On the Density of Free Codes over Finite Chain Rings

Violetta Weger

Technical University of Munich

Combinatorics 2022
June 3, 2022

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

Motivation

Large interest in code-based cryptography in

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

Motivation

Large interest in code-based cryptography in

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

How do random codes behave over finite chain rings?

Large interest in code-based cryptography in

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

How do random codes behave over finite chain rings?

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

Outline

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

- $\mathbb{Z}/p^s\mathbb{Z}$
- $GR(p^s, r)$

Ring-Linear Coding Theory

	Classical	$\mathcal{R}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	
Code	$\mathcal{C} \subseteq \mathbb{F}_q^n$ linear subspace	
Parameters	length n dimension k	
Number of Codes	$\begin{bmatrix} n \\ k \end{bmatrix}_q$	

Ring-Linear Coding Theory

	Classical	$\mathcal{R}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	Finite chain ring $\mathcal{R}$
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 ?
Number of Codes	$\begin{bmatrix} n \\ k \end{bmatrix}_q$	?

Ring-Linear Coding Theory

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

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

If $k = K$, i.e., subtype $(k, 0, \ldots, 0)$ we say that $\mathcal{C}$ is a **free code**.

Ring-Linear Coding Theory

	Classical	$\mathcal{R}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	Finite chain ring $\mathcal{R}$
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 $\mathcal{R}$-dimension k rank K
Number of Codes	$\begin{bmatrix} n \\ k \end{bmatrix}_q$	?

How likely is it that a random code is free?

How likely is it that a random code is free?

If $P(n)$ is the probability of a random code of a fixed rate $R = \frac{k}{n}$ to be free, then we denote by

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

the **density** of free codes.

How likely is it that a random code is free?

If $P(n)$ is the probability of a random code of a fixed rate $R = \frac{k}{n}$ to be free, then we denote by

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

the **density** of free codes.

$$P(n) = \frac{\text{number of free codes of } \mathcal{R} - \text{dimension } k}{\text{number of codes of } \mathcal{R} - \text{dimension } k}.$$

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 $\mathcal{R}$*-dimension* 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.

$L(s,k)$: the set of all possible subtypes for $\mathcal{R}$-dimension k

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

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

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

$L(s,k)$: the set of all possible subtypes for $\mathcal{R}$-dimension k

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

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

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

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

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

Counting Codes

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

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

Usual q-multinomial coefficient for $n = k_1 + \cdots + k_s$:

$$\begin{bmatrix} n \\ k_1, \ldots, k_s \end{bmatrix}_q = \prod_{i=1}^{s} \begin{bmatrix} \sum_{j=1}^{i} k_j \\ k_i \end{bmatrix}_q.$$

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

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

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

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

Ole S. Warnaar “The Andrews-Gordon identities and q-multinomial coefficients”, Communications in mathematical physics, 1997.

	Classical	$\mathcal{R}$-Linear
Ambient space	Finite field $\mathbb{F}_q$	Finite chain ring $\mathcal{R}$
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 $\mathcal{R}$-dimension k rank K
Number of Codes	$\begin{bmatrix} n \\ k \end{bmatrix}_q$	$\begin{bmatrix} n \\ ks \end{bmatrix}_q^{(s)}$

The q-**Pochhammer symbol**

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

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 $\mathcal{R}$-dimension k is given by

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

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.

Andrews-Gordon Identity

Theorem (Andrews-Gordon Identity)

For $\mid q \mid < 1$ *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 $N_i = n_i + \cdots + n_{s-1}$.

For $s = 2$ this recovers the first Rogers-Ramanujan identity.

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.

Density of Free Codes

Theorem

The density as $n \to \infty$ of free codes in $\mathcal{R}^n$ of $\mathcal{R}$-dimension 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 $K_i = \sum_{j=2}^{i} k_j$.

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

Density of Free Codes

Theorem

The density as $n \to \infty$ of free codes in $\mathcal{R}^n$ of $\mathcal{R}$-dimension 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 $K_i = \sum_{j=2}^{i} k_j$.

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

Generalized identity:

Jehanne Dousse and Robert Osburn. "A q-multisum identity arising from finite chain ring probabilities." 2021.

Bounds

Theorem

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

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

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

Density for Fixed Rank

$C(s,K)$: set of weak compositions of K into s parts

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

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

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

Density for Fixed Rank

$C(s, K)$: set of weak compositions of K into s parts

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

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

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

Classical Gilbert-Varshamov Bound

- Random Hamming-metric codes over $\mathbb{F}_q$ 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 over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ achieve the GV bound

  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: additive 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

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

Gilbert-Varshamov Bound

The asymptotic Gilbert-Varshamov bound now states that

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

Theorem

For any additive weight we have that a random code over a finite chain ring achieves the Gilbert-Varshamov bound with high probability.

Examples for additive weights: Lee metric, Hamming metric, homogeneous metric, ...

What parameters should we expect?

- Free codes of fixed rate as $n \to \infty$ are neither sparse nor dense independent of the rate, and have density at least $(1/q)_\infty$.
- Free codes of fixed rank-rate as $n \to \infty$ are either dense or sparse, depending on $R' = K/n$.
- The minimum distance of a random code is given by the Gilbert-Varshamov bound with high probability as $n \to \infty$.

Open Problems

- Establish a simplified condition on $(k_1, \ldots, k_s), (\bar{k}_1, \ldots, \bar{k}_s) \in L(s,k)$ 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?

Thank you!