

Constant-Rank Codes and Their Connection to Constant-Dimension Codes

Maximilien Gadouleau

Department of Electrical and Computer Engineering

Lehigh University

Work done in collaboration with Zhiyuan Yan

June 5, 2008

Outline

- Review: constant-dimension codes and rank metric codes
- Connection between constant-dimension codes and constant-rank codes
- Constant-rank codes
 - Bounds
 - Constructions
 - Asymptotic results

Error correction in network coding

- Random network coding highly susceptible to errors.
⇒ Error control for random network coding crucial
- Some schemes use the network topology, others [KK07] assume no knowledge of the network
- Network coding is done via linear combinations: vector space conservation.
⇒ we consider a vector space is sent, the network adds and deletes some dimensions
- CDC's used for error correction in noncoherent random network coding in [KK07]

Constant-dimension codes (CDC)

- $E_r(q, n)$: set of r -dimensional subsets of $\text{GF}(q)^n$
- Constant-dimension code (CDC): subset of $E_r(q, n)$
- Subspace distance: for $\mathcal{U}, \mathcal{V} \in E_r(q, n)$,

$$d_s(\mathcal{U}, \mathcal{V}) \stackrel{\text{def}}{=} \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V}) = 2 \dim(\mathcal{U} + \mathcal{V}) - 2r$$

- Minimum subspace distance of a code $d_s = 2d$
- $A_s(q, n, 2d, r)$: maximum cardinality of an $(n, 2d, r)$ CDC over $\text{GF}(q)$

Research on constant-dimension codes

- Codes on Grassmannians studied in [Chi87]
- Code construction in [KK07] based on rank metric codes, decoding algorithms
- More upper bounds in [XF08], connection to constant Hamming weight codes
- Maximum cardinality of a CDC with given minimum distance is still unknown
- \Rightarrow we study CDC's via constant rank codes

The rank metric

- $\mathbf{x} = (x_0, \dots, x_{n-1}) \in \text{GF}(q^m)^n$. Expand all the coordinates into m -dimensional vectors over $\text{GF}(q) \Rightarrow \mathbf{X} \in \text{GF}(q)^{m \times n}$.
 $\text{rk}(\mathbf{x}) \stackrel{\text{def}}{=} \text{rank}(\mathbf{X})$
- $\text{rk}(\mathbf{x}) =$ number of linearly independent coordinates of \mathbf{x} over $\text{GF}(q)$
 $\Rightarrow \text{rk}(\mathbf{x}) \leq w_{\text{H}}(\mathbf{x})$
- Rank metric. Minimum rank distance of a code d_{R}
- Singleton bound: for a code of length n and cardinality M over $\text{GF}(q^m)$,

$$d_{\text{R}} \leq n - \log_{q^m} M + 1$$

Equality: maximum rank distance (MRD) codes. Counterpart of MDS codes

Applications of rank metric codes

- Data storage
- Public-key and private-key cryptosystems
- Space-time coding
- Network coding

Notations

- For $\mathbf{x} \in \text{GF}(q^m)^n$, the row span of \mathbf{X} is denoted as $\mathcal{E}'(\mathbf{x})$
- $\Rightarrow \mathcal{E}'(\mathbf{x}) \in E_{\text{rk}(\mathbf{x})}(q, n)$
- Number of vectors with rank r : $N_r(q^m, n)$
- Intersection of balls with rank radii r and s with distance between their respective centers d : $J(r, s, d)$
- Number of codewords with rank i in an $(n, n - d + 1, d)$ linear MRD code: $M(q^m, n, d, i)$

Connection between CDC's and CRC's

- Constant-rank code (CRC): subset of $\text{GF}(q^m)^n$ where all codewords have rank r
- $A_R(q^m, n, d, r)$: maximum cardinality of an (n, d, r) CRC over $\text{GF}(q^m)$
- Straightforward construction of CDC's from CRC's: $\mathcal{E}'(C)$. It preserves the minimum distance
- C is an $(n, d + r, r)$ CRC over $\text{GF}(q^m)$ ($2 \leq d \leq r, n \leq m$).
 $\Rightarrow \mathcal{E}'(C)$ is a CDC in $E_r(q, n)$ with cardinality $|C|$ and minimum subspace distance $d_s \geq 2d$
- $\Rightarrow A_R(q^m, n, d + r, r) \leq A_S(q, n, 2d, r)$

Connection between optimal CDC's and optimal CRC's

- We can also construct CRC's from CDC's
- For all q , $2 \leq 2r \leq n \leq m$, and $2 \leq d \leq r$,

$$A_R(q^m, n, d + r, r) \geq \min\{A_S(q, n, 2d, r), A_S(q, m, 2r, r)\}.$$

- Proof: construction of a CRC whose row span forms an $(n, 2d, r)$ CDC, and whose column span forms an $(m, 2r, r)$ CDC
- $\Rightarrow A_R(q^m, n, d + r, r) = A_S(q, n, 2d, r)$ if $d = r$ or if $m \geq (n - r)(r - d + 1) + r + 1$
- \Rightarrow Optimal CRC's over large enough fields lead to optimal CDC's

Why study constant-rank codes

- We can solve the problem of finding optimal CDC's by finding optimal CRC's instead
- Many results known for rank metric codes. Many are similar to the Hamming metric
- Many results known for constant Hamming weight codes can be adapted
- Rank metric codes have a natural group structure
- Duality vector-matrix
- Additional degree of freedom: m

Constant-rank codes

- Interested in $A_R(q^m, n, d, r)$ for $d \geq 1$
- $A_R(q^m, n, 1, r) = N_r(q^m, n)$, $A_R(q^m, n, d, r) = 1$ if $d > 2r$, $\Rightarrow 2 \leq d \leq r$.
 $A_R(q^m, n, d, r) = A_R(q^n, m, d, r) \Rightarrow m \geq n$

- Many bounds can be derived for CRC's

- Gilbert and Hamming bounds for CRC's:

$$\frac{N_r(q^m, n)}{\sum_{i=0}^{d-1} J(q^m, n, i, r, r)} \leq A_R(q^m, n, d, r) \leq \frac{N_r(q^m, n)}{\sum_{i=0}^t J(q^m, n, i, r, r)}$$

- Generalized Hamming bound: $A_R(q^m, n, d, r) \leq \frac{N_s(q^m, n)}{\sum_{i=0}^t J(q^m, n, i, s, r)}$ for
 all $0 \leq s \leq n$

Bounds on CRC's

- Johnson bounds for CRC's:

$$A_{\mathbb{R}}(q^m, m, d, m) \leq q^{m-1}(q^m - 1)A_{\mathbb{R}}(q^{m-1}, m-1, d, m-1)$$

$$A_{\mathbb{R}}(q^m, n, d, r) \leq \frac{q^n - 1}{q^{n-r} - 1} A_{\mathbb{R}}(q^m, n-1, d, r)$$

- Singleton bound for CRC's:

$$A_{\mathbb{R}}(q^m, n, d, r) \leq \sum_{j=r-i}^{\min\{n-i, r\}} A_{\mathbb{R}}(q^m, n-i, d-i, j)$$

- Bassalygo-Elias bound: $A_{\mathbb{R}}(q^m, n, d, r) \geq N_r(q^m, n)q^{m(-d+1)}$
- If $r < d$, can be refined to $A_{\mathbb{R}}(q^m, n, d, r) \geq N_r(q^n, n)q^{n(-d+1)}$

Constructions of CRC's

- For $r \geq d$, trivial construction: codewords with rank r in an $(n, n - d + 1, d)$ MRD code.

$$\Rightarrow A_{\text{R}}(q^m, n, d, r) \geq M(q^m, n, d, r)$$

- For $r < d$, cosets of codes with minimum rank distance d
- \Rightarrow For all $0 \leq s \leq n$,

$$A_{\text{R}}(q^m, n, d, r) \geq \frac{\sum_{i=0}^n M(q^m, n, d, i) J(s, r, i)}{N_s(q^m, n)}$$

- $\Rightarrow A_{\text{R}}(q^m, n, d, r) \geq \begin{bmatrix} n \\ r \end{bmatrix} q^{n(r-d+1)}$ and $A_{\text{R}}(q^m, n, r + 1, r) = \begin{bmatrix} n \\ r \end{bmatrix}$

Asymptotic results

- Maximum asymptotic rate of rank metric codes determined in [GY06], that of CDC's determined in [KK07]

- Maximum asymptotic rate of CRC's partly determined

- Normalized parameters: $\nu = \frac{n}{m}$, $\rho = \frac{r}{m}$, $\delta_R = \frac{d_R}{m}$, $0 \leq \rho, \delta_R \leq \nu \leq 1$.

Asymptotic rate $a_R(\nu, \delta_R, \rho) \stackrel{\text{def}}{=} \lim_{m \rightarrow \infty} \sup \left[\log_{q^{m^2}} A_R(q^m, n, d_R, r) \right]$

- For $0 \leq \delta_R \leq \rho$,

$$a_R(\nu, \delta_R, \rho) = \rho(1 + \nu - \rho) - \delta_R \quad (25)$$

- For $\rho \leq \delta_R \leq \min\{2\rho, \nu\}$,

$$\max\{0, \rho(2\nu - \rho) - \nu\delta_R\} \leq a_R(\nu, \delta_R, \rho) \leq \min\{(\nu - \rho)(2\rho - \delta_R), \rho(\nu - \delta_R)\} \quad (26)$$

Asymptotic results

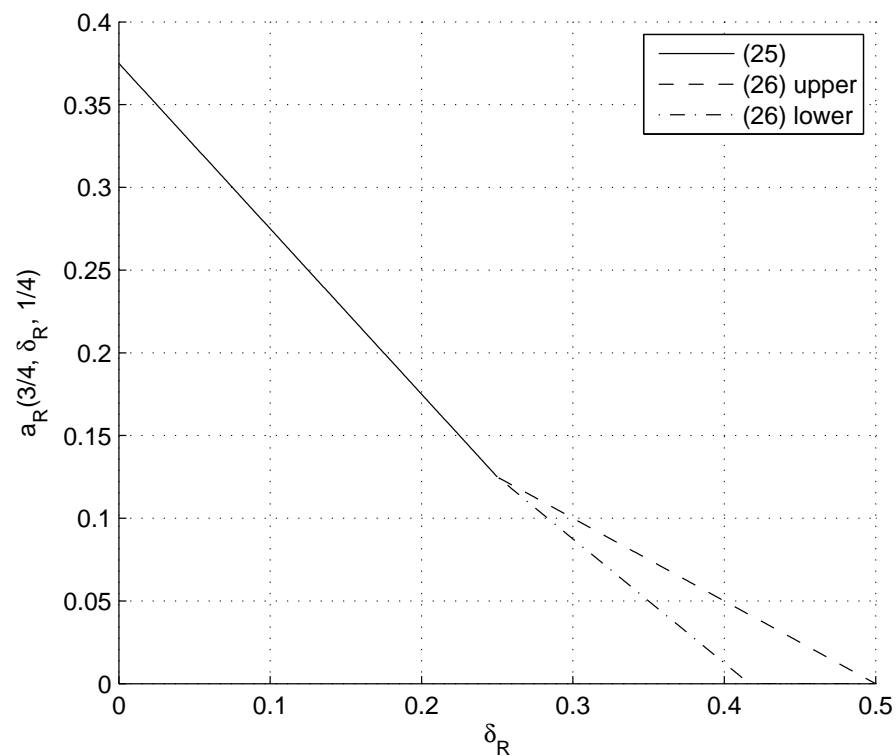


Figure 1: Asymptotic bounds on the maximal rate of a constant-rank code as a function of δ_R , with $\nu = 3/4$ and $\rho = 1/4$.

Conclusion and future work

- Connection between CDC's and CRC's
- The problem of finding optimal CDC's can be solved by finding optimal CRC's
- Properties of CRC's, and work on the asymptotic rate of CRC's
- Future work:
 - More bounds on CRC's
 - Asymptotic rate of CRC's
 - Stronger connection between CDC's and CRC's

Bibliography

- [KK07] R. Koetter and F. Kschischang, “Coding for Errors and Erasures in Random Network Coding,” *submitted to IEEE Trans. IT*
- [Chi87] L. Chihara, “On the zeros of the Askey-Wilson polynomials with applications to coding theory,” *SIAM J. Math. Anal.*
- [XF08] S.-T. Xia and F.-W. Fu “Johnson Type Bounds on Constant Dimension Codes,” *submitted to Designs, Codes, and Cryptography*
- [GY06] M. Gadouneau and Z. Yan, “Properties of Rank Metric Codes,” *Proc. IEEE Globecom 2006*
- [GY08] M. Gadouneau and Z. Yan, “Constant-Rank Codes and Their Connection to Constant-Dimension Codes,” *to be submitted to IEEE Trans. IT*