On the Hardness of the Lee Syndrome Decoding Problem

Violetta Weger

University College Dublin

CBCrypto 2021
22. June 2021

joint work with Karan Khathuria, Anna-Lena Horlemann, Massimo Battaglioni, Paolo Santini and Edoardo Persichetti

Outline

Ring-Linear Coding Theory

	Classical	$\mathbb{Z}/p^s\mathbb{Z}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	
Code	$\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace	
Parameters	length n dimension k	
Systematic Form	$\mathbf{G} = [\mathrm{Id}_k \mid \mathbf{A}]$ $\mathbf{H} = [\mathbf{B} \mid \mathrm{Id}_{n-k}]$	

Ring-Linear Coding Theory

	Classical	$\mathbb{Z}/p^s\mathbb{Z}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	Integer residue ring $\mathbb{Z}/p^s\mathbb{Z}$
Code	$\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace	$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ $\mathbb{Z}/p^s\mathbb{Z}$-submodule
Parameters	length n dimension k	length n ?
Systematic Form	$\mathbf{G} = [\mathrm{Id}_k \mid \mathbf{A}]$ $\mathbf{H} = [\mathbf{B} \mid \mathrm{Id}_{n-k}]$	? ?

Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code with

$$| \mathcal{C} | = (p^s)^{k_1}(p^{s-1})^{k_2} \cdots p^{k_s}$$

Then we say $\mathcal{C}$ has

- subtype $(k_1, \ldots, k_s)$
- type $k = \sum_{i=1}^{s} \frac{s-i+1}{s} k_i = \log_{p^s}(| \mathcal{C} |)$
- rate $R = k/n$
- rank $K = \sum_{i=1}^{s} k_i$
- free rank k_1

$$0 \leq k_1 \leq k \leq K \leq n.$$

Systematic Form

$$\mathbf{G} = \begin{pmatrix} \mathrm{Id}_{k_1} & * & \cdots & * & * \\ 0 & p\mathrm{Id}_{k_2} & \cdots & p* & p* \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & p^{s-1}\mathrm{Id}_{k_s} & p^{s-1}* \end{pmatrix} \in (\mathbb{Z}/p^s\mathbb{Z})^{K\times n}$$

$$\mathbf{H} = \begin{pmatrix} * & * & \cdots & * & \mathrm{Id}_{n-K} \\ p* & p* & \cdots & p\mathrm{Id}_{k_s} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ p^{s-1}* & p^{s-1}\mathrm{Id}_{k_2} & \cdots & 0 & 0 \end{pmatrix} \in (\mathbb{Z}/p^s\mathbb{Z})^{(n-k_1)\times n}$$

Definition (Lee Metric)

For $x \in \mathbb{Z}/p^s\mathbb{Z}$, and $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}/p^s\mathbb{Z})^n$, we define

- *Lee weight of x:* $wt_L(x) = \min\{x, \mid p^s - x \mid\}$
- *Lee weight of $\mathbf{x}$:* $wt_L(\mathbf{x}) = \sum_{i=1}^{n} wt_L(x_i)$
- *Lee distance between $\mathbf{x}$ and $\mathbf{y}$:* $d_L(\mathbf{x}, \mathbf{y}) = wt_L(\mathbf{x} - \mathbf{y})$

Definition (Minimum Lee Distance)

$\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ a linear code has minimum Lee distance

$$d(\mathcal{C}) = \min\{d_L(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \neq \mathbf{y} \in \mathcal{C}\}$$

$$0 \leq \mathrm{wt}_H(\mathbf{x}) \leq \mathrm{wt}_L(\mathbf{x}) \leq \lfloor \frac{p^s}{2} \rfloor n.$$

NP-Hardness

Problem (Syndrome Decoding Problem)

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}, \mathbf{s} \in \mathbb{F}_q^{n-k}$ *and* $t \in \mathbb{N}$, *find* $\mathbf{e} \in \mathbb{F}_q^n$ *such that* $\mathbf{He}^\top = \mathbf{s}^\top$ *and* $wt_H(\mathbf{e}) \leq t$.

Problem (Given Weight Codeword Problem)

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ *and* $t \in \mathbb{N}$, *find* $\mathbf{c} \in \mathbb{F}_q^n$ *such that* $\mathbf{He}^\top = \mathbf{0}$ *and* $wt_H(\mathbf{c}) = t$.

- NP-completeness over $\mathbb{F}_2$:

Elwyn Berlekamp, Robert J. McEliece, Henk Van Tilborg "On the inherent intractability of certain coding problems", IEEE Transactions on Information Theory, 1978.

- NP-completeness over $\mathbb{F}_q$:

Alexander Barg "Some new NP-complete coding problems", Problemy Peredachi Informatsii, 1994.

NP-Hardness

$\mathcal{R}$ a finite ring with unity, and $\mathrm{wt} : \mathcal{R} \to \mathbb{R}_{\geq 0}$ such that

1. $\mathrm{wt}(0) = 0$,
2. $\mathrm{wt}(1) = 1$,
3. $\mathrm{wt}(x) \geq 1$ for all $x \neq 0$,
4. additive, i.e., for $\mathbf{x} \in \mathcal{R}^n$: $\mathrm{wt}(\mathbf{x}) = \sum_{i=1}^{n} \mathrm{wt}(x_i)$.

Problem (Additive Weight SDP)

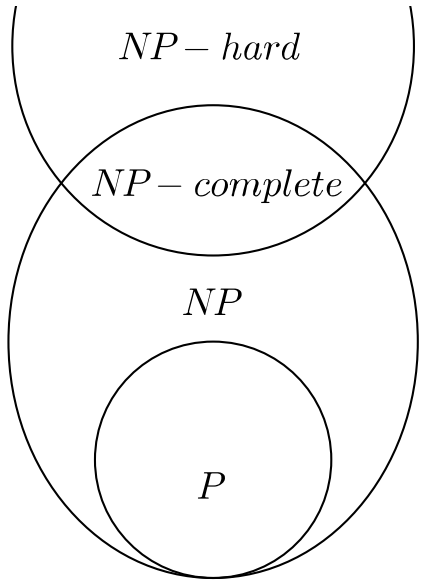
Given $\mathbf{H} \in \mathcal{R}^{(n-k)\times n}, \mathbf{s} \in \mathcal{R}^{n-k}$ *and* $t \in \mathbb{N}$, *find* $\mathbf{e} \in \mathcal{R}^n$ *such that* $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$ *and* $wt(\mathbf{e}) \leq t$.

Problem (Additive Weight GWCP)

Given $\mathbf{H} \in \mathcal{R}^{(n-k)\times n}$ *and* $t \in \mathbb{N}$, *find* $\mathbf{c} \in \mathcal{R}^n$ *such that* $\mathbf{H}\mathbf{e}^\top = \mathbf{0}$ *and* $wt(\mathbf{c}) = t$.

NP-Hardness

- NP-complete = NP-hard ∩ NP
- NP: check a candidate for a solution in polynomial time



- NP-hard: at least as hard as the hardest problem in NP

Polynomial time reduction

To show: $\mathcal{P}_1 \in$ NP-hard

1. choose $\mathcal{P}_2 \in$ NP-hard
2. take I a random instance of $\mathcal{P}_2$
3. transform (poly. time) to $\varphi(I)$ an instance of $\mathcal{P}_1$
4. solve $\mathcal{P}_1$ on $\varphi(I)$: get solution $\varphi(s)$
5. transform (poly. time) to s the solution of $\mathcal{P}_2$ on instance I

Problem (3-D Matching Problem)

Given a finite set T, $U \subseteq T \times T \times T$, find $W \subseteq U$ with $|\, W \,| = |\, T \,|$ and no two elements of W agree on any coordinate.

Reduction to AW-SDP

Let

$$U = \{\mathbf{a}_1, \ldots, \mathbf{a}_u\}$$
$$T = \{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$$

- $\mathbf{s} \in \mathcal{R}^{3t}$ all one vector
- weight t
- $\mathbf{H}^\top \in \mathcal{R}^{u \times 3t}$ incidence matrix

Example

$$T = \{a, b, c\}$$
$$U = \{(c, a, b), (c, b, c), (a, b, c), (b, c, a)\}$$

$$\mathbf{H}^\top = \begin{array}{c|ccccccccc} & a & b & c & a & b & c & a & b & c \\ \hline (c,a,b) & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ (c,b,c) & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ (a,b,c) & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ (b,c,a) & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}$$

Problem (3-D Matching Problem)

Given a finite set T, $U \subseteq T \times T \times T$, find $W \subseteq U$ with $|\, W \,| = |\, T \,|$ and no two elements of W agree on any coordinate.

Reduction to AW-SDP

Let

$$U = \{\mathbf{a}_1, \ldots, \mathbf{a}_u\}$$
$$T = \{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$$

- $\mathbf{s} \in \mathcal{R}^{3t}$ all one vector
- weight t
- $\mathbf{H}^\top \in \mathcal{R}^{u \times 3t}$ incidence matrix
- solve AW-SDP get $\mathbf{e} \in \mathcal{R}^n$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ and has weight t
- $W = \{\mathbf{a}_i \mid \mathbf{e}_i \neq 0\}$

Example

$$T = \{a, b, c\}$$
$$U = \{(c, a, b), (c, b, c), (a, b, c), (b, c, a)\}$$

$$\mathbf{H}^\top = \begin{array}{c|ccccccccc} & a & b & c & a & b & c & a & b & c \\ \hline (c,a,b) & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ (c,b,c) & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ (a,b,c) & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ (b,c,a) & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}$$

$$\mathbf{e} = (1, 0, 1, 1)$$
$$W = \{(c, a, b), (a, b, c), (b, c, a)\}$$

Reduction to GWCP

$$\mathbf{H}^\top = \begin{array}{c|ccccc} & 3t & u & (3t \text{ times}) & & u \\ \hline u & \overline{\mathbf{H}}^\top & \mathrm{Id}_u & \cdots & & \mathrm{Id}_u \\ 3t & -\mathrm{Id}_{3t} & \mathbf{0} & \cdots & & \mathbf{0} \\ u & \mathbf{0} & -\mathrm{Id}_u & & & \mathbf{0} \\ (3t \text{ times}) & \vdots & & \ddots & & \\ u & \mathbf{0} & \mathbf{0} & & & -\mathrm{Id}_u \end{array}$$

set weight $w = 3t^2 + 4t$

$$\mathbf{c} = (\underbrace{\mathbf{a}}_{u}, \underbrace{\mathbf{b}}_{3t}, \underbrace{\mathbf{c}_1}_{u}, \cdots, \underbrace{\mathbf{c}_{3t}}_{u})$$

$$\mathbf{c} = (\mathbf{a}, \mathbf{b}, \mathbf{c}_1, \cdots, \mathbf{c}_{3t})$$

$$\begin{aligned} \mathbf{a}\overline{\mathbf{H}}^{\top} &= \mathbf{b} \\ \mathbf{a} &= \mathbf{c}_1 \\ &\vdots \\ \mathbf{a} &= \mathbf{c}_{3t} \end{aligned}$$

$$\mathbf{c} = (\mathbf{a}, \mathbf{b}, \mathbf{c}_1, \cdots, \mathbf{c}_{3t})$$

$$\begin{aligned} \mathbf{a}\overline{\mathbf{H}}^{\top} &= \mathbf{b} \\ \mathbf{a} &= \mathbf{c}_1 \\ &\vdots \\ \mathbf{a} &= \mathbf{c}_{3t} \end{aligned}$$

$$\mathrm{wt}(\mathbf{c}) = \mathrm{wt}(\mathbf{b}) + \mathrm{wt}(\mathbf{a})(3t+1) = 3t + t \cdot (3t+1) = 3t^2 + 4t.$$

We get: $\mathrm{wt}(\mathbf{b}) = 3t$ and $\mathbf{a}$ is a solution to

$$\mathbf{a}\overline{\mathbf{H}}^{\top} = \mathbf{b} = \mathbf{1}.$$

$$\mathbf{c} = (\mathbf{a}, \mathbf{b}, \mathbf{c}_1, \cdots, \mathbf{c}_{3t})$$

$$\begin{aligned} \mathbf{a}\overline{\mathbf{H}}^{\top} &= \mathbf{b} \\ \mathbf{a} &= \mathbf{c}_1 \\ &\vdots \\ \mathbf{a} &= \mathbf{c}_{3t} \end{aligned}$$

$$\mathrm{wt}(\mathbf{c}) = \mathrm{wt}(\mathbf{b}) + \mathrm{wt}(\mathbf{a})(3t+1) = 3t + t \cdot (3t+1) = 3t^2 + 4t.$$

We get: $\mathrm{wt}(\mathbf{b}) = 3t$ and $\mathbf{a}$ is a solution to

$$\mathbf{a}\overline{\mathbf{H}}^{\top} = \mathbf{b} = \mathbf{1}.$$

Problem over $\mathcal{R}$: $\mathrm{wt}(\mathbf{b}) \not\leq 3t$ but $\mathrm{wt}(\mathbf{b}) \leq 3tM$

Reduction to AW-GWCP

$$\mathbf{H}^\top = \begin{array}{c|cccc} & 3t & u & (3tM \text{ times}) & u \\ \hline u & \overline{\mathbf{H}}^\top & \mathrm{Id}_u & \cdots & \mathrm{Id}_u \\ 3t & -\mathrm{Id}_{3t} & \mathbf{0} & \cdots & \mathbf{0} \\ u & \mathbf{0} & -\mathrm{Id}_u & & \mathbf{0} \\ (3tM \text{ times}) & \vdots & & \ddots & \\ u & \mathbf{0} & \mathbf{0} & & -\mathrm{Id}_u \end{array}$$

set weight $w = 3t^2M^2 + 4t + 1$

$$\mathbf{c} = (\underbrace{\mathbf{a}}_{u}, \underbrace{\mathbf{b}}_{3t}, \underbrace{\mathbf{c}_1}_{u}, \cdots, \underbrace{\mathbf{c}_{3tM}}_{u})$$

ISD Algorithms

- 1962: Prange's first ISD algorithm

$$\mathbf{H}\mathbf{e}^\top = [\mathrm{Id}_{n-k} \mid \mathbf{B}](\mathbf{e}_{IC}, \mathbf{e}_I)^\top = \mathbf{s}^\top \Rightarrow \mathbf{e}_{IC} = \mathbf{s}$$

Eugene Prange "The use of information sets in decoding cyclic codes", IEEE Transactions on Information Theory, 1962.

- Classical ISD algorithms: Stern

$$\mathbf{e}_{IC} = (\mathbf{e}', \mathbf{0}), \quad \mathrm{wt}(\mathbf{e}_{IC}) = t - v,$$
$$\mathbf{e}_I = (\mathbf{e}_1, \mathbf{e}_2), \quad \mathrm{wt}(\mathbf{e}_i) = v/2.$$

Jacques Stern "A method for finding codewords of small weight", International Colloquium on Coding Theory and Applications, 1988.

- Recent Improvements: Partial Gaussian Elimination (PGE)

$$\mathbf{H}\mathbf{e}^\top = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & \mathbf{A} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} \begin{pmatrix} \overline{\mathbf{e}}^\top \\ \mathbf{e}'^\top \end{pmatrix} = \begin{pmatrix} \mathbf{s}_1^\top \\ \mathbf{s}_2^\top \end{pmatrix}$$

$$\overline{\mathbf{e}} + \mathbf{e}'\mathbf{A}^\top = \mathbf{s}_1, \ \mathbf{e}'\mathbf{B}^\top = \mathbf{s}_2$$

$$\mathrm{wt}(\overline{\mathbf{e}}) = t - v, \ \mathrm{wt}(\mathbf{e}') = v$$

Matthieu Finiasz, Nicolas Sendrier "Security bounds for the design of code-based cryptosystems", 2009.

ISD Algorithms

- Recent Improvements: Partial Gaussian Elimination (PGE)

$$\mathbf{H}\mathbf{e}^\top = \begin{pmatrix} \mathrm{Id}_{n-k-\ell} & \mathbf{A} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} \begin{pmatrix} \overline{\mathbf{e}}^\top \\ \mathbf{e}'^\top \end{pmatrix} = \begin{pmatrix} \mathbf{s}_1^\top \\ \mathbf{s}_2^\top \end{pmatrix}$$

$$\overline{\mathbf{e}} + \mathbf{e}'\mathbf{A}^\top = \mathbf{s}_1, \ \mathbf{e}'\mathbf{B}^\top = \mathbf{s}_2$$

$$\mathrm{wt}(\overline{\mathbf{e}}) = t - v, \ \mathrm{wt}(\mathbf{e}') = v$$

Matthieu Finiasz, Nicolas Sendrier "Security bounds for the design of code-based cryptosystems", 2009.

- Solve smaller SDP instance
  - Wagner's approach: partition $\mathbf{e}' = (\mathbf{e}_1, \mathbf{e}_2)$, $\mathrm{wt}(\mathbf{e}_i) = v/2$
  - Representation technique: $\mathbf{e}' = \mathbf{e}_1 + \mathbf{e}_2$, $\mathrm{wt}(\mathbf{e}_i) = v/2 + \varepsilon$

Anja Becker, Antoine Joux, Alexander May, Alexander Meurer "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding", 2012.

Alexander May, Alexander Meurer, Enrico Thomae "Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$", 2011.

Generalized ideas to $\mathbb{Z}/p^s\mathbb{Z}$ in the Lee metric

- Two-blocks: like Stern with intermediate sums and early abort
- Finiasz-Sendrier: using Wagner's approach (only one level!)
- Representation technique on a levels
- BJMM

Generalized ideas to $\mathbb{Z}/p^s\mathbb{Z}$ in the Lee metric

- Two-blocks: like Stern with intermediate sums and early abort
- Finiasz-Sendrier: using Wagner's approach (only one level!)
- Representation technique on a levels
- BJMM
- s-blocks: iteratively solves the $s+1$ parity-check equations in smaller subrings (taking care of kernels when lifting)

How to analyse complexity?

Fix the rate $R = k/n$, take random code with minimum distance achieving the GV bound

- Random codes over $\mathbb{F}_q$ in the Hamming metric achieve the GV bound

Alexander Barg, G. David Forney "Random codes: Minimum distances and error exponents", IEEE Transactions on Information Theory, 2002.

John Pierce "Limit distribution of the minimum distance of random linear codes", IEEE Transactions on Information Theory, 1967.

- Random rank-metric codes achieve the GV bound

Pierre Loidreau "Asymptotic behaviour of codes in rank metric over finite fields", Designs, codes and cryptography, 2014.

How to analyse complexity?

Fix the rate $R = k/n$, take random code with minimum distance achieving the GV bound

- Random codes over $\mathbb{F}_q$ in the Hamming metric achieve the GV bound

Alexander Barg, G. David Forney "Random codes: Minimum distances and error exponents", IEEE Transactions on Information Theory, 2002.

John Pierce "Limit distribution of the minimum distance of random linear codes", IEEE Transactions on Information Theory, 1967.

- Random rank-metric codes achieve the GV bound

Pierre Loidreau "Asymptotic behaviour of codes in rank metric over finite fields", Designs, codes and cryptography, 2014.

- Random Lee-metric codes achieve the GV bound

Eimear Byrne, Anna-Lena Horlemann-Trautmann, Karan Khathuria, Violetta Weger "Density of free modules over finite chain rings", 2021.

Asymptotics

The asymptotic cost is given by

$$q^{(e(R,q)+o(1))n}.$$

We compare the exponents $e^* = \max_{0 \leq R \leq 1} e(q, R)$.

Let $q = 7^2$ and $\lim_{n \to \infty} k_1/n = \lambda R$.

	$\lambda = 1$	$\lambda = 0.75$	$\lambda = 0.5$
Two-Blocks	0.0761	0.0978	0.1211
s-Blocks	0.1030	0.0736	0.0471
Wagner $a = 1$	0.0761	0.0978	0.1211
Rep. tech. $a = 1$	0.0886	0.1154	0.1457
Rep. tech. $a = 2$	0.0932	0.1221	0.1557
BJMM	0.0932	0.1219	0.1554

Comparison to Hamming metric

For $\lambda = 1, q = 4$:

	e^*
Lee Metric	
s-Blocks	0.05601
Stern/Wagner $a = 1$	0.05142
Rep. tech. $a = 1$	0.05358
Rep. tech. $a = 2$	0.05435
BJMM	0.05443
Hamming Metric	
Stern	0.04987
BJMM-MO	0.04294

Open Problems

- Find Lee-metric code such that
  - large error correction capability
  - efficient decoding algorithm
  - large family of codes
- build a ZKID using Lee metric

Thank you!