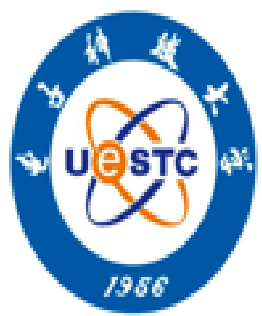
List Decoding of Cover-Metric Codes up to the Singleton Bound

Liu Shu

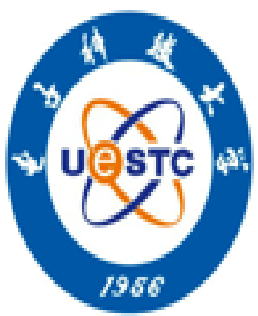
The National Key Laboratory of Science and Technology on Communications
University of Electronic Science and Technology of China

3 July 2018

Table of Contents

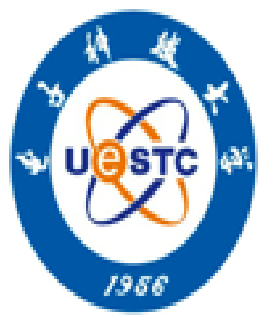


Overview



List Decoding of Cover-metric Codes up to the Singleton Bound

- Joint work with Chaoping Xing and Chen Yuan
- Published in *IEEE Transactions on Information Theory*, 64(4), pp. 2410-2416, 2018.
- Motivations
  - *Crisscross error patterns* can be found in various data storage and communication systems.
  - A. Wachter-Zeh [2] showed that every cover-metric code can be list decoded up to the *Johnson-like bound* [1] and an efficient list decoding algorithm was proposed.



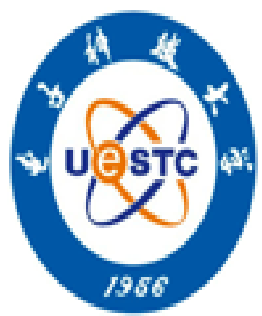
[1] Johnson bound is better than Johnson-like bound

Unique Decoding vs. List Decoding

- Unique decoding

  Output a unique codeword, correct error up to half the minimum distance.

- List decoding
  - Independently introduced by Elias and Wozencraft in the late 50's.
  - Correct error beyond unique decoding barrier, output a list of codewords.
  - Goal: determine the optimal trade-offs between *the information rate*, *the decoding radius* and *the list size*.



Cover-metric Codes

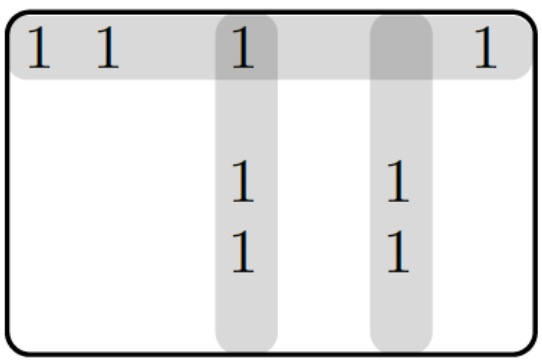
- Applications

  To combat *crisscross error*[2] in data storage and communication systems.

- Cover-metric code C

  a set of $n \times m$ $(n \leq m)$ matrices over $\mathbb{F}_q$.

- Cover of a matrix



A set of lines (rows and columns) such that all nonzero elements of the matrix are contained in these lines.

[2] To corrupt the columns and rows of data stored in an array.

Cover-metric Codes

- Cover weight

  The cover weight of $X \in \mathbb{F}_q^{n\times m}$, denoted by $\mathrm{wt}_{\mathsf{C}}(X)$, is the minimum size of all covers of X. The cover weight $\mathrm{wt}_{\mathsf{C}}(X) \leq n$.

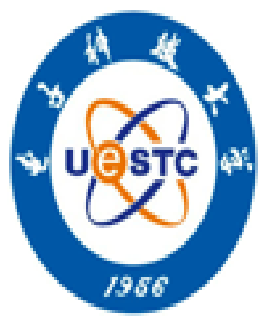
- Cover distance

  For any $X, Y \in \mathbb{F}_q^{n\times m}$, the cover distance between X and Y is

$$d_{\mathsf{C}}(X, Y) := \mathrm{wt}_{\mathsf{C}}(X - Y).$$

- Minimum cover distance of C

$$d_{\mathsf{C}} := \min_{X,Y\in\mathsf{C}, X\neq Y} d_{\mathsf{C}}(X, Y).$$



Cover-metric Codes

- Relative minimum cover distance and information rate of C

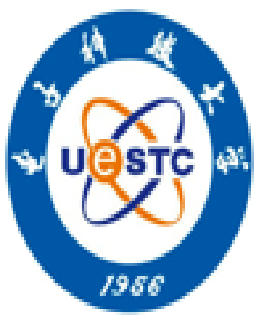
$$\delta(\mathsf{C}) = \frac{d_{\mathsf{C}} - 1}{n} \quad \text{and} \quad R(\mathsf{C}) = \frac{\log_q |\mathsf{C}|}{mn}.$$

- Every cover-metric code C must obey the Singleton bound

$$R(\mathsf{C}) + \delta(\mathsf{C}) \leq 1.$$

- $\mathbb{F}_q$-linear cover-metric code C_q

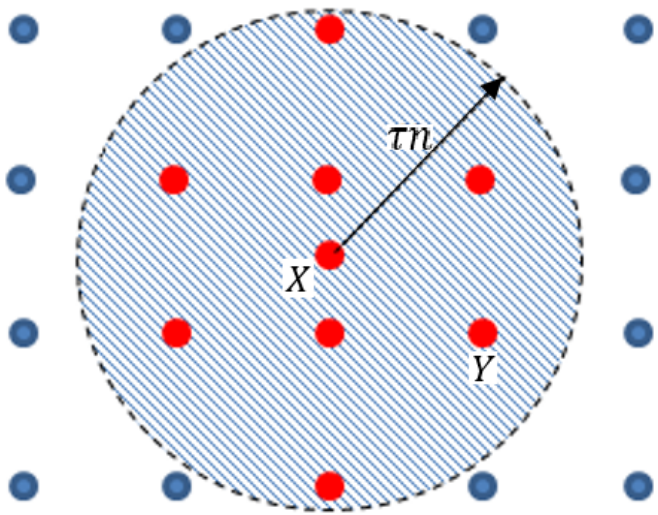
  A subspace of $\mathbb{F}_q^{n \times m}$, denoted by $[n \times m, k, d_{\mathsf{C}}]$.



Cover-Metric Ball

Let $\tau \in (0,1)$ and $X \in \mathbb{F}_q^{n\times m}$. The cover-metric ball centred at X and radius τn is defined by

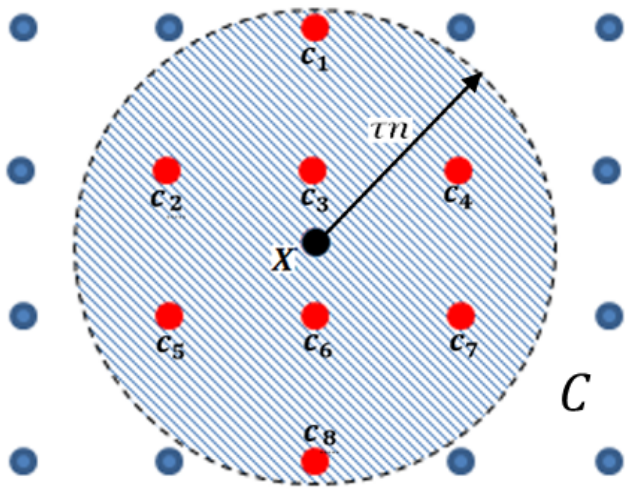
$$\mathcal{B}_{\mathsf{C}}(X,\tau n) := \{Y \in \mathbb{F}_q^{n\times m} : d_{\mathsf{C}}(X,Y) \leq \tau n\}.$$



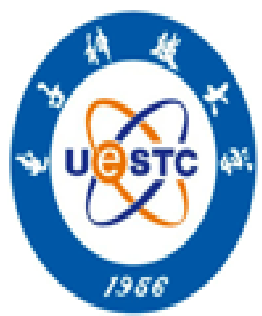
$(\tau n, \mathcal{L})^{\mathsf{C}}$-List Decodability

For an integer $\mathcal{L} \geq 1$ and a real $\tau \in (0, 1)$. A cover-metric code C is said to be $(\tau n, \mathcal{L})^{\mathsf{C}}$-list decodable if for every $X \in \mathbb{F}_q^{n \times m}$,

$$|\mathcal{B}_{\mathsf{C}}(X, \tau n) \cap \mathsf{C}| \leq \mathcal{L}.$$

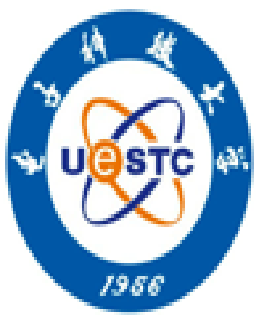


Overview



Main Results

- Limit of list decodability
  - Upper and lower bounds on the size of a cover-metric ball.
  - List decoding of every cover-metric code cannot exceed the Singleton bound.
- List decoding of random cover-metric codes
  - List decodability of random cover-metric codes
  - List decodability of random $\mathbb{F}_q$-linear cover-metric codes
- Explicit constructions
  - Converting from rank-metric codes
  - Converting from Hamming metric codes



Bounds

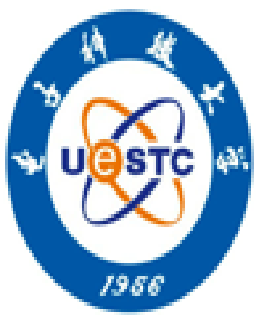
Given a matrix $A \in \mathbb{F}_q^{n\times m}$, the size of the cover-metric ball $\mathcal{B}_{\mathsf{C}}(A,d)$ is bounded by

$$q^{md} \leq |\mathcal{B}_{\mathsf{C}}(A,d)| \leq (d+1) \times 2^{(m+n)H_2\left(\frac{d}{m+n}\right)} q^{md},$$

where $H_2(x)$ is the binary entropy function, where $H_2(x) := -x\log_2(x) - (1-x)\log_2(1-x)$.

Limit of list decodability

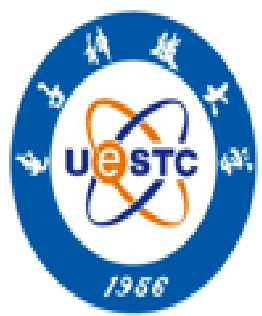
A cover-metric code of rate R in $\mathbb{F}_q^{n\times m}$ is $(\tau, \mathcal{L})^{\mathsf{C}}$-list decodable with list size $\mathcal{L} = \mathrm{poly}(m,n)$, then $\tau \leq 1 - R$.



List Decoding of Random Cover-metric Codes

For small $\epsilon \in (0,1)$, with a probability at least $1-2^{-mn/2}$, we have the following results:

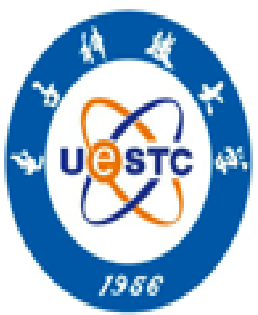
Random codes	Decoding radius τ	List size $\mathcal{L}$
cover-metric codes	Singleton bound	$O(1/\epsilon)$
$\mathbb{F}_q$-linear cover-metric codes	Singleton bound	$\exp(O(1/\epsilon))$



Explicit Constructions

- Converting from rank-metric codes, for small $\epsilon > 0$

Ratio ρ	Decoding radius τ	List size $\mathcal{L}$	Decoding algorithm running time
$0(\epsilon^2)$	Singleton bound	$\exp(O(1/\epsilon))$	$\text{poly}(m, 1/\epsilon)$



Explicit Constructions

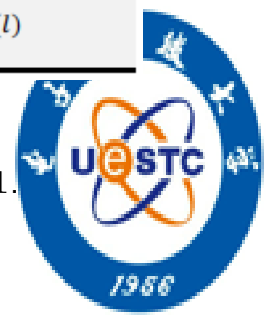
- Converting from rank-metric codes, for small $\epsilon > 0$

Ratio ρ	Decoding radius τ	List size $\mathcal{L}$	Decoding algorithm running time
$0(\epsilon^2)$	Singleton bound	$\exp(O(1/\epsilon))$	$\text{poly}(m, 1/\epsilon)$

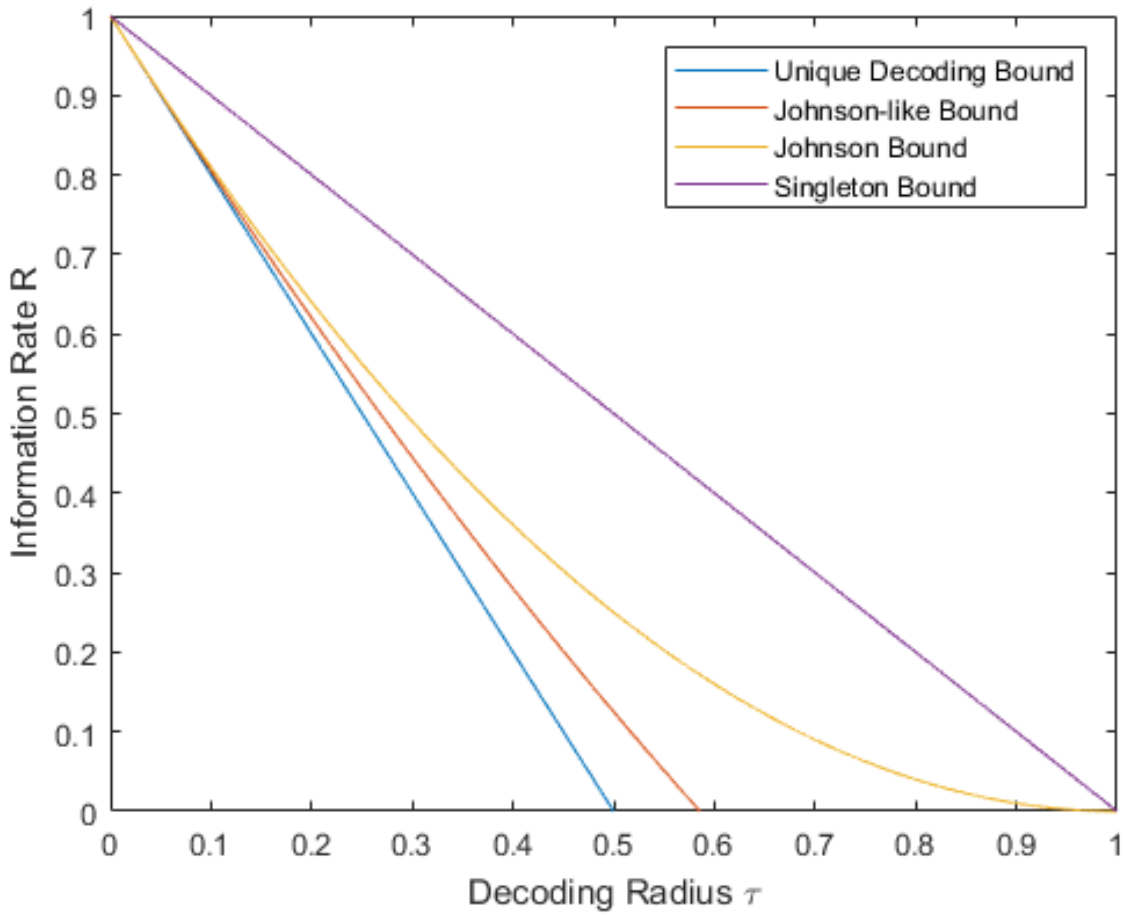
- Converting from Hamming metric codes, for small $\epsilon > 0$

	Field $\mathbf{q}$	Decoding radius τ	List size $\mathcal{L}$	Decoding algorithm running time
Ours	q	Johnson bound	$O(1/\epsilon)$	$O(m^6 \log^3 q\, /\epsilon^5)$
Ours	$\Omega(1/\epsilon^2)$	Johnson bound	$O(1/\epsilon)$	$\text{poly}(m, 1/\epsilon)$
[2]	q	Johnson-like bound	$O(1/\epsilon)$	$\text{poly}(m, 1/\epsilon)$
Ours	$m^{O(1/\epsilon^2)}$	Singleton bound	$(1/\epsilon)^{O(1/\epsilon)}$	$\text{poly}(mn, 1/\epsilon)$
Ours	$\exp(O(1/\epsilon^2))$	Singleton bound	$l := 2^{2^{(\log^* m)}}$	$(mn)^{O(1)}(1/\epsilon)^{O(l)}$

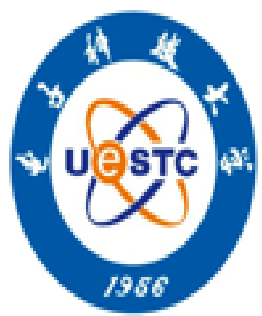
where $\log^* m$ denotes the number of iterated logarithms to the base 2 needed to reach a number below 1.



Decoding Radius of Cover-metric Codes



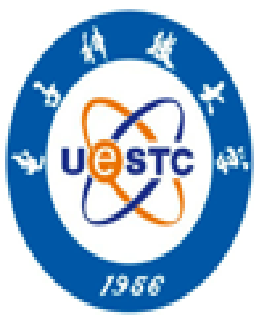
Overview



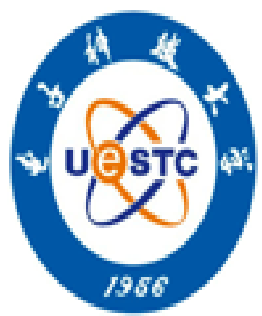
Future Research

Design new efficient list decoding algorithms of cover-metric codes

- Known
  1. Converting from rank-metric and Hamming metric codes, cover-metric codes can be efficiently list decoded up to the Singleton bound with sacrifice of the ratio ρ or the field size q [1].
  2. Take a rank-metric code with the ratio $\rho = 1$, the corresponding cover-metric codes has decoding radius far away from the Singleton bound [3].
- How to efficiently list decode cover-metric codes up to the Singleton bound with constant field size, polynomial list size and the ratio $\rho = 1$?



Thank you!



References

[1] S. Liu, C. Xing and C. Yuan, List Decoding of Cover-metric Codes Up to the Singleton Bound,*IEEE Transactions on Information Theory*, 64(4), pp. 2410-2416, April 2018.

[2] A. Wachter-Zeh, List decoding of crisscross errors, *IEEE Transactions on Information Theory*, 63(1), pp. 142-149, 2017.

[3] C. Xing and C. Yuan, A new class of rank-metric codes and their list decoding beyond the unique decoding radius, *IEEE Transactions on Information Theory*, 2017.