt packets injected at the application level by a malicious user

Issue

The very essence of network coding—packet mixing—makes it highly prone to *error propagation*. This essentially rules out classical error correction.

Error Propagation



This Motivates Error Correction in Network Coding, e.g.,

Deterministic (Coherent) Network Coding:

1. N. Cai and R. W. Yeung, "Network coding and error correction," ITW 2002.
2. R. W. Yeung $\Leftrightarrow$ N. Cai, "Network error correction, Part I: Basic concepts and upper bounds; Part II: Lower bounds," *Comm. in Inform. and Systems*, 2006.
3. R. Matsumoto, "Construction algorithm for network error-correcting codes attaining the Singleton bound," *IEICE Trans. Funda.*, 2007.
4. Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Inf. Theory*, 2008.
5. S. Yang, R. W. Yeung, and C. K. Ngai "Refined Coding Bounds and Constructions for Coherent Network Error Correction," *IEEE Trans. Inf. Theory*, 2011.

This Motivates Error Correction in Network Coding, e.g.,

Random Network Coding:

1. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard and M. Effros, "Resilient network coding in the presence of Byzantine adversaries," *IEEE Trans. Inf. Theory*, 2008.
2. R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, 2008.
3. D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, 2008.
4. A. Montanari and R. Urbanke, "Coding for network coding," 2007, preprint. Available: http://arxiv.org/abs/0711.3935

The Key Idea

In the absence of errors, the transmitter injects X, the receiver collects $Y = AX$. Unfortunately, A is completely unknown to the transmitter and to the receiver (or so we assume).

Q:

What property of X is preserved in AX?

The Key Idea

In the absence of errors, the transmitter injects X, the receiver collects $Y = AX$. Unfortunately, A is completely unknown to the transmitter and to the receiver (or so we assume).

Q:

What property of X is preserved in AX?

A:

Left multiplication by A performs *row operations* on $X \Rightarrow$ the rows of AX lie in the **row space** of X.

The Key Idea

In the absence of errors, the transmitter injects X, the receiver collects $Y = AX$. Unfortunately, A is completely unknown to the transmitter and to the receiver (or so we assume).

Q:

What property of X is preserved in AX?

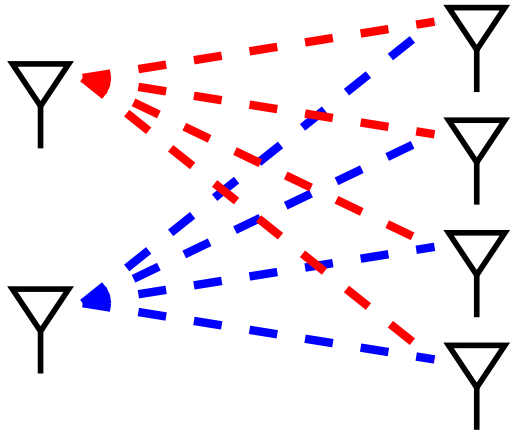
A:

Left multiplication by A performs *row operations* on $X \Rightarrow$ the rows of AX lie in the **row space** of X.

Thus we may attempt to transmit information via the selection, at the transmitter, of a *vector space* from some appropriate codebook of spaces.

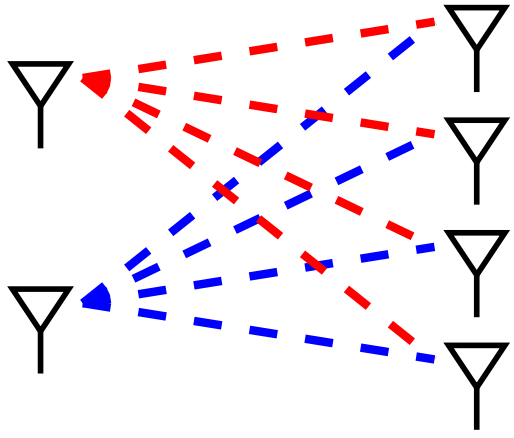
Noncoherent Multi-antenna Channels

The network coding channel resembles the noncoherent multi-antenna channel, **only over $\mathbb{F}_q$ rather than $\mathbb{C}$.**



Noncoherent Multi-antenna Channels

The network coding channel resembles the noncoherent multi-antenna channel, **only over $\mathbb{F}_q$ rather than $\mathbb{C}$.**



This subspace approach is inspired by [ZheTse02] ("Communication on the Grassmannian manifold"), where messages are *also* encoded in the choice by the transmitter of an appropriate vector space V.

We will, however, define a different metric on subspaces.

The Operator Channel (A Convenient Abstraction of Random Linear Network Cdoing)

Let $\mathcal{P}_q(n)$ denote the the set of all subspaces of an n-dimensional vector space over $\mathbb{F}_q$.

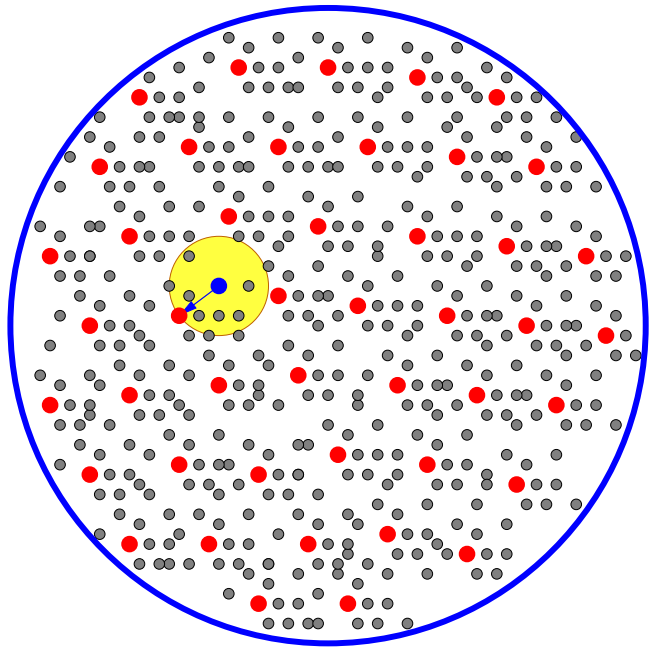
- The transmitter selects a vector space $V \in C$ from some collection of $C \subseteq \mathcal{P}_q(n)$ of spaces.
- The transmitter signals this choice by the injection into the network of a basis for V.
- The receiver gathers packets, and forms the vector space U that they span.
- We may write

$$U = \mathcal{H}_k(V) \oplus E,$$

where $\mathcal{H}_k(\cdot)$ is an "erasure operator" that projects onto a randomly chosen k-subspace and E denotes an "error space" intersecting trivially with V.

Part II

Coding for the Operator Channel



Classical Coding Theory

Transmitter: emits a **vector**, e.g., an element of $\mathbb{F}_q^n$.

Receiver: receives a **vector**, possibly corrupted by noise.

Goal of Code Design: to construct a large collection of **vectors**, well-separated according to some metric (e.g., Hamming distance).

Classical Coding Theory

Transmitter: emits a **vector**, e.g., an element of $\mathbb{F}_q^n$.

Receiver: receives a **vector**, possibly corrupted by noise.

Goal of Code Design: to construct a large collection of **vectors**, well-separated according to some metric (e.g., Hamming distance).

This Work

Transmitter: emits a **vector space**, e.g., an element of $\mathcal{P}_q(n)$ (the projective space of order n over $\mathbb{F}_q$).

Receiver: receives a **vector space**, possibly corrupted by noise.

Goal of Code Design: construct a large collection of **vector spaces**, well-separated according to some metric.

Subspace Distance [KK08]

Let A and B be elements of $\mathcal{P}_q(n)$.

Definition

The subspace distance between A and B is defined as

$$d_S(A,B) := \dim(A+B) - \dim(A \cap B).$$

We may also write

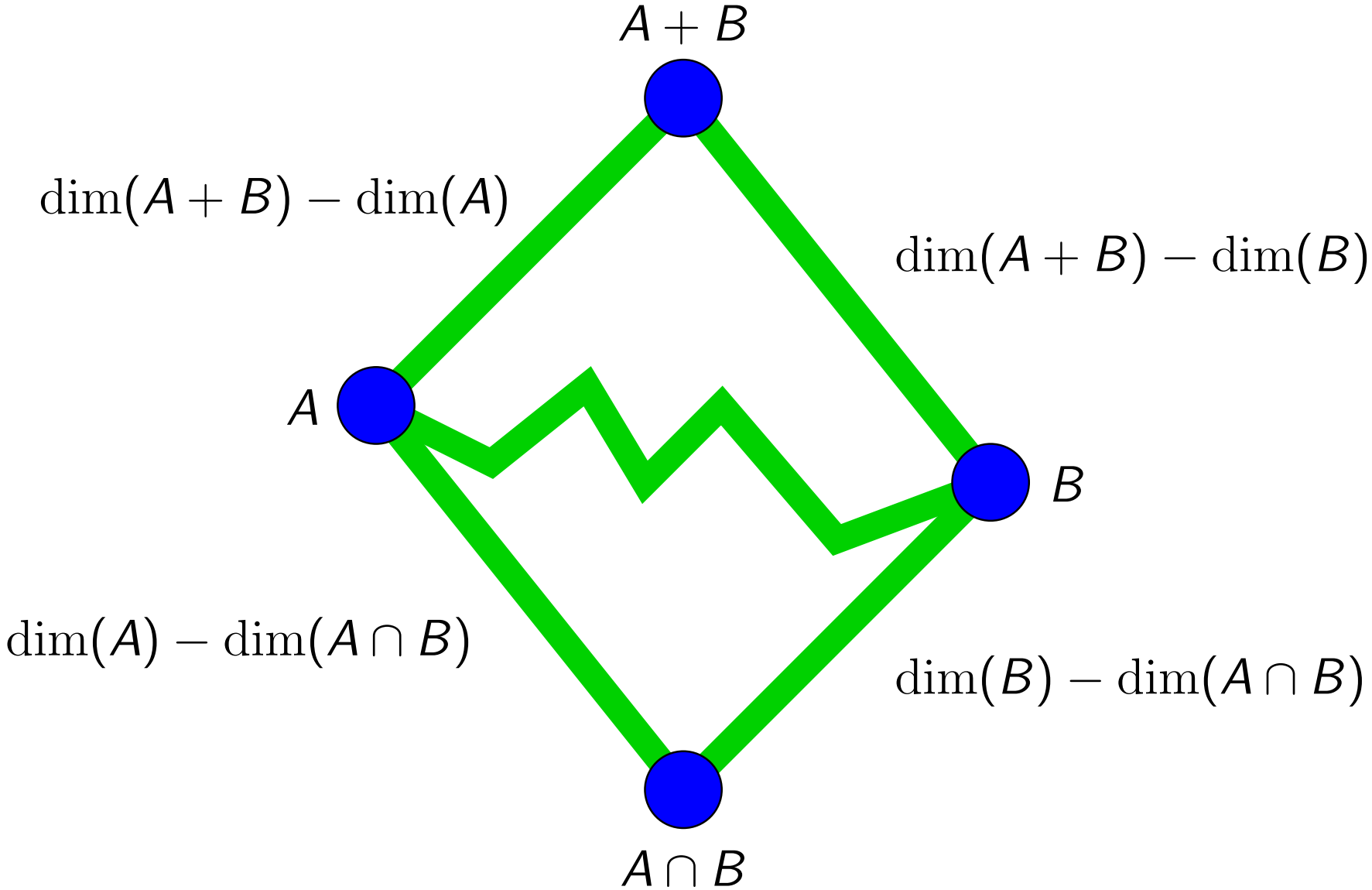
$$\begin{aligned} d_S(A,B) &= \dim(A) + \dim(B) - 2\dim(A \cap B) \\ &= 2\dim(A+B) - \dim(A) - \dim(B) \end{aligned}$$

Theorem

The function $d_S(A,B) = \dim(A+B) - \dim(A \cap B)$ is a metric on the space $\mathcal{P}_q(n)$.

Remark:

$d_S(A, B)$ is the length of a geodesic between A and B in the undirected Hasse graph representing the lattice of subspaces.

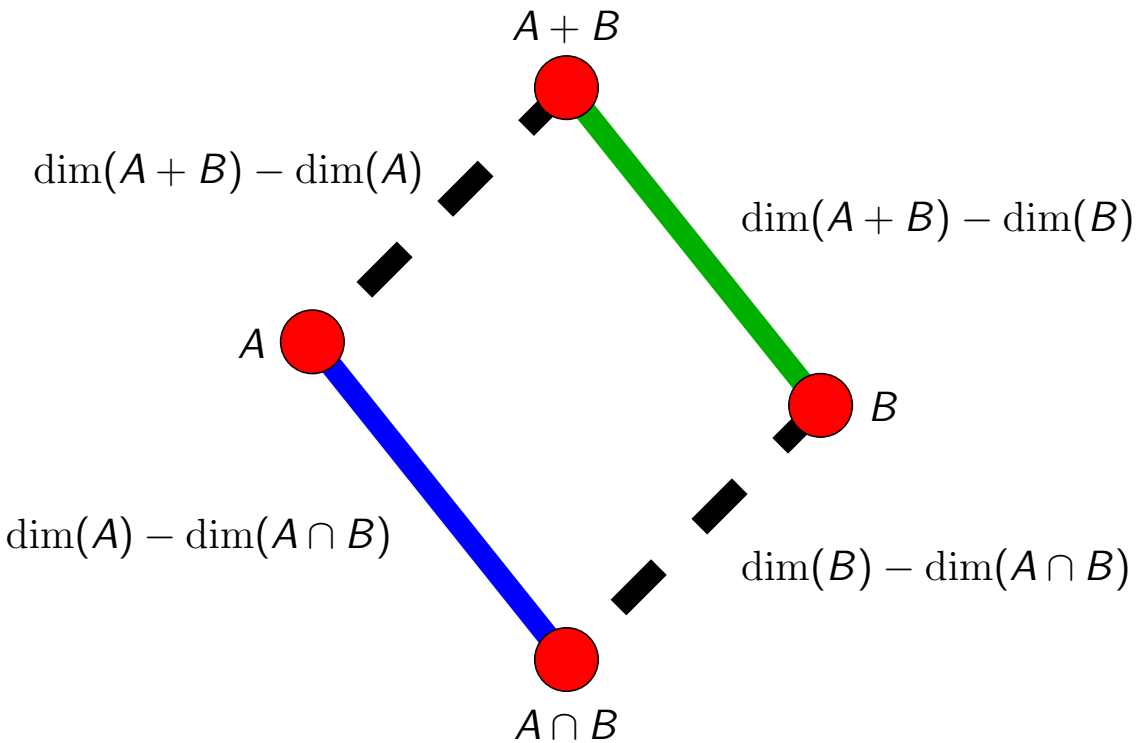


Injection Distance [SK08]

Definition: (Injection Distance)

$$d(A,B) \triangleq \max\{\dim(\mathbf{A}), \dim(\mathbf{B})\} - \dim(\mathbf{A} \cap \mathbf{B})$$
$$= \dim(A+B) - \min\{\dim(A), \dim(B)\}$$

$d(\cdot,\cdot)$ is a **metric** that counts **the minimum number of packet injections required to transform one space to another**.



Subspace Distance vs. Injection Disance

- $d_S(A, B)$ is equal to the the minimum number of **insertions and deletions of generators** that are required to transform a basis for A into a basis for B.
  (Analogous to Hamming distance in classical coding theory, which is equal to the minimum number of symbol changes required to transform a vector A into a vector B.)
- $d(A, B)$ is equal to the minimum number of **packet insertions** needed to transform a basis for A into a basis for B: a *single* packet insertion can simultaneously delete a generator and insert another one.
- If $\dim(A) = \dim(B)$, then $d(A, B) = \frac{1}{2} d_S(A, B)$ (and in general $d(A, B) \geq \frac{1}{2} d_S(A, B)$).
- $d(A, B)$ can be intepreted as a geodesic in a "generalized Grassmann graph."

Some Definitions

The set of all subspaces of an n-dimensional vector space forms a **projective space** $\mathcal{P}_q(n)$. The set of all ℓ-dimensional subspaces of an n-dimensional vector space is called a **Grassmannian** $\mathcal{G}_q(n, \ell)$.

A **subspace code** $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is a collection of subspaces in $\mathcal{P}_q(n)$. If $\mathcal{C} \subseteq \mathcal{G}_q(n, \ell)$ then $\mathcal{C}$ is a **constant-dimension code** of dimension ℓ.

Definitions (cont'd)

The **minimum distance** of $\mathcal{C}$ is denoted by

$$d(\mathcal{C}) = \min_{X,Y \in \mathcal{C}, X \neq Y} d(X, Y)$$

The **maximum dimension** of $\mathcal{C}$ is denoted by

$$\ell(\mathcal{C}) = \max_{X \in \mathcal{C}} \dim(()X)$$

We call $\mathcal{C}$ an $(n, d)_q$ code if $d(\mathcal{C}) = d$; we call $\mathcal{C}$ an $(n, d, \ell)_q$ code if, additionally, $\mathcal{C} \subseteq \mathcal{G}_q(n, \ell)$.

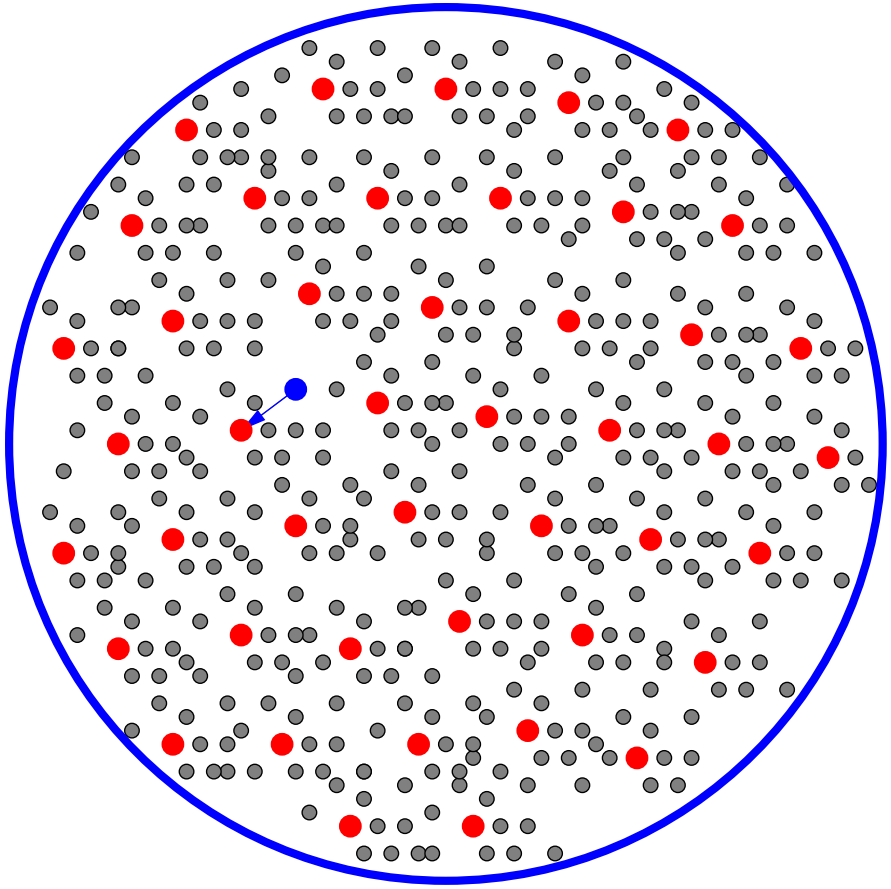
Normalized parameters

rate: $R = \log_q |\mathcal{C}|/(n\ell)$
normalized dimension: $\lambda = \ell(\mathcal{C})/n$
normalized minimum distance : $\delta = d(\mathcal{C})/n$

Minimum Distance Decoding

Definition

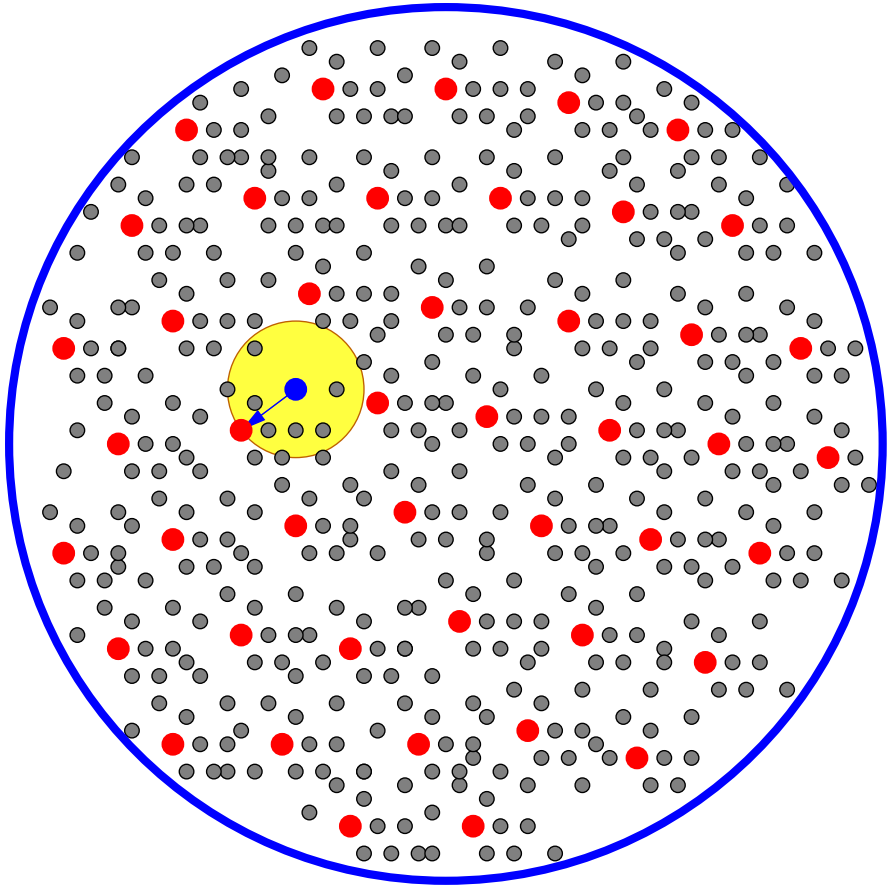
A *minimum distance decoder* for $\mathcal{C}$ takes the output U of an operator channel and returns a nearest codeword $V \in \mathcal{C}$, i.e., a codeword V satisfying, for all $X \in \mathcal{C}$, $d(U, V) \leq d(U, X)$.



Minimum Distance Decoding

Definition

A *minimum distance decoder* for $\mathcal{C}$ takes the output U of an operator channel and returns a nearest codeword $V \in \mathcal{C}$, i.e., a codeword V satisfying, for all $X \in \mathcal{C}$, $d(U, V) \leq d(U, X)$.



Error-and-Erasure Correcting Capability

Assume we use a code $\mathcal{C}$ for transmission over a random linear network coding channel. Let ρ denote the number of erasures induced by the channel ("rank deficiency," in the absence of adversarial errors) and let t denote the maximum number of packets that an adversary may inject.

Theorem

A minimum distance decoder for $\mathcal{C}$ will produce the transmitted space V from the received space (for all possible choices of adversarial error) if and only if

$$d(\mathcal{C}) > 2t + \rho.$$

This theorem motivates the construction of codes with large minimum injection distance.

Gaussian Coefficients

For any non-negative integer i, define

$$[\![i]\!]_q := \begin{cases} 1 & \text{if } i = 0, \\ q^i - 1 & \text{if } i > 0. \end{cases},$$

and let

$$[\![i]\!]_q! := \prod_{j=0}^{i} [\![j]\!]_q.$$

Definition

The *Gaussian coefficient* $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is defined as

$$\begin{bmatrix} n \\ m \end{bmatrix}_q := \begin{cases} \frac{[\![n]\!]_q!}{[\![m]\!]_q![\![n-m]\!]_q!} & 0 \leq m \leq n \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

The number of ℓ-dimensional subspaces of an n-dimensional vectors space over F_q equals $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$.

Asymptotically, the Gaussian coefficient $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$ behaves as $q^{\ell(n-\ell)}$.

Theorem

The Gaussian coefficient $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$ satisfies

$$1 \leq q^{-\ell(n-\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q < 4$$

for $0 < \ell < n$.

(NB: the number of spaces spanned by $\ell \times n$ matrices of the form $[I\ X]$ gives the lower bound.)

Spheres in the Grassmann Graph

Let W be an n dimensional vector space and let $\mathcal{G}(n, \ell)$ be the dimension-ℓ Grassmannian.

Definition

The sphere $S(V, \ell, t)$ of radius t centered at a space V in $\mathcal{G}(n, \ell)$ is the set of all subspaces U that satisfy $d(U, V) \leq t$,

$$S(V, \ell, t) = \{U \in \mathcal{G}(n, \ell) \mid d(U, V) \leq t\}.$$

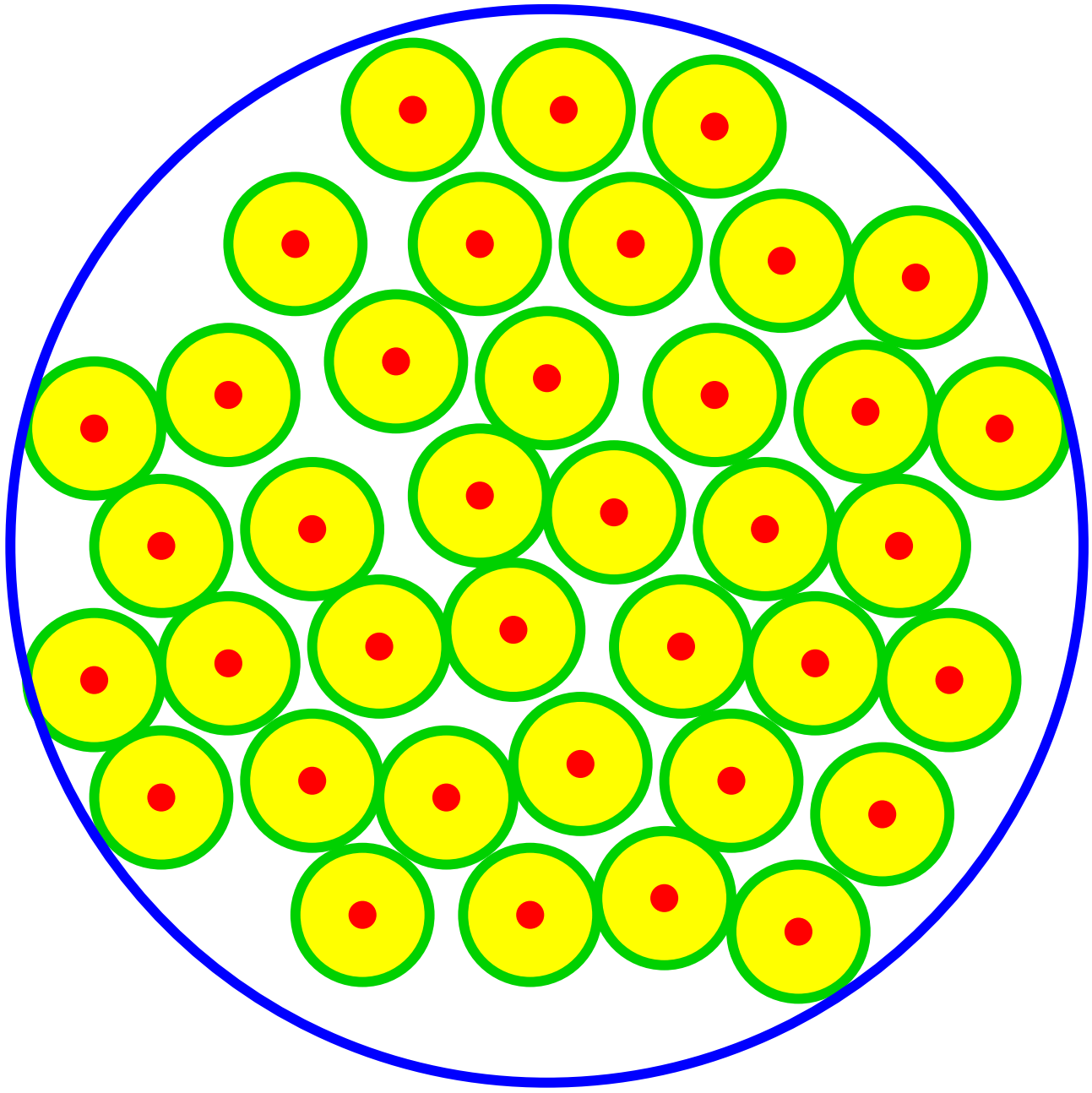
Theorem

The number of spaces in $S(V, \ell, t)$ is independent of V and equals

$$|S(V, \ell, t)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n-\ell \\ i \end{bmatrix}$$

for $t \leq \ell$.

Sphere-Packing (Hamming) Bound



Sphere-Packing (Hamming) Bound

Let $\mathcal{C}$ be a collection of spaces in $\mathcal{G}(n,\ell)$ such that $d(\mathcal{C})$ is at least s. Let $t = \lfloor \frac{s-1}{2} \rfloor$.

Theorem

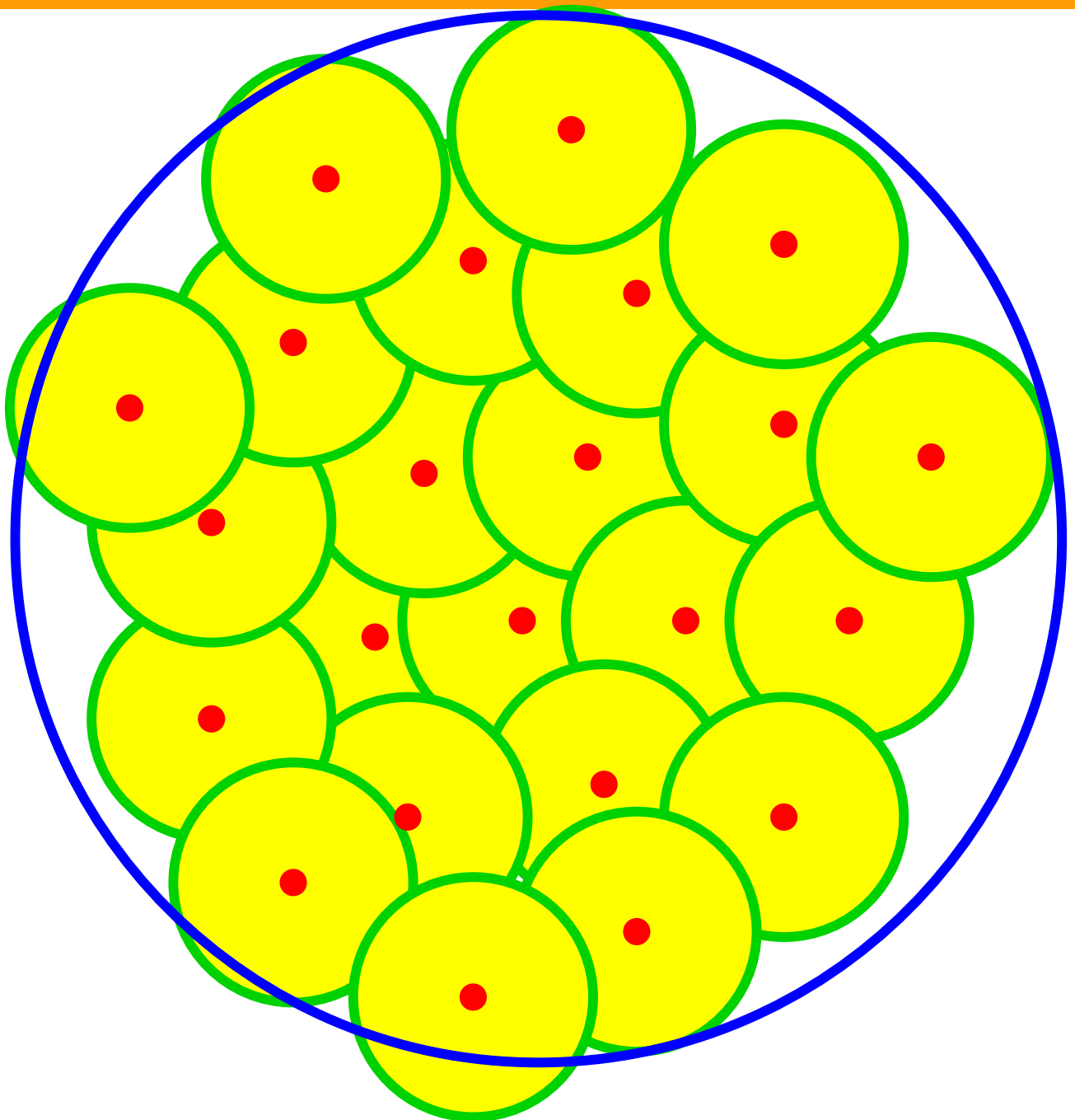
$$\begin{aligned} |\mathcal{C}| &\leq \frac{|\mathcal{G}(n,\ell)|}{|S(V,\ell,t)|} \\ &= \frac{\begin{bmatrix} n \\ \ell \end{bmatrix}}{|S(V,\ell,t)|} \\ &< 4q^{(\ell-t)(n-t-\ell)} \end{aligned}$$

In terms of normalized parameters R, λ and δ we have

$$R \leq (1-\delta/2)(1-\lambda(\frac{\delta}{2}+1)) + o(1),$$

where $o(1) \to 0$ as $n \to \infty$.

Sphere-Covering (Gilbert) Bound



Sphere-Covering (Gilbert) Bound

Theorem

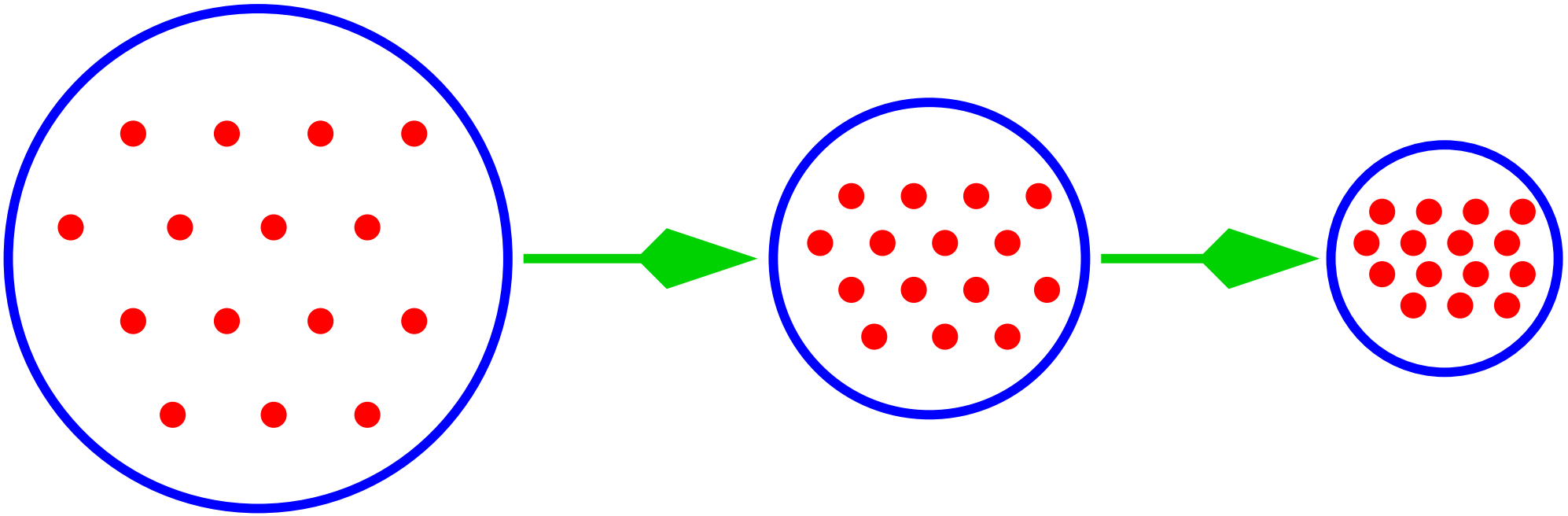
There exists a code $\mathcal{C}'$ with distance $d(\mathcal{C}') \geq s$ such that

$$\begin{aligned} |\mathcal{C}'| &\geq \frac{|\mathcal{G}(n,\ell)|}{|S(V,\ell,s-1)|} \\ &= \frac{\begin{bmatrix} n \\ \ell \end{bmatrix}}{|S(V,\ell,s-1)|} \\ &> \frac{1}{16t} q^{(\ell-s+1)(n-s-\ell+1)} \end{aligned}$$

In terms of normalized parameters, there exists a code C' such that

$$R \geq (1-\delta)(1-\lambda(\delta+1)) + o(1).$$

Singleton Bound



Singleton Bound

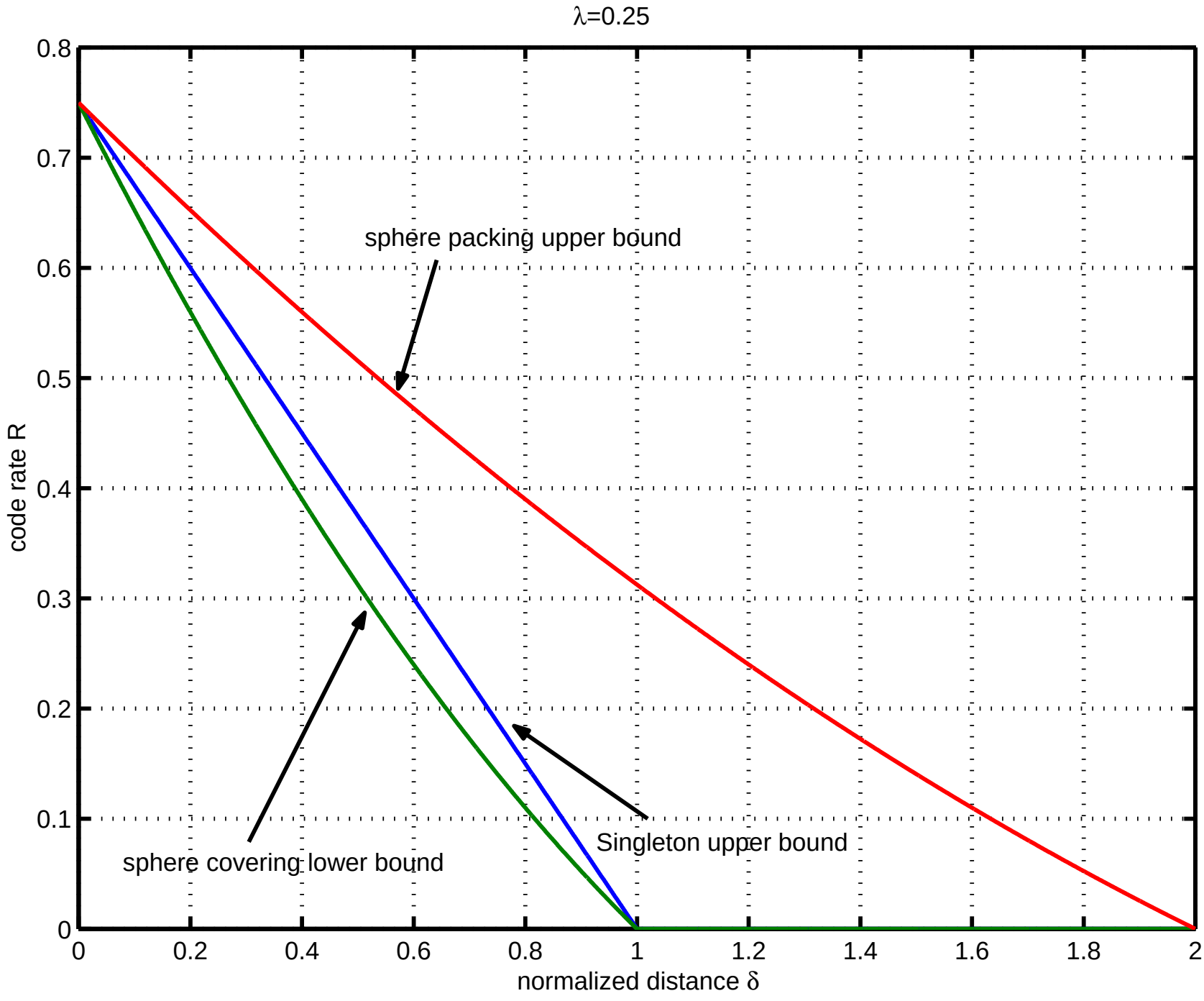
Theorem

A q-ary code $\mathcal{C} \subset \mathcal{G}(n, \ell)$ of type $(n, \ell, \log_q |\mathcal{C}|, d)$ must satisfy

$$|\mathcal{C}| \leq \begin{bmatrix} n - (d-2)/2 \\ \ell - (d-2)/2 \end{bmatrix}_q.$$

In terms of normalized parameters,

$$R \leq (1-\delta)(1-\lambda) - \frac{1}{\lambda n}(1 - \lambda + o(1))$$


λ=0.25
sphere packing upper bound
Singleton upper bound
sphere covering lower bound
code rate R
normalized distance δ
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

More bounds:

1. Xia, S.T., Fu, F.W.: Johnson type bounds on constant dimension codes. *Designs, Codes and Cryptography*, **50**(2) (February 2009) 163–172
2. Gadouleau, M., Yan, Z.: Packing and Covering Properties of Subspace Codes for Error Control in Random Linear Network Coding, *IEEE Trans. Inf. Theory*, 2010.
3. Etzion, T., Vardy, A.: Error-correcting codes in projective space. *IEEE Trans. Inf. Theory*, 2011.
4. Ahlswede, R., Aydinian, H.: On error control for random network coding. In: *IEEE Workshop on Network Coding, Theory and Applications*. (2009)

Lifted Rank-Metric Codes

A *rank-metric code* $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ is a matrix code used in the context of the rank metric.

Definition

The *rank distance* between matrices $X, Y \in \mathbb{F}_q^{n \times m}$ is defined as $d_R(X, Y) = \operatorname{rank}(Y - X)$.

The minimum rank distance of $\mathcal{C}$ will be denoted by $d_R(\mathcal{C})$.

Singleton bound for rank metric codes

$$|\mathcal{C}| \leq q^{\max\{n,m\}(\min\{n,m\}-d+1)}$$

for every code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $d_R(\mathcal{C}) = d$.

Codes that achieve this bound are called *maximum-rank-distance* (MRD) codes and linear MRD codes are known to exist for all choices of parameters q, n, m and $d \leq \min\{n, m\}$.

Gabidulin Codes (1985)

Assume $n \leq m$. Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$, and let $\theta : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ be a vector space isomorphism, where the elements in $\mathbb{F}_q^m$ are regarded as row vectors.

Let $\mathbb{F}_{q,m}^n[x]$ denote the set of linearized polynomials, i.e., all polynomials of the form $f(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$, where $f_i \in \mathbb{F}_{q^m}$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ be elements that are linearly independent when regarded as vectors in $\mathbb{F}_q^m$, and let $0 \leq d \leq n$.

Evaluation Map

A *Gabidulin code* $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ is defined as

$$\mathcal{C} = \left\{ [\theta(f(\alpha_1)), \ldots, \theta(f(\alpha_n))]^T, \ f(x) \in \mathbb{F}_{q,m}^{(n-d+1)}[x] \right\}.$$

Theorem: Gabidulin codes are MRD.

Lifting Construction

Lifting a Matrix

For a matrix $X \in \mathbb{F}_q^{k \times m}$, let the subspace

$$\Lambda(X) \triangleq \left\langle \begin{bmatrix} I_{k \times k} & X \end{bmatrix} \right\rangle \in \mathcal{G}_q(k+m, k)$$

be called the *lifting* of X.

Lifting a Matrix Code

Similarly, for a matrix code $\mathcal{C} \subseteq \mathbb{F}_q^{k \times m}$, let the subspace code

$$\Lambda(\mathcal{C}) \triangleq \{\Lambda(X), X \in \mathcal{C}\}$$

be called the *lifting* of $\mathcal{C}$.

We have $|\Lambda(\mathcal{C})| = |\mathcal{C}|$ and note that $\Lambda(\mathcal{C})$ is a constant-dimension code.

Relating Rank Distance and Subspace Distance

Theorem

For all $X, X' \in \mathbb{F}_q^{k\times m}$ and all $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$,

$$\mathrm{d}(\Lambda(X), \Lambda(X')) = \mathrm{d}_{\mathrm{R}}(X, X'),$$
$$\mathrm{d}(\Lambda(\mathcal{C})) = \mathrm{d}_{\mathrm{R}}(\mathcal{C}).$$

Relating Rank Distance and Subspace Distance

Theorem

For all $X, X' \in \mathbb{F}_q^{k\times m}$ and all $\mathcal{C} \subseteq \mathbb{F}_q^{k\times m}$,

$$\mathrm{d}(\Lambda(X), \Lambda(X')) = \mathrm{d}_{\mathrm{R}}(X, X'),$$
$$\mathrm{d}(\Lambda(\mathcal{C})) = \mathrm{d}_{\mathrm{R}}(\mathcal{C}).$$

Proof: We have

$$\begin{aligned}
\mathrm{d}(\Lambda(X), \Lambda(X')) &= \dim(\Lambda(X) + \Lambda(X')) - \min\{\dim(\Lambda(X)), \dim(\Lambda(X'))\} \\
&= \mathrm{rank} \begin{bmatrix} I & X \\ I & X' \end{bmatrix} - k \\
&= \mathrm{rank} \begin{bmatrix} I & X \\ 0 & X' - X \end{bmatrix} - k \\
&= \mathrm{rank}(X' - X).
\end{aligned}$$

The second statement immediately follows from the first.

Optimality of the Lifting Construction

In particular, let $\mathcal{C} \subseteq \mathbb{F}_q^{k\times(n-k)}$ be an MRD code with $\mathrm{d_R}(\mathcal{C}) = d$ and, without loss of generality, let $k \leq n-k$.

Lifted MRD Code

Then $\Lambda(\mathcal{C})$ is an (n, d, k) code with cardinality

$$|\Lambda(\mathcal{C})| = q^{(n-k)(k-d+1)}.$$

Singleton Bound

It is shown in [KK08] that a constant-dimension code $\mathcal{C}$ must satisfy

$$|\mathcal{C}| \leq \begin{bmatrix} n-d+1 \\ n-k \end{bmatrix}_q < h(q)q^{(n-k)(k-d+1)}$$

where $h(q)$ is a constant depending only on q.

Thus, lifted MRD codes are asympotically optimal constant-dimension codes.

Decoding Lifted Rank-Metric Codes

Recall $X = \begin{bmatrix} I & \mathbf{c} \end{bmatrix}$. Let $Y = \begin{bmatrix} \hat{A} & \mathbf{y} \end{bmatrix}$ and assume Y is full rank.

Special case

Suppose $\hat{A}$ is invertible. Applying Gaussian elimination, we get

$$\bar{Y} = \hat{A}^{-1} Y = \hat{A}^{-1} \begin{bmatrix} \hat{A} & \mathbf{y} \end{bmatrix} = \begin{bmatrix} I & \hat{A}^{-1}\mathbf{y} \end{bmatrix} = \begin{bmatrix} I & \mathbf{r} \end{bmatrix}.$$

The matrix $\mathbf{r}$ will be called the *received word*.

It follows that the decoding problem becomes

$$\hat{\mathbf{c}} = \operatorname*{argmin}_{\mathbf{c} \in \mathcal{C}} \operatorname{rank}(\mathbf{r} - \mathbf{c}).$$

In this case, decoding amounts to minimum distance decoding in the rank metric. This problem will be referred to as *traditional rank decoding*.

Example: Rank Errors

Let $n = 4$ and $q = 5$. Suppose that

$$
\begin{aligned}
Y &= AX + BZ \\
&= \begin{bmatrix} 2 & 4 & 2 & 4 \\ 0 & 0 & 3 & 3 \\ 1 & 0 & 4 & 3 \\ 0 & 4 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & c_1 \\ 0 & 1 & 0 & 0 & c_2 \\ 0 & 0 & 1 & 0 & c_3 \\ 0 & 0 & 0 & 1 & c_4 \end{bmatrix} + \begin{bmatrix} 4 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & z \end{bmatrix} \\
&= \begin{bmatrix} 1 & 2 & 4 & 0 & 2c_1 + 4c_2 + 2c_3 + 4c_4 + 4z \\ 0 & 0 & 3 & 3 & 3c_3 + 3c_4 \\ 2 & 2 & 2 & 2 & c_1 + 4c_3 + 3c_4 + z \\ 0 & 4 & 1 & 4 & 4c_2 + c_3 + 4c_4 \end{bmatrix} = \begin{bmatrix} \hat{A} & \mathbf{y} \end{bmatrix}
\end{aligned}
$$

Example: Rank Errors

Performing Gaussian elimination on Y, we obtain

$$\bar{Y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 3c_2 + 2c_3 + c_4 + z \\ 0 & 1 & 0 & 0 & 3c_1 + 2c_2 + 4c_3 + 2c_4 + 2z \\ 0 & 0 & 1 & 0 & 4c_1 + 3c_2 + 3c_3 + c_4 + z \\ 0 & 0 & 0 & 1 & c_1 + 2c_2 + 3c_3 + 4z \end{bmatrix} = \begin{bmatrix} & r_1 \\ I & r_2 \\ & r_3 \\ & r_4 \end{bmatrix}.$$

Note that

$$\mathbf{r} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \\ 1 \\ 4 \end{bmatrix} \begin{bmatrix} 4c_1 + 3c_2 + 2c_3 + c_4 + z \end{bmatrix}.$$

Thus, the error word $\mathbf{e} \triangleq \mathbf{r} - \mathbf{c}$ has rank 1.

Decoding Lifted Rank-Metric Codes

In general, $\hat{A}$ may not be invertible.

Applying Gaussian elimination, we may obtain (for example)

$$\bar{Y} = \left[\begin{array}{ccccccc|cccc} 1 & 0 & 0 & * & 0 & * & 0 & r_{11} & r_{12} & \cdots & r_{1m} \\ 0 & 1 & 0 & * & 0 & * & 0 & r_{21} & r_{22} & \cdots & r_{2m} \\ 0 & 0 & 1 & * & 0 & * & 0 & r_{31} & r_{32} & \cdots & r_{3m} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & * & 0 & r_{51} & r_{52} & \cdots & r_{5m} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & r_{71} & r_{72} & \cdots & r_{7m} \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & * & * & \cdots & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & * & * & \cdots & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & * & * & \cdots & * \end{array}\right]$$

Decoding Lifted Rank-Metric Codes

Thus, we can always write $\bar{Y}$ in this form:

$$\bar{Y} = \begin{bmatrix} I + \hat{L} I_{\mathcal{U}}^T & \mathbf{r} \\ 0 & \hat{E} \end{bmatrix}$$

where r is $n \times m$,

$\hat{L}$ is $n \times \mu$,

$\hat{E}$ is $\delta \times m$.

We will say that the tuple $(\mathbf{r}, \hat{L}, \hat{E})$ is a *reduction* of Y.

Note

- Each column of $\hat{L}$ corresponds to an erased packet:
  $\Longrightarrow$ We will say that μ *erasures* have occurred.
- Each row of $\hat{E}$ corresponds to an extraneous packet:
  $\Longrightarrow$ We will say that δ *deviations* have occurred.

Decoding Lifted Rank-Metric Codes

Theorem

Let $(\mathbf{r}, \hat{L}, \hat{E})$ be a reduction of Y. Then the decoding problem becomes

$$\hat{\mathbf{c}} = \underset{\mathbf{c} \in \mathcal{C}}{\operatorname{argmin}} \operatorname{rank} \begin{bmatrix} \mathbf{r} - \mathbf{c} & \hat{L} \\ \hat{E} & 0 \end{bmatrix}.$$

This problem can be seen as a *generalized decoding problem* for rank-metric codes.

Correction Capabilities

Suppose μ erasures and δ deviations occurred. Then the decoding is guaranteed to be successful if:

- Traditional rank decoding:

$$\operatorname{rank}(\mathbf{r}-\mathbf{c}) \leq \frac{d-1}{2}$$

- Generalized rank decoding:

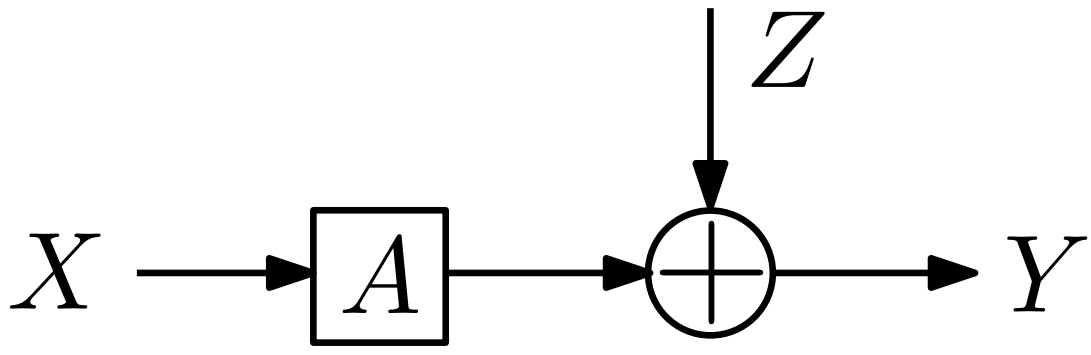
$$\operatorname{rank}(\mathbf{r}-\mathbf{c}) \leq \frac{d-1}{2}+\frac{\mu+\delta}{2}$$

Conclusion

Taking into account side information about erasures and deviations allows an increased correction capability.

Part III

A Random Error Model



Basic Model

A linear matrix channel

$$Y = AX + Z$$

where

- X and Y are $n \times m$ matrices
- A is $n \times n$, nonsingular, drawn uniformly at random
- Z $(= BE)$ is $n \times m$ with rank $\leq t$

The statistics of Z depends on the error model:

- Omniscient adversary model [J&08]
- Randomized error model
- Other models [J&08]

---

[1] Jaggi *et al.*, "Resilient network coding in the presence of Byzantine adversaries," *IEEE Trans. IT*, 2008.

Omniscient Adversary Model

The adversary:

- knows A and X and has unlimited computational power
- can freely choose Z (provided rank $Z \leq t$)

Results [KK08, SKK08]

- The channel "capacity" is approximately

$$C \approx (m-n)(n-2t) \qquad q\text{-ary symbols/channel use}$$

- Codes that achieve this rate are known

---

[2] Kötter & Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. IT*, 2008.

[3] Silva, Kschischang & Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. IT*, 2008.

Randomized Error Model

The error matrix Z is drawn:

- uniformly at random among all matrices of rank t
- independently from A and X

Results [MU07]

- Lower bound on capacity (for $n, m \to \infty$):

$$C \geq (m - n - t)(n - t) \qquad q\text{-ary symbols/channel use}$$

- A coding scheme with decoding complexity $\mathcal{O}(n^3 m)$ that can asymptotically achieve this rate

(Finite n, m? Random sparse graphs really necessary?)

[4] Montanari & Urbanke, "Coding for network coding," 2007, preprint.

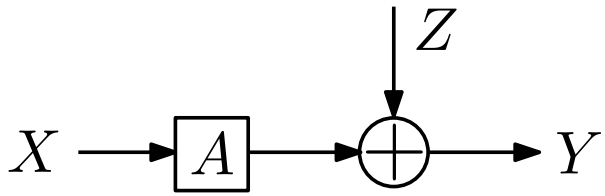
Our Contributions

1. Improved lower and upper bounds on capacity for any channel parameters (n, m, t, q)
2. Exact capacity expressions when $m \to \infty$ or $q \to \infty$
3. A coding scheme that:
   - achieves capacity (when $m \to \infty$ or $q \to \infty$)
   - has lower decoding complexity: $\mathcal{O}(n^2 m)$
   - has a better-decaying probability of error

Multiplicative-Additive Matrix Channel (MAMC)

Channel model:

$$Y = AX + Z$$



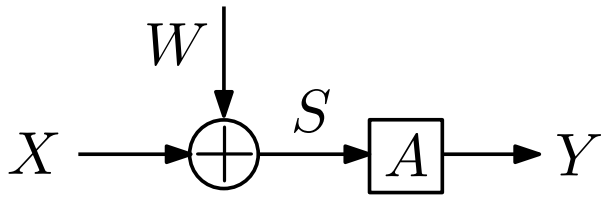
where

- A is $n \times n$, nonsingular, drawn uniformly at random
- Z is $n \times m$ with rank t, drawn uniformly at random
- A, X and Z are independent.

MAMC: Alternative Formulation

A trick:

$$Y = AX + Z$$
$$Y = A(X + A^{-1}Z)$$
$$Y = A(X + W)$$



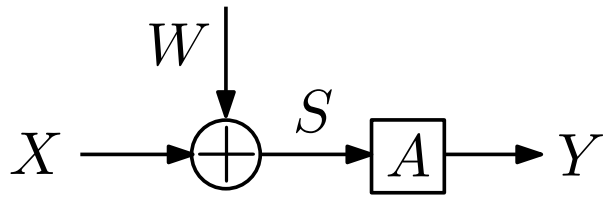
where

- A is $n \times n$, nonsingular, drawn uniformly at random
- W is $n \times m$ with rank t, drawn uniformly at random
- A, X and W are independent.

We will use this formulation in the following results.

MAMC = MMC + AMC

$$Y = A(X + W)$$



$$\begin{cases} S = X + W & \text{Additive Matrix Channel (AMC)} \\ Y = AS & \text{Multiplicative Matrix Channel (MMC)} \end{cases}$$

Multiplicative Matrix Channel (MMC)

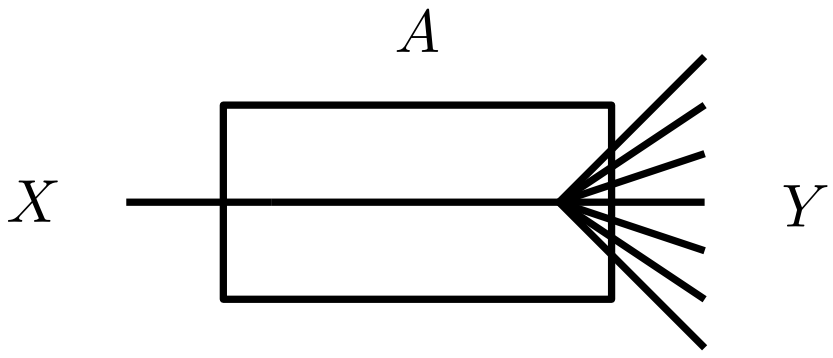
Channel model:

$$Y = AX$$

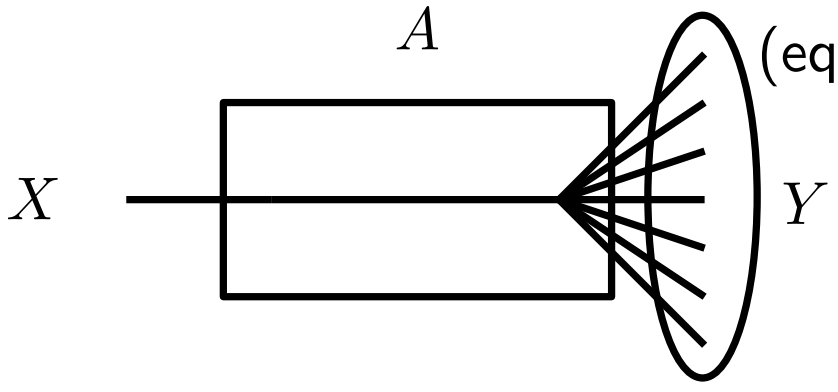
where

- A is $n \times n$, nonsingular, drawn uniformly at random
- A and X are independent.

MMC: Capacity

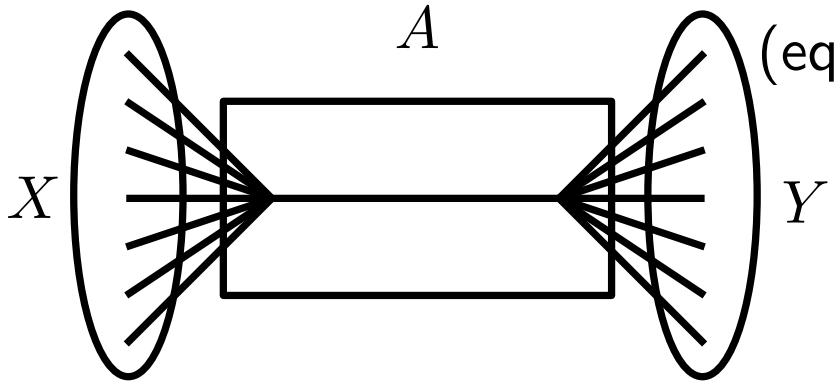


MMC: Capacity



set of matrices with
the same row space
(equivalence class)

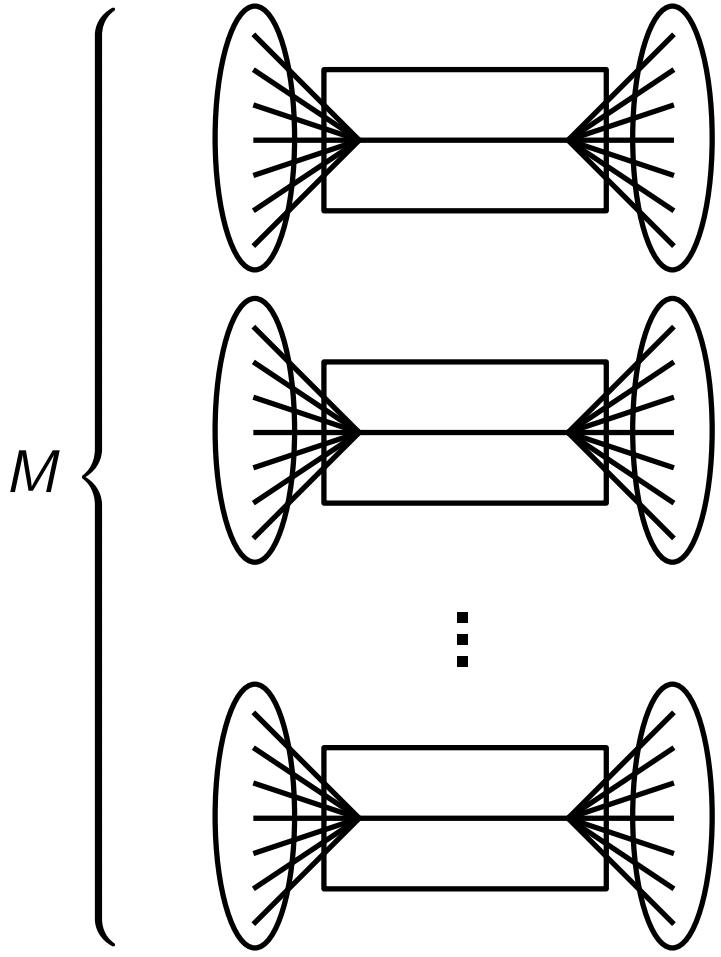
MMC: Capacity



set of matrices with
the same row space
(equivalence class)

zero-capacity channel

MMC: Capacity



The capacity of the overall channel is $\log M$, where M is the number of equivalence classes.

MMC: Capacity

Let $\begin{bmatrix} m \\ k \end{bmatrix}_q$ denote the number of k-dimensional subspaces of $\mathbb{F}_q^m$.

Proposition

$$C_{\text{MMC}} = \log_q \sum_{k=0}^{n} \begin{bmatrix} m \\ k \end{bmatrix}_q .$$

Capacity-achieving code

For each subspace $\mathcal{V}$ of $\mathbb{F}_q^m$ with dimension at most n, include a single matrix whose row space is $\mathcal{V}$.

- Communication occurs through subspace selection [KK08]
- Siavoshani, Mohajer, Fragouli, Diggavi arrive at the essentially the same conclusion with an even more general class of matrices A.

[5] Siavoshani, Mohajer, Fragouli & Diggavi "On the Capacity of Noncoherent Network Coding," *IEEE Trans. Inf. Theory*, 2011.

MMC: Capacity and a Coding Scheme

From now on, assume that n and t grow in proportion to m.

Proposition

Assume $n \leq m/2$. For large m or large q,

$$C_{\mathrm{MMC}} \approx (m-n)n = mn - n^2.$$

Capacity-achieving code (for large m or q):

$$X = \begin{bmatrix} I_{n\times n} & D_{n\times(m-n)} \end{bmatrix}$$

where $D \in \mathbb{F}_q^{n\times(m-n)}$ is a data matrix.

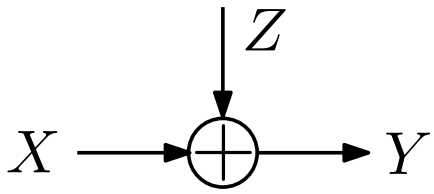
Strategy: Channel Sounding

Entries of I can be regarded as "pilot symbols."

Additive Matrix Channel (AMC)

Channel model:

$$Y = X + Z$$



where

- Z is $n \times m$ with rank t, drawn uniformly at random
- X and Z are independent.

AMC: Capacity

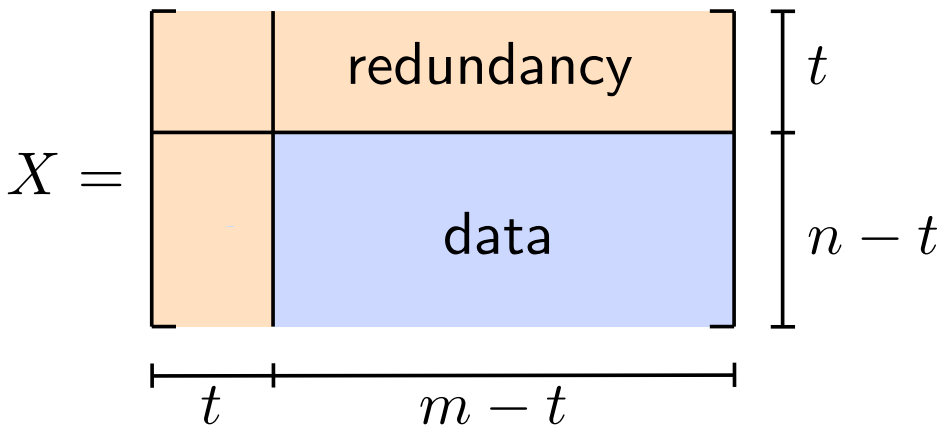
Let $\mathcal{T}_{n\times m,t}$ be the set of $n \times m$ matrices over $\mathbb{F}_q$ with rank t.

Proposition

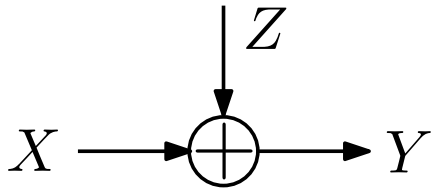
$$C_{\text{AMC}} = nm - \log_q |\mathcal{T}_{n\times m,t}|.$$

For large m or large q,

$$C_{\text{AMC}} \approx (m-t)(n-t).$$



AMC: A Coding Scheme



Strategy: Error Trapping

The all-zero rows and columns of X can be seen as "error traps" that help determine the error matrix Z.

Error trapping works if enough of $\text{rank}(Z)$ "falls into" the traps.

$$X = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \\ 0 & & \end{bmatrix} \quad \begin{matrix} t \\ n-t \end{matrix} \qquad \begin{matrix} t & m-t \end{matrix}$$

AMC: A Coding Scheme

Data matrix: $D \in \mathbb{F}_q^{(n-t)\times(m-t)}$

Transmitted and error matrices:

$$X = \begin{bmatrix} 0 & 0 \\ 0 & D \end{bmatrix} \qquad Z = \begin{bmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{bmatrix}$$

With high probability, rank $Z_1 = t$. Assume this is the case. Gaussian elimination on Z would give:

$$\begin{bmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{bmatrix} \xrightarrow{\text{row op.}} \begin{bmatrix} I & \bar{Z}_2 \\ Z_3 & Z_4 \end{bmatrix} \xrightarrow{\text{row op.}} \begin{bmatrix} I & \bar{Z}_2 \\ 0 & 0 \end{bmatrix}$$

Received matrix:

$$Y = X + Z = \begin{bmatrix} Z_1 & Z_2 \\ Z_3 & D + Z_4 \end{bmatrix} \xrightarrow{\text{row op.}} \begin{bmatrix} I & \bar{Z}_2 \\ 0 & D \end{bmatrix}.$$

AMC: A Coding Scheme

- Decoding amounts to performing t steps of Gaussian elimination on the received matrix Y.

  Complexity: $\mathcal{O}(tnm)$ operations in $\mathbb{F}_q$.

- The probability of failure can be bounded as:

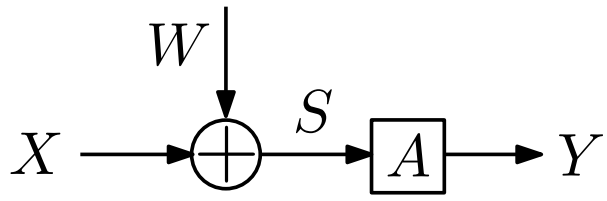
$$P_f < \frac{2t}{q^{1+\epsilon m}}.$$

Proposition

This coding scheme can achieve the capacity of the AMC when either $q \to \infty$ or $m \to \infty$.

Multiplicative-Additive Matrix Channel

$$Y = A(X + W)$$



$$\begin{cases} S = X + W & \text{Additive Matrix Channel (AMC)} \\ Y = AS & \text{Multiplicative Matrix Channel (MMC)} \end{cases}$$

MAMC: Capacity

Theorem (upper bound)

For $n \leq m/2$,

$$C_{\mathrm{MAMC}} \leq (m-n)(n-t) + \log_q 4(n+1)(t+1).$$

Theorem (lower bound)

Assume $n \leq m$. For any $\epsilon \geq 0$, we have

$$C_{\mathrm{MAMC}} \geq (m-n)(n-t-\epsilon t) - \log_q 4 - \frac{2tnm}{q^{1+\epsilon t}}.$$

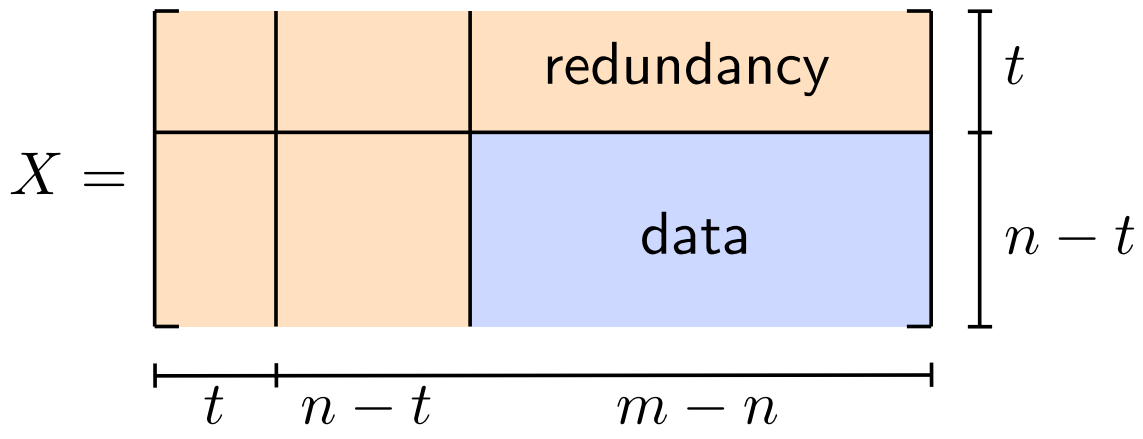
These upper and lower bounds match when $q \to \infty$ or $m \to \infty$.

MAMC: Capacity

Corollary

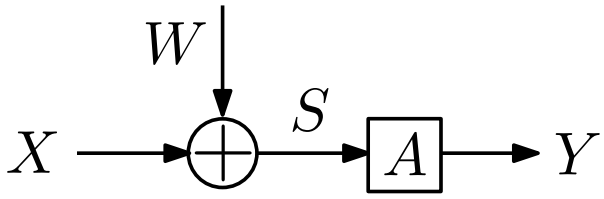
For large m or large q,

$$C_{\mathsf{MAMC}} \approx (m-n)(n-t).$$



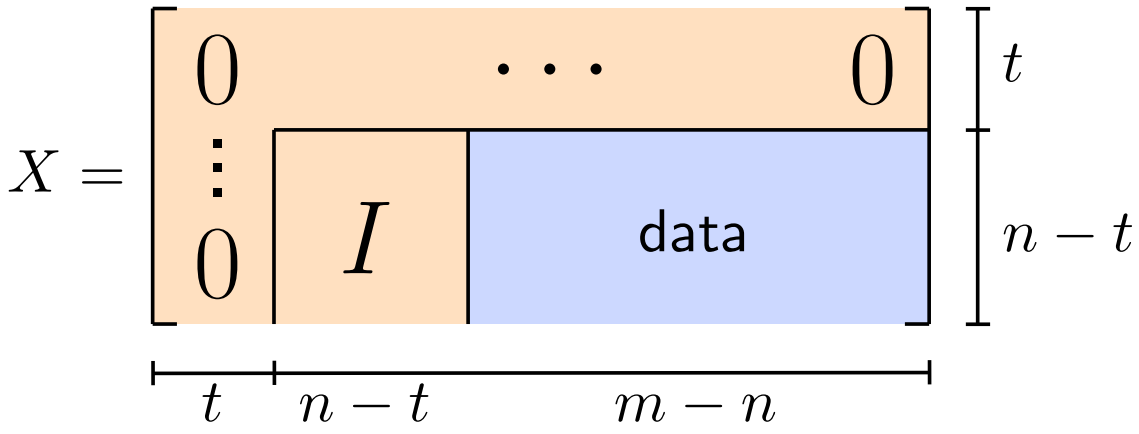
Compare with [MU07]: $R \approx (m-n-t)(n-t)$.

MAMC: A Coding Scheme



Strategy: Channel Sounding + Error Trapping

Use channel sounding "inside" and error trapping "outside" (but not the opposite!)



MAMC: A Coding Scheme

Data matrix: $D \in \mathbb{F}_q^{(n-t)\times(m-n)}$

Transmitted and error matrices:

$$X = \begin{bmatrix} 0 & 0 & 0 \\ 0 & I & D \end{bmatrix} \qquad W = \begin{bmatrix} W_1 & W_2 & W_3 \\ W_4 & W_5 & W_6 \end{bmatrix}$$

As before, assume that rank $W_1 = t$.

Converting $S = X + W$ to reduced row echelon (RRE) form:

$$S = X + W = \begin{bmatrix} W_1 & W_2 & W_3 \\ W_4 & I + W_5 & D + W_6 \end{bmatrix}$$

$$\xrightarrow{\text{row op.}} \begin{bmatrix} I & \bar{W}_2 & \bar{W}_3 \\ 0 & I & D \end{bmatrix} \xrightarrow{\text{row op.}} \begin{bmatrix} I & 0 & \tilde{W}_3 \\ 0 & I & D \end{bmatrix}.$$

But since $Y = AS$, we have $\mathrm{RRE}(Y) = \mathrm{RRE}(S)$.

MAMC: A Coding Scheme

- Decoding amounts to performing full Gaussian elimination on the received matrix Y.

  Complexity: $\mathcal{O}(n^2 m)$ operations in $\mathbb{F}_q$.
  (cubic on the number of symbols, rather than quartic)

- As before, the probability of failure can be bounded as:

$$P_f < \frac{2t}{q^{1+\epsilon m}}.$$

Theorem

This coding scheme can achieve the capacity of the MAMC when either $q \to \infty$ or $m \to \infty$.

Conclusions

When errors occur according to a random model:

1. Less redundancy is required (as compared with an adversarial model): only a single redundant packet for each error packet injected
2. Capacity-achieving codes (for large m or q) can be easily designed by a combination of "channel sounding" and "error trapping". Moreover, decoding is just Gaussian elimination!

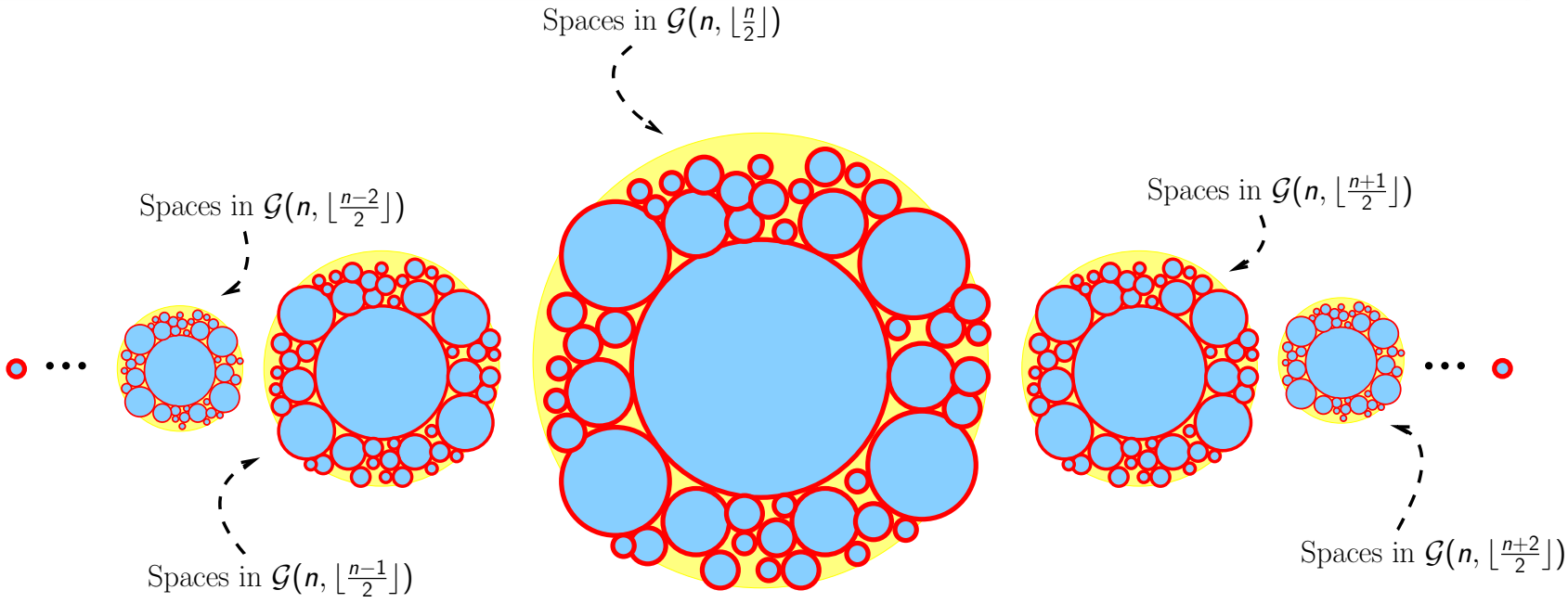
(Question: what to do when q and m are small?)

See also:

M. Jafari Siavoshani, S. Mohajer, C. Fragouli and S. Diggavi, "On the Capacity of Non-Coherent Network Coding," *IEEE Trans. on Inform. Theory*, 2011.
(Considered is an MMC, $Y[t] = G[t]X[t]$, with entries of $G[t]$ chosen iid uniform over $\mathbb{F}_q$.)

Part IV

Beyond Constant Dimension Codes



Representation of Vector Spaces in $\mathcal{P}_q(n)$

Recall ...

Every vector space in $\mathcal{P}_q(n)$ arises **uniquely** as the row-space of a matrix in **Reduced Row Echelon Form (RREF)**.

$$U = \left\langle \begin{bmatrix} 1 & u_{12} & 0 & u_{14} & 0 & 0 & u_{17} \\ 0 & 0 & 1 & u_{24} & 0 & 0 & u_{27} \\ 0 & 0 & 0 & 0 & 1 & 0 & u_{37} \\ 0 & 0 & 0 & 0 & 0 & 1 & u_{47} \end{bmatrix} \right\rangle$$

$$u_{ij} \in \mathbb{F}_q$$

$$V = \left\langle \begin{bmatrix} 1 & v_{12} & v_{13} & 0 & 0 & v_{16} & v_{17} \\ 0 & 0 & 0 & 1 & 0 & v_{26} & v_{27} \\ 0 & 0 & 0 & 0 & 1 & v_{36} & v_{37} \end{bmatrix} \right\rangle$$

$$v_{ij} \in \mathbb{F}_q$$

Representation of Vector Spaces in $\mathcal{P}_q(n)$

Definition:
$V = \langle X \rangle \in \mathcal{P}_q(n)$
where X is in RREF.
$p(V)$, **profile vector** of V:
a binary vector of length n, has non-zero elements **only** in positions where X has a **leading** 1.

$$U = \left\langle \begin{bmatrix} \mathbf{1} & u_{12} & \mathbf{0} & u_{14} & \mathbf{0} & \mathbf{0} & u_{17} \\ \mathbf{0} & 0 & \mathbf{1} & u_{24} & \mathbf{0} & \mathbf{0} & u_{27} \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{1} & \mathbf{0} & u_{37} \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & \mathbf{1} & u_{47} \end{bmatrix} \right\rangle$$

$$\rightarrow p(U) = \mathbf{1}0\mathbf{1}0\mathbf{1}\mathbf{1}0$$

$$V = \left\langle \begin{bmatrix} \mathbf{1} & v_{12} & v_{13} & \mathbf{0} & \mathbf{0} & v_{16} & v_{17} \\ \mathbf{0} & 0 & 0 & \mathbf{1} & \mathbf{0} & v_{26} & v_{27} \\ \mathbf{0} & 0 & 0 & \mathbf{0} & \mathbf{1} & v_{36} & v_{37} \end{bmatrix} \right\rangle$$

$$\rightarrow p(V) = \mathbf{1}00\mathbf{1}\mathbf{1}00$$

Representation of Vector Spaces in $\mathcal{P}_q(n)$

Remark ...

- All the spaces of the form

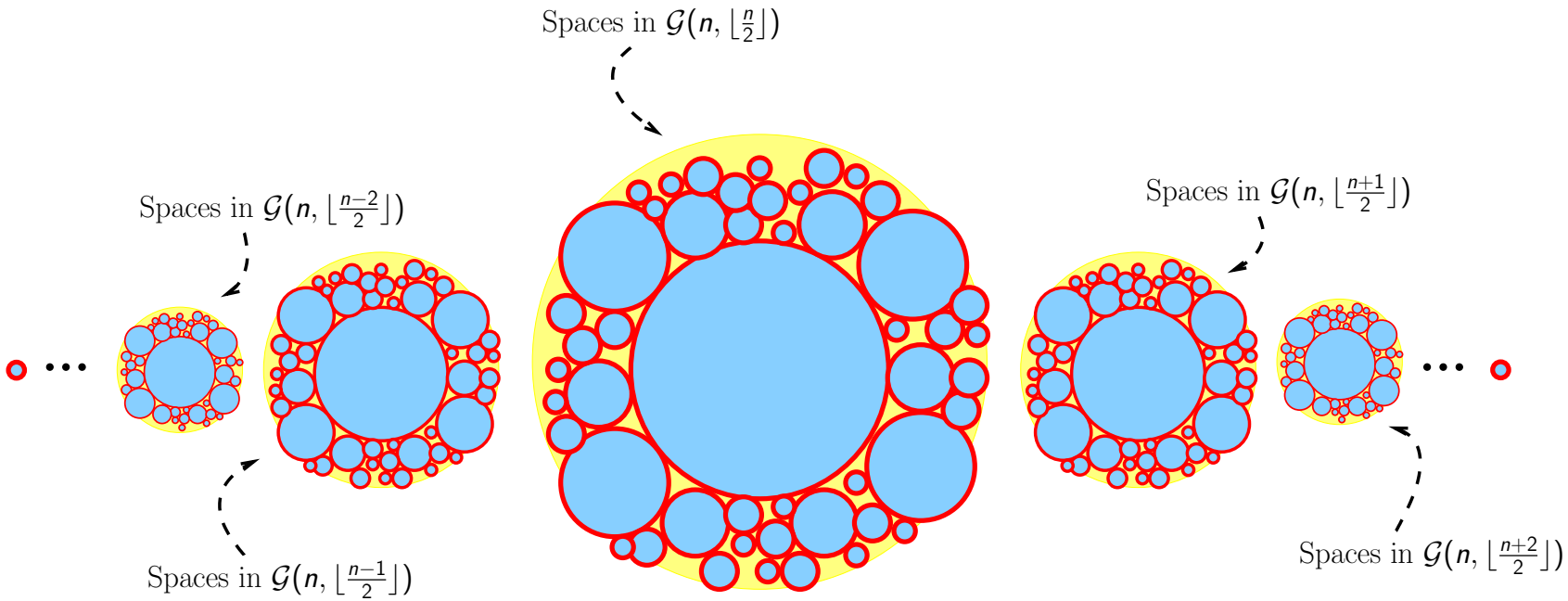
$$U = \left\langle \begin{bmatrix} 1 & \bullet & 0 & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 1 & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{bmatrix} \right\rangle$$

  have 1010110 as their profile vector.

- Such spaces form a *Schubert cell*, i.e., given a binary n-tuple v, define

$$\mathcal{S}(v) = \{U \in \mathcal{P}_q(n) : p(U) = v\}.$$

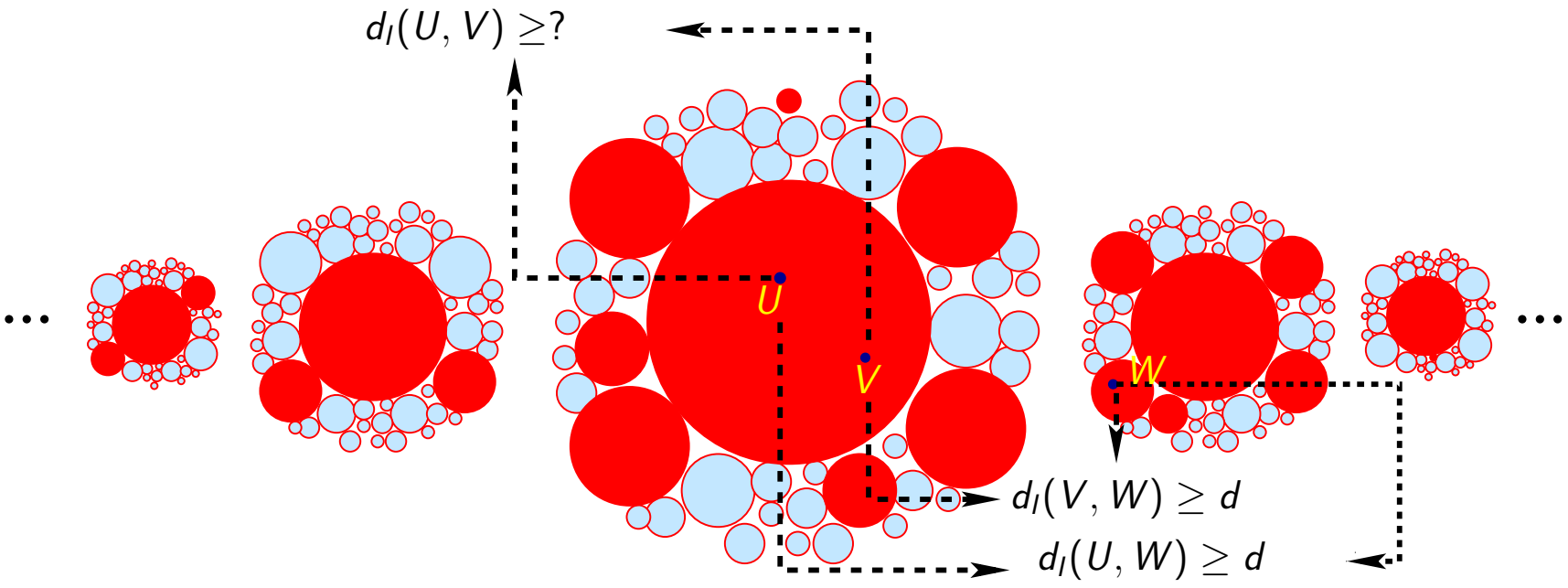
Partitioning $\mathcal{P}_q(n)$



1. Vector spaces within each **Schubert cell** have the **same** profile vector.
2. The cell with profile vector $\overbrace{111\cdots1}^{k}\overbrace{0\cdots000}^{n-k}$ is called the **Principal Schubert cell** in $\mathcal{G}_q(n,k)$.
3. $\mathcal{P}_q(n)$ is **mostly** occupied by $\mathcal{G}(n, \lfloor \frac{n}{2} \rfloor)$.
4. $\mathcal{G}(n,\cdot)$ is **mostly** occupied its **principal Schubert cell**.

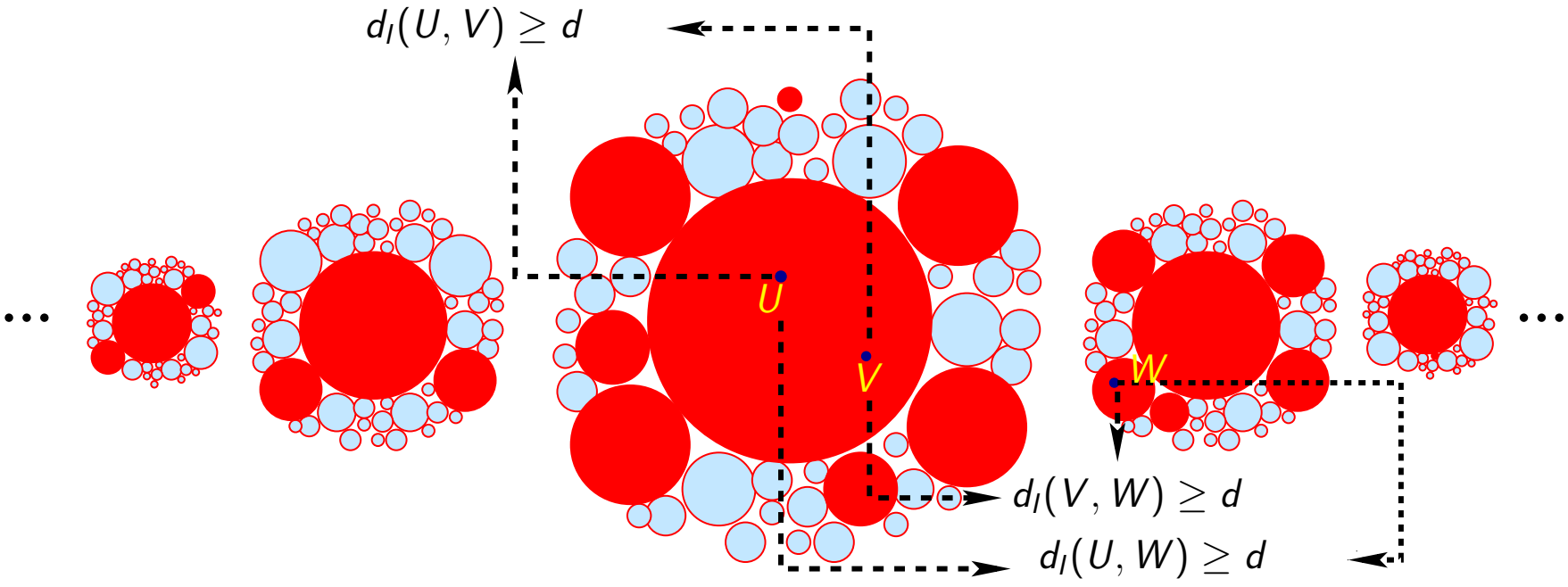
Code Design: Step I

Select a set of *cells* in $\mathcal{P}_q(n)$ with *minimum inter-cell distance* d.



Code Design: Step II

Select a **subset** of vector-spaces **within each cell** with *minimum intra-cell distance* d.

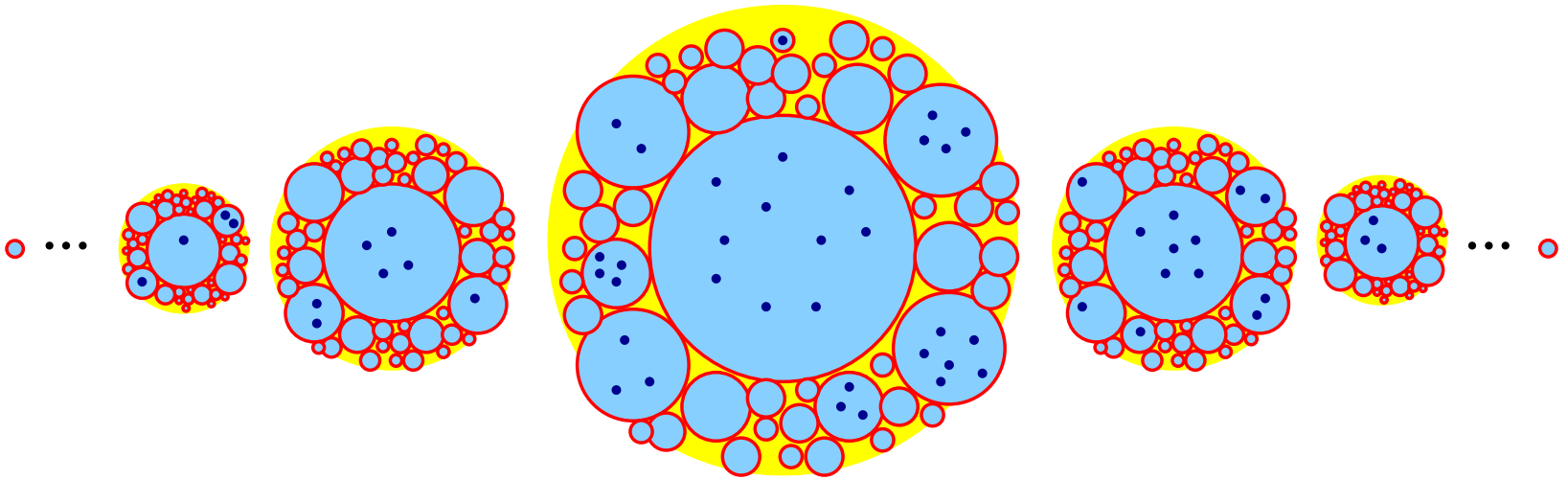


Code Construction in $\mathcal{P}_q^n$

Code Construction Problem:

Given a minimum injection distance d construct a set $\mathcal{C} \subseteq \mathcal{P}_q^n$ such that,

$$\textbf{for all } U, V \in \mathcal{C}\ d(U, V) \geq d.$$



•'s in the figure represent spaces in $\mathcal{P}_q(n)$ selected to be in $\mathcal{C}$.

Preserving the Inter-Cell Distance

Definition: For $x,\ y\ \in \{0,1\}^n$ let $N(x,y)$ the number of $1 \to 0$ transitions from x to y.

Example:

$$\begin{aligned} x &= (1\mathbf{11}000) \\ y &= (1\mathbf{00}101) \\ \to &\quad \mathbf{N(x,y) = 2} \end{aligned}$$

Theorem: Let U and V be two vector spaces in $\mathcal{P}_q^n$, with profile vectors u and v, respectively. Then,

$$d(U,V) \geq \max\{N(u,v), N(v,u)\} = d_a(u,v)$$

$\Rightarrow$ Select the profile vectors according to a **binary asymmetric code** with minimum distance $d_a \geq d$.

Previous result [ES09]: $d_S(U,V) \geq d_H(u,v)$.

Preserving the Intra-Cell Distance

We already know the solution for spaces of the form,

$$\begin{bmatrix} 1 & 0 & 0 & \bullet & \bullet & \bullet & \bullet \\ 0 & 1 & 0 & \bullet & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & \bullet & \bullet & \bullet & \bullet \end{bmatrix} \rightarrow \begin{bmatrix} \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet \end{bmatrix}$$

(lifted rank-metric code construction of [KK08])
What about spaces in other cells?

$$\begin{bmatrix} 1 & \bullet & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{bmatrix} \rightarrow \begin{bmatrix} \bullet & \bullet & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{bmatrix} \rightarrow \begin{bmatrix} \bullet & \bullet \\ 0 & \bullet \end{bmatrix}$$

Remark ... For two spaces $U = \langle X \rangle$ and $V = \langle Y \rangle$ with the same profile vector, $d(U, V) = \mathrm{rank}(X - Y) = d_R(X, Y)$.

Preserving the Intra-Class Distance

For example for $M = \begin{bmatrix} \bullet & \bullet & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \end{bmatrix}$ we may take a subcode $C' \subseteq C$ such that,

every $c \in C'$ has the form $\begin{bmatrix} r_{11} & r_{12} & r_{13} & r_{14} \\ 0 & 0 & r_{23} & r_{24} \\ 0 & 0 & r_{33} & r_{34} \end{bmatrix}$ where, $r_{ij} \in \mathbb{F}_q$, and C is a rank-metric code.

Theorem:

If M is an $m \times n$ matrix with a total of w $\bullet$'s, C' is the *largest subcode* of a linear MRD code with $d_R(C') = \delta$, we have

$$\dim(C)' \geq w - \max\{m, n\}(\delta - 1)$$

Selecting the Profile Vectors

Intuitively we would like to select profile vectors that result in lifted rank-metric codes of highest cardinality.

Example:

$$1001100 \rightarrow \begin{bmatrix} 1 & \bullet & \bullet & 0 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{bmatrix}$$

$$0001010 \rightarrow \begin{bmatrix} 0 & 0 & 0 & 1 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{bmatrix}$$

1001100 would be preferable over 0001010.

Our Profile Selection Algorithm

Given a minimum asymmetric distance $d_a \geq d$,

1. First, we calculate **a score** for each $v \in \{0,1\}^n$ based on **the dimension of the lifted rank-metric code induced by** v.
2. Then, we use a standard greedy algorithm that,
   - Maintains a list of available profile vectors $A \subseteq \{0,1\}^n$.
   - At each step an available profile vector $v \in A$ with **the highest score** is added, and vectors within asymmetric distance d of v are made unavailable.
   - The algorithm proceeds until $A = \emptyset$.

A Small Example

For $n = 5$, $q = 2$ and $d = 2$ we obtain a total of 14 codewords.

$v \in \{0,1\}^5$	$2^{\text{score}(v,d)}$
11100	8
10010	2
11111	1
01011	1
01000	1
00101	1

Numerical Results ($q = 2$)

n	d	[KK08]	$\log_q \lvert C_1 \rvert$	$\log_q \lvert C_2 \rvert$
5	2	**3**	**3.16993**	**3.80735**
6	2	**6**	**6.14975**	**6.39232**
6	3	**3**	**3.16993**	**3.45943**
7	2	**8**	**8.17991**	**8.69000**
7	3	**4**	**4.08746**	**4.24793**
8	2	**12**	**12.1595**	**12.3633**
8	4	**4**	**4.08746**	**4.24793**
9	2	**15**	**15.1731**	**15.6402**
9	4	**5**	**5.04439**	**5.12928**
11	2	**24**	**24.1582**	**24.6321**
12	6	**6**	**6.02237**	**6.06609**
13	2	**35**	**35.1586**	**35.6303**
13	3	**28**	**28.0032**	**28.0265**
14	7	**7**	**7.01123**	**7.03342**
15	2	**48**	**48.1586**	**48.6291**

C_1 = our *non-constant-dimension* codes for d_S.
C_2 = our *non-constant-dimension* codes for d.

More Constructions

1. Gadouleau, M., Yan, Z.: Packing and covering properties of Subspace Codes for Error Control in Random Linear Network Coding, *IEEE Trans. on Inf. Theory*, 2010.
2. Etzion, T., Vardy, A.: Error-correcting codes in projective space, *IEEE Trans. on Inf. Theory*, 2011.
3. Ahlswede, R., Aydinian, H.: On error control for random network coding. *IEEE Workshop on Network Coding, Theory and Applications*, 2009.
4. Skachek, V.: Recursive code construction for random networks, *IEEE Trans. on Inf. Theory*, 2010.
5. Manganiello, F., Gorla, E., Rosenthal, J.: Spread codes and spread decoding in network coding. *ISIT*, 2008.
6. Gabidulin, E., Bossert, M.: Algebraic codes for network coding, *Probl. Peredach. Inf*, 2009.
7. Etzion, T., Silberstein, N.: Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inf. Theory*, 2009.
8. Kohnert, A., Kurz, S.: Construction of large constant dimension codes with a prescribed minimum distance. *Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth* (2008) 31–42

Conclusions

Error control in random linear network coding introduces new and interesting problems in coding theory:

- Construction of codes on the Grassmann graph,
- or in the underlying projective geometry,
- decoding algorithms,
- bounds, etc.

No time to talk about:

- security against wiretappers in networks with random linear network coding (an Ozarow-Wyner-type coset coding scheme based on lifted rank-metric codes) — see Silva and Kschischang, *IEEE Trans. Inf. Theory*, 2011.
- lattice-based physical-layer network coding, implementing a form of Nazer-Gastpar compute-and-forward relaying — see tomorrow's talk by C. Feng.