

On the Density of Free Codes over Finite Chain Rings

Violetta Weger

University College Dublin



SIAM AG21
August 17, 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 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?

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?

- 1 Ring-Linear Coding Theory
- 2 Parameters: Density of Free Codes
- 3 Minimum Distance: Gilbert-Varshamov Bound
- 4 Open Problems

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*: $q = |\mathcal{R}/\langle \pi \rangle|$.

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

Example

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

	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	

	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 ?

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

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

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

Systematic Form

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

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

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

$$\mathbf{G} = (\text{Id}_k \quad A) \in (\mathbb{Z}/p^s\mathbb{Z})^{k \times n}.$$

Question: Density of Free Codes

Let us fix a rate $R = k/n$. A code of given type k , can have any subtype (k_1, \dots, 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

Let us fix a rate $R = k/n$. A code of given type k , can have any subtype (k_1, \dots, 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

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

if the limit exists.

Proposition

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

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

Corollary

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

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



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

Definition

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

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

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

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

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

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

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

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

We want to compute

$$\lim_{n \rightarrow \infty} P(n).$$

We want to compute

$$\lim_{n \rightarrow \infty} P(n).$$

Example

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

$$\sim 0.59546.$$

- The *Gaussian coefficient*

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

- The *Gaussian coefficient*

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

- The *q-Pochhammer symbol*

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

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

- The *Gaussian coefficient*

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

- The *q-Pochhammer symbol*

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

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

We apply

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^{(n-k)k} \begin{bmatrix} n \\ k \end{bmatrix}_{1/q}$$

on the density

$$\lim_{n \rightarrow \infty} \frac{q^{(n-k)k(s-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q}{M(n, k, q, s)} = \lim_{n \rightarrow \infty} \frac{\begin{bmatrix} n \\ k \end{bmatrix}_{1/q}}{q^{-(n-k)ks} M(n, k, q, s)}.$$

Density of Free Codes

We apply

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^{(n-k)k} \begin{bmatrix} n \\ k \end{bmatrix}_{1/q}$$

on the density

$$\lim_{n \rightarrow \infty} \frac{q^{(n-k)k(s-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q}{M(n, k, q, s)} = \lim_{n \rightarrow \infty} \frac{\begin{bmatrix} n \\ k \end{bmatrix}_{1/q}}{q^{-(n-k)ks} M(n, k, q, s)}.$$

For $k = Rn$ with $0 < R < 1$ we have

$$\lim_{n \rightarrow \infty} \begin{bmatrix} n \\ k \end{bmatrix}_{1/q} = \frac{1}{(1/q)_\infty}.$$

Density of Free Codes

We apply

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^{(n-k)k} \begin{bmatrix} n \\ k \end{bmatrix}_{1/q}$$

on the density




$$\lim_{n \rightarrow \infty} \frac{q^{(n-k)k(s-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q}{M(n, k, q, s)} = \lim_{n \rightarrow \infty} \frac{\begin{bmatrix} n \\ k \end{bmatrix}_{1/q}}{q^{-(n-k)ks} M(n, k, q, s)}.$$

For $k = Rn$ with $0 < R < 1$ we have

$$\lim_{n \rightarrow \infty} \begin{bmatrix} n \\ k \end{bmatrix}_{1/q} = \frac{1}{(1/q)_{\infty}}.$$

What is the limit of $q^{-(n-k)ks} M(n, k, q, s)$?

The answer can be found in

-  George E. Andrews and Rodney J. Baxter. “Lattice gas generalization of the hard hexagon model. III. q -trinomial coefficients”, Journal of statistical physics, 1987.
-  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.
-  Anne Schilling and S. Ole Warnaar. “Supernomial coefficients, polynomial identities and q -series”, The Ramanujan Journal, 1998.

Theorem

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

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

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



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

		Density
$s = 2$	$q = 2$	0.59546
	$q = 3$	0.84191
	$q = 5$	0.95049
	$q = 7$	0.97627
$s = 3$	$q = 2$	0.47084
	$q = 3$	0.79666
	$q = 5$	0.94102
	$q = 7$	0.97295
$s = 4$	$q = 2$	0.42109
	$q = 3$	0.78230
	$q = 5$	0.93915
	$q = 7$	0.97248

Table: Density of free codes in \mathcal{R}^n of a given type

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.

Theorem (Rogers-Ramanujan Identities)

Let $|q| < 1$, 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

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

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

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.

Theorem

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

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

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

		Lower Bound	Exact	Upper Bound
$s = 2$	$q = 2$	0.46026	0.59546	0.74688
	$q = 3$	0.65750	0.84191	0.88752
	$q = 5$	0.79867	0.95049	0.95999
	$q = 7$	0.85678	0.97627	0.97959
$s = 3$	$q = 2$	0.35536	0.47084	0.98413
	$q = 3$	0.58922	0.79666	0.99862
	$q = 5$	0.76770	0.94102	0.99994
	$q = 7$	0.83959	0.97295	$1 - 8.5 \cdot 10^{-6}$
$s = 4$	$q = 2$	0.31866	0.42109	0.99976
	$q = 3$	0.56950	0.78230	$1 - 1.8 \cdot 10^{-6}$
	$q = 5$	0.76180	0.93915	$1 - 4.1 \cdot 10^{-9}$
	$q = 7$	0.83719	0.97248	$1 - 7.2 \cdot 10^{-11}$

Table: Density of free codes in \mathcal{R}^n of a given type

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 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 $q \rightarrow \infty$ is 1.*

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 $q \rightarrow \infty$ is 1.*
- The density of free codes in \mathcal{R}^n of type k for $s \rightarrow \infty$ is $(1/q)_\infty$.*

The set of weak compositions of K into s parts is denoted by $C(s, K)$,

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

The set of weak compositions of K into s parts is denoted by $C(s, K)$,

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

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

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

The set of weak compositions of K into s parts is denoted by $C(s, K)$,

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

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

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

The probability to have a free code of rank-rate $R' = K/n$ is

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

We want to compute

$$\lim_{n \rightarrow \infty} P'(n) = \lim_{n \rightarrow \infty} \frac{q^{(n-K)K(s-1)} \begin{bmatrix} n \\ K \end{bmatrix}_q}{W(n, K, q, s)}.$$

We want to compute

$$\lim_{n \rightarrow \infty} P'(n) = \lim_{n \rightarrow \infty} \frac{q^{(n-K)K(s-1)} \begin{bmatrix} n \\ K \end{bmatrix}_q}{W(n, K, q, s)}.$$

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 $n \rightarrow \infty$ 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?

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

- 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 over \mathbb{F}_q 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: weight function on \mathcal{R}^n .
- $$V(n, w) := |\{v \in \mathcal{R}^n \mid \text{wt}(v) \leq w\}|.$$
- N : the maximal weight an element of \mathcal{R}^n can achieve.

- $$g(\delta) := \lim_{n \rightarrow \infty} \frac{1}{n} \log_{q^s} (V(n, \delta N)).$$

- $AL(n, d)$: the maximal size of a code in \mathcal{R}^n having minimum distance d

- $$\bar{R}(\delta) := \limsup_{n \rightarrow \infty} \frac{1}{n} \log_{q^s} AL(n, \delta N).$$

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.

Open Problems

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

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

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

Thank you!