# Behaviour of Random Ring-Linear Codes

**Violetta Weger**

**Technical University of Munich**

**ACCESS**
**October 5, 2021**

**joint work with Eimear Byrne, Anna-Lena Horlemann and Karan Khathuria**

Large interest in code-based cryptography in

- new metrics, such as sum-rank metric, Lee metric,
- new ambient spaces, such as finite chain rings.

# Motivation

Large interest in code-based cryptography in

- new metrics, such as sum-rank metric, Lee metric,
- new ambient spaces, such as finite chain rings.

**How do random codes behave over finite chain rings?**

# Motivation

Large interest in code-based cryptography in

- new metrics, such as sum-rank metric, Lee metric,
- new ambient spaces, such as finite chain rings.

**How do random codes behave over finite chain rings?**

- What parameters should we expect?
- What minimum distance should we expect?

# Outline

# Finite Chain Rings

**Definition (Chain Ring)**

*A ring $\mathcal{R}$ is called a chain ring, if the ideals of $\mathcal{R}$ form a chain: for all ideals $I, J \subseteq \mathcal{R}$ we either have $I \subseteq J$ or $J \subseteq I$.*

Let $\langle \pi \rangle$ be the unique maximal ideal of $\mathcal{R}$.

- $s$ is the **nilpotency index**: the smallest positive integer such that $\pi^s = 0$.
- $q$ is the **size of the residue field**: $q = \mid \mathcal{R}/\langle \pi \rangle \mid$.

Thus, $\mid \mathcal{R} \mid = q^s$.

**Example**

- $\mathbb{F}_q[X;\sigma]/(X^s)$ *for some* $\sigma \in Aut(\mathbb{F}_q)$,
- $GR(p^s, r)$ : *for* $s = 1 : \mathbb{F}_{p^r}$ *and for* $r = 1 : \mathbb{Z}/p^s\mathbb{Z}$,

| | Classical | $\mathcal{R}$-Linear |
|---|---|---|
| Ambient space | Finite field $\mathbb{F}_q$ | |
| Linear code | $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace | |
| Parameters | length $n$ dimension $k$ | |

# Ring-Linear Coding Theory

| | Classical | $\mathcal{R}$-Linear |
|---|---|---|
| Ambient space | Finite field $\mathbb{F}_q$ | Finite chain ring $\mathcal{R}$ |
| Linear code | $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace | $\mathcal{C} \subseteq \mathcal{R}^n$ $\mathcal{R}$-submodule |
| Parameters | length $n$ dimension $k$ | length $n$ ? |

Let $\mathcal{C} \subseteq \mathcal{R}^n$ be a code, then

$$\mathcal{C} \cong \underbrace{\langle 1 \rangle \times \cdots \times \langle 1 \rangle}_{k_1} \times \underbrace{\langle \pi \rangle \times \cdots \times \langle \pi \rangle}_{k_2} \times \cdots \times \underbrace{\langle \pi^{s-1} \rangle \times \cdots \times \langle \pi^{s-1} \rangle}_{k_s}.$$

Then we say $\mathcal{C}$ has

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

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

If $k_1 = k = K$, we say that $\mathcal{C}$ is a **free code**.

### Systematic Form

If $\mathcal{C}$ has subtype $(k_1, \ldots, k_s)$ and rank $K$ then

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

If $\mathcal{C}$ is a free code, then

$$G = \begin{pmatrix} \mathrm{Id}_k & A \end{pmatrix} \in (\mathbb{Z}/p^s\mathbb{Z})^{k\times n}.$$

# Question: Density of Free Codes

Fix $n$ and a rate $R = k/n$. A code $\mathcal{C} \subseteq \mathcal{R}^n$ of rate $R$, can have any subtype $(k_1, \ldots, k_s)$ with

$$k = \sum_{i=1}^{s} \frac{s-i+1}{s} k_i.$$

**How likely is it that a random code is free?**

# Question: Density of Free Codes

Fix $n$ and a rate $R = k/n$. A code $\mathcal{C} \subseteq \mathcal{R}^n$ of rate $R$, can have any subtype $(k_1, \ldots, k_s)$ with

$$k = \sum_{i=1}^{s} \frac{s-i+1}{s} k_i.$$

**How likely is it that a random code is free?**

Probability of a free code:

$$P(n) = \frac{\text{number of free codes of type } k}{\text{number of all codes of type } k}.$$

Then, the density of free codes is given by

$$\lim_{n \to \infty} P(n),$$

if the limit exists.

# Counting Codes

**Proposition**

*The number of codes of $\mathcal{R}^n$ with subtype $(k_1, \ldots, k_s)$ is given by*

$$N_{n,q}(k_1, \ldots, k_s) = q^{\sum_{i=1}^{s}(n-\sum_{j=1}^{i} k_j)\sum_{j=1}^{i-1} k_j} \prod_{i=1}^{s} \begin{bmatrix} n - \sum_{j=1}^{i-1} k_j \\ k_i \end{bmatrix}_q,$$

**Corollary**

*The number of free codes of type $k$ is then given by*

$$N_{n,q}(k, 0, \ldots, 0) = q^{(n-k)k(s-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

Thomas Honold and Ivan Landjev "Linear codes over finite chain rings", The electronic journal of combinatorics, 2000.

# Counting Codes

**Definition**

*Let $L(s,n,k)$ to be the set of all possible subtypes for type $k$:*

$$L(s,n,k) := \left\{ (k_1, \ldots, k_s) \mid \sum_{i=1}^{s} k_i \frac{s-i+1}{s} = k, \sum_{i=1}^{s} k_i \leq n \right\}.$$

# Counting Codes

**Definition**

*Let $L(s,n,k)$ to be the set of all possible subtypes for type $k$:*

$$L(s,n,k) := \left\{ (k_1,\dots,k_s) \mid \sum_{i=1}^{s} k_i \frac{s-i+1}{s} = k, \sum_{i=1}^{s} k_i \leq n \right\}.$$

The number of codes in $\mathcal{R}^n$ of type $k$ is

$$M(n,k,q,s) := \sum_{(k_1,\dots,k_s)\in L(s,n,k)} N_{n,q}(k_1,\dots,k_s).$$

# Counting Codes

The number of $[n, k]$ linear codes over $\mathbb{F}_q$ is given by the $q$-**binomial coefficient**

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

# Counting Codes

The number of $[n, k]$ linear codes over $\mathbb{F}_q$ is given by the $q$**-binomial coefficient**

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

**Definition**

The $q$**-multinomial coefficient** is defined as

$$\begin{bmatrix} n \\ m \end{bmatrix}_q^{(r)} := \sum_{j_1+\cdots+j_r=m} q^{\sum_{\ell=1}^{r-1}(n-j_\ell)j_{\ell+1}} \begin{bmatrix} n \\ j_1 \end{bmatrix}_q \begin{bmatrix} j_1 \\ j_2 \end{bmatrix}_q \cdots \begin{bmatrix} j_{r-1} \\ j_r \end{bmatrix}_q.$$

$$M(n, k, q, s) = \begin{bmatrix} n \\ ks \end{bmatrix}_q^{(s)}.$$

Ole S. Warnaar "The Andrews–Gordon identities and $q$-multinomial coefficients", Communications in mathematical physics, 1997.

# Density of Free Codes

The probability to have a free code of rate $R = k/n$ is

$$P(n) = \frac{q^{(n-k)k(s-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q}{M(n,k,q,s)}.$$

# Density of Free Codes

The probability to have a free code of rate $R = k/n$ is

$$P(n) = \frac{q^{(n-k)k(s-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q}{M(n,k,q,s)}.$$

**Example**

*The density of free codes over $\mathbb{Z}/4\mathbb{Z}$ is*

$$\sim 0.59546.$$

# Combinatorial Tools

The $q$-**Pochhammer symbol**

$$(a;q)_r = \prod_{i=0}^{r-1} \left(1 - aq^i\right), \quad (a;q)_\infty = \prod_{i=0}^{\infty} \left(1 - aq^i\right).$$

We denote by $(q)_r = (q;q)_r$.

- $$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} = \frac{(q)_n}{(q)_k (q)_{n-k}}.$$
- Generating function for partitions: $\sum_{n \geq 0} p(n) q^n = \frac{1}{(q)_\infty}$
- Series involving $(a;q)_r$ are called $q$-**series**
- $q$-binomial theorem:

$$\sum_{n \geq 0} \frac{(a;q)_n}{(q)_n} z^n = \frac{(az;q)_\infty}{(z;q)_\infty}.$$

# Density of Free Codes

Anne Schilling. "Multinomials and polynomial bosonic forms for the branching functions of the $\widehat{su}_M(2) \times \widehat{su}_N(2)/\widehat{su}_{M+N}(2)$ conformal coset models", Nuclear Physics B, 1996.

## Theorem

*The density as $n \to \infty$ of free codes in $\mathcal{R}^n$ of type $k$ is given by*

$$d(q,s) = \left( \sum_{\substack{k_2,\ldots,k_s \geq 0 \\ s \mid K_2+\cdots+K_s}} \frac{(1/q)^{K_2^2+\cdots+K_s^2-(K_2+\cdots+K_s)^2/s}}{(1/q)_{k_2}\cdots(1/q)_{k_s}} \right)^{-1},$$

*where* $K_i = \sum_{j=2}^{i} k_j$.

Eimear Byrne, Anna-Lena Horlemann, Karan Khathuria and Violetta Weger "Density of Free Modules over Finite Chain Rings", 2021.

# Special case $s = 2$

If $s = 2$ we can write this nicer:

$$\frac{2}{(-\sqrt{1/q}; 1/q)_\infty + (\sqrt{1/q}; 1/q)_\infty}.$$

In fact,

$$\frac{2}{(-\sqrt{1/2}; 1/2)_\infty + (\sqrt{1/2}; 1/2)_\infty} \sim 0.59546.$$


George E. Andrews and Rodney J. Baxter. "Lattice gas generalization of the hard hexagon model. III. $q$-trinomial coefficients", Journal of statistical physics, 1987.

Lucy Joan Slater. "Further Identities of the Rogers-Ramanujan Type", Proceedings of the London Mathematical Society, 1952.

# Rogers-Ramanujan Identities

**Theorem (Rogers-Ramanujan Identities)**

*Let* $\mid q \mid < 1$, *then*

$$\sum_{n \geq 0} \frac{q^{n^2}}{(q)_n} = \frac{1}{(q;q^5)_\infty (q^4;q^5)_\infty},$$

*and*

$$\sum_{n \geq 0} \frac{q^{n^2+n}}{(q)_n} = \frac{1}{(q^3;q^5)_\infty (q^2;q^5)_\infty}.$$

Srinivasa Ramanujan and Leonard James Roger. "Proof of certain identities in combinatory analysis.", Proc. Cambridge Philos. Soc, 1919.

# Andrews-Gordon Identity

## Theorem (Andrews-Gordon Identity)

*For* $|\, q \,| < 1$ *it holds that*

$$AGI(q,s) := \sum_{n_1,\dots,n_{s-1}\geq 0} \frac{q^{N_1^2+\cdots+N_{s-1}^2}}{(q)_{n_1}\cdots(q)_{n_{s-1}}}$$
$$= \frac{(q^s;q^{2s+1})_\infty (q^{s+1};q^{2s+1})_\infty (q^{2s+1};q^{2s+1})_\infty}{(q)_\infty},$$

*where* $N_i = n_i + \cdots + n_{s-1}$.


George E. Andrews. “An analytic generalization of the Rogers-Ramanujan identities for odd moduli.”, Proceedings of the National Academy of Sciences, 1974.

Basil Gordon. “A combinatorial generalization of the Rogers-Ramanujan identities”, American Journal of Mathematics, 1961.

**Theorem**

*The density as $n \to \infty$ of free codes in $\mathcal{R}^n$ of type $k$ is given by*

$$d(q,s) = \left( \sum_{\substack{k_2,\dots,k_s \geq 0 \\ s \mid K_2+\dots+K_s}} \frac{(1/q)^{K_2^2+\dots+K_s^2-(K_2+\dots+K_s)^2/s}}{(1/q)_{k_2}\cdots(1/q)_{k_s}} \right)^{-1},$$

*where* $K_i = \sum_{j=2}^{i} k_j$.

$$AGI(1/q,s) = \sum_{k_2,\dots,k_s \geq 0} \frac{(1/q)^{K_2^2+\dots+K_s^2}}{(1/q)_{k_2}\cdots(1/q)_{k_s}}$$

# Bounds

**Theorem**

*The density as $n \to \infty$ of free codes in $\mathcal{R}^n$ of type $k$ denoted by $d(q,s)$ can be bounded as follows:*

$$0 < (1/q)_\infty \leq AGI\left(1/q, s\right)^{-1} \leq d(q,s) \leq AGI(1/q', s)^{-1} < 1,$$

*for $q' := q^{s^2-s}$.*

## Other Densities

**Corollary**

*The probability for a code in $\mathcal{R}^n$ of type $k$ to be free is at least $(1/q)_\infty$.*

| $q$ | 2 | 3 | 5 | 7 | 11 | 13 |
|---|---|---|---|---|---|---|
| $(1/q)_\infty$ | 0.2888 | 0.5601 | 0.7603 | 0.8368 | 0.9008 | 0.9172 |

# Other Densities

**Corollary**

*The probability for a code in $\mathcal{R}^n$ of type $k$ to be free is at least $(1/q)_\infty$.*

| $q$ | 2 | 3 | 5 | 7 | 11 | 13 |
|---|---|---|---|---|---|---|
| $(1/q)_\infty$ | 0.2888 | 0.5601 | 0.7603 | 0.8368 | 0.9008 | 0.9172 |

**Corollary**

*The density of free codes in $\mathcal{R}^n$ of type $k$ for $q \to \infty$ is 1.*

# Density for Fixed Rank

The set of weak compositions of $K$ into $s$ parts is

$$C(s, K) := \left\{ (k_1, \ldots, k_s) \mid 0 \leq k_i \leq K, \sum_{i=1}^{s} k_i = K \right\}.$$

The number of codes in $\mathcal{R}^n$ of rank $K$ is given by

$$W(n, K, q, s) := \sum_{(k_1, \ldots, k_s) \in C(s,K)} N_{n,q}(k_1, \ldots, k_s).$$

# Density for Fixed Rank

The set of weak compositions of $K$ into $s$ parts is

$$C(s, K) := \left\{ (k_1, \dots, k_s) \mid 0 \leq k_i \leq K, \sum_{i=1}^{s} k_i = K \right\}.$$

The number of codes in $\mathcal{R}^n$ of rank $K$ is given by

$$W(n, K, q, s) := \sum_{(k_1, \dots, k_s) \in C(s,K)} N_{n,q}(k_1, \dots, k_s).$$

**Theorem**

*Let $K$ and $n$ be positive integers with $K = R'n$. The density of free codes in $\mathcal{R}^n$ of given rank $K$ for $n \to \infty$ is*

$$\begin{cases} 0 & \text{if } 1/2 < R' < 1, \\ 1 & \text{if } R' < 1/2, \\ \geq AGI(1/q, s)^{-1} & \text{if } R' = 1/2. \end{cases}$$

**What parameters should we expect?**

- Free codes of fixed rate as $n \to \infty$ are neither sparse nor dense. The density is independent of the rate and at least $(1/q)_\infty$.
- Free codes of fixed rank-rate as $n \to \infty$ is either dense or sparse, depending on $R' = K/n$.
- For large enough $q$, we expect a random code of fixed type to be free.

## Open Problems

- Establish a simplified condition on $(k_1, \ldots, k_s), (\bar{k}_1, \ldots, \bar{k}_s) \in L(s, n, k)$ such that we have

$$N_{n,q}(k_1, \ldots, k_s) \leq N_{n,q}(\bar{k}_1, \ldots, \bar{k}_s).$$

- For a fixed subtype $(k_1, \ldots, k_s)$ what is the density of codes having this subtype?

# Minimum Distance

We can endow $\mathcal{R}$ with several metrics:

- Hamming metric
- Euclidean metric
- Homogeneous metric
- Lee metric, if $\mathcal{R} = \mathbb{Z}/p^s\mathbb{Z}$

For a code $\mathcal{C} \subseteq \mathcal{R}^n$ its **minimum distance** is given by

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

# Minimum Distance

**Definition (Lee Metric)**

$$\begin{array}{rcccl} x \in \mathbb{Z}/p^s\mathbb{Z} & : & \mathrm{wt}_L(x) & = & \min\{x, \mid p^s - x \mid\}, \\ x \in (\mathbb{Z}/p^s\mathbb{Z})^n & : & \mathrm{wt}_L(x) & = & \sum_{i=1}^n \mathrm{wt}_L(x_i), \\ x, y \in (\mathbb{Z}/p^s\mathbb{Z})^n & : & d_L(x,y) & = & \mathrm{wt}_L(x-y). \end{array}$$

**Example ($\mathbb{Z}/4\mathbb{Z}$)**

$$\begin{array}{ll} \mathrm{wt}_L(0) = 0 & \mathrm{wt}_L(2) = 2 \\ \mathrm{wt}_L(1) = 1 & \mathrm{wt}_L(3) = 1 \end{array}$$

For $M = \lfloor \frac{p^s}{2} \rfloor$:

- $$0 \leq \mathrm{wt}_H(x) \leq \mathrm{wt}_L(x) \leq M\mathrm{wt}_H(x) \leq Mn,$$
- $$d_H(\mathcal{C}) \leq d_L(\mathcal{C}) \leq M d_H(\mathcal{C}).$$

# Classical Singleton Bound

**Theorem (Singleton Bound)**

*A code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension $k$ has minimum Hamming distance*

$$d_H(\mathcal{C}) \leq n - k + 1.$$

Codes that achieve this bound are called *maximum distance separable (MDS) codes.*

- For $n \leq q + 1$ we have a construction of MDS codes: (extended) RS codes
- For $q \to \infty$ MDS codes have density 1
- For $n \to \infty$ MDS codes have density 0 (assuming the MDS conjecture)

**How do maximum Lee distance (MLD) codes behave?**

- What is the analog of the Singleton bound in the Lee metric?
- Are MLD codes dense for $n$ or $q$ going to infinity?

# Some Observations

1. Clearly $d_L(\mathcal{C}) \leq M d_H(\mathcal{C})$
2. Hamming Singleton bound: $d_H(\mathcal{C}) \leq n - k + 1$
3. If $d_L(\mathcal{C}) \leq a d_H(\mathcal{C})$, then

$$\left\lfloor \frac{d_L(\mathcal{C}) - 1}{a} \right\rfloor \leq d_H(\mathcal{C}) - 1$$

   for any such $a$.

# Some Observations

**Proposition**

*For a linear code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of rank $K$ we have*

$$d_H(\mathcal{C}) \leq n - K + 1.$$

- $\mathcal{C}' = \mathcal{C} \cap \langle p^{s-1} \rangle$.
- $\mathcal{C}$ has subtype $(k_1, \ldots, k_s)$ and a generator matrix $G$ in standard form:

$$\mathcal{C}' = \left\{ xG \mid x \in p^{s-1} \left(\mathbb{Z}/p^s\mathbb{Z}\right)^{k_1} \times \cdots \times \left(\mathbb{Z}/p^s\mathbb{Z}\right)^{k_s} \right\}.$$

- $|\mathcal{C}'| = p^{k_1 + \cdots + k_s} = p^K$.
- $\mathcal{C}'$ can be identified with an $[n, K]$ linear code over $\mathbb{F}_p$.

Steven T. Dougherty and Keisuke Shiromoto "MDR codes over $\mathbb{Z}_k$", IEEE Transactions on Information Theory, 2000.

# Singleton Bounds in the Lee Metric

**Theorem (Shiromoto)**

*For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type $k$, we have that*

$$\left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor \leq n - k.$$

Easily follows as $d_L(\mathcal{C}) \leq M d_H(\mathcal{C}) \leq M(n-k+1)$ and the floor remark [3.]

# Singleton Bounds in the Lee Metric

### Theorem (Shiromoto)

*For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type $k$, we have that*

$$\left\lfloor \frac{d_L(\mathcal{C}) - 1}{M} \right\rfloor \leq n - k.$$

Easily follows as $d_L(\mathcal{C}) \leq M d_H(\mathcal{C}) \leq M(n-k+1)$ and the floor remark [3.]

### Example

Let us consider the code $\mathcal{C} = \langle (1,2) \rangle$ over $\mathbb{Z}/5\mathbb{Z}$, which has $M = 2, n = 2, k = 1$ and $d_L = 3$. This code attains the bound of Shiromoto as

$$\left\lfloor \frac{3-1}{2} \right\rfloor = 2 - 1.$$

Keisuke Shiromoto "Singleton bounds over finite rings.", Journal of Algebraic Combinatorics, 2000.

**How many codes attain this bound?**

**How many codes attain this bound?**

**Theorem**

*The only linear codes that attain this Singleton bound are equivalent to* $\mathcal{C} = \langle (1,2) \rangle \subseteq (\mathbb{Z}/5\mathbb{Z})^2$.

**Theorem (Alderson-Huntemann)**

*For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type $1 < k < n$ a positive integer, we have that*

$$d_L(\mathcal{C}) \leq M(n-k).$$

# Singleton Bounds in the Lee Metric

**Theorem (Alderson-Huntemann)**

*For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type $1 < k < n$ a positive integer, we have that*

$$d_L(\mathcal{C}) \leq M(n-k).$$

**Example**

Let $\mathcal{C}_3 = \langle (2,0,1),(1,3,4) \rangle$ over $\mathbb{Z}/5\mathbb{Z}$. Here we have $n=3, k=2, M=2$ and $d_L = 2$. This code attains the bound of Alderson-Huntemann since

$$d_L = 2 = M(n-k) = 2.$$

Tim L. Alderson and Svenja Huntemann "On maximum Lee distance codes.", Journal of Discrete Mathematics, 2013.

**How many codes attain this bound?**

**How many codes attain this bound?**

**Theorem**

*The only linear codes that attain this Singleton bound are*

- *for $p$ odd:*
  - *codes with* $p^s = 5, k+1 \leq n \leq k+3$,
  - *free codes with* $p^s \in \{7, 9\}, n = k+1$,
- *for* $p = 2:$
  - *free codes with* $s = 2, k+1 \leq n \leq k+2$,
  - *free codes with* $s = 3, n = k+1$,
  - $k+1 = K \in \{n, n-1\}$.

**How many codes attain this bound?**

**Theorem**

*The only linear codes that attain this Singleton bound are*

- *for $p$ odd:*
  - *codes with* $p^s = 5, k+1 \leq n \leq k+3,$
  - *free codes with* $p^s \in \{7, 9\}, n = k+1,$
- *for* $p = 2:$
  - *free codes with* $s = 2, k+1 \leq n \leq k+2,$
  - *free codes with* $s = 3, n = k+1,$
  - $k+1 = K \in \{n, n-1\}.$

- The density of MLD codes is 0 for $n \to \infty$
- The density of MLD codes is 0 for $p \to \infty$

Let wt be any weight and $d$ be the minimum distance of $\mathcal{C}$, then

$$d(|\mathcal{C}|-1) \leq \sum_{c \in \mathcal{C}} \mathrm{wt}(c).$$

For the Lee metric, this yields the bound:

$$d_L(\mathcal{C}) \leq \frac{|\mathcal{C}|}{|\mathcal{C}|-1} \overline{\mathrm{wt}}_L(\mathcal{C}),$$

where

$$\overline{\mathrm{wt}}_L(\mathcal{C}) := \frac{1}{|\mathcal{C}|} \sum_{a \in \mathcal{C}} \mathrm{wt}_L(a)$$

is the **average Lee weight of the code** $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$.

The average Lee weight over $\mathbb{Z}/p^s\mathbb{Z}$ is given by

$$\overline{D} = \begin{cases} \frac{p^{2s}-1}{4p^s} & \text{if } p \text{ is odd,} \\ 2^{s-2} & \text{if } p = 2. \end{cases}$$

**Theorem (Wyner and Graham)**

*For any code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type $k$ we have that*

$$d_L(\mathcal{C}) \leq \frac{n\overline{D}}{1 - 1/p^{sk}}.$$

Since

$$\overline{\mathrm{wt}}_L(\mathcal{C}) \leq n\overline{D}.$$

Aaron D. Wyner and Ronald L. Graham "An upper bound on minimum distance for a $k$-ary code.", Inf. Control., 1968.

# Plotkin Bounds in the Lee Metric

For any subcode $\mathcal{C}'$

$$d_L(\mathcal{C}) \leq \frac{\mid \mathcal{C}' \mid}{\mid \mathcal{C}' \mid -1} \overline{wt}_L(\mathcal{C}').$$

**Theorem (Chiang and Wolf)**

*For a free linear code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of type $k$ we have that*

$$d_L(\mathcal{C}) \leq \frac{(n-k+1)\overline{D}}{1-1/p^s}.$$

- Choose a $(n-k) \times n$ parity-check matrix $H$ for the code $\mathcal{C}$.
- Form the $(n-1) \times n$ matrix $H'$ by appending the rows of the $(k-1) \times n$ matrix $[Id_{k-1} \mid 0]$ to $H$.
- The code with parity-check matrix $H'$ is a subcode that contains a word $c$ with $\mathrm{wt}_H(c) \leq n-k+1$: $\mathcal{C}' = \langle c \rangle$.

J. Chung-Yaw Chiang and Jack K. Wolf "On channels and codes for the Lee metric", Information and Control, 1971.

# Plotkin Bounds in the Lee Metric

**Theorem**

*For any linear code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ of free rank $k_1 \geq 1$ we have that*

$$d_L(\mathcal{C}) \leq \frac{(n - k_1 + 1)\overline{D}}{1 - 1/p^s}.$$

- choose a $(n - k_1) \times n$ parity-check matrix $H$ for the code $\mathcal{C}$.
- Form the $(n-1) \times n$ matrix $H'$ by appending the rows of the $(k_1 - 1) \times n$ matrix $[Id_{k_1 - 1} \mid 0]$ to $H$.
- The code with parity-check matrix $H'$ is a subcode that contains a word of Hamming weight at most $n - k_1 + 1$.

$$d_L(\mathcal{C}) \leq \frac{|\langle c\rangle|}{|\langle c\rangle| - 1}\overline{\mathrm{wt}}_L(\langle c\rangle),$$

for a minimum Hamming weight codeword $c$.

- If we can take $c$ in the free part: we get the Chiang and Wolf bound with $k_1$.
- If $c \in \langle p^{s-\ell}\rangle$: how do we bound $\overline{\mathrm{wt}}_L(\langle c\rangle)$?

**We introduce the support subtype**

- For $j \in \{1, \dots, n\}$ let $\pi_j$ be the $j$-th coordinate map.
- Define

$$n_i(\mathcal{C}) := |\{j \in \{1, \dots, n\} \ \mid \ \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|.$$

- For a code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, we call $(n_0, \dots, n_s)$ its support subtype.

**We introduce the support subtype**

- For $j \in \{1, \ldots, n\}$ let $\pi_j$ be the $j$-th coordinate map.
- Define

$$n_i(\mathcal{C}) := |\{j \in \{1, \ldots, n\} \mid \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|.$$

- For a code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, we call $(n_0, \ldots, n_s)$ its support subtype.

**Example**

Let $\mathcal{C}$ be the code over $\mathbb{Z}/8\mathbb{Z}$ generated by

$$G = \begin{pmatrix} 1 & 3 & 5 & 0 & 2 \\ 0 & 2 & 4 & 2 & 6 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 4 & 4 \end{pmatrix}$$

then $\mathcal{C}$ has subtype $(1, 1, 2)$ and support subtype $(3, 2, 0, 0)$.

**We introduce the support subtype**

- For $j \in \{1, \dots, n\}$ let $\pi_j$ be the $j$-th coordinate map.
- Define

$$n_i(\mathcal{C}) := |\{j \in \{1, \dots, n\} \mid \langle \pi_j(\mathcal{C}) \rangle = \langle p^i \rangle\}|.$$

- For a code $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$, we call $(n_0, \dots, n_s)$ its support subtype.

**Example**

Let $\mathcal{C}$ be the code over $\mathbb{Z}/8\mathbb{Z}$ generated by

$$G = \begin{pmatrix} \color{red}{1} & \color{red}{3} & \color{red}{5} & \color{blue}{0} & \color{blue}{2} \\ \color{red}{0} & \color{red}{2} & \color{red}{4} & \color{blue}{2} & \color{blue}{6} \\ \color{red}{0} & \color{red}{0} & \color{red}{4} & \color{blue}{0} & \color{blue}{0} \\ \color{red}{0} & \color{red}{0} & \color{red}{0} & \color{blue}{4} & \color{blue}{4} \end{pmatrix}$$

then $\mathcal{C}$ has subtype $(1, 1, 2)$ and support subtype $(\color{red}{3}, \color{blue}{2}, 0, 0)$.

# Plotkin Bounds in the Lee Metric

**Lemma**

*Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be a linear code of support subtype $(n_0, \ldots, n_s)$. Then*

$$\overline{wt}_L(\mathcal{C}) = \begin{cases} \frac{1}{4p^s}\left(p^{2s}|n-n_s| - \sum_{i=0}^{s-1} p^{2i} n_i\right) & \text{if } p \text{ is odd,} \\ 2^{s-2}|n-n_s| & \text{if } p=2. \end{cases}$$

# Plotkin Bounds in the Lee Metric

**Theorem**

*Let $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ be linear code. Let $\ell \in \{1, \dots, s\}$ such that there exists $y \in \mathcal{C}$ satisfying $wt_H(y) = d_H(y)$ and $y \in \langle p^{s-\ell} \rangle$. Then*

$$d_L(\mathcal{C}) \leq \begin{cases} \dfrac{p^{s-\ell}(p^\ell + 1)}{4} d_H(\mathcal{C}) & \text{if } p \text{ is odd,} \\[2ex] \dfrac{2^{s-2+\ell}}{2^\ell - 1} d_H(\mathcal{C}) & \text{if } p = 2. \end{cases}$$

Eimear Byrne and Violetta Weger "Bounds in the Lee Metric", in preparation.

# Plotkin Bound in the Lee Metric

We can always choose $\ell = 1$ (there is always a minimal Hamming weight codeword in the socle)

## Corollary

*Let* $\mathcal{C} \subseteq (\mathbb{Z}/p^s\mathbb{Z})^n$ *be a linear code of rank* $K$. *Then*

$$\left\lfloor \frac{d_L(\mathcal{C}) - 1}{A} \right\rfloor \leq n - K,$$

*for*

$$A := \begin{cases} \dfrac{p^{s-1}(p+1)}{4} & \text{if } p \text{ is odd}, \\ 2^{s-1} & \text{if } p = 2. \end{cases}$$

Eimear Byrne and Violetta Weger "Bounds in the Lee Metric", in preparation.

**Example**

We consider the code $\mathcal{C} = \langle (0,1,1),(2,0,0),(0,0,2)\rangle \subset (\mathbb{Z}/4\mathbb{Z})^3$. This code attains the new bound for $\ell = 1$ since

$$d_L = 2 = 2(n-K+1).$$

It does not attain the bound of Chiang and Wolf with $k_1$, as

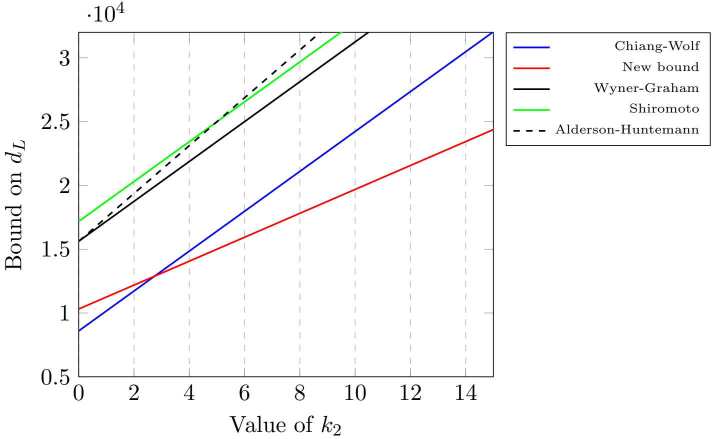
$$d_L \leq \frac{4}{3}(3-1+1) = 4.$$

We also note that we cannot choose $\ell = 2$, since the only codewords that have minimal Hamming weight are divisible by 2. In fact:

$$d_L = 2 \not\leq \frac{4}{3} = \frac{4}{3}(3-3+1).$$

# Comparison of Bounds

Comparison of bounds for codes over $\mathbb{Z}/5^5\mathbb{Z}$ of type $(10, k_2, 0, 0, 0)$ and length $2K, K = 10 + k_2$.



# Density

Note that in order to meet the new bound with $\ell = 1$, we need

1. the socle $\mathcal{C}' = \mathcal{C} \cap \langle p^{s-1} \rangle$ is an MDS code, we can identify it with a $[n, K]$ linear code over $\mathbb{F}_p$,
2. a $x \in \mathcal{C}'$ which generates a Lee-equidistant code.

# Density

Note that in order to meet the new bound with $\ell = 1$, we need

1. the socle $\mathcal{C}' = \mathcal{C} \cap \langle p^{s-1} \rangle$ is an MDS code, we can identify it with a $[n, K]$ linear code over $\mathbb{F}_p$,
2. a $x \in \mathcal{C}'$ which generates a Lee-equidistant code.

$$\Downarrow$$

1. Due to the MDS conjecture: assume $n \leq p + 1$ and $K \leq p$.
2. Due to the characterization of Lee-equidistant codes of Wood: $x$ consists of repetitions of $(\pm 1, \ldots, \pm \frac{p-1}{2})$.

Jay Wood "The structure of linear codes of constant weight", Transactions of the American Mathematical Society, 2002.

# Density

Note that in order to meet the new bound with $\ell = 1$, we need

1. the socle $\mathcal{C}' = \mathcal{C} \cap \langle p^{s-1} \rangle$ is an MDS code, we can identify it with a $[n, K]$ linear code over $\mathbb{F}_p$,
2. a $x \in \mathcal{C}'$ which generates a Lee-equidistant code.

$$\Downarrow$$

1. Due to the MDS conjecture: assume $n \leq p + 1$ and $K \leq p$.
2. Due to the characterization of Lee-equidistant codes of Wood: $x$ consists of repetitions of $(\pm 1, \ldots, \pm \frac{p-1}{2})$.

Can put either 1 or 2 repetitions!

Jay Wood "The structure of linear codes of constant weight", Transactions of the American Mathematical Society, 2002.

## Density

**Proposition**

*Let* $\mathcal{C} \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ *have rank* $K$*. If* $\mathcal{C}$ *meets the new bound then length* $n \leq p+1$ *and either*

$$K = n - p + 2 \leq 3 \text{ and } d_L(\mathcal{C}) = \frac{p^{s-1}(p^2-1)}{4},$$

*or*

$$K = n + 1 - \frac{p-1}{2} \leq \frac{p+5}{2} \text{ and } d_L(\mathcal{C}) = \frac{p^{s-1}(p^2-1)}{8}.$$

# Density

- For $n \to \infty$: the socle $\mathcal{C}'$ is an MDS code over $\mathbb{F}_p$, by the MDS conjecture the density of such codes is zero.
- For $p \to \infty$: Lee-equidistant cyclic modules over $\mathbb{F}_p$ of length $\frac{p-1}{2}$ or $p-1 \leq n \leq p+1$ have density zero.

# Classical Gilbert-Varshamov Bound

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


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 over $\mathbb{F}_q$ achieve the GV bound with high probability


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


**Do ring-linear codes also attain the GV bound?**

# Gilbert-Varshamov Bound

- wt: weight function on $\mathcal{R}^n$.
- $$V(n,w) := \mid \{v \in \mathcal{R}^n \mid \mathrm{wt}(v) \leq w\} \mid .$$
- $N$: the maximal weight an element of $\mathcal{R}^n$ can achieve.
- $$g(\delta) := \lim_{n\to\infty} \frac{1}{n} \log_{q^s}\left(V(n,\delta N)\right).$$
- $AL(n,d)$: the maximal size of a code in $\mathcal{R}^n$ having minimum distance $d$
- $$\overline{R}(\delta) := \limsup_{n\to\infty} \frac{1}{n} \log_{q^s} AL(n,\delta N).$$

# Gilbert-Varshamov Bound

The asymptotic Gilbert-Varshamov bound now states that

$$\overline{R}(\delta) \geq 1 - g(\delta).$$

The asymptotic Gilbert-Varshamov bound now states that

$$\overline{R}(\delta) \geq 1 - g(\delta).$$

**Theorem**

*For the Lee metric, Hamming metric and homogeneous metric, we have that a random code over a finite chain ring achieves the Gilbert-Varshamov bound with high probability.*

Eimear Byrne, Anna-Lena Horlemann, Karan Khathuria and Violetta Weger "Density of Free Modules over Finite Chain Rings", 2021.

### Summary

- Linear MLD codes are sparse.
- Plotkin-optimal linear codes in the Lee metric are sparse.
- Random linear codes over finite chain rings attain the GV bound.

### Open Problems

- Give a construction of optimal codes for the new bound (for any subtype).
- Is there some other way to give a 'better' Singleton-like bound?

# Thank you!