Algebraic Codes for Random Linear Network Coding

Maximilien Gadouleau

Crestic
Université de Reims Champagne-Ardenne

August 21, 2009

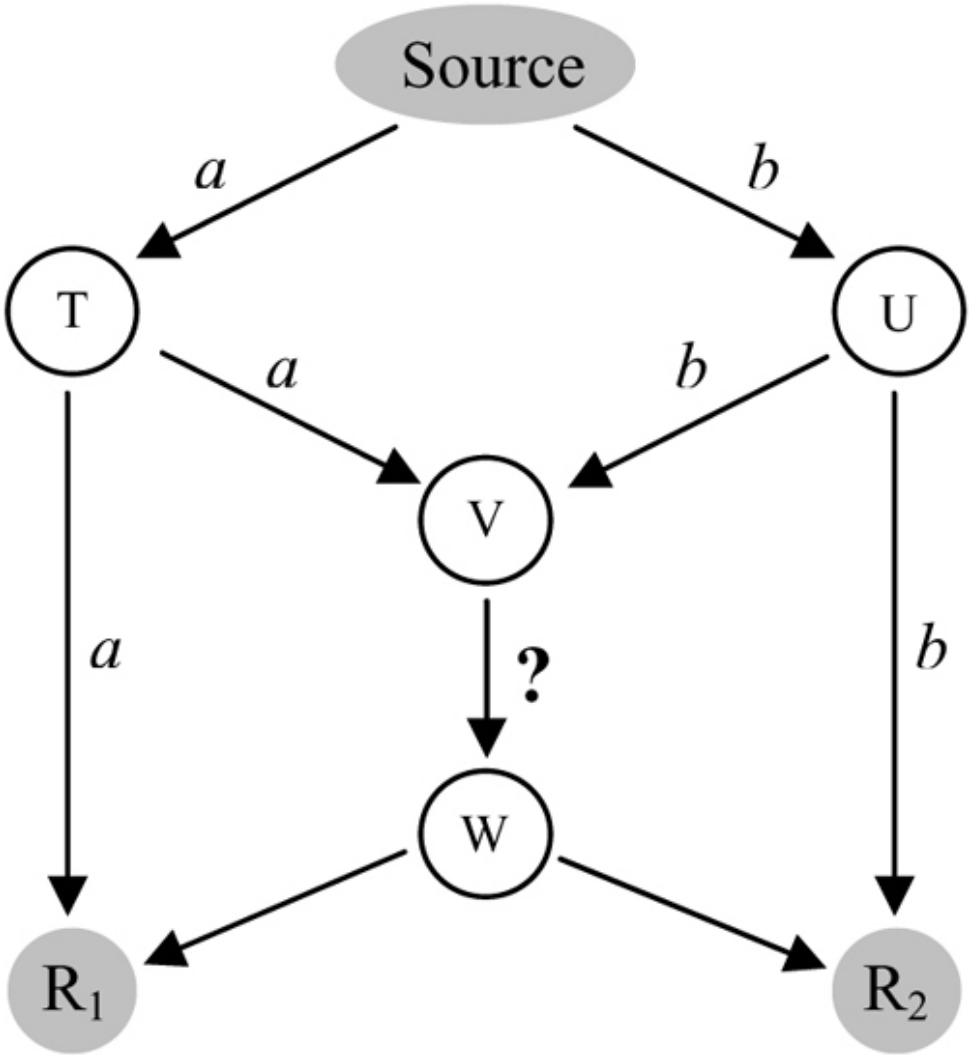
Outline

Outline

Network coding

- Traditional routing: store and forward.
  Does not achieve the highest throughput for multicast
- Network coding allows intermediate nodes to combine packets
- Only perform linear combinations of packets.
  $\Rightarrow$ Linear network coding
- Results in higher throughput for multicast, robustness, and adaptability

Network coding example



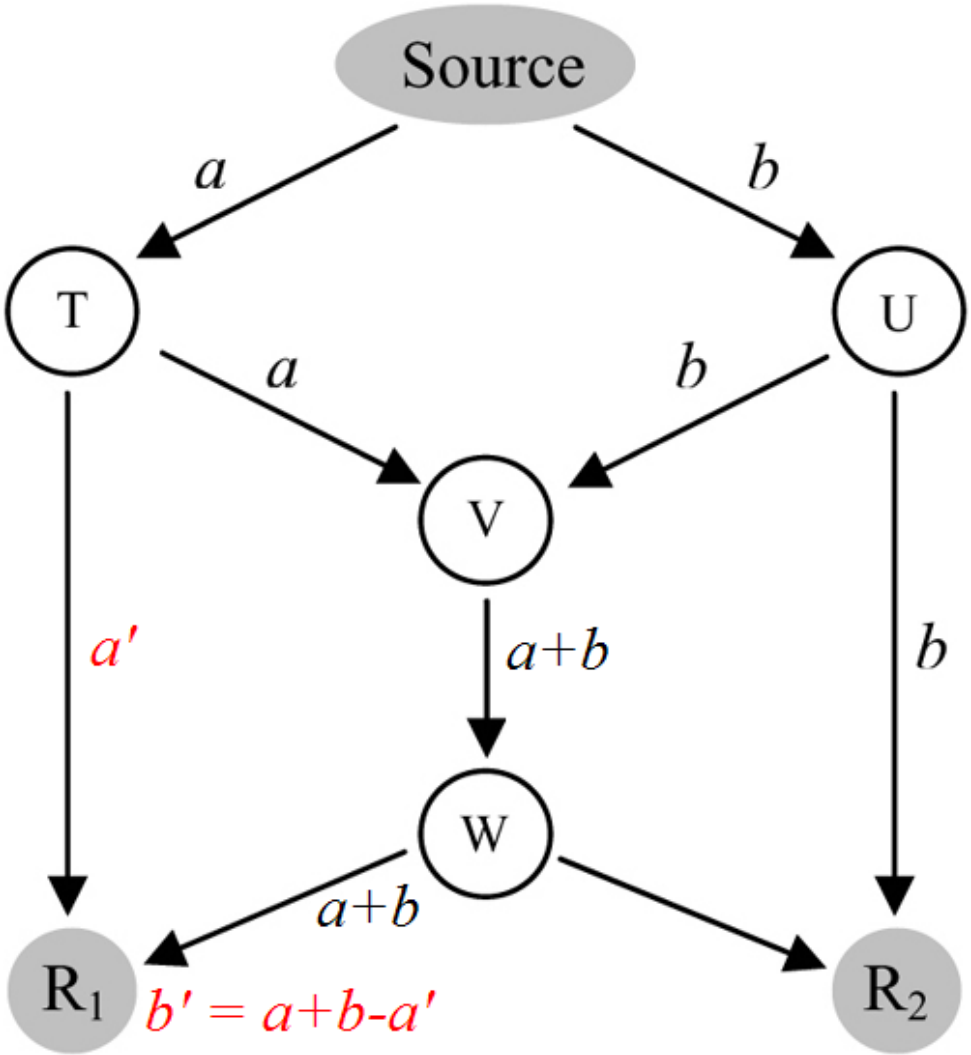
Random linear network coding (RLNC)

- Fixing the linear combinations requires knowledge of the network and is too rigid
- Solution: choosing linear combinations at random
- In example, 1 chance out of 3 to be successful.
  However, probability of success tends to 1 with field size
- Header to keep track of linear combinations.
  $\Rightarrow (\mathbf{I}_r|\mathbf{M})$, where $\mathbf{M} = \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix}$
- Easy to decode: receive $(\mathbf{L}|\mathbf{LM})$, compute $\mathbf{L}^{-1}(\mathbf{LM})$

Error control for RLNC

- RLNC highly sensitive to errors
- Many types of errors
  - Link errors
  - Packet losses
  - Malfunctioning nodes
  - Adversary on the network
- Errors are highly detrimental: one packet error can corrupt all packets after linear combination

Error in network coding example



Operator channel

- RLNC preserves the row space of the input matrix.
  $\Rightarrow$ Modeled as transmission of a linear subspace
- Two ways to modify the subspace
  - Erasure: deletion of a dimension
  - Error: addition of a dimension
- Operator channel: send U, receive

$$V = H(U) \oplus E.$$

  H performs erasures, E are errors
- Error control in RLNC is a coding theory problem, where codewords are subspaces

Projective space and subspace codes

- Subspace code: set of subspaces of $\mathrm{GF}(q)^n$.
  $\Rightarrow$ Subset of the projective space
- Metrics:
  - subspace distance d_S for network errors
  - injection distance d_I for adversarial channels
- V obtained from U after ϵ erasures and ρ errors.

$$\begin{aligned} d_S(U,V) &= \epsilon + \rho = \dim(U+V) - \dim(U \cap V) \\ d_I(U,V) &= \max\{\epsilon, \rho\} = \max\{\dim(U), \dim(V)\} - \dim(U \cap V) \end{aligned}$$

- For any subspace code, $d_I(\mathcal{C}) \leq d_S(\mathcal{C}) \leq 2d_I(\mathcal{C})$

Grassmannian and CDCs

- Constant-dimension code (CDC): set of subspaces of $\mathrm{GF}(q)^n$ with dimension r.
  $\Rightarrow$ Subset of the Grassmannian
- $d_S(U^\perp, V^\perp) = d_S(U, V) \Rightarrow$ assume $r \leq \frac{n}{2}$
- Advantages:
  - $d_S(\mathcal{C}) = 2d_I(\mathcal{C})$ for a CDC.
    $\Rightarrow$ Versatility, and maximum d_S
  - Simplified decoding procedure
- Relation to rank metric codes through the lifting operation

Rank metric codes

- Rank metric code: set of matrices in $\mathrm{GF}(q)^{m\times n}$
- Applications to data storage, cryptography, space-time coding
- Rank distance: $d_{\mathrm{R}}(\mathbf{M},\mathbf{N}) = \mathrm{rk}(\mathbf{M}-\mathbf{N})$.
  $d_{\mathrm{R}}(\mathbf{M}^T,\mathbf{N}^T) = d_{\mathrm{R}}(\mathbf{M},\mathbf{N}) \Rightarrow$ assume $m \geq n$
- Optimal codes: MRD codes. Gabidulin codes: RS-like MRD codes. Decoding algorithms for Gabidulin codes

Liftings of rank metric codes

- Lifting: $\mathbf{M} \in \mathrm{GF}(q)^{m\times n}$, $I(\mathbf{M})$ is the row space of $(\mathbf{I}_m|\mathbf{M})$
- $d_\mathrm{I}(I(\mathbf{M}), I(\mathbf{N})) = d_\mathrm{R}(\mathbf{M}, \mathbf{N})$
- $\mathcal{C}$ rank metric code in $\mathrm{GF}(q)^{r\times(n-r)}$.
  $\Rightarrow I(\mathcal{C})$ CDC, and $d_\mathrm{S}(I(\mathcal{C})) = 2d_\mathrm{I}(I(\mathcal{C})) = 2d_\mathrm{R}(\mathcal{C})$
- Error control in RLNC using liftings is a rank metric problem
- KK code: lifting of (transposed) Gabidulin code.
  Nearly optimal CDC, bounded subspace distance decoding algorithm

Overview of results

- Rank metric codes
  - Covering properties *(IT 08 + to appear in CL 09)*
  - MacWilliams identity *(EURASIP 08)*
  - DEP *(IT 08)*
  - Constant-rank codes *(submitted to IT)*
- CDCs
  - Construction and covering properties of CDCs *(submitted to IT)*
  - DEP of CDCs *(submitted to IT)*
- Subspace codes: Packing and covering properties *(submitted to IT)*

Outline

Rank metric codes

- Sphere covering
  - Geometric properties (volumes of balls and their intersections)
  - Bounds and constructions
  - Covering radius of known codes
- MacWilliams identity
  - Polynomial form previously unknown
  - Binomial and power moments of the rank distribution
- Decoder error probability
  - Exact DEP of codes given their distance distribution
  - Upper bounds on the DEP
  - MRD codes have the highest DEP up to a scalar

CRCs

- Motivation: study CDCs and their relations to rank metric codes
- Constant-rank code (CRC): rank metric code where all codewords have the same rank
- Row space of a CRC is a CDC with related minimum distance
- Optimal CRC in $\mathrm{GF}(q)^{m\times n}$ with rank r and $d_\mathrm{R} = d + r$ for m large enough.
  $\Rightarrow$ Row space: optimal CDC of length n and dimension r with $d_\mathrm{I} = d$
- We also study CRCs. Many results for $d_\mathrm{R} \leq r$, fewer for $d_\mathrm{R} > r$

Outline

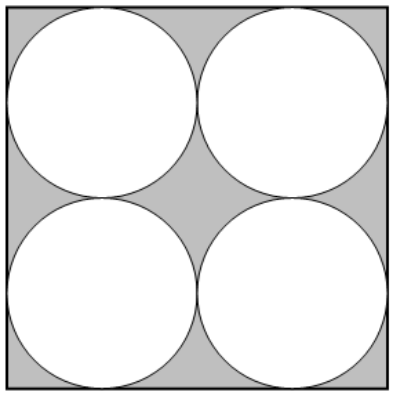
DEP of CDCs

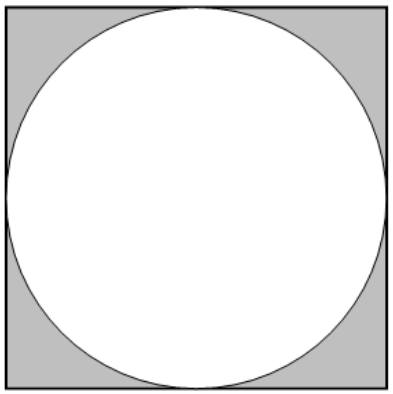
- Two decoders: bounded subspace distance, bounded injection distance
- Bounded distance decoder (BDD): finds the unique nearest codeword at distance $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$
- Decoder has three outputs: success, failure, or error.
  Success iff received subspace at distance $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$.
  Error or failure otherwise
- Error more detrimental than failure.
  $\Rightarrow$ Focus on decoder error probability (DEP)

DEP of CDCs

- Symmetric operator channel: all subspaces after ϵ erasures and ρ errors equiprobable.
  $\Rightarrow$ Same dimension and same distance are equiprobable
- Results:
  - Exact DEP for all CDCs based on distance distribution
  - Bounds on the DEP of all liftings
  - Liftings of MRD have maximum DEP up to a scalar
- Bounded subspace distance decoder corrects more errors and has higher DEP than bounded injection decoder

Sphere packing





- How many spheres of same radius can be packed in a space?
  $\Rightarrow$ Max cardinality of a code with a given minimum distance $A(d)$
- Crucial for error correcting code design

Construction of CDCs

- KK code $\mathcal{E}^0$: $\mathcal{D}^0 \subseteq \mathrm{GF}(q)^{r\times(n-r)}$ is a (transposed) Gabidulin code with $d_\mathrm{R} = d$, where $d_\mathrm{S} = 2d_\mathrm{I} = 2d$.
  $E^0_{0,j} = R(\mathbf{I}_r|\mathbf{D}^0_j)$
- Layer $\mathcal{E}^k$ for $1 \leq k \leq \left\lfloor \frac{r}{d} \right\rfloor$: $\mathcal{C}^k \subseteq \mathrm{GF}(q)^{(r-kd)\times kd}$, $\mathcal{D}^k \subseteq \mathrm{GF}(q)^{r\times(n-r-kd)}$ are (transposed) Gabidulin codes with $d_\mathrm{R} = d$ or trivial codes.
  $$E^k_{i,j} = R\left(\begin{array}{c|c|c|c} \mathbf{I}_{r-kd} & \mathbf{C}^k_i & \mathbf{0} & \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{I}_{kd} & \mathbf{D}^k_j \end{array}\right)$$
- Augmented KK code $\mathcal{E} = \bigcup_{k=0}^{\left\lfloor \frac{r}{d} \right\rfloor} \mathcal{E}^k$

Augmented KK codes

- $d_{\mathrm{I}}(R(\mathbf{A}), R(\mathbf{B})) \geq d_{\mathrm{I}}(R(\mathbf{A}_1), R(\mathbf{B}_1))$, where $\mathbf{A}_1$, $\mathbf{B}_1$ are subsets of columns
  $\Rightarrow d_{\mathrm{I}} = d, d_{\mathrm{S}} = 2d_{\mathrm{I}} = 2d$
- Properly contains a KK code. Greatest cardinality for $d < r$
- Enhanced BDD for augmented KK code:
  - Corrects more than bounded subspace distance decoder
  - Complexity on the same order as BDD of KK code

EBDD$(k, \mathbf{A})$

Input: k and $\mathbf{A} = (\mathbf{A}_1|\mathbf{A}_2|\mathbf{A}_3)$, $\mathbf{A}_1 \in \mathrm{GF}(q)^{a\times(r-kd)}$, $\mathbf{A}_2 \in \mathrm{GF}(q)^{a\times kd}$, $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$
Output: $(E^k_{i,j}, d_k, f_k)$

1. If $k = 0$, decoder of $\mathcal{E}^0 \Rightarrow E^0_{0,j}$, calculate $d_k = d_S(R(\mathbf{A}), E^0_{0,j})$, and return $(E^0_{0,j}, d_k, 0)$
2. Decoder of $I(\mathcal{C}^k)$ on $(\mathbf{A}_1|\mathbf{A}_2) \Rightarrow \mathbf{C}^k_i$
3. Decoder of $I(\mathcal{D}^k)$ on $(\mathbf{A}_1|\mathbf{A}_3) \Rightarrow \mathbf{D}^k_j$
4. Calculate $d_k = d_S(R(\mathbf{A}), E^k_{i,j})$,
   $f_k = 2d - \max\{d_S(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_i)), d_S(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}^k_j))\}$,
   and return $(E^k_{i,j}, d_k, f_k)$

Decoder for $\mathcal{E}$

Input: $\mathbf{A} = (\mathbf{A}_0|\mathbf{A}_3)$, $\mathbf{A}_0 \in \mathrm{GF}(q)^{a\times r}$, $\mathbf{A}_3 \in \mathrm{GF}(q)^{a\times(n-r)}$
Output: The unique nearest codeword in $\mathcal{E}$ from $R(\mathbf{A})$ or failure

1. If $\mathrm{rk}(\mathbf{A}) < r-d+1$, return failure
2. Calculate $r-\mathrm{rk}(\mathbf{A}_0) = ld+m$, with $0 \le l \le \left\lfloor \frac{r}{d} \right\rfloor$ and $0 \le m < d$
3. $\mathrm{EBDD}(l,\mathbf{A}) \Rightarrow (E^l_{i,j}, d_l, f_l)$. If $d_l \le d-1$, return $E^l_{i,j}$
4. If $m = 0$, return failure.
   Otherwise $\mathrm{EBDD}(l+1,\mathbf{A}) \Rightarrow (E^{l+1}_{s,t}, d_{l+1}, f_{l+1})$.
   If $d_{l+1} \le d-1$, return $E^{l+1}_{s,t}$
5. If $d_l < \min\{d+m, f_l, d_{l+1}, f_{l+1}, 2d-m\}$, return $E^l_{i,j}$.
   If $d_{l+1} < \min\{d+m, d_l, f_l, f_{l+1}, 2d-m\}$, return $E^{l+1}_{s,t}$
6. Return failure

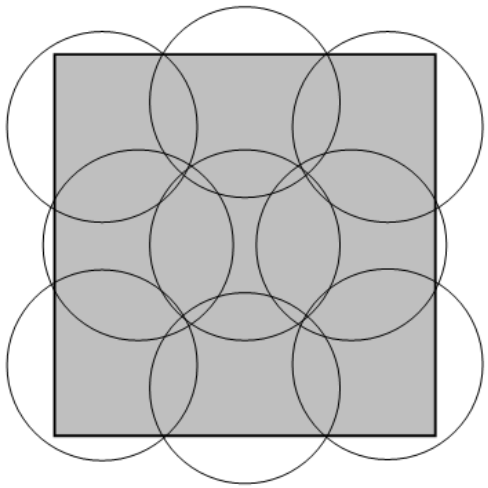
Packing properties of subspace codes

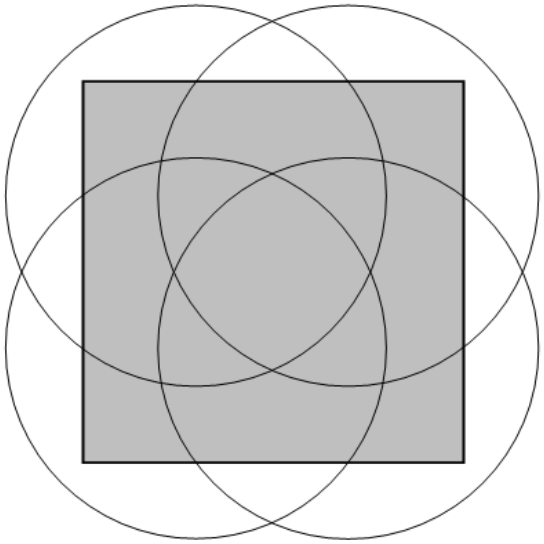
- Max cardinality of a subspace code (resp., CDC) with minimum injection distance d: $A_{\mathrm{I}}(d)$ (resp., $A_{\mathrm{C}}(r,d)$)
- Upper bound:

$$A_{\mathrm{I}}(d) \leq \sum_{r} A_{\mathrm{C}}(r,d) \sim A_{\mathrm{C}}\left(\left\lfloor \frac{n}{2} \right\rfloor, d\right)$$

- Lower bound: $A_{\mathrm{I}}(d) \geq A_{\mathrm{C}}(r,d)$. Nearly tight for $r = \left\lfloor \frac{n}{2} \right\rfloor$
- Same situation for the subspace metric: $A_{\mathrm{S}}(d) \sim A_{\mathrm{C}}(\left\lfloor \frac{n}{2} \right\rfloor, \left\lceil \frac{d}{2} \right\rceil)$
- CDCs optimal up to a scalar for both metrics.
  $\Rightarrow$ Nearly optimal codes in the injection metric with $d_{\mathrm{S}} = 2d_{\mathrm{I}}$

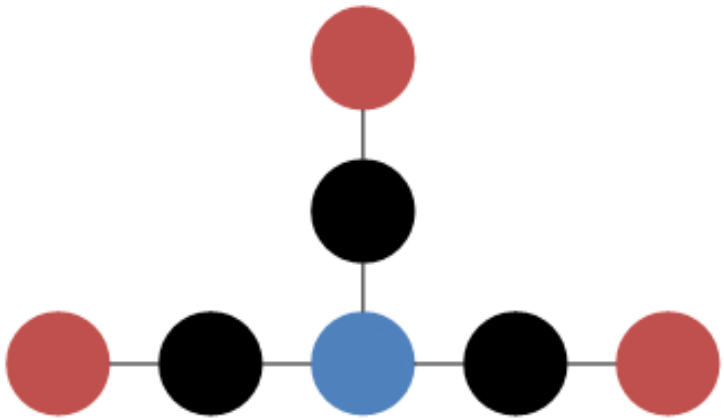
Sphere covering





- How many spheres needed to cover a space?
  $\Rightarrow$ Min cardinality of a code with a given covering radius $K(\rho)$
- Applications: minimum distance decoding, decoding with erasures, data compression
- Sphere covering bound: $K(\rho) \geq \frac{|E|}{\max V(\rho)}$
- Greedy upper bound: $K(\rho) \lesssim \frac{|E|}{\min V(\rho)}$

Sphere covering example



- Sphere covering bound: $K(1) \geq \left\lceil \frac{7}{4} \right\rceil = 2$
- Greedy construction: $K(1) \leq 4$
- However, $K(1) = 3$

Covering properties of CDCs

- We study how CDCs cover the Grassmannian.
  Min cardinality of a CDC with covering radius ρ: $K_{\mathrm{C}}(r, \rho)$
- Volume of a ball equal for all centers.
  $\Rightarrow$ Sphere covering bound asymptotically tight
- The Grassmannian with the injection metric is an association scheme.
  Intersection of two spheres with radii u and s and distance between their centers d: $J_{\mathrm{C}}(u, s, d)$
- Refinement of the sphere covering bound based on linear programming

Refined sphere covering bound for CDCs

- For $0 \leq \delta \leq \rho$, let $T_\delta = \min \sum_{i=0}^{r} A_i(\delta)$, subject to

$$\begin{aligned} A_i(\delta) &= 0 \text{ for } 0 \leq i \leq \delta - 1, \\ 1 \leq A_\delta(\delta) &\leq N_{\mathrm{C}}(\delta), \\ 0 \leq A_i(\delta) &\leq N_{\mathrm{C}}(i) \text{ for } \delta + 1 \leq i \leq r, \\ \sum_{i=0}^{r} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{C}}(l, s, i) &\geq N_{\mathrm{C}}(l) \text{ for } 0 \leq l \leq r. \end{aligned}$$

  Then $K_{\mathrm{C}}(r, \rho) \geq \max_{0 \leq \delta \leq \rho} T_\delta$

- Proof: U subspace at distance δ from a CDC with covering radius ρ, $A_i(\delta)$ distance distribution from U

Covering with liftings

- Liftings have covering radius r. Proof: consider $R(\mathbf{0}_r|\mathbf{M})$.
  $\Rightarrow$ Liftings are not optimal packing CDCs
- Construction of covering CDCs based on liftings.
  Min cardinality of a code with rank radius ρ: $K_{\mathrm{R}}(\rho)$
- $\mathcal{C}$ optimal rank metric covering code.
  $L(\mathcal{C})$: all possible permutations of liftings of codewords in $\mathcal{C}$.
  $\Rightarrow |L(\mathcal{C})| \leq \binom{n}{r} K_{\mathrm{R}}(\rho)$
- $L(\mathcal{C})$ has covering radius ρ. Proof: all subspaces are permutations of liftings
- Asymptotically optimal but not good for finite values

Covering in the injection metric

- Min cardinality of a subspace code with injection covering radius ρ: $K_{\mathrm{I}}(\rho)$
- Volume of a ball depends on the dimension of its center
- However, $V_{\mathrm{I}}(r,\rho) \sim f(\rho)$.
  $\Rightarrow$ Sphere covering bound asymptotically tight
- Construction using covering CDCs: $K_{\mathrm{I}}(\rho) \leq \sum_{r=0}^{n} K_{\mathrm{C}}(r,\rho)$.
  Asymptotically optimal

Covering in the subspace metric

- Min cardinality of a subspace code with subspace covering radius ρ: $K_{\mathrm{S}}(\rho)$
- Volume of a ball depends on the dimension of its center and $V_{\mathrm{S}}(r,\rho) \sim g(r,\rho)$
- Sphere covering bound, construction using CDCs: not asymptotically tight
- We derive asymptotically tight lower and upper bounds

Outline

Conclusion and Future Work

- Summary of results
- Future work:
  - RLNC: implementation and related problems
  - Constructions of packing and covering CDCs and subspace codes
  - Connection between subspace codes and rank metric codes
  - Decoding of error control codes for RLNC

Definitions of subspace and injection metrics

$$\begin{aligned} d_{\mathrm{S}}(U,V) &= \dim(U+V) - \dim(U \cap V) \\ &= \dim(U) + \dim(V) - 2\dim(U \cap V) \\ &= 2\dim(U+V) - \dim(U) - \dim(V) \end{aligned}$$

$$\begin{aligned} d_{\mathrm{I}}(U,V) &= \frac{1}{2} d_{\mathrm{S}}(U,V) + \frac{1}{2} |\dim(U) - \dim(V)| \\ &= \max\{\dim(U), \dim(V)\} - \dim(U \cap V) \\ &= \dim(U+V) - \min\{\dim(U), \dim(V)\} \end{aligned}$$

$$|\dim(U) - \dim(V)| \leq d_{\mathrm{I}}(U,V) \leq d_{\mathrm{S}}(U,V) \leq \dim(U) + \dim(V)$$

Injection distance of liftings

For $\mathbf{M}, \mathbf{N} \in \mathrm{GF}(q)^{r\times(n-r)}$,

$$\begin{aligned} d_{\mathrm{I}}(I(\mathbf{M}), I(\mathbf{N})) &= \mathrm{rk}\left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{M} \\ \hline \mathbf{I}_r & \mathbf{N} \end{array}\right) - r \\ &= \mathrm{rk}\left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{M} \\ \hline 0 & \mathbf{M}-\mathbf{N} \end{array}\right) - r \\ &= \mathrm{rk}(\mathbf{M}-\mathbf{N}) \end{aligned}$$

CRCs

Theorem

For all $\mathbf{X}, \mathbf{Y} \in \mathrm{GF}(q)^{m\times n}$,

$$\begin{aligned} & d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})) + d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y})) - |\mathrm{rk}(\mathbf{X}) - \mathrm{rk}(\mathbf{Y})| \\ & \leq d_{\mathrm{R}}(\mathbf{X}, \mathbf{Y}) \\ & \leq \min\{d_{\mathrm{I}}(R(\mathbf{X}), R(\mathbf{Y})), d_{\mathrm{I}}(C(\mathbf{X}), C(\mathbf{Y}))\} + \min\{\mathrm{rk}(\mathbf{X}), \mathrm{rk}(\mathbf{Y})\}. \end{aligned}$$

Therefore, for a CRC $\mathcal{C}$:

$$d_{\mathrm{I}}(R(\mathcal{C})) + d_{\mathrm{I}}(C(\mathcal{C})) \leq d_{\mathrm{R}}(\mathcal{C}) \leq \min\{d_{\mathrm{I}}(R(\mathcal{C})), d_{\mathrm{I}}(C(\mathcal{C}))\} + r.$$

Optimal CRCs

Proposition

For all q, $2 \leq d \leq r \leq n \leq m$,

$$\min\{A_{\mathrm{C}}(q,n,r,d), A_{\mathrm{C}}(q,m,r,r)\} \leq A_{\mathrm{R}}(q,m,n,r,d+r) \leq A_{\mathrm{C}}(q,n,r,d).$$

For $2r \leq n$, $A_{\mathrm{C}}(q,n,r,d) \sim q^{(n-r)(r-d+1)}$, $A_{\mathrm{C}}(q,m,r,r) \sim q^{m-r}$.
$\Rightarrow$ For $m \geq (n-r)(r-d+1)+r+1$, $A_{\mathrm{C}}(q,m,r,r) \geq A_{\mathrm{C}}(q,n,r,d)$

f_k

Lemma

Suppose the output of $\mathrm{EBDD}(k, \mathbf{A})$ *is* $(E^k_{i,j}, d_k, f_k)$, *then* $d_S(R(\mathbf{A}), E^k_{u,v}) \geq f_k$ *for any* $E^k_{u,v} \in \mathcal{E}^k$ *provided* $(u,v) \neq (i,j)$.

Proof.

We have

$$f_k = \min\{2d - d_S(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_i)), 2d - d_S(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}^k_j))\}.$$

When $u \neq i$,

$$\begin{aligned} d_S(R(\mathbf{A}), E^k_{u,v}) &\geq d_S(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_u)) \\ &\geq d_S(I(\mathbf{C}^k_i), I(\mathbf{C}^k_u)) - d_S(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_i)) \\ &\geq 2d - d_S(R(\mathbf{A}_1|\mathbf{A}_2), I(\mathbf{C}^k_i)) \geq f_k. \end{aligned}$$

Similarly, when $v \neq j$, we obtain

$$d_S(R(\mathbf{A}), E^k_{u,v}) \geq 2d - d_S(R(\mathbf{A}_1|\mathbf{A}_3), I(\mathbf{D}^k_j)) \geq f_k.$$

□