University of Zurich
Institute of Mathematics

Master Thesis

Weight-induced distance functions on $\mathbb{Z}/p^s\mathbb{Z}$-codes

Author:
Niklas Gassner

Supervisor:
Professor Dr. Joachim Rosenthal
Co-supervisor:
Violetta Weger

Spring Semester 2020

Niklas Gassner
niklas.gassner@uzh.ch

Abstract

The classical way of studying codes is by equipping them with the Hamming weight and the Hamming distance. As a generalization of this, one can study codes equipped with weights and their induced distance. In this master thesis, we study linear $\mathbb{Z}/p^s\mathbb{Z}$-codes equipped with weight-induced distances and show a Plotkin bound for them.

As a concrete example, we will study the p-adic c-distance on codes. We will show that the minimum p-adic c-distance is equivalent to the minimum Hamming distance of a code and develop an analogue of the sphere-packing bound and Plotkin bound for codes equipped with this distance. We will further show that bounds obtained by equipping the code with the Hamming distance are sharper.

Finally, we study the compressed distance on codes, which is another example of a weight-induced distance function. We establish an analogue of the sphere-packing bound and an analogue of the Plotkin bound for $\mathbb{Z}/4\mathbb{Z}$-codes, study the relation with the minimum Hamming distance and relate $\mathbb{Z}/p^s\mathbb{Z}$-codes to $\mathbb{Z}/p^2\mathbb{Z}$-codes. This will be done by extending $\mathbb{Z}/p^s\mathbb{Z}$-codes and then projecting to $(\mathbb{Z}/p^2\mathbb{Z})^n$.

Niklas Gassner
niklas.gassner@uzh.ch

Acknowledgements

I would like to express my sincere gratitude towards my supervisor Professor Dr. Joachim Rosenthal and my co-supervisor Violetta Weger for providing me with guidance and relevant literature while leaving me an immense amount of freedom. Without them, this thesis would have been impossible.

I would like to thank the WhatsApp group "Rhombenkuboktaeder", especially Severin Schraven, Simon Grüning and Marino Gambarara, for helping me out with LaTeX and writing style problems.

Thank you to Celine Gassner for helping me with the intricacies of the English language.

I would further like to thank Yannis Bähni for allowing me to use his LaTeX header and helping me with the formatting.

Finally, I would like to thank my family and friends for bearing and supporting me during these chaotic times.

Niklas Gassner
niklas.gassner@uzh.ch

Contents

1 Introduction, Conventions and Notations . . . 4
1.1 Introduction . . . 4
1.2 Conventions and Notations . . . 5
2 Coding Theory over Finite Fields . . . 6
2.1 Linear Codes . . . 6
2.2 The Sphere-packing Bound . . . 8
2.3 The Singleton Bound . . . 9
2.4 The Gilbert-Varshamov Bound . . . 10
2.5 The Plotkin Bound . . . 11
3 Codes over Finite Rings . . . 12
3.1 Measuring Distances in $(\mathbb{Z}/p^s\mathbb{Z})^n$ . . . 12
3.2 Codes and the Hamming Distance . . . 14
3.3 Bounds on Codes. . . . 16
4 The P-adic Distance on Codes . . . 21
4.1 The P-adic Distance . . . 21
4.2 The P-adic Distance on Codes . . . 23
4.3 Cardinalities of Balls . . . 24
4.4 Relation with the Hamming Distance . . . 25
4.5 An Inferior Upper Bound on Codes . . . 26
4.6 The Plotkin Bound . . . 27
4.7 Behaviour under Projections . . . 29
5 The Compressed Distance . . . 31
5.1 The Compressed Distance on Codes . . . 32
5.2 The Sphere-Packing Bound for the Compressed Distance . . . 33
5.3 On the Plotkin Bound for the Compressed Distance . . . 35
5.4 On the cH-ratio: The Case $\delta = 1$ . . . 37
5.5 Further Results about the cH-ratio . . . 41
5.6 Relation to $s = 2$ . . . 42
5.6.1 Construction . . . 43
5.6.2 Independence of Choices of $\check{t}_i$ . . . 44
5.6.3 Properties . . . 45
5.6.4 Independence of ϕ and the Generators $t_1, ..., t_l$. . . . 47
5.6.5 Behaviour of the Distances . . . 48
5.7 Constructing first Examples . . . 50
5.8 A Nontrivial Example . . . 50
5.9 A More Sophisticated Example . . . 51
References . . . 54

Niklas Gassner
niklas.gassner@uzh.ch

1. Introduction, Conventions and Notations.

1.1. Introduction.

In number theory, the p-adic integers are an object of interest. Algebraically, we may describe them as the subring

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

We can embed $\mathbb{Z}$ in this ring and one can show that it is both local and a principal ideal domain. This ring can be equipped with the p-adic norm: for a nonzero element x, we let n be maximal such that p^n divides x. Then the norm of x is given by $(\frac{1}{p})^n$.

By concatenating this norm, we obtain a weight function on $\mathbb{Z}/p^s\mathbb{Z}$ and thus an induced distance function on $(\mathbb{Z}/p^s\mathbb{Z})^n$. Our goal is to study the behaviour of $\mathbb{Z}/p^s\mathbb{Z}$-codes when equipped with this distance. We focus heavily on proving analogues of classical bounds on codes.

In Chapter 2, we review classical coding theory over finite fields and bounds obtained by equipping codes with the Hamming distance. The most important results for this thesis will be the sphere-packing bound, the Singleton bound and the Plotkin bound. All of these bounds can be found in the literature and understanding them and their proofs will be essential when we prove analogues and generalizations of them for codes over $\mathbb{Z}/p^s\mathbb{Z}$ in later chapters.

This whole chapter is based on the books [Rot06] and [Lin82].

In Chapter 3, we introduce linear $\mathbb{Z}/p^s\mathbb{Z}$-codes, weight functions and distance functions on $(\mathbb{Z}/p^s\mathbb{Z})^n$ and show that every weight function induces a distance function. Upto this point, the chapter is based on definitions from [Gab12] with minor changes. To our knowledge, the rest of this chapter is not described in the literature. We show that every distance function with the property, that the distance of two elements is the same as the distance of their difference to the zerovector, is induced by a weight function. Inspired by homogeneous weight functions which we encountered in [GO04], but were originally introduced in [CH97], we introduce semi-homogeneous weights. Finally, we show a new Plotkin bound for linear codes equipped with semi-homogeneous weights.

In Chapter 4, we introduce the p-adic c-distance on codes over $\mathbb{Z}/p^s\mathbb{Z}$ by defining the p-adic c-norm on $\mathbb{Z}/p^s\mathbb{Z}$. This is a weight function obtained by giving nonunits less weight than units in a way such that the "closer" an element is to zero, the less weight it has. We then extend this to $(\mathbb{Z}/p^s\mathbb{Z})^n$ and take the induced distance. Then we begin to study linear codes equipped with this distance:

We show Theorem 4.24, the main result of this chapter. This theorem says that knowing the minimum p-adic c-distance of a linear code is equivalent to knowing the minimum Hamming distance of said code. Further, we establish an analogue of the sphere-packing

Niklas Gassner
niklas.gassner@uzh.ch

bound for the p-adic c-distance. We then show that the p-adic c-distance is a semi-homogeneous weight and deduce from this a Plotkin bound. We will also show that the sphere-packing bound and the Plotkin bound obtained from Hamming distance are sharper than their analogue obtained from the p-adic c-distance. Finally, we show that free codes preserve their minimum p-adic c-distance under the projection to $(\mathbb{Z}/p\mathbb{Z})^n$ and deduce the important result that free codes preserve their minimum Hamming distance under this projection. This result will be used in proofs of Chapter 5.

To our knowledge codes equipped with this distance have not been studied in the literature and hence the results in this chapter are new.

Chapter 5 contains the main result of the thesis. We define the Overweight as the most extreme weight function that still satisfies the triangle inequality. We then investigate the Compressed Distance, the distance function induced from this weight. We establish a version of the sphere-packing bound for the Compressed Distance. We show that the Overweight is semi-homogeneous exactly on the rings $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$, which allows us to deduce a Plotkin bound for $\mathbb{Z}/4\mathbb{Z}$-codes. We obtained this bound independently from [GO04], where it is shown that the same bound also holds for nonlinear codes.

Then, we relate the minimum Compressed Distance with the minimum Hamming distance by studying their ratio. Finally, we state and proof Theorem 5.41. This theorem is the main result of the thesis and states that we can extend a code such that the projection to $\mathbb{Z}/p^2\mathbb{Z}$ of the extension has the same minimum Hamming distance as the initial code. The proof of this theorem shows that this extension can be explicitly constructed if we are given an explicit isomorphism. Finding this isomorphism, however, is a nontrivial problem. Finally, we construct some examples of codes with fixed parameters that achieve bounds.

To our knowledge, all results in this chapter are new contributions.

1.2. Conventions and Notations.

For the remainder of this thesis, 0 is an element of $\mathbb{N}$, s and n are nonzero natural numbers and p is a natural prime number.

Given a set A and a subset B, we write $A \subsetneq B$ if A is a proper subset, and $A \subset B$ if $A \subsetneq B$ or $A = B$. Given an element $r \in \mathbb{Z}$, its equivalence class in $\mathbb{Z}/p^s\mathbb{Z}$ will be denoted with $\overline{r}$. The image of a map ϕ will be denoted with $\mathrm{Im}(\phi)$ and, if ϕ is a homomorphism, $\mathrm{Ker}(\phi)$ denotes its kernel. Further, if S is a subset of a group G, $\langle S \rangle$ denotes the subgroup generated by S.

Starting from Section 3, all codes will be linear unless explicitly mentioned otherwise.

Niklas Gassner
niklas.gassner@uzh.ch

2. Coding Theory over Finite Fields.

We will start by giving a rough introduction to classical coding theory. The crucial part of coding theory is that we can correct a certain amount of errors depending on the parameters of the code. In order to measure how far apart vectors are, one needs to fix a metric.

As it will be a main emphasis in later sections, we will focus on bounds for codes.

NOTATION 2.1. Let p be a positive prime number, and $m \in \mathbb{N}_{\geq 1}$. Then we denote by $\mathbb{F}_{p^m}$ the field with p^m elements (which is unique up to isomorphism).

As a natural way of measuring distances, one introduces the Hamming distance which counts the number of distinct entries of two n-tuples.

DEFINITION 2.2 (p.6, [Rot06]). Let $F = \mathbb{F}_{p^m}$ and $x = (x_i)_{i=1}^n, y = (y_i)_{i=1}^n \in F^n$. The Hamming distance d_H of x and y is defined as

$$d_H(x, y) := |\{i \in \{1, ..., n\} \mid x_i \neq y_i\}|.$$

LEMMA 2.3. *Let $F = \mathbb{F}_{p^m}$ and $x = (x_i)_{i=1}^n, y = (y_i)_{i=1}^n \in F^n$. Then we have that $d_H(x, y) = d_H(x - y, 0)$.*

Proof. Let $i \in \{1, ..., n\}$. Then $x_i \neq y_i$ if and only if $x_i - y_i \neq 0$, so the statement follows. □

LEMMA 2.4. *Let $x, y, z \in F^n$. Then the following hold:*

- $d_H(x, y) = 0$ *if and only if* $x = y$,
- $d_H(x, y) = d_H(y, x)$,
- $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$.

We will see in Proposition 3.16, that the Hamming distance on $(\mathbb{Z}/p^s\mathbb{Z})^n$ is a distance function. The proof of this can easily be adapted to the case over finite fields.

2.1. Linear Codes.

To make it easier to understand codes, we give them more algebraic structure. A natural way to do is to define them as a subvectorspace of F^n.

This subsection is based on pages 6 and 26 - 32 in [Rot06].

DEFINITION 2.5 (p.26, [Rot06]). A linear $[n, k]$ code over a field $F = \mathbb{F}_{p^m}$ is a subvectorspace of F^n of dimension k.

TERMINOLOGY 2.6. An element of a code is called a codeword.

NOTATION 2.7. From now on, F will always be a finite field (and hence $F = \mathbb{F}_{p^m}$ for some $m \in \mathbb{N}_{\geq 1}$ and a prime p).

A very important parameter of a code is the minimum distance two distinct codewords achieve. In the case of the Hamming distance, we will see that this parameter determines how many errors we can correct.

DEFINITION 2.8 (p.6, [Rot06]). Let C be a linear nonzero $[n, k]$ code over a finite field F. The minimum Hamming distance of C is defined as

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

NOTATION 2.9. Let C be a nonzero linear code. We write C is a $[n, k, d]$ code if C is a $[n, k]$ code and $d = d_H(C)$.

The minimum distance of a linear code can also be defined as the minimal distance of a nonzero codeword to the zero vector.

LEMMA 2.10 (p.28, Proposition 2.1, [Rot06]). *Let C be a linear nonzero $[n, k]$ code over F. Then $d_H(C) = \min\{d_H(x, 0) \mid x \in C \setminus \{0\}\}$.*

Proof. Using Lemma 2.3, we obtain for any $x, y \in C$ that $d_H(x, y) = d_H(x - y, 0)$. Now $x - y \in C$ since C is a subvectorspace of F^n, so we conclude. □

We defined a linear $[n, k]$ code as subvectorspace of F^n. So, naturally, we can represent it as the rowspan of a matrix.

DEFINITION 2.11 (p. 27, [Rot06]). Let C be a nonzero linear $[n, k, d]$ code over F. A generator matrix of C is a $k \times n$ matrix whose k rows are a basis of C.

REMARK 2.12. Let C be a linear $[n, k, d]$ code over F and G a $k \times n$ matrix with coefficients in F. We can write elements of F^k as row vectors and define a linear map as follows:

$$\begin{aligned} \phi : F^k &\to F^n, \\ u &\mapsto uG. \end{aligned}$$

Then G is a generator matrix of C if and only if $\mathrm{Im}(\phi) = C$. Stated differently, G is a $k \times n$ matrix such that $C = \{xG \mid x \in F^k\}$.

Another way to represent a code is as the kernel of a matrix, which turns out to provide useful information about the minimum distance of a code.

DEFINITION 2.13 (p.29, [Rot06]). Let C be a linear $[n, k, d]$ code over F. A parity-check matrix H over F is an $(n - k) \times n$ matrix H satisfying

$$c \in C \Leftrightarrow Hc^T = 0.$$

THEOREM 2.14 (p.31, Theorem 2.2, [Rot06]). *Let C be a nonzero linear code with minimum distance d and H a parity-check matrix of C. Then: The minimum distance d is the largest integer such that every $d - 1$ columns in H are linearly independent.*

The idea of the proof is as in (p. 31, [Rot06]), but the proof is reformulated.

Niklas Gassner
niklas.gassner@uzh.ch

Proof. Write $H = \begin{bmatrix} h_1^T & h_2^T & ... & h_n^T \end{bmatrix}$, that is h_i is the i'th column of H. Let

$$c = (c_i)_{i=1}^n \in C \setminus \{0\}$$

and let

$$\text{supp}(c) = \{j \in \{1, ..., n\} \mid c_j \neq 0\}.$$

be the support of c. Since $Hc^T = 0$ we obtain that

$$0 = \sum_{i=1}^{n} c_i h_i^T = \sum_{j \in \text{supp}(c)} c_j h_j^T.$$

From Lemma 2.10, there exists a codeword $\hat{c} = (\hat{c}_i)_{i=1}^n$ of C with exactly d nonzero entries. Thus

$$0 = \sum_{j \in supp(\hat{c})} \hat{c}_j h_j^T,$$

so we deduce that there exist d columns of H that are linearly dependent.

Further, let $t > 0$ with $t < d$ and assume by contradiction that there exist t linearly dependent columns of H. Let L be a subset of $\{1, ..., n\}$ of cardinality t such that $(h_j^T)_{j \in L}$ are linearly dependent. Pick $(x_j)_{j \in L} \in F^L$ such that not all x_j's are zero and $\sum_{j \in L} x_j h_j^T = 0$.

For $j \in \{1, ..., n\} \setminus L$ set $x_j = 0$ and define $x := (x_i)_{i=1}^n$. Then $x \neq 0$, $d_H(x, 0) = t$ and

$$Hx^T = \sum_{i=1}^{n} x_i h_i^T = \sum_{j \in L} x_j h_j^T = 0,$$

so $x \in C$. But $d_H(x, 0) = t < d_H(C)$, a contradiction. □

2.2. The Sphere-packing Bound.

In this subsection, we follow pages 95-96 in [Rot06]. We will reformulate all results for linear codes.

If we are given a code C with minimum distance d, then we can choose a radius r such that balls of radius r around elements of C do not intersect. We formalize this observation to obtain the sphere-packing bound. Note that we do not use linearity in any proofs, so the result also holds for nonlinear codes.

We start by defining a ball of radius r around x as the set of vectors with distance at most r to x,

Definition 2.15. Let $x \in F^n$, $r \in \mathbb{R}_{\geq 0}$. The ball of radius r around x is defined as

$$B_r(x) := \{y \in F^n \mid d_H(x, y) \leq r\}.$$

For the Hamming distance, we can easily compute the size of such balls.

Niklas Gassner
niklas.gassner@uzh.ch

LEMMA 2.16. *Let $x \in F^n$, $q = |F|$, $r \in \mathbb{R}_{\geq 0}$. Then*

$$|B_r(x)| = \sum_{k=0}^{\lfloor r \rfloor} \binom{n}{k} (q-1)^k.$$

Proof. We have that $d_H(x, y) = d_H(x - y, 0)$, so we may assume that $x = 0$.

For any $y \in F^n$, it holds that $y \in B_r(0)$ if and only if y has at most $\lfloor r \rfloor$ nonzero entries. For all $k \in \{0, 1, ..., \lfloor r \rfloor\}$, we first choose the position of k nonzero entries, so we have $\binom{n}{k}$ choices. Further, there are $q - 1$ nonzero elements in F, so we conclude that there are $\binom{n}{k}(q-1)^k$ choices of elements with k nonzero entries. Summing over all such k, we obtain the result. □

Finally, we can state the sphere-packing bound, which gives us an upper bound on the cardinality of a $[n, k, d]$ code for a given n and d.

THEOREM 2.17 (p. 95, Theorem 4.3, [Rot06]). *Let $q = |F|$ and let C be a nonzero linear $[n, k, d]$ code over F. Then*

$$|C| \cdot |B_{\lfloor \frac{d-1}{2} \rfloor}(0)| \leq q^n.$$

The proof is taken from (p. 95-96, [Rot06]).

Proof. Let $r = \left\lfloor \frac{d-1}{2} \right\rfloor$ and $x, y \in C$.

Claim: $B_r(x) \cap B_r(y) = \emptyset$.

Proof: Assume $z \in B_r(x) \cap B_r(y)$. Then, using Lemma 2.4,

$$d_H(x, y) \leq d_H(x, z) + d_H(y, z) \leq 2r \leq d - 1,$$

a contradiction to $d_H(x, y) \geq d_H(C) = d$.

It follows that the union of balls of radius r around elements of C is disjoint, hence

$$|C||B_r(0)| = |\bigcup_{x \in C} B_r(x)| \leq |F^n| = q^n.$$

□

REMARK 2.18. This result and its proof tell us that a code C of distance d can correct up to $r = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors in the following sense: Let y be an element obtained by altering at most r entries of an element $x \in C$. Formulated differently, y is obtained by adding a vector, called error vector, with at most r nonzero entries to x. Then x is the only element in C that satisfies $d_H(x, y) \leq r$.

2.3. The Singleton Bound.

With a simple observation, we obtain another bound on the size of a linear $[n, k, d]$ code for fixed parameters n, d, named the Singleton bound after Richard Collom Singleton who published it in [Sin64]. Note that the result can easily be adapted to the case of nonlinear codes, as the idea of the proof does not require the code to be linear.

THEOREM 2.19 (p.57, Corollary 5.2.2, [Lin82]). *Let C be a nonzero linear $[n, k, d]$ code over F. Then $k \leq n - d + 1$.*

The proof is also taken from (p. 57, [Lin82]), rewritten with more details.

Proof. Let C be such a code. By erasing the $d-1$ last entries of all codewords, we obtain a new code $\tilde{C} \subset F^{n-d+1}$. If x and y are distinct elements of C, then they must have at least d distinct entries. So if we erase $d-1$ entries, we obtain again two distinct elements of $\tilde{C}$. Thus

$$|F|^k = |F^k| = |C| = |\tilde{C}| \leq |F^{n-d+1}| = |F|^{n-d+1},$$

from which the result follows. □

REMARK 2.20. As mentioned before, the Singleton bound is a bound on the size of a $[n, k, d]$ code for fixed n and minimum distance d. However, the bound can also be used as a bound on the minimum distance d on a code for fixed n and k. Combining this with Remark 2.18, we obtain an upper bound on how many errors an $[n, k]$ code can correct.

We define MDS codes as codes that reach this bound. While they will be of little importance for later chapters, they play an important role in coding theory.

DEFINITION 2.21 (p. 57, [Lin82]). Let C be an $[n, k, d]$ code over F. We call C an MDS code if $k = n - d + 1$.

2.4. The Gilbert-Varshamov Bound.

Most bounds on codes are upper bounds on the size or parameters of a code. However, they usually do not give any information about whether a code reaching the bound exists. The Gilbert-Varshamov bound differs, as it shows the existence codes with certain properties.

Following (p. 95, [Rot06]), we introduce the following notation:

NOTATION 2.22. Let $q = |F|$. We denote the volume of a ball of radius r in F^n with $V_q(n, r)$. That is

$$V_q(n, r) := |B_r(0)|.$$

We will now prove the Gilbert-Varshamov bound. This bound was proved by Edgar Gilbert in [Gil52] and independently by Rom Varshamov in [Var57]. However, we will give the version found in Ron Roth's book.

THEOREM 2.23 (p.97, Theorem 4.4, [Rot06]). *Let $F = \mathbb{F}_q$ and let $n, k \in \mathbb{N}_{\geq 1}$ and $d \in \mathbb{N}_{\geq 2}$ such that*

$$V_q(n-1, d-2) < q^{n-k}.$$

Then there exists a linear $[n, k]$ code C over F with $d_H(C) \geq d$.

The proof is taken from (p.97-98, [Rot06]).

Recall that Theorem 2.14 states that the minimum distance d of a code C is the maximal number, such that every $d-1$ columns in a parity check matrix of C are linearly independent.

Niklas Gassner
niklas.gassner@uzh.ch

Proof. We prove this by constructing a $(n-k) \times n$ parity check matrix such that every $d-1$ columns are linearly independent and then conclude by Theorem 2.14:

We start with the $(n-k) \times (n-k)$ identity matrix and add columns as follows: assume that for $(n-k) < l \leq n$ we have constructed a matrix

$$\begin{bmatrix} h_1^T & h_2^T & ... & h_{l-1}^T \end{bmatrix} \in Mat_{(n-k)\times(l-1)}(F)$$

with columns $h_1^T, ..., h_{l-1}^T \in F^{n-k}$ such that every $d-1$ columns are linearly independent. Write

$$L = \left\{ \sum_{i=1}^{l-1} x_i h_i^T \;\middle|\; x_i \in F, \text{ at most } d-2 \, x_i \text{ are nonzero} \right\}.$$

We can write every element in L as $\sum_{i=1}^{l-1} x_i h_i^T$ for a (not necessarily unique)

$$x = (x_i)_{i=1}^{l-1} \in B_{d-2}(0) \subset F^{l-1}.$$

Hence

$$|L| \leq V_q(l-1, d-2) \leq V_q(n-1, d-2) < q^{n-k},$$

using our assumption in the last inequality. It follows that $F^{n-k} \setminus L$ is nonempty. Thus, picking any $h_l \in F^{n-k} \setminus L$, we see that

$$\tilde{H} := \begin{bmatrix} h_1^T & h_2^T & ... & h_l^T \end{bmatrix}$$

is a matrix such that every $d-1$ columns are linearly independent. □

2.5. The Plotkin Bound.

Finally, we introduce the Plotkin bound, which is obtained by giving a lower bound and an upper bound on the sum of the distances of all pairs of elements in a code. This bound was first published in [Plo60], but we will give the version from Ron Roth's book.

Proposition 2.24 (p.37, Problem 2.7, [Rot06]). *Let C be a linear $[n, k, d]$ code over a finite field F of cardinality q. Then*

$$d \leq \frac{q^{k-1} n (q-1)}{q^k - 1}.$$

We will see an own proof for codes over $\mathbb{Z}/p^s\mathbb{Z}$ at the end of Section 3. The methods used in this proof can easily be adapted to the case of finite fields, so we will omit the proof here.

Niklas Gassner
niklas.gassner@uzh.ch

3. Codes over Finite Rings.

In the following chapter, we will investigate bounds of codes over $\mathbb{Z}/p^s\mathbb{Z}$. We will first generalize the notion of the Hamming distance to distance functions and give a way, to construct such distance functions with additional properties.

Our main results are Proposition 3.6, which says that a distance function is weight-induced if and only if it is induced by a weight function, and Theorem 3.30, a generalization of the Plotkin bound for linear codes.

3.1. Measuring Distances in $(\mathbb{Z}/p^s\mathbb{Z})^n$.

To generalize the Hamming distance, we introduce distance functions. As a way to construct such functions, we further introduce weight functions.

Note that our notion of weight is similar, but not identical to the definition of a norm on (p.67, [Gab12]) since we additionally require that $\mathrm{wt}(x) = \mathrm{wt}(-x)$ for all $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$.

Definition 3.1. A weight function on $(\mathbb{Z}/p^s\mathbb{Z})^n$ is a function

$$\mathrm{wt} : (\mathbb{Z}/p^s\mathbb{Z})^n \to \mathbb{R}$$

satisfying the following properties for all $x, y \in (\mathbb{Z}/p^s\mathbb{Z})^n$:

- $\mathrm{wt}(x) \geq 0$ and $\mathrm{wt}(x) = 0$ if and only if $x = 0$ (positive definiteness),
- $\mathrm{wt}(x) = \mathrm{wt}(-x)$,
- $\mathrm{wt}(x + y) \leq \mathrm{wt}(x) + \mathrm{wt}(y)$.

One can think of the weight of an element as the distance to the zero vector of said element. This is particularly evident in the following example.

Example 3.2 (Section 2.1, [AH13]). The Lee weight on $\mathbb{Z}/p^s\mathbb{Z}$ is given by choosing the set of representatives of $\mathbb{Z}/p^s\mathbb{Z}$ to be $\{0, 1, ..., p^s - 1\}$ and then defining

$$\begin{aligned} \mathrm{wt}_L : \mathbb{Z}/p^s\mathbb{Z} &\to \mathbb{R}, \\ x &\mapsto \min\{x, p^s - x\}. \end{aligned}$$

Further, the Lee distance on $(\mathbb{Z}/p^s\mathbb{Z})^n$ is given by

$$\begin{aligned} \mathrm{wt}_{L,n} : \mathbb{Z}/p^s\mathbb{Z} &\to \mathbb{R}, \\ (x_i)_{i=1}^n &\mapsto \sum_{i=1}^{n} \mathrm{wt}_L(x_i). \end{aligned}$$

Definition 3.3. A distance function on $(\mathbb{Z}/p^s\mathbb{Z})^n$ is a function

$$d : (\mathbb{Z}/p^s\mathbb{Z})^n \times (\mathbb{Z}/p^s\mathbb{Z})^n \to \mathbb{R},$$

such that for all $x, y, z \in (\mathbb{Z}/p^s\mathbb{Z})^n$ we have that

- $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$,
- $d(x, y) = d(y, x)$ (symmetry),
- $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

Niklas Gassner
niklas.gassner@uzh.ch

A distance function d is called weight-induced if, in addition to the above, we have that $d(x,y) = d(x-y,0)$ for all $x, y \in (\mathbb{Z}/p^s\mathbb{Z})^n$.

Given a weight function wt, we can define a distance function as follows:

$$d_{\mathrm{wt}} : (\mathbb{Z}/p^s\mathbb{Z})^n \times (\mathbb{Z}/p^s\mathbb{Z})^n \to \mathbb{R},$$
$$(x,y) \mapsto \mathrm{wt}(x-y).$$

In fact, this distance function is weight-induced, which explains the terminology.

LEMMA 3.4. *The function d_{wt} is a weight-induced distance function.*

Proof. We first prove that d_{wt} is a distance function:

Let $x, y, z \in (\mathbb{Z}/p^s\mathbb{Z})^n$. It follows directly from the positive definiteness of wt that $d_{\mathrm{wt}}(x,y) \geq 0$ and that $d_{\mathrm{wt}}(x,y) = 0$ if and only if $x = y$. As for the symmetry condition, we have that

$$d_{\mathrm{wt}}(x,y) = \mathrm{wt}(x-y) = \mathrm{wt}(-(x-y)) = \mathrm{wt}(y-x) = d_{\mathrm{wt}}(y,x).$$

For the triangle inequality, we obtain that

$$d_{\mathrm{wt}}(x,z) = \mathrm{wt}(x-z) = \mathrm{wt}((x-y)+(y-z)) \leq \mathrm{wt}(x-y)+\mathrm{wt}(y-z) = d_{\mathrm{wt}}(x,y)+d_{\mathrm{wt}}(y,z).$$

Finally, d_{wt} is clearly weight-induced, so the statement follows. □

The following example can also be found in [Section 2.1, [AH13]] with a different formulation of the definition.

EXAMPLE 3.5. The Lee metric on $\mathbb{Z}/p^s\mathbb{Z}$ is defined by

$$d_L : \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{R},$$
$$(\overline{x}, \overline{y}) \mapsto \min\{|r-s| : (r,s) \in \mathbb{Z}^2 \text{ and } \overline{r} = \overline{x}, \overline{s} = \overline{y}\}.$$

Its extension to $(\mathbb{Z}/p^s\mathbb{Z})^n$ is defined by

$$d_{L,n} : (\mathbb{Z}/p^s\mathbb{Z})^n \times (\mathbb{Z}/p^s\mathbb{Z})^n \to \mathbb{R},$$
$$((x_i)_{i=1}^n, (y_i)_{i=1}^n) \mapsto \sum_{i=1}^n d_L(x_i, y_i).$$

One can easily see that $d_L = d_{\mathrm{wt}_L}$ and that $d_{L,n} = d_{\mathrm{wt}_{L,n}}$.

The following result and its proof tell us that, for a given weight function, the weight of an element is indeed the distance to the zero vector for some weight-induced distance function.

PROPOSITION 3.6. *A distance function d is weight-induced if and only if $d = d_{\mathrm{wt}}$ for some weight function* wt.

Proof. "⇐": Immediately from Lemma 3.4.
"⇒": Let $x, y, z \in (\mathbb{Z}/p^s\mathbb{Z})^n$ and assume that d is weight-induced. Define a function wt by

$$\mathrm{wt}(x) := d(x,0).$$

One can easily see that $d_{\mathrm{wt}} = d$.
Claim: wt is a weight-function.
Proof: Clearly, wt is positive definite. Also

$$\mathrm{wt}(x) = d(x,0) = d(0,x) = d(0-x,0) = d(-x,0) = \mathrm{wt}(-x),$$

where we used that d is weight-induced in the third equality.

Further, using the triangle inequality of d, we obtain that

$$\mathrm{wt}(x+y) = d(x+y,0) = d(x,-y) \leq d(x,0) + d(0,-y) = d(x,0) + d(y,0) = \mathrm{wt}(x) + \mathrm{wt}(y),$$

where we used that d is weight-induced in the second and third equality. This concludes the proof of our claim and hence our proposition. □

Finally, we show that we can extend weight functions and distance functions on $\mathbb{Z}/p^s\mathbb{Z}$ to weight functions and distance functions on $(\mathbb{Z}/p^s\mathbb{Z})^n$ by summing the weights or distances of their entries.

Let $\mathrm{wt} : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{R}$ be a weight function. Then we can define an induced weight function on $(\mathbb{Z}/p^s\mathbb{Z})^n$ as follows:

$$\begin{aligned} \mathrm{wt}_n(x) : (\mathbb{Z}/p^s\mathbb{Z})^n &\to \mathbb{R} \\ (x_i)_{i=1}^n &\mapsto \sum_{i=1}^n \mathrm{wt}(x_i). \end{aligned}$$

Lemma 3.7. *The function* wt_n *is a weight function.*

Proof. All three conditions follow immediately from the definition of wt. □

Similarly, given a distance function $d : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{R}$, we can define a distance function

$$\begin{aligned} d_n : (\mathbb{Z}/p^s\mathbb{Z})^n \times (\mathbb{Z}/p^s\mathbb{Z})^n &\to \mathbb{R} \\ ((x_i)_{i=1}^n, (y_i)_{i=1}^n) &\mapsto \sum_{i=1}^n d(x_i, y_i). \end{aligned}$$

Lemma 3.8. *The function* d_n *is a distance function. Further, if* d *is weight-induced, then so is* d_n*.*

Proof. Clear. □

3.2. Codes and the Hamming Distance.

We will now give the notion of a code as a subgroup or submodule of $(\mathbb{Z}/p^s\mathbb{Z})^n$. Note that this notion is weaker than in the case over fields, since we do not always have the notion of a basis.

Definition 3.9. Let $n \in \mathbb{N}$. A linear $\mathbb{Z}/p^s\mathbb{Z}$-code of length n is a subgroup C of $(\mathbb{Z}/p^s\mathbb{Z})^n$.

Remark 3.10. Equivalently, a $\mathbb{Z}/p^s\mathbb{Z}$-code of length n is a $\mathbb{Z}$-submodule or a $\mathbb{Z}/p^s\mathbb{Z}$-submodule of $(\mathbb{Z}/p^s\mathbb{Z})^n$.

We will only consider linear codes over $\mathbb{Z}/p^s\mathbb{Z}$, so from now on, all codes are linear $\mathbb{Z}/p^s\mathbb{Z}$-codes.

The Hamming distance can be defined in a similar way on $\mathbb{Z}/p^s\mathbb{Z}$.

DEFINITION 3.11. Let $v = (v_i)_{i=1}^n, w = (w_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$. The Hamming distance d_H of v and w is defined as

$$d_H(v, w) := |\{v_i \mid v_i \neq w_i\}|.$$

NOTATION 3.12. If there is no ambiguity, the Hamming distance between v and w will simply be denoted with $d(v, w)$.

To show that this is a weight-induced distance function, we introduce the Hamming weight.

DEFINITION 3.13. The Hamming weight on $\mathbb{Z}/p^s\mathbb{Z}$ is the weight given by

$$\begin{aligned} \mathrm{wt}_H : \mathbb{Z}/p^s\mathbb{Z} &\to \mathbb{R}, \\ x &\mapsto \begin{cases} 0 & x = 0, \\ 1 & x \neq 0. \end{cases} \end{aligned}$$

The Hamming weight on $(\mathbb{Z}/p^s\mathbb{Z})^n$ is defined as

$$\begin{aligned} \mathrm{wt}_{H_n} : \mathbb{Z}/p^s\mathbb{Z} &\to \mathbb{R}, \\ (x_i)_{i=1}^n &\mapsto \sum_{i=1}^n \mathrm{wt}_H(x_i). \end{aligned}$$

LEMMA 3.14. *The Hamming weight is a weight function.*

Proof. One can easily see that wt_H is a weight function. Now from 3.7, we see that wt_{H_n} as sum of the weights of the entries is again a weight function. □

NOTATION 3.15. From now on, we will simply write wt_H instead of wt_{H_n}.

PROPOSITION 3.16. *The Hamming distance is a weight-induced distance function.*

Proof. One can see that the Hamming distance $d_H = d_{\mathrm{wt}_H}$, the distance induced by the Hamming weight. So the result follows from Lemma 3.4, which tells us that it is both a distance and weight-induced. □

As in classical coding theory over fields, we can also define the minimum Hamming distance of a code.

DEFINITION 3.17. Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code. The minimum Hamming distance $d_H(C)$ of the code is defined as

$$d_H(C) := \min\{d_H(v, w) \mid v, w \in C, v \neq w\}.$$

Further, $d_H(\{0\}) := \infty$.

Niklas Gassner
niklas.gassner@uzh.ch

LEMMA 3.18. *Let C be a nonzero code of length n. Then*

$$d_H(C) = \min\{d_H(v,0) \mid v \in C \setminus \{0\}\}.$$

Proof. By Proposition 3.16, the Hamming distance is weight-induced. Hence

$$d_H(v,w) = d_H(v-w,0)$$

for all $v, w \in C$. Since C is a group, we have that $v - w \in C$, so the statement follows. □

3.3. Bounds on Codes.

In this subsection, we will investigate under which conditions some of the bounds on codes from the first chapter hold for $\mathbb{Z}/p^s\mathbb{Z}$-codes and weight functions. While some of them can easily be adapted, others require that the weight function satisfies additional properties. We start by studying the Hamming distance.

Similar to the finite field case, we can establish a sphere-packing bound. We start by defining balls of radius r around elements of $(\mathbb{Z}/p^s\mathbb{Z})^n$.

DEFINITION 3.19. Let $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$ and $r \in \mathbb{R}_{\geq 0}$. The ball $B_r(v)$ of radius r around v with respect to the Hamming distance is defined as

$$B_r(v) := \{w \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid d_H(v,w) \leq r\}.$$

We will now give a version of the sphere-packing bound for linear $\mathbb{Z}/p^s\mathbb{Z}$-codes. One can find the statement in greater generality in (p.32, [Lin82]).

THEOREM 3.20. *Let $t \in \mathbb{N}$ and $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n with $d_H(C) \geq 2t+1$. Then*

$$|C| \leq \frac{p^{sn}}{\sum_{k=0}^{t} \binom{n}{k}(p^s-1)^k}.$$

To prove the theorem, we introduce the following lemmata:

LEMMA 3.21. *Let $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$ and $r \in \mathbb{R}_{\geq 0}$. The cardinality of the ball of radius r around v is given by*

$$|B_r(v)| = \sum_{k=0}^{\lfloor r \rfloor} \binom{n}{k}(p^s-1)^k.$$

Proof. The proof is exactly as the proof of Lemma 2.16, which states the cardinality of a ball over finite fields. □

LEMMA 3.22. *Let $t \in \mathbb{N}$ and $v = (v_i)_{i=1}^n, w = (w_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$. Then we have that $d_H(v,w) \geq 2t+1$ if and only if $B_t(v) \cap B_t(w) = \emptyset$.*

Proof. " $\Rightarrow$ ": Assume that $d_H(v,w) \geq 2t+1$ and, by contradiction, that there exists an $x \in B_t(v) \cap B_t(w)$. Then, using the triangle inequality, we obtain that

$$d(v,w) \leq d(v,x) + d(x,w) \leq 2t < 2t+1,$$

Niklas Gassner
niklas.gassner@uzh.ch

a contradiction to the assumption that $d_H(v,w) \geq 2t+1$.
" $\Leftarrow$ ": Assume, by contraposition, that $d_H(v,w) \leq 2t$. Define J to be the set of positions in which v and w differ, that is

$$J := \{i \in \{1,...,n\} \mid v_i \neq w_i\}.$$

If $|J| \geq t+1$, pick some subset I of J of cardinality t. If $|J| \leq t$, pick $I = J$. Note that in both cases $|J \setminus I| \leq t$. Define for all $i \in \{1,...,n\}$ an element x_i as follows:

$$x_i := \begin{cases} v_i = w_i & i \in \{1,...,n\} \setminus J, \\ v_i & i \in I, \\ w_i & i \in J \setminus I. \end{cases}$$

Then $x := (x_i)_{i=1}^n$ satisfies $d_H(v,x) \leq t$ and $d_H(w,x) \leq t$. Hence $x \in B_t(v) \cap B_t(w)$. □

Finally, we can prove Theorem 3.20.

Proof. The proof is exactly the same as the proof of Theorem 2.17, the sphere-packing bound over finite fields. □

What follows is another classical result, known as Singleton bound. The reader may find it in (p.57, [Lin82]). Again, we will only give the result for $\mathbb{Z}/p^s\mathbb{Z}$-codes.

PROPOSITION 3.23. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n and minimum Hamming distance d. Then $|C| \leq (p^s)^{n-d+1}$.*

Proof. Exactly as in the proof of Theorem 2.19, the Singleton bound over finite fields. □

Similar to the finite field case, we define MDS-codes to be codes that reach this upper bound.

DEFINITION 3.24 (p.334, [Rot06]). A code $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ of distance d is called maximum distance separable code (MDS-code) if $|C| = (p^s)^{n-d+1}$.

The remainder of this chapter will be dedicated to generalizing the Plotkin bound to distance functions on $\mathbb{Z}/p^s\mathbb{Z}$ constructed from a weight function on $\mathbb{Z}/p^s\mathbb{Z}$. This bound is obtained by giving a lower bound and an upper bound on the sum of the distances of all pairs of elements in a code. Given an element $a \in \mathbb{Z}/p^s\mathbb{Z}$, we start by counting the number of pairs of elements of a code with difference a in a fixed entry.

DEFINITION 3.25. Let $\mathrm{wt} : (\mathbb{Z}/p^s\mathbb{Z})^n \to \mathbb{R}_{\geq 0}$ be a weight function and $A \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a subset. Then the average weight of A is defined as

$$\overline{\mathrm{wt}}(A) := \frac{\sum_{x \in A} \mathrm{wt}(x)}{|A|}.$$

It turns out, that we need weights to satisfy an additional property for our Plotkin bound on linear codes.

DEFINITION 3.26. Let $\mathrm{wt} : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{R}_{\geq 0}$ be a weight function. We call wt semi-homogeneous if $\overline{\mathrm{wt}}(p^k(\mathbb{Z}/p^s\mathbb{Z})) \leq \overline{\mathrm{wt}}(\mathbb{Z}/p^s\mathbb{Z})$ for all $k \in \{0,1,...,s\}$.

Niklas Gassner
niklas.gassner@uzh.ch

REMARK 3.27. Note that this notion only differs slightly from the notion of a homogeneous weight, which was introduced by Ioana Constantinescu and Werner Heise in [CH97] and can be found in [GO04]. A homogeneous weight must satisfy that the average weight on all nonzero ideals is constant and that elements that generate the same ideal must have the same weight. We only require the average weight of ideals to be bounded by the average weight of our ring $\mathbb{Z}/p^s\mathbb{Z}$.

First, we observe that the number of codewords with a fixed entry x can only take two values.

LEMMA 3.28. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n, $x \in \mathbb{Z}/p^s\mathbb{Z}$ and let*

$$N_{x,k} := |\{(y_i)_{i=1}^n \in C \mid y_k = x\}|.$$

Then $N_{x,k} = 0$ or $N_{x,k} = N_{0,k}$.

Proof. Let $p_k : C \to \mathbb{Z}/p^s\mathbb{Z}$ be the projection onto the k-th coordinate, which is a group homomorphism.

Assume $N_{x,k} \neq 0$. Then there exists a $y = (y_i)_{i=1}^n \in C$ with $y_k = x$. Now, for any $z \in C$, we have that $p_k(z) = p_k(y)$ if and only if $z - y \in \operatorname{Ker}(p_k)$. Hence

$$N_{x,k} = |\operatorname{Ker}(p_k)| = N_{0,k}.$$

□

Now we count the number of pairs $(x, y) \in C^2$ with a fixed difference in the k-th entry.

LEMMA 3.29. *We will use the same notation as in Lemma 3.28. Let $a \in \mathbb{Z}/p^s\mathbb{Z}$. If $N_{a,k} \neq 0$, then there are $|C| \cdot |\operatorname{Ker}(p_k)|$ pairs $((x_i)_{i=1}^n, (y_i)_{i=1}^n) \in C^2$ with $x_k - y_k = a$. If $N_{a,k} = 0$, then there are no such pairs.*

Proof. If $N_{a,k} = 0$, then no such pairs exist since C is closed under subtraction.

Assume $N_{a,k} \neq 0$. Fix $y = (y_i)_{i=1}^n \in C$ and let $x = (x_i)_{i=1}^n \in C$. Then $x_k - y_k = a$ if and only if $x_k = y_k + a$. Again, by closedness of C, $N_{y_k+a,k} \neq 0$. Hence, by Lemma 3.28, we have that $N_{y_k+a,k} = |\operatorname{Ker}(p_k)|$.

Since we chose y arbitrarily, we conclude that there exist $|C| \cdot |\operatorname{Ker}(p_k)|$ such pairs. □

Finally, we are ready to generalize the Plotkin bound to distance functions induced by semi-homogeneous weight-functions on $(\mathbb{Z}/p^s\mathbb{Z})$. We will then conclude the chapter by showing that the Hamming distance is such a distance.

THEOREM 3.30 (Generalized Plotkin bound for linear codes). *Let $\mathrm{wt} : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{R}_{\geq 0}$ be a semi-homogeneous weight-function, wt_n be the induced weight on $(\mathbb{Z}/p^s\mathbb{Z})^n$ and $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ a code of length n with $d_{\mathrm{wt}_n}(C) = d$. Assume that $d > n \cdot \overline{\mathrm{wt}}(\mathbb{Z}/p^s\mathbb{Z})$. Then*

$$|C| \leq \frac{d}{d - n \cdot \overline{\mathrm{wt}}(\mathbb{Z}/p^s\mathbb{Z})}.$$

While being more general, the proof follows the same steps as (p.57,[Lin82]).

Niklas Gassner
niklas.gassner@uzh.ch

Proof. Again, we use the same notation as in Lemma 3.28 and in its proof. Additionally, given some $x \in C$, denote with x_k its k-th entry. Fix a $k \in \{1, ..., n\}$.

Note first that $p_k(C)$ is a subgroup of $\mathbb{Z}/p^s\mathbb{Z}$, hence there exists some $m \leq s$ with $p_k(C) = p^m(\mathbb{Z}/p^s\mathbb{Z})$. Also note that, as a consequence of the isomorphism theorem for groups, we have that $|\operatorname{Im}(p_k)| \cdot |\operatorname{Ker}(p_k)| = |C|$. Thus, if we add the distances of the k'th entries of all pairs, we obtain that

$$\begin{aligned}
\sum_{(x,y)\in C^2} \operatorname{wt}(x_k - y_k) &= \sum_{z\in \operatorname{Im}(p_k)} (\operatorname{wt}(z)|\operatorname{Ker}(p_k)||C|) \\
&= |\operatorname{Ker}(p_k)||C| \sum_{z\in \operatorname{Im}(p_k)} \operatorname{wt}(z) \\
&= |\operatorname{Ker}(p_k)||C||\operatorname{Im}(p_k)| \cdot \overline{\operatorname{wt}}(p^m(\mathbb{Z}/p^s\mathbb{Z})) \\
&= |C|^2 \cdot \overline{\operatorname{wt}}(p^m(\mathbb{Z}/p^s\mathbb{Z})) \\
&\leq |C|^2 \cdot \overline{\operatorname{wt}}(\mathbb{Z}/p^s\mathbb{Z}),
\end{aligned}$$

where we used Lemma 3.29 in the first equality, $|\operatorname{Im}(p_k)| \cdot |\operatorname{Ker}(p_k)| = |C|$ in the last equality and the assumption that wt is semi-homogeneous in the inequality.

Since all distinct pairs $(x, y) \in C^2$ have distance at least d from each other, we now obtain that

$$\begin{aligned}
|C|(|C| - 1)d &\leq \sum_{(x,y)\in C^2} \operatorname{wt}_n(x - y) \\
&= \sum_{k=1}^{n} \sum_{(x,y)\in C^2} \operatorname{wt}(x_k - y_k) \\
&\leq |C|^2 \cdot n \cdot \overline{\operatorname{wt}}(\mathbb{Z}/p^s\mathbb{Z}).
\end{aligned}$$

Dividing both sides by $|C|$ and rearranging the inequality gives

$$|C|(d - n \cdot \overline{\operatorname{wt}}(\mathbb{Z}/p^s\mathbb{Z})) \leq d.$$

The result then follows from the assumption that $d - n \cdot \overline{\operatorname{wt}}(\mathbb{Z}/p^s\mathbb{Z})) > 0$. □

If we reformulate the theorem, we obtain an upper bound on the minimum distance d of a code.

Remark 3.31. If we assume C to be nonzero, we can rearrange the statement from Theorem 3.30 to

$$d \leq \frac{|C| \cdot n \cdot \overline{\operatorname{wt}}(\mathbb{Z}/p^s\mathbb{Z})}{|C| - 1}.$$

It can be seen in the proof of Theorem 3.30 that we do not need the assumption that $d > n \cdot \overline{\operatorname{wt}}(\mathbb{Z}/p^s\mathbb{Z})$ for this formulation of the theorem.

Corollary 3.32. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n with $d_H(C) = d > n\frac{p^s-1}{p^s}$. Then*

$$|C| \leq \frac{d}{d - n\frac{p^s-1}{p^s}}.$$

Niklas Gassner
niklas.gassner@uzh.ch

Proof. Recall that d_H is induced by the weight wt_H given by $\mathrm{wt}_H(0) = 0$ and $\mathrm{wt}_H(x) = 1$ for all $x \in (\mathbb{Z}/p^s\mathbb{Z}) \setminus \{0\}$. Thus we have that

$$\overline{\mathrm{wt}}_H(p^k(\mathbb{Z}/p^s\mathbb{Z})) = \frac{p^{s-k} - 1}{p^{s-k}} = 1 - \frac{1}{p^{s-k}},$$

so it follows that wt_H is semi-homogeneous. The result now follows from Theorem 3.30. □

Niklas Gassner
niklas.gassner@uzh.ch

4. The P-adic Distance on Codes.

The p-adic distance is a way to measure distance on the so called p-adic numbers, an extension of the rational numbers. Since the distance has appearances in number theory and algebra, it is natural to ask whether we can use it to measure distances on codes. And indeed, with slight adaptations, we can define the p-adic distance on $\mathbb{Z}/p^s\mathbb{Z}$.

The most important results in this chapter are Theorem 4.24, which shows that knowing the minimum p-adic c-distance of a code is equivalent to knowing the minimum Hamming distance, and Corollary 4.43, which states that free codes preserve their minimum Hamming distance under the natural projection to $(\mathbb{Z}/p\mathbb{Z})^n$.

We remind the reader of the convention that all codes are linear, unless explicitly mentioned otherwise.

4.1. The P-adic Distance.

In this subsection, we define the p-adic distance for codes over $\mathbb{Z}/p^s\mathbb{Z}$. We start by giving an algebraic lemma. This will be fundamental for the rest of this thesis, as it allows us to easily define weight functions on $\mathbb{Z}/p^s\mathbb{Z}$.

LEMMA 4.1. *Let $\overline{r} \in \mathbb{Z}/p^s\mathbb{Z} \setminus \{\overline{0}\}$. Then there exists a unit $\overline{u}$ and a unique $v \in \{0, ..., s-1\}$ such that $\overline{r} = \overline{up}^v$.*

Proof. The existence of such a factorization follows directly from the existence of a prime factorization in $\mathbb{Z}$.

To prove uniqueness, assume $\overline{r} = \overline{up}^v$, $\overline{r} = \overline{tp}^w$ are two factorizations where $\overline{u}, \overline{t}$ are units. Then there exist representants $r, r' \in \mathbb{Z}$ of $\overline{r}$ with $r = up^v$, $r' = tp^w$ for some $u, p \in \mathbb{Z}$ with $\gcd(u, p) = 1 = \gcd(t, p)$. Since r and r' are both representants of $\overline{r}$, it follows that $r - r' = kp^s$ for some $k \in \mathbb{Z}$. Now, p^v divides r and $v < s$, hence $p^v | (r + kp^s)$. Since $r + kp^s = r'$, we obtain that $v \leq w$.

By exchanging the roles of v and w, we obtain that $w \leq v$, hence $v = w$. □

REMARK 4.2. In general, $\overline{u}$ is not unique. For example, in $\mathbb{Z}/4\mathbb{Z}$ we have that $\overline{2} = \overline{1}\cdot\overline{2} = \overline{3}\cdot\overline{2}$.

NOTATION 4.3. We will from now on omit the $\overline{\ }$ for elements in $\mathbb{Z}/p^s\mathbb{Z}$.

COROLLARY 4.4. *Let A be a subgroup of $\mathbb{Z}/p^s\mathbb{Z}$. Then there exists a $k \in \{0, 1, ..., s\}$ such that $A = p^k(\mathbb{Z}/p^s\mathbb{Z})$.*

Proof. Subgroups of $\mathbb{Z}/p^s\mathbb{Z}$ are $\mathbb{Z}$-submodules of $\mathbb{Z}/p^s\mathbb{Z}$ and hence $\mathbb{Z}/p^s\mathbb{Z}$-submodules of $\mathbb{Z}/p^s\mathbb{Z}$. So subgroups and ideals coincide.

Now, if $A = \{0\}$, then $A = p^s(\mathbb{Z}/p^s\mathbb{Z})$. If $A \neq \{0\}$ pick k minimal such that there exists a unit $u \in (\mathbb{Z}/p^s\mathbb{Z})^*$ with $up^k \in A$. Since A is an ideal it follows that $p^k \in A$ and one can easily deduce from Lemma 4.1 that $A = p^k(\mathbb{Z}/p^s\mathbb{Z})$. □

We define the p-adic c-norm, which measures how far an element is from being a unit: elements that are closer to being a unit have bigger norm.

Niklas Gassner
niklas.gassner@uzh.ch

DEFINITION 4.5. Let $r \in \mathbb{Z}/p^s\mathbb{Z}$, $c \in \mathbb{R}_{\geq 1}$ be a fixed constant. We define the p-adic c-norm $\|r\|_{p,c}$ as

$$\|r\|_{p,c} := \begin{cases} 0 & r = 0, \\ \frac{1}{c^v} & r = up^v \text{ with } u \text{ a unit, } v \in \{0, 1, ..., s-1\}. \end{cases}$$

NOTATION 4.6. The case $c = p$ will be denoted with $\|\cdot\|_p$.

From now on, unless explicitly mentioned otherwise, c will be a real constant greater than or equal to one.

We observe that the p-adic distance is a weight function.

LEMMA 4.7. *For all $r, t \in \mathbb{Z}/p^s\mathbb{Z}$, the p-adic c-norm satisfies the following:*

(1) $\|r\|_{p,c} \geq 0$ and $\|r\|_{p,c} = 0$ if and only if $r = 0$,
(2) $\|-r\|_{p,c} = \|r\|_{p,c}$,
(3) $\|r \cdot t\|_{p,c} \leq \|r\|_{p,c} + \|t\|_{p,c}$ where equality holds if and only if $rt \neq 0$,
(4) $\|r + t\|_{p,c} \leq max\{\|r\|_{p,c}, \|t\|_{p,c}\}$. Further, if $\|r\|_{p,c} \neq \|t\|_{p,c}$, then equality holds.

In particular, it is a weight function as defined in Definition 3.1.

Proof. (1) - (3) follow directly from the definition.
(4): If $r = 0$ or $t = 0$, both statements are clear. Now, assume $r = up^v \neq 0 \neq mp^w = t$, where u, m are units. We may assume that $v \leq w$. Thus $p^v | t$, hence $p^v | (r + t)$. We get that

$$\|r + t\|_{p,c} \leq \frac{1}{c^v} = max\{\|r\|_{p,c}, \|t\|_{p,c}\}.$$

Now, assume that $v < w$. Then $r + t = p^v(u + p^{w-v}m)$. Since u is a unit, p does not divide u. But $p | p^{w-v}m$, hence $p \nmid u + p^{w-v}m$. It follows that

$$\|r + t\|_{p,c} = \frac{1}{c^v} = max\{\|r\|_{p,c}, \|t\|_{p,c}\}.$$

□

Just like all weight functions, the p-adic c-distance induces a weight-induced distance function.

DEFINITION 4.8. Let $a, b \in \mathbb{Z}/p^s\mathbb{Z}$. The p-adic c-distance of a and b is defined as

$$d_{p,c}(a, b) := \|a - b\|_{p,c}.$$

LEMMA 4.9. *The p-adic distance is a weight-induced distance function. That is, for all $x, y, z \in \mathbb{Z}/p^s\mathbb{Z}$, we have that*

(1) $d_{p,c}(x, y) = d_{p,c}(x - y, 0)$,
(2) $d_{p,c}(x, y) = d_{p,c}(y, x)$,
(3) $d_{p,c}(x, z) \leq d_{p,c}(x, y) + d_{p,c}(y, z)$.

Proof. This follows directly from Proposition 3.6. □

4.2. The P-adic Distance on Codes.

We will now extend the p-adic c-norm to higher dimensions.

DEFINITION 4.10. Let $a = (a_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$. The p-adic c-norm of a is defined as

$$\|a\|_{p,c,n} := \sum_{i=1}^{n} \|a_i\|_{p,c}.$$

PROPOSITION 4.11. *Let $x, y, z \in (\mathbb{Z}/p^s\mathbb{Z})^n$. Then*

(1) $\|x\|_{p,c,n} \geq 0$ and $\|x\|_{p,c,n} = 0$ if and only if $x = 0$,
(2) $\|x\|_{p,c,n} = \|-x\|_{p,c,n}$,
(3) $\|x + y\|_{p,c,n} \leq \|x\|_{p,c,n} + \|y\|_{p,c,n}$.

In particular, it is a weight function as defined in Definition 3.1.

Proof. All three statements follow directly from Lemma 3.7 and Lemma 4.7. □

Similarly, we extend the p-adic c-distance to vectors.

DEFINITION 4.12. Let $a = (a_i)_{i=1}^n, b = (b_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$. The p-adic c-distance of a and b is defined as

$$d_{p,c,n}(a, b) := \sum_{i=1}^{n} d_{p,c}(a_i, b_i).$$

REMARK 4.13. Equivalently, $d_{p,c,n}(a, b) = \|a - b\|_{p,c,n}$. In particular, $\|a\|_{p,c,n} = d_{p,c,n}(a, 0)$ for all $a \in (\mathbb{Z}/p^s\mathbb{Z})^n$.

NOTATION 4.14. In the case $n = 1$, we have that $\|\cdot\|_{p,c,n}$ and $\|\cdot\|_{p,c}$ coincide, so we will from now on omit the n and simply write $\|\cdot\|_{p,c}$ for $\|\cdot\|_{p,c,n}$. Similarly, we will also write $d_{p,c}$ for $d_{p,c,n}$.

We show that the extended p-adic c-distance is also a weight-induced distance function.

LEMMA 4.15. *Let $x, y, z \in (\mathbb{Z}/p^s\mathbb{Z})^n$. Then*

(1) $d_{p,c}(x, y) = d_{p,c}(x - y, 0)$,
(2) $d_{p,c}(x, y) = d_{p,c}(y, x)$,
(3) $d_{p,c}(x, y) \leq d_{p,c}(x, z) + d_{p,c}(z, y)$,
(4) $d_{p,c}(px, 0) \leq \frac{1}{c} d_{p,c}(x, 0)$.

Proof. (1),(2) and (3) follow directly from Lemma 3.8 and Lemma 4.9, and (4) follows from Lemma 4.7. □

In a similar way to the minimum Hamming distance of a code, we can also define the minimum p-adic c-distance of a code.

DEFINITION 4.16. Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n. The minimum p-adic c-distance of C is defined as

$$d_{p,c}(C) := \min\{d_{p,c}(x, y) \mid x, y \in C, x \neq y\}.$$

Further, $d_{p,c}(\{0\}) := \infty$.

As an analogue to Lemma 3.18, we can characterize the minimum p-adic c-distance of a code as the minimal distance of a nonzero element to the zero vector.

LEMMA 4.17. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n. Then*

$$d_{p,c}(C) = \min\{d_{p,c}(x,0) \mid x \in C\}.$$

Proof. This follows directly from Lemma 4.15 (1). □

4.3. Cardinalities of Balls.

Just like for the Hamming distance, we can show a sphere-packing bound for the p-adic c-distance. To do so, we compute the cardinalities of balls. However, we will see later that the sphere-packing bound for the p-adic distance is always less sharp than the sphere-packing bound for the Hamming distance.

CONVENTION 4.18. For the following section we will fix $c > 1$.

We start by defining the ball or radius r around v as the set of all elements having distance less than or equal to r to v.

DEFINITION 4.19. Let $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$, $r \in \mathbb{R}_{\geq 0}$. The ball $B_{r,p,c}(v)$ of radius r with respect to the p-adic c-distance around v is defined as

$$B_{r,p,c}(v) := \{w \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid d_{p,c}(v,w) \leq r\}.$$

Our goal is to compute the cardinality of such a ball. As a first step, we compute the number of elements in $\mathbb{Z}/p^s\mathbb{Z}$ with a fixed p-adic c-norm.

LEMMA 4.20. *Let $v \leq s$. Then the cardinality of the ideal $p^v(\mathbb{Z}/p^s\mathbb{Z})$ is p^{s-v}.*

Proof. By the third isomorphism theorem, $(\mathbb{Z}/p^s\mathbb{Z})/(p^v(\mathbb{Z}/p^s\mathbb{Z})) \cong \mathbb{Z}/p^v\mathbb{Z}$. Hence

$$p^v = \frac{|\mathbb{Z}/p^s\mathbb{Z}|}{|p^v\mathbb{Z}/p^s\mathbb{Z}|} = \frac{p^s}{|p^v\mathbb{Z}/p^s\mathbb{Z}|},$$

so the result immediately follows. □

LEMMA 4.21. *The number of elements in $\mathbb{Z}/p^s\mathbb{Z}$ of p-adic c-norm m is*

$$\begin{cases} 1 & m = 0, \\ (p-1)p^{s-v-1} & m = \frac{1}{c^v} \text{ for some } v \in \{0, ..., s-1\}. \end{cases}$$

Proof. Case 1: $m = 0$. Clear.
Case 2: $m = \frac{1}{c^v}$.

Let $r \in \mathbb{Z}/p^s\mathbb{Z}$. The element r has norm $\frac{1}{c^v}$ if and only if $r \in p^v(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{v+1}(\mathbb{Z}/p^s\mathbb{Z})$. So, by Lemma 4.20, there exist $p^{s-v} - p^{s-v-1}$ such elements. □

Finally, we obtain a formula for the cardinality of such balls.

Niklas Gassner
niklas.gassner@uzh.ch

THEOREM 4.22. *Let $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$, $r \in \mathbb{R}_{\geq 1}$. Set*

$$I_r = \left\{ (i_0, i_1, ..., i_s) \in \mathbb{N}^{s+1} \;\middle|\; \sum_{j=0}^{s} i_j = n \text{ and } \sum_{j=0}^{s-1} \frac{i_j}{c^j} \leq r \right\}.$$

Then we have that

$$|B_{r,p,c}(v)| = \sum_{(i_0,...,i_s)\in I_r} \binom{n}{i_0} \prod_{j=1}^{s-1} \binom{n - \sum_{k=0}^{j-1} i_k}{i_j} \prod_{m=0}^{s-1} ((p-1)p^{s-m-1})^{i_m}.$$

Proof. By Lemma 4.15, it suffices to treat the case $v = 0$.

Note that I_r is the set of all $s+1$-tuples $(i_0, i_1, ..., i_s)$ such that a vector in $(\mathbb{Z}/p^s\mathbb{Z})^n$ with i_j entries of p-adic c-norm $\frac{1}{c^j}$ for $j \leq s-1$ and i_s zero entries has distance less than or equal to r to the zerovector.

By Lemma 4.20, the number of elements in $(\mathbb{Z}/p^s\mathbb{Z})^n$ with i_j entries of norm $\frac{1}{c^j}$ for $j < s$ and i_s zero entries is

$$\binom{n}{i_0}((p-1)p^{s-1}) \cdot \binom{n-i_0}{i_1}((p-1)p^{s-2}) \cdot ... \cdot \binom{n-(i_0+...+i_s-2)}{i_{s-1}}(p-1).$$

The result follows now from the definition of I_r. □

This might look intimidating, but with additional conditions, we obtain the following corollary.

COROLLARY 4.23. *Let $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$, $c > n$ and $r = k\frac{1}{c^{s-1}}$ for some $k \in \{0, 1, ..., n\}$. Then*

$$|B_{r,p,c}(v)| = \sum_{m=0}^{k} \binom{n}{m}(p-1)^m.$$

Proof. We apply Theorem 4.22. Since $c > n$ we have that $\frac{1}{c^j} > r$ for $j < s-1$. Thus, for any $(i_0, i_1, ..., i_s) \in I_r$, we must have that $i_j = 0$ for $j < s-1$, so the statement follows. □

4.4. Relation with the Hamming Distance.

In this subsection, we will prove the most important theorem of the section about the p-adic distance. This theorem gives us a formula for the minimum p-adic c-distance of a code which depends only on the minimum Hamming distance, the ring $\mathbb{Z}/p^s\mathbb{Z}$ and the choice of the constant $c \in \mathbb{R}_{\geq 1}$. This formula will be of major importance when we compare bounds on codes obtained from the p-adic c-distance with bounds we got from the Hamming distance.

THEOREM 4.24. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n. Then $d_{p,c}(C) = \frac{1}{c^{s-1}} d_H(C)$.*

Niklas Gassner
niklas.gassner@uzh.ch

Proof. "≥": Let $v = (v_i)_{i=1}^n$ be any nonzero element of C. The Hamming distance $d_H(v, 0)$ is the number of nonzero entries of v, and every nonzero entry has p-adic c-norm greater or equal to $\frac{1}{c^{s-1}}$. Thus we obtain that

$$d_{p,c}(v, 0) \geq \frac{1}{c^{s-1}} d_H(v, 0) \geq \frac{1}{c^{s-1}} d_H(C).$$

"≤": Pick $v = (v_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n \setminus \{0\}$ with $d_H(v, 0)$ minimal. Let $t \in \mathbb{N}$ be maximal with $p^t v \neq 0$. Note:

(1) We have that $d_H(p^t v, 0) \leq d_H(v, 0)$.
(2) By the choice of v we have that $d_H(p^t v, 0) \geq d_H(v, 0)$.

Thus, $d_H(p^t v, 0) = d_H(v, 0)$. Further, by the choice of t, all entries of $p^t v$ are either p^{s-1} or 0. Hence we get that

$$d_{p,c}(C) \leq d_{p,c}(p^t v) = \frac{1}{c^{s-1}} d_H(v, 0) = \frac{1}{c^{s-1}} d_H(C).$$

□

This allows us to use the sphere-packing bound obtained from the Hamming distance for a code whose minimum p-adic c-distance is known.

COROLLARY 4.25. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n, $t \in \mathbb{N}$ such that $d_{p,c}(C) = \frac{2t+1}{c^{s-1}}$. Then $|C| \leq \frac{p^{sn}}{\sum_{k=0}^{t} \binom{n}{k}(p^s-1)^k}$.*

Proof. By Theorem 4.24 we have that $d_H(C) = 2t + 1$. The result now follows from Theorem 3.20. □

COROLLARY 4.26. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n and let $t \in \mathbb{N}$ such that $d_{p,c}(C) = \frac{2t+1}{c^{s-1}}$. Then C can correct up to t errors.*

Proof. By Theorem 4.24, $d_H(C) = 2t+1$, so the code can correct up to t errors by Remark 2.18. □

We also obtain a version of the Singleton bound for the p-adic c-distance.

COROLLARY 4.27. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n with $d_{p,c}(C) = \frac{1}{c^{s-1}}k$. Then we have that*

$$|C| \leq (p^s)^{n-k+1}.$$

Proof. By Theorem 4.24 we have that C is a code of Hamming distance k. The result then follows directly from Proposition 3.23. □

4.5. An Inferior Upper Bound on Codes.

In this subsection we complete the proof of the sphere-packing bound for p-adic distance. Finally, we show that the sphere-packing bound in Corollary 4.25 is sharper.

The following lemma gives a sufficient condition for balls of radius r with respect to the p-adic c-distance to be disjoint. Recall that we have a similar condition for balls of radius

Niklas Gassner
niklas.gassner@uzh.ch

r with respect to Hamming distance to be disjoint in Lemma 3.22, which was necessary and sufficient.

LEMMA 4.28. *Let $t \in \mathbb{N}$, $r = \frac{t}{c^{s-1}}$ and $v, w \in (\mathbb{Z}/p^s\mathbb{Z})^n$. If $d_{p,c}(v,w) \geq \frac{2t+1}{c^{s-1}}$, then $B_{r,p,c}(v) \cap B_{r,p,c}(w) = \emptyset$.*

Proof. Given that $d_{p,c}(v,w) \geq \frac{2t+1}{c^{s-1}}$, assume, by contradiction, that there exists an element x such that $x \in B_{r,p,c}(v) \cap B_{r,p,c}(w)$. Then $d_{p,c}(v,x) \leq \frac{t}{c^{s-1}}$ and $d_{p,c}(x,w) \leq \frac{t}{c^{s-1}}$. Now, using the triangle inequality from Lemma 4.15, we obtain that

$$d_{p,c}(v,w) \leq d_{p,c}(v,x) + d_{p,c}(x,w) \leq \frac{2t}{c^{s-1}} < \frac{2t+1}{c^{s-1}},$$

contradicting our assumption. □

Under these conditions, we give an analogue of the sphere-packing bound for codes. While these conditions may look restrictive, we know from Theorem 4.24 that they are sufficient to investigate linear codes.

COROLLARY 4.29. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n with $d_{p,c} = \frac{2t+1}{c^{s-1}}$ and $r = \frac{t}{c^{s-1}}$. Then we have that*

$$|C| \leq \frac{p^{sn}}{|B_{r,p,c}(0)|}.$$

We will see that the bound for Hamming distance is sharper.

LEMMA 4.30. *Let $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$ and $r \in \mathbb{R}_{\geq 0}$. Then we have that $B_{r,p,c}(v) \subset B_{c^{s-1}r}(v)$.*

Proof. By Proposition 3.16 and Lemma 4.15, it suffices to check $v = 0$. Now, assume that $w \in B_{r,p,c}(0)$. Then $d_{p,c}(w,0) \leq c^{s-1} d_H(w,0)$, hence $w \in B_{c^{s-1}r}(0)$. □

REMARK 4.31. This, in particular, tells us that Corollary 4.29 does not add anything new to the table. Indeed, if $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ is a code with $d_{p,c}(C) = \frac{2t+1}{c^{s-1}}$ and $r = \frac{t}{c^{s-1}}$, then the code satisfies $|C| \leq \frac{p^{sn}}{|B_{r,p,c}(0)|}$. Now, from Theorem 4.24, we also have that $|C| \leq \frac{p^{sn}}{|B_t(0)|}$. But, from Lemma 4.30, $\frac{p^{sn}}{|B_{r,p,c}(0)|} \geq \frac{p^{sn}}{|B_t(0)|}$, so the bound resulting from the Hamming distance is sharper.

4.6. The Plotkin Bound.

We investigate the Plotkin bound for the p-adic distance. It turns out that, once again, the Plotkin bound for the Hamming distance is sharper.

We continue by showing that the p-adic norm is a semi-homogeneous weight, so that we can use Theorem 3.30. Recall, that this means that the average weight satisfies $\overline{\mathrm{wt}}_{p,c}(p^m(\mathbb{Z}/p^s\mathbb{Z})) \leq \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z})$ for all $m \in \{0,1,...,s\}$.

Then, we will show that the Plotkin bound for the Hamming distance always is sharper.

LEMMA 4.32. *Let $m \in \{0, ..., s-1\}$. The average weight of $(p^m(\mathbb{Z}/p^s\mathbb{Z}))$ with respect to the p-adic weight is given by*

$$\overline{\mathrm{wt}}_{p,c}(p^m(\mathbb{Z}/p^s\mathbb{Z})) = \sum_{k=m}^{s-1}(p^{m-k} - p^{m-k-1})\frac{1}{c^k}.$$

Proof. Using Lemma 4.20, there are $p^{s-k} - p^{s-k-1}$ elements in $p^k(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{k+1}(\mathbb{Z}/p^s\mathbb{Z})$, all of norm $\frac{1}{c^k}$, so summing over all k we obtain that

$$\overline{\mathrm{wt}}_{p,c}(p^m(\mathbb{Z}/p^s\mathbb{Z})) = \frac{\sum_{k=m}^{s-1}(p^{s-k} - p^{s-k-1})\frac{1}{c^k}}{p^{s-m}} = \sum_{k=m}^{s-1}(p^{m-k} - p^{m-k-1})\frac{1}{c^k}.$$

□

REMARK 4.33. Since for $c = 1$ we have that $\|x\|_{p,c} = d_H(x, 0)$. Thus the average Hamming weight and the average p-adic weight should coincide. Indeed, $\overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z}) = \frac{p^s-1}{p^s}$, which is also the average weight with respect to the Hamming distance.

COROLLARY 4.34. *The p-adic c-norm is a semi-homogeneous weight function.*

Proof. From Lemma 4.32, we have that

$$\begin{aligned}
\overline{\mathrm{wt}}_{p,c}(p^m(\mathbb{Z}/p^s\mathbb{Z})) &= \sum_{k=m}^{s-1}(p^{m-k} - p^{m-k-1})\frac{1}{c^k} \\
&= \sum_{k=0}^{s-m-1}(p^{-k} - p^{-k-1})\frac{1}{c^{k+m}} \\
&\leq \sum_{k=0}^{s-1}(p^{-k} - p^{-k-1})\frac{1}{c^k} \\
&= \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z}).
\end{aligned}$$

□

Now, let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n with $d_{p,c}(C) = \frac{d}{c^{s-1}}$ and assume that $d_{p,c}(C) > n \cdot \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z})$. Then, from Theorem 3.30, we obtain that

$$|C| \leq \frac{\frac{d}{c^{s-1}}}{\frac{d}{c^{s-1}} - n \cdot \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z})} = \frac{d}{d - c^{s-1}n \cdot \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z})}.$$

We will now show that, again, the Hamming distance gives a sharper bound.

LEMMA 4.35. *Let wt_H be the Hamming weight on $\mathbb{Z}/p^s\mathbb{Z}$ and $c \in \mathbb{R}_{\geq 1}$. Then we have that*

$$\mathrm{wt}_H(\mathbb{Z}/p^s\mathbb{Z}) \leq c^{s-1}\,\mathrm{wt}_{p,c}(\mathbb{Z}/p^s\mathbb{Z}).$$

Proof. We have the following:

$$\overline{\mathrm{wt}}_H(\mathbb{Z}/p^s\mathbb{Z}) = \frac{p^s - 1}{p^s}$$

Niklas Gassner
niklas.gassner@uzh.ch

$$
\begin{aligned}
&= \frac{\sum_{k=0}^{s-1}(p^{s-k}-p^{s-k-1})}{p^s} \\
&\leq \frac{\sum_{k=0}^{s-1}(p^{s-k}-p^{s-k-1})c^{s-k-1}}{p^s} \\
&= c^{s-1}\frac{\sum_{k=0}^{s-1}(p^{s-k}-p^{s-k-1})\frac{1}{c^k}}{p^s} \\
&= c^{s-1}\overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z}).
\end{aligned}
$$

□

Corollary 4.36. *The Plotkin bound for the Hamming distance is sharper than the Plotkin-bound for the p-adic distance. That is:*

let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n with $d_{p,c}(C) = \frac{d}{c^{s-1}}$. Assume that, in addition, we have that $\frac{d}{c^{s-1}} > n \cdot \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z})$. Then we have that

$$|C| \leq \frac{d}{d - n\frac{p^s-1}{p^s}} \leq \frac{d}{d - c^{s-1}n \cdot \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z})}.$$

Proof. By Theorem 4.24 the minimum distance satisfies $d_H(C) = d$. From Lemma 4.35, it follows that

$$d > n\frac{p^{s-1}-1}{p^s} = n \cdot \overline{\mathrm{wt}}_H(\mathbb{Z}/p^s\mathbb{Z}),$$

so the first inequality follows from Corollary 3.32.

Now, again from Lemma 4.35, we obtain that

$$d - n\frac{p^s-1}{p^s} \geq d - c^{s-1}n \cdot \overline{\mathrm{wt}}_{p,c}(\mathbb{Z}/p^s\mathbb{Z}),$$

so the second inequality follows. □

4.7. Behaviour under Projections.

A natural question that arises is how do codes behave under the canonical projections to $(\mathbb{Z}/p\mathbb{Z})^n$. This allows us to gain information about $\mathbb{Z}/p^s\mathbb{Z}$-codes by studying $\mathbb{Z}/p\mathbb{Z}$-codes. As vector spaces, they have stronger properties and thus are easier to understand.

To simplify notation, we fix the integer s.

Notation 4.37. For $k \leq s$, denote with π_k the natural projection $\pi_k : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ which sends a class modulo p^s to its class modulo p^k. The map π_1 will simply be denoted as π.

Notation 4.38. Further, denote with π_k^n the induced map

$$\begin{aligned}
\pi_k^n : (\mathbb{Z}/p^s\mathbb{Z})^n &\to (\mathbb{Z}/p^k\mathbb{Z})^n, \\
(x_i)_{i=1}^n &\mapsto (x_i \bmod p^k)_{i=1}^n.
\end{aligned}$$

The map π_1^n will simply be denoted as π^n.

REMARK 4.39. Observe that π_k is a group homomorphism, hence π_k^n is as well. In particular, π_k^n sends $\mathbb{Z}/p^s\mathbb{Z}$-codes to $\mathbb{Z}/p^k\mathbb{Z}$-codes.

NOTATION 4.40. Recall that in $\mathbb{Z}/p\mathbb{Z}$ the Hamming distance d_H and the p-adic c-distance $d_{p,c}$ coincide, so both will simply be denoted with d.

LEMMA 4.41. *Let $v = (v_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$. Then we have that*

$$d(\pi^n(v), 0) = |\{v_i \mid v_i \in (\mathbb{Z}/p^s\mathbb{Z})^*\}|.$$

Proof. If $v_i \in (\mathbb{Z}/p^s\mathbb{Z})^*$, then $\pi(v_i) \neq 0$. Further, if $v_i \notin (\mathbb{Z}/p^s\mathbb{Z})^*$, then $p|v_i$ or $v_i = 0$. In both cases we obtain that $\pi(v_i) = 0$. □

THEOREM 4.42. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code. Then the minimum p-adic c-distance satisfies $d_{p,c}(C) \leq \frac{1}{c^{s-1}} d(\pi^n(C))$. If C is a free code, equality holds.*

Proof. If $\pi^n(C) = \{0\}$, both statements are clear, so we assume this is not the case.
"$\leq$": Pick $v = (v_i)_{i=1}^n \in C \setminus \{0\}$ with $\pi^n(v) \neq 0$ and $d(\pi^n(v), 0)$ minimal. By Lemma 4.41, $d(\pi^n(v), 0)$ is the number of units in the entries of v, hence we obtain that

$$d_{p,c}(C) \leq d_{p,c}(p^{s-1}v, 0) = \frac{1}{c^{s-1}} d(\pi^n(v), 0) = \frac{1}{c^{s-1}} d(\pi^n(C)).$$

Now assume that C is a free code. We prove the case $c > 1$ since the case $c = 1$ can be proved similarly.
"$\geq$": Let $(b_i)_{i=1}^m$ be a basis of C and pick $v \in C \setminus \{0\}$ with $d_{p,c}(v, 0) = k\frac{1}{c^{s-1}}$, minimal (where we used Theorem 4.24).

Write $v = \sum_{i=1}^m \lambda_i b_i$ with $\lambda_i \in \mathbb{Z}/p^s\mathbb{Z}$ for all $i \in \{1, ..., m\}$. Since $d_{p,c}(v, 0)$ is minimal, it follows that $pv = 0$. It follows that $\sum_{i=1}^m p\lambda_i b_i = 0$, so, by linear independence, we obtain that $p\lambda_i = 0$ for all $i \in \{1, ..., m\}$. Hence $\lambda_i \in \{0, up^{s-1} \mid u \in (\mathbb{Z}/p^s\mathbb{Z})^*\}$ for all $i \in \{1, ..., m\}$ with at least one λ_i nonzero.

In particular, there exists a $w \in C \setminus \{0\}$ with $p^{s-1}w = v$. It follows that w has k entries that are units. Thus, by Lemma 4.41, we conclude that

$$d_{p,c}(C) = d_{p,c}(v, 0) = k\frac{1}{c^{s-1}} = \frac{1}{c^{s-1}} d(\pi^n(w), 0) \geq \frac{1}{c^{s-1}} d(\pi^n(C)).$$

□

By combining the relation of the minimum Hamming distance and the minimum p-adic c-distance of a code with this theorem, we obtain an analogue of the statement for Hamming distance.

COROLLARY 4.43. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code. Then $d_H(C) \leq d(\pi^n(C))$. If C is a free code, equality holds.*

Proof. Follows directly from Theorem 4.24 and Theorem 4.42. □

REMARK 4.44. In the proof of Theorem 4.43 we omitted the case $c = 1$. Note that in the proof of Corollary 4.43 we can pick a $c > 1$. Then the case $c = 1$ follows from this corollary since $d_{p,1} = d_H$.

5. The Compressed Distance.

We have seen that the bounds obtained by decreasing the weight of elements in $p(\mathbb{Z}/p^s\mathbb{Z})$ are less sharp than the classical bounds obtained from the Hamming distance.

So, naturally, we investigate what happens when we increase the weight of elements in $p(\mathbb{Z}/p^s\mathbb{Z})$.

Our most important results will be Corollary 5.17, an analogue of the sphere-packing bound, and Theorem 5.41, which relates the Hamming distance of a $\mathbb{Z}/p^s\mathbb{Z}$-code for s greater than or equal to two to the Hamming distance of a $\mathbb{Z}/p^2\mathbb{Z}$-code. The proof of this theorem is also important, as it gives an almost explicit way of constructing this code.

As in the chapters before, we follow the convention that all codes are linear unless explicitly mentioned otherwise.

The following definition will be crucial for the rest of the thesis.

Definition 5.1. The overweight function is defined as

$$\begin{aligned} \mathrm{Wt} : \mathbb{Z}/p^s\mathbb{Z} &\to \mathbb{R}_{\geq 0}, \\ x &\mapsto \begin{cases} 0 & x = 0, \\ 1 & x \in (\mathbb{Z}/p^s\mathbb{Z})^*, \\ 2 & else. \end{cases} \end{aligned}$$

Remark 5.2. Equivalently, we can define the overweight function as

$$\begin{aligned} \mathrm{Wt} : \mathbb{Z}/p^s\mathbb{Z} &\to \mathbb{R}_{\geq 0}, \\ x &\mapsto \begin{cases} 0 & x = 0, \\ 1 & x \in (\mathbb{Z}/p^s\mathbb{Z}) \setminus p(\mathbb{Z}/p^s\mathbb{Z}), \\ 2 & x \in p(\mathbb{Z}/p^s\mathbb{Z}) \setminus \{0\}. \end{cases} \end{aligned}$$

Lemma 5.3. *The overweight function is a weight function. That is:*

(1) $\mathrm{Wt}(x) \geq 0$ *for all* $x \in \mathbb{Z}/p^s\mathbb{Z}$ *and* $\mathrm{Wt}(x) = 0$ *if and only if* $x = 0$,
(2) $\mathrm{Wt}(x) = \mathrm{Wt}(-x)$ *for all* $x \in \mathbb{Z}/p^s\mathbb{Z}$,
(3) $\mathrm{Wt}(x + y) \leq \mathrm{Wt}(x) + \mathrm{Wt}(y)$ *for all* $x, y \in \mathbb{Z}/p^s\mathbb{Z}$.

Proof. (1) and (2) are clear.
(3) : Assume that $y = 0$. Then $\mathrm{Wt}(x) = \mathrm{Wt}(x+y)$ and $\mathrm{Wt}(x) = \mathrm{Wt}(x)+\mathrm{Wt}(y)$. Similarly, the case $x = 0$ follows.

Now, assume x and y are both nonzero. Then

$$\mathrm{Wt}(x + y) \leq 2 \leq \mathrm{Wt}(x) + \mathrm{Wt}(y).$$

□

Remark 5.4. In a sense, the overweight is the "most extreme" function to still be a weight function. If we further increase the weight of nonzero nonunits, then $\mathrm{Wt}(x + y) \leq \mathrm{Wt}(x) + \mathrm{Wt}(y)$ no longer holds.

Niklas Gassner
niklas.gassner@uzh.ch

Recall, that given a weight function $\mathrm{wt} : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{R}$, we have an induced distance function on $(\mathbb{Z}/p^s\mathbb{Z})^n$ given by

$$d_{\mathrm{wt}_n} : (\mathbb{Z}/p^s\mathbb{Z})^n \times (\mathbb{Z}/p^s\mathbb{Z})^n \to \mathbb{R},$$
$$((x_i)_{i=1}^n, (y_i)_{i=1}^n) \mapsto \sum_{i=1}^n \mathrm{wt}(x_i - y_i).$$

We use this to define a distance function.

Definition 5.5. Let Wt_n be the weight function on $(\mathbb{Z}/p^s\mathbb{Z})^n$ induced by Wt. The compressed distance is defined as

$$\check{d} := d_{\mathrm{Wt}_n}.$$

By construction, the compressed distance is weight-induced.

Lemma 5.6. *The compressed distance is a weight-induced distance function.*

Proof. Follows directly from Proposition 3.6. □

5.1. The Compressed Distance on Codes.

Analogously to Definition 2.8, we define the minimum compressed distance as the minimal distance between two distinct codewords.

Definition 5.7. Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n. The minimum compressed distance of C is defined as

$$\check{d}(C) := \min\{\check{d}(x, y) \mid (x, y) \in C^2 \text{ and } x \neq y \}.$$

Further, $\check{d}(\{0\}) := \infty$.

The compressed distance is weight-induced, so we can once again characterize the minimum compressed distance ofa code as the minimal distance of all nonzero codewords to the zero vector.

Lemma 5.8. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code. Then*

$$\check{d}(C) = \min\{\check{d}(x, 0) \mid x \in C \setminus \{0\}\}.$$

Proof. By Lemma 5.6 we have that $\check{d}$ is weight-induced, so for any x, y we have that $\check{d}(x, y) = \check{d}(x - y, 0)$. Further, if $(x, y) \in C^2$, then $x - y \in C$, so the statement follows. □

We want to relate the minimum compressed distance with the minimum Hamming distance. Observe first that the minimum compressed distance of a code must be between the minimum Hamming distance and twice the minimum Hamming distance.

Lemma 5.9. *Let d_H denote the Hamming distance and $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code. Then we have that*

$$d_H(C) \leq \check{d}(C) \leq 2d_H(C).$$

Proof. Clear. □

We introduce the cH-ratio as the ratio of the minimum compressed distance to the minimum Hamming distance. We will further investigate this ratio in later subsections, as it helps us to relate these two distances.

DEFINITION 5.10. Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code. The compressed/Hamming-ratio (cH-ratio) δ_C of C is the unique $\delta_C \in [1,2]$ with $\check{d}(C) = \delta_C d_H(C)$.

NOTATION 5.11. If there is no ambiguity as to which C is meant, we simply write δ for δ_C.

The following examples show that δ can indeed take values in between 1 and 2:

EXAMPLE 5.12. The following are examples for different cH-ratios:

(1) $\mathbb{Z}/4\mathbb{Z}$ is a code over $\mathbb{Z}/4\mathbb{Z}$ of length 1 with $\delta = 1$.
(2) $2(\mathbb{Z}/4\mathbb{Z})$ is a code over $\mathbb{Z}/4\mathbb{Z}$ of length 1 with $\delta = 2$.
(3) The code $C := \langle \begin{pmatrix} 1 & 1 & 1 & 2 \end{pmatrix} \rangle \subset (\mathbb{Z}/4\mathbb{Z})^4$ satisfies $d_H(C) = 3$, $\check{d}(C) = 5$ and hence $\delta = \frac{5}{3}$.

5.2. The Sphere-Packing Bound for the Compressed Distance.

As for previous distance functions, we want to establish an analogue of the sphere-packing bound for the compressed distance. The approach is the same as for other distances: we compute the cardinalities of balls and show that balls of radius t around elements $v, w \in (\mathbb{Z}/p^s\mathbb{Z})^n$ do not intersect if $\check{d}(v,w)$ is big enough.

As before, we define balls with radius r around an element $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$ as the set of elements with distance less than or equal to r to x.

DEFINITION 5.13. Let $r \in \mathbb{R}_{\geq 0}$, $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$. The ball $B_{r,\check{d}}(x)$ of radius r with respect to the compressed distance and center x is defined as

$$B_{r,\check{d}}(x) := \{y \in (\mathbb{Z}/p^s\mathbb{Z})^n \mid \check{d}(x,y) \leq r\}.$$

Our goal is to show that balls around elements do not intersect if and only if these elements have compressed distance big enough. For this we introduce the following lemma, which tells us that if elements of $\mathbb{Z}/p^s\mathbb{Z}$ have compressed distance 2, then there exists an element in $\mathbb{Z}/p^s\mathbb{Z}$ having distance 1 to both of them.

LEMMA 5.14. *Let $x, y \in \mathbb{Z}/p^s\mathbb{Z}$ with $\mathrm{Wt}(x-y) = 2$. Then $\mathrm{Wt}(y-(x+1)) = \mathrm{Wt}(x-(x+1)) = 1$.*

Proof. The case $s = 1$ is tautological since such x, y do not exist. Hence we are left with the case $s \geq 2$. Let $x, y \in \mathbb{Z}/p^s\mathbb{Z}$ such that $\mathrm{Wt}(x-y) = 2$. This implies that $x - y \in p(\mathbb{Z}/p^s\mathbb{Z})$ and hence also $y - x \in p(\mathbb{Z}/p^s\mathbb{Z})$. It follows that $y - (x+1) \in (\mathbb{Z}/p^s\mathbb{Z}) \setminus p(\mathbb{Z}/p^s\mathbb{Z})$, which implies that $\mathrm{Wt}(y-(x+1)) = 1$.

Further, $x - (x+1) = -1$, which is a multiplicative unit, so $\mathrm{Wt}(x-(x+1)) = 1$. □

We give a sufficient and necessary condition for balls around elements to be disjoint. Note that we only need the condition to be sufficient for the proof of the sphere-packing bound.

Niklas Gassner
niklas.gassner@uzh.ch

LEMMA 5.15. *Let $t \in \mathbb{N}$ and $x = (x_i)_{i=1}^n, y = (y_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$. Then $\check{d}(x,y) \geq 2t+1$ if and only if $B_{t,\check{d}}(x) \cap B_{t,\check{d}}(y) = \emptyset$.*

Proof. " $\Rightarrow$ " : Clear.
" $\Leftarrow$ " : Assume, by contraposition, that $\check{d}(x,y) \leq 2t$. Notice that necessarily we have that $\left\lceil \frac{1}{2}\check{d}(x,y) \right\rceil \leq t$.

For all $j \in \{0,1,2\}$, we define I_j as the set of indices $k \in \{1,...,n\}$ such that the distance of x_k and y_k is j. That is

$$\begin{aligned} I_1 &:= \{j \in \{1,...,n\} \mid \mathrm{Wt}(x_j - y_j) = 1\}, \\ I_2 &:= \{j \in \{1,...,n\} \mid \mathrm{Wt}(x_j - y_j) = 2\}, \\ I_0 &:= \{1,...,n\} \setminus (I_1 \cup I_2). \end{aligned}$$

Notice that $\check{d}(x,y) = |I_1| + 2|I_2|$. We can write $I_1 = \{i_1,...,i_{|I_1|}\}$ and define

$$J_1 := \{i_1,...,i_{\left\lceil \frac{|I_1|}{2} \right\rceil}\}.$$

Further, for all $k \in \{1,...,n\}$, we define z_k as

$$z_k := \begin{cases} x_j = y_j & k \in I_0, \\ x_j & k \in J_1, \\ y_j & k \in I_1 \setminus J_1, \\ x_j + 1 & \in I_2. \end{cases}$$

and set $z := (z_i)_{i=1}^n$. Then, using Lemma 5.14 in the second equality, we obtain that

$$\check{d}(x,z) = \sum_{i=1}^n \mathrm{Wt}(x_i - z_i) = |I_1 \setminus J_1| + |I_2| \leq \frac{1}{2}(|I_1| + 2|I_2|) = \frac{1}{2}\check{d}(x,y) \leq t$$

and

$$\check{d}(y,z) = \sum_{i=1}^n \mathrm{Wt}(y_i - z_i) = |J_1| + |I_2| = \left\lceil \frac{|I_1|}{2} \right\rceil + |I_2| = \left\lceil \frac{|I_1|}{2} + |I_2| \right\rceil = \left\lceil \frac{1}{2}\check{d}(x,y) \right\rceil \leq t,$$

where we once again used Lemma 5.14 in the second equality. Hence, $z \in B_{t,\check{d}}(x) \cap B_{t,\check{d}}(y)$, which concludes the proof. □

We give an explicit formula for the cardinality of balls with respect to the compressed distance.

PROPOSITION 5.16. *Let $x \in (\mathbb{Z}/p^s\mathbb{Z})^n$ and $t \in \{0,1,...,2n+1\}$. Then we have that*

$$|B_{t,\check{d}}(x)| = \sum_{k=0}^{\left\lfloor \frac{t}{2} \right\rfloor} \sum_{m=0}^{\min\{t-2k, n-k\}} \binom{n}{k} (p^{s-1}-1)^k \binom{n-k}{m} (p^s - p^{s-1})^m.$$

Niklas Gassner
niklas.gassner@uzh.ch

Proof. From Lemma 5.6, it suffices to treat the case $x = 0$.

Now, assume $y = (y_i)_{i=1}^n$ has k entries y_i with $\mathrm{Wt}(y_i) = 2$, m entries y_i such that $\mathrm{Wt}(y_i) = 1$ and all other entries are zero.

Then $y \in B_{t,\check{d}}(x)$ if and only if $2k+m \leq t$. But this holds if and only if $k \in \{0, ..., \lfloor \frac{t}{2} \rfloor\}$ and $m \leq t - 2k$. Since we have already chosen k positions for entries y_i with $\mathrm{Wt}(y_i) = 2$, we also have that $m \leq n - k$, hence it follows that $m \leq \min\{t - 2k, n - k\}$.

There are $p^{s-1} - 1$ elements x in $\mathbb{Z}/p^s\mathbb{Z}$ of $\mathrm{Wt}(x) = 2$ and $p^s - p^{s-1}$ elements x with $\mathrm{Wt}(x) = 1$.

So, for fixed k, m with $2k + m \leq t$, we choose k positions for entries with $Wt = 2$. This gives us $\binom{n}{k}$ possibilities for the choice of positions and $(p^{s-1} - 1)$ possibilities of elements of weight two for each entry, hence we obtain $\binom{n}{k}(p^{s-1} - 1)^k$ possibilities.

Further, we choose m positions from the remaining $n-k$ positions for elements of weight one. For each entry, there are $(p^s - p^{s-1})$ choices of elements of weight one, which gives us $\binom{n-k}{m}(p^s - p^{s-1})^m$ possibilities.

Combining this, we obtain that the number of choices of vectors $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$ with $\check{d}(0, v) = 2k + m$ is

$$\binom{n}{k}(p^{s-1} - 1)^k \binom{n-k}{m}(p^s - p^{s-1})^m.$$

Summing over all such pairs (k, m), we obtain the result. □

We finally obtain the sphere-packing bound for compressed distance by combining previous results.

Corollary 5.17. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n, $t \in \mathbb{N}$ and assume that $\check{d}(C) \geq 2t + 1$. Then we have that*

$$|C| \leq \frac{p^{sn}}{\sum_{k=0}^{\lfloor \frac{t}{2} \rfloor} \sum_{m=0}^{\min\{t-2k, n-k\}} \binom{n}{k}(p^{s-1} - 1)^k \binom{n-k}{m}(p^s - p^{s-1})^m}.$$

Proof. Let $x \neq y$ be elements of C. Lemma 5.15 implies that $B_{t,\check{d}}(x) \cap B_{t,\check{d}}(y) = \emptyset$. Thus, we obtain that

$$|C||B_{t,\check{d}}(0)| = |\bigsqcup_{x \in C} B_{t,\check{d}}(x)| \leq |(\mathbb{Z}/p^s\mathbb{Z})^n| = p^{sn}.$$

Necessarily we have that $t \leq 2n + 1$, so dividing by $|B_{t,\check{d}}(0)|$ and using Proposition 5.16, we obtain the result. □

5.3. On the Plotkin Bound for the Compressed Distance.

Recall that, in order to use the Plotkin bound from Theorem 3.30, we require our weight function to be semi-homogeneous. So we investigate under which conditions for p and s the average weight satisfies $\overline{\mathrm{Wt}}(p^m(\mathbb{Z}/p^s\mathbb{Z})) \leq \overline{\mathrm{Wt}}(\mathbb{Z}/p^s\mathbb{Z})$ for all $m \in \{0, 1, ..., s\}$.

To do so, we first give a formula for $\overline{\mathrm{Wt}}(p^m(\mathbb{Z}/p^s\mathbb{Z})$.

LEMMA 5.18. *Let $m \in \{0, 1, ..., s\}$. Then we have that*

$$\overline{\mathrm{Wt}}(p^m(\mathbb{Z}/p^s\mathbb{Z})) = \begin{cases} \frac{p^s+p^{s-1}-2}{p^s} & m = 0, \\ 2\frac{p^{s-m}-1}{p^{s-m}} & m \in \{1, ..., s\}. \end{cases}$$

Proof. Case 1: $m = 0$.

From the isomorphism theorems, it follows that $|p(\mathbb{Z}/p^s\mathbb{Z})| = p^{s-1}$. Hence, there are $p^{s-1}-1$ elements x with $\mathrm{Wt}(x) = 2$, $p^s - p^{s-1}$ elements x with $\mathrm{Wt}(x) = 1$ and one element of weight 0. Adding these weights and dividing by p^s, we obtain the result.

Case 2: $m > 0$.

Similarly, we have $p^{s-m} - 1$ elements of weight 2 and one element of weight 0. Dividing by $p^{s-m} = |p^m(\mathbb{Z}/p^s\mathbb{Z})|$ yields the claim. □

It turns out that $p = 2$ and $s = 2$ is the only nontrivial case for which the overweight is semi-homogeneous.

PROPOSITION 5.19. *The overweight* Wt *is semi-homogeneous if and only if $s = 1$ or $\mathbb{Z}/p^s\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$.*

Proof. "⇒": Assume first, by contraposition, that $s \geq 2$ and $p > 2$. Then, using Lemma 5.18, we have that

$$\overline{\mathrm{Wt}}(\mathbb{Z}/p^s\mathbb{Z}) = 1 + \left(\frac{1}{p} - \frac{2}{p^s}\right) = 1 + \frac{p^{s-1} - 2}{p^s}$$

and

$$\overline{\mathrm{Wt}}(p(\mathbb{Z}/p^s\mathbb{Z})) = 1 + \left(1 - \frac{2}{p^{s-1}}\right) = 1 + \frac{p^s - 2p}{p^s}.$$

So it suffices to show that $p^{s-1} - 2 < p(p^{s-1} - 2)$, which holds since $p^{s-1} - 2 > 0$.

Now assume, again by contraposition, that $p = 2$ and $s \geq 3$. In this case,

$$\overline{\mathrm{Wt}}(\mathbb{Z}/2^s\mathbb{Z}) = 1 + \left(\frac{1}{2} - \frac{1}{2^{s-1}}\right)$$

and

$$\overline{\mathrm{Wt}}(2(\mathbb{Z}/2^s\mathbb{Z})) = 1 + \left(1 - \frac{1}{2^{s-2}}\right).$$

Now, since $s \geq 3$,

$$\left(\frac{1}{2} - \frac{1}{2^{s-1}}\right) < \frac{1}{2} < \left(1 - \frac{1}{2^{s-1}}\right).$$

"⇐": The case $s = 1$ is trivial, and for $\mathbb{Z}/4\mathbb{Z}$ we have that

$$\overline{\mathrm{Wt}}(\mathbb{Z}/4\mathbb{Z}) = 1 = \overline{\mathrm{Wt}}(2(\mathbb{Z}/4\mathbb{Z}).$$

□

Niklas Gassner
niklas.gassner@uzh.ch

REMARK 5.20. In fact, we have shown that Wt is a homogeneous weight: the average weight on nonzero ideals is constant and if two elements generate the same ideal, then they have the same weight. In [GO04], one can find a generalization of the Plotkin bound for codes over Frobenius rings equipped with a homogeneous weight. This version of the bound does not require that the code is linear. We end this remark with the note that the ring $\mathbb{Z}/p^s\mathbb{Z}$ is a Frobenius ring for all primes p and all natural numbers s.

Using this result, we obtain a different Plotkin bound for codes over $\mathbb{Z}/4\mathbb{Z}$.

COROLLARY 5.21 (A different Plotkin bound for $\mathbb{Z}/4\mathbb{Z}$). *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n with minimum Hamming distance d. Let $\check{d}(C) = \delta d$ and assume that $\delta d > n$. Then we have that*

$$|C| \leq \frac{\delta d}{\delta d - n}.$$

Proof. This follows directly from combining Theorem 3.30, Lemma 5.18 and Proposition 5.19. □

REMARK 5.22. This bound is only useful when δ is close to 2. If we let δ approach 1, the Plotkin bound for Hamming distance becomes sharper.

REMARK 5.23. This bound can also be obtained from our literature. On $\mathbb{Z}/4\mathbb{Z}$, Lee distance and compressed distance coincide. If we combine the remark in the introduction of [GO04] that the Lee weight on $\mathbb{Z}/4\mathbb{Z}$ is homogeneous with Theorem 2.2 of the same article, we obtain that the same bound also holds for nonlinear codes.

5.4. On the cH-ratio: The Case $\delta = 1$.

We will now investigate the compressed/Hamming-ratio δ. Our ultimate goal, which is still an open problem, is giving criterions to compute δ without knowing the Hamming distance of a code. We start by treating the case $\delta = 1$.

The following lemma gives a characterization of this case via the minimum Hamming weight codewords.

LEMMA 5.24. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n with $\check{d}(C) = \delta d_H(C)$. The cH-ratio δ satisfies $\delta = 1$ if and only if there exists $v = (v_i)_{i=1}^n \in C \setminus \{0\}$ with $d_H(v, 0) = d_H(C)$ and all entries of v are either 0 or multiplicative units.*

Proof. " $\Rightarrow$ ": Assume $\delta = 1$, that is $d_H(C) = \check{d}(C)$. Then there exists an element $v = (v_i)_{i=1}^n \in C \setminus \{0\}$ with $\check{d}(v, 0) = \check{d}(C) = d_H(C)$. We also have that

$$d_H(C) \leq d_H(v, 0) \leq \check{d}(v, 0),$$

so $d_H(v, 0) = \check{d}(v, 0)$. But this happens if and only if all nonzero entries of v are units.
" $\Leftarrow$ ": Assume that such v exists, then

$$\check{d}(C) \leq \check{d}(v, 0) = d_H(v, 0) = d_H(C).$$

Since $d_H(C) \leq \check{d}(C)$ always holds, we obtain that $\check{d}(C) = d_H(C)$, so $\delta = 1$. □

Niklas Gassner
niklas.gassner@uzh.ch

We introduce a lemma, which gives us valuable information about the entries of a vector of minimal Hamming weight.

LEMMA 5.25. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code and $v = (v_i)_{i=1}^n \in C \setminus \{0\}$ with $d_H(v,0) = d_H(C)$.*

Then there exists a $k \in \{0,1,...,s-1\}$ such that $v_i \in (p^k(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{k+1}(\mathbb{Z}/p^s\mathbb{Z})) \cup \{0\}$ for all $i \in \{1,...,n\}$.

Proof. Given such $v = (v_i)_{i=1}^n$, pick $m \in \mathbb{N}$ maximal such that $p^m v \neq 0$. Notice that, by the choices of m and v, $d_H(p^m v, 0) = d_H(v,0)$.

Now assume that, for some fixed $i \in \{1,...,n\}$, the entry v_i is nonzero. By the maximality of m and since $d_H(p^m v, 0) = d_H(v,0)$ we must have that $p^m v_i \in p^{s-1}(\mathbb{Z}/p^s\mathbb{Z}) \setminus \{0\}$, which forces $v_i \in p^{s-m-1}(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{s-m}(\mathbb{Z}/p^s\mathbb{Z})$. □

Recall that π^n is the map

$$\begin{aligned}(\mathbb{Z}/p^s\mathbb{Z})^n &\to (\mathbb{Z}/p\mathbb{Z})^n,\\ (x_i)_{i=1}^n &\mapsto (x_i \bmod p)_{i=1}^n\end{aligned}$$

given in Notation 4.38. Since this is a group homomorphism, the image of a $\mathbb{Z}/p^s\mathbb{Z}$-code under this map is a $\mathbb{Z}/p\mathbb{Z}$-code. Also note that in $(\mathbb{Z}/p\mathbb{Z})^n$ all distances we have studied so far coincide, so we will simply denote them with d.

The following lemma tells us that the Hamming distance of the projection of a code is always greater than or equal to the Hamming distance of the code.

LEMMA 5.26. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code. Assume there exists a $w \in C \setminus \{0\}$ with $\pi^n(w) \neq 0$. Then w has at least $d_H(C)$ entries that are units.*

Proof. Such $w = (w_i)_{i=1}^n \in C \setminus \{0\}$ must have at least one entry that is a unit, hence $p^{s-1}w \neq 0$. Further, $d_H(p^{s-1}w, 0) \geq d_H(C)$, so there exist at least $d_H(C)$ entries w_i with $p^{s-1}w_i \neq 0$. But such entries must be units, so we conclude. □

Recall Lemma 4.41, which states that for $v = (v_i)_{i=1}^n \in (\mathbb{Z}/p^s\mathbb{Z})^n$ the Hamming distance satisfies $d_H(\pi^n(v), 0) = |\{v_i \mid v_i \in (\mathbb{Z}/p^s\mathbb{Z})^*\}|$.

We obtain a necessary condition for a code to satisfy $\delta_C = 1$, based on the Hamming distances of the code and its projection.

PROPOSITION 5.27. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n with cH-ratio δ. If $\delta = 1$, then $d(\pi^n(C)) = \check{d}(C)$ and $d(\pi^n(C)) = d_H(C)$.*

Proof. Note that π^n sends units to units and all nonunits to 0, so for all $v \in (\mathbb{Z}/p^s\mathbb{Z})^n$ we have that $d(\pi^n(v), 0) \leq \check{d}(v,0)$.

Now, assume that $\delta = 1$. By Lemma 5.24, we can pick $v = (v_i)_{i=1}^n \in C \setminus \{0\}$ with $\check{d}(C) = \check{d}(v,0)$, such that all entries v_i are 0 or units. In particular, $\pi^n(v) \neq 0$. Further, we have that

$$d(\pi^n(C)) \leq d(\pi^n(v), 0) \leq \check{d}(v,0) = \check{d}(C).$$

Niklas Gassner
niklas.gassner@uzh.ch

Now, let $w \in C \setminus \{0\}$ with $\pi^n(w) \neq 0$. Then, combining Lemma 5.26 and Lemma 4.41, we obtain that

$$d(\pi^n(w), 0) \geq d_H(C) = \check{d}(C).$$

Since w is arbitrary, we obtain that $d(\pi^n(C)) \geq \check{d}(C)$, which forces $d(\pi^n(C)) = \check{d}(C)$.

We conclude by noting that $\delta = 1$ is, by definition, equivalent to $d_H(C) = \check{d}(C)$. □

Example 5.28. The following examples show that the converses do not hold:

- The code $C := \langle \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \end{pmatrix} \rangle \subset (\mathbb{Z}/4\mathbb{Z})^3$ satisfies $\check{d}(C) = 2 = d(\pi^n(C))$ but $d_H(C) = 1$, so $\delta = 2$.
- The code $C := \langle \begin{pmatrix} 1 & 1 & 1 & 2 \end{pmatrix} \rangle \subset (\mathbb{Z}/4\mathbb{Z})^4$ satisfies $d_H(C) = 3 = d(\pi^n(C))$, but $\check{d}(C) = 5$, so $\delta = \frac{5}{3}$.

However, with some extra assumptions we can show the converse.

We will use some standard notation: given $r \in (\mathbb{Z}/p^s\mathbb{Z})$ and a subset $S \subset (\mathbb{Z}/p^s\mathbb{Z})^n$, we will denote with rS the set $rS = \{rs \mid s \in S\}$.

Further, given a map $\phi : X \to Y$ and a subset $S \subset X$, we will denote with $\phi|_S$ the restriction of ϕ to S.

Remark 5.29. The kernel of π^n is $(p(\mathbb{Z}/p^s\mathbb{Z}))^n = p(\mathbb{Z}/p^s\mathbb{Z})^n$ and hence, given any subgroup $A \subset (\mathbb{Z}/p^s\mathbb{Z})^n$, the kernel of $\pi^n|_A$ is given by

$$\mathrm{Ker}(\pi^n|_A) = A \cap (p(\mathbb{Z}/p^s\mathbb{Z}))^n = A \cap p(\mathbb{Z}/p^s\mathbb{Z})^n.$$

In particular $x \in \mathrm{Ker}(\pi^n|_A)$ if and only if $x \in A$ and $p^{s-1}x = 0$.

Proposition 5.30. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code satisfying $\mathrm{Ker}(\pi^n|_C) = pC$ and $d(\pi^n(C)) = \check{d}(C)$. Then we have that $\delta = 1$.*

Even though we will prove something more general in the next subsection, we will give a proof of this proposition at the end of this subsection.

Remark 5.31. If we replace in Proposition 5.30 the assumption $d(\pi^n(C)) = \check{d}(C)$ with $d(\pi^n(C)) = d_H(C)$, the statement does not hold. Indeed, the code $\langle \begin{pmatrix} 1 & 1 & 1 & 2 \end{pmatrix} \rangle \subset (\mathbb{Z}/4\mathbb{Z})^4$ from Example 5.28 satisfies these assumptions but $\delta = \frac{5}{3}$.

It turns out that the condition $\mathrm{Ker}(\pi^n|_C) = pC$ is a characterization of free $\mathbb{Z}/p^s\mathbb{Z}$-submodules of $(\mathbb{Z}/p^s\mathbb{Z})^n$. We will do a short algebraic interlude to prove this.

Theorem 5.32. *Let $A \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a subgroup. Then the following are equivalent:*

(1) A is free as $(\mathbb{Z}/p^s\mathbb{Z})$-module.
(2) $\mathrm{Ker}(\pi^n|_A) = pA$.

Proof. "(1) ⇒ (2)": Assume that A is free as $\mathbb{Z}/p^s\mathbb{Z}$-module. Note that $pA \subset \mathrm{Ker}(\pi^n|_A)$ always holds, so we only need to show that $\mathrm{Ker}(\pi^n|_C) \subset pA$.

Let $v \in \mathrm{Ker}(\pi^n|_A)$ and pick a $\mathbb{Z}/p^s\mathbb{Z}$-basis $\{b_i \mid i \in I\}$ of A. There exist unique λ_i's in $\mathbb{Z}/p^s\mathbb{Z}$ such that $v = \sum_{i \in I} \lambda_i b_i$. But $v \in \mathrm{Ker}(\pi^n|_A)$, so we have that $p^{s-1}v = 0$. This forces that

$$\sum_{i \in I} p^{s-1}\lambda_i b_i = 0,$$

Niklas Gassner
niklas.gassner@uzh.ch

so by the linear independence of the b_i's we obtain that $p^{s-1}\lambda_i = 0$ for all $i \in I$.

It follows that $p|\lambda_i$ or $\lambda_i = 0$ for all $i \in I$, hence $v \in pA$. This shows the claim that $\mathrm{Ker}(\pi^n|_A) \subset pA$.

"(2) $\Rightarrow$ (1)": Assume that $\mathrm{Ker}(\pi^n|_A) = pA$. Using that $|A|$ divides p^{sn}, we obtain from the classification of finite abelian groups that there exist $n_1, ..., n_s \in \mathbb{N}$ such that

$$A \cong (\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s}$$

as $\mathbb{Z}$-module and hence also as $\mathbb{Z}/p^s\mathbb{Z}$-module. One can see that A is free as $\mathbb{Z}/p^s\mathbb{Z}$-module if and only if $n_1 = n_2 = ... = n_{s-1} = 0$.

Fix such an isomorphism $\phi : A \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s}$. Further, pick a $k \in \{1, ..., s-1\}$ and consider the following natural inclusion maps

$$i_k : (\mathbb{Z}/p^k\mathbb{Z})^{n_k} \to \{0\} \times ... \times \{0\} \times (\mathbb{Z}/p\mathbb{Z})^{n_k} \times \{0\} \times ... \times \{0\},$$

$$i : \{0\} \times ... \times \{0\} \times (\mathbb{Z}/p\mathbb{Z})^{n_k} \times \{0\} \times ... \times \{0\} \to (\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s},$$

which are clearly homomorphisms of $\mathbb{Z}/p^s\mathbb{Z}$-modules.

Assume, by contradiction, that $n_k > 0$. For $m \in \{1, ..., n_k\}$, let

$$e_m := \begin{pmatrix} 0 & ... & 0 & 1 & 0 & ... & 0 \end{pmatrix} \in (\mathbb{Z}/p^k\mathbb{Z})^{n_k} \setminus \{0\},$$

where the 1 is in the m'th entry.

We observe that

(1) $e_m \neq px$ for all $x \in (\mathbb{Z}/p^k\mathbb{Z})^{n_k}$. Since scalar multiplication is defined entrywise we have that $i(i_k(e_m)) \neq py$ for all $y \in (\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^s\mathbb{Z})^{n_s}$ and, since ϕ is an isomorphism of $\mathbb{Z}/p^s\mathbb{Z}$-modules, we have that $\phi(i(i_k(e_m))) \neq pz$ for all $z \in A$.

(2) $p^k e_m = 0$, hence

$$p^k \phi(i(i_k(e_m))) = \phi(i(i_k(p^k e_m))) = \phi(i(i_k(0))) = 0.$$

By assumption $\mathrm{Ker}(\pi^n|_A) = pA$, so the first observation forces $\phi(i(i_k(e_m))) \notin \mathrm{Ker}(\pi^n|_A)$. But, using that $k < s$, the second observation forces $\phi(i(i_k(e_m))) \in \mathrm{Ker}(\pi^n|_A)$, a contradiction.

Thus, we conclude that $n_k = 0$ for $k < s$, which shows the statement. □

We can now give a very short proof of Proposition 5.30. Recall that Corollary 4.43 states that any free code C satisfies $d_H(C) = d(\pi^n(C))$.

Proof. By Theorem 5.32, C is a free code. Hence, by Corollary 4.43, we obtain that $d(\pi^n(C)) = d_H(C)$. We assume that $\mathrm{d}(\pi^n(C)) = \check{d}(C)$, so it follows that $d_H(C) = \check{d}(C)$ which is equivalent to saying that $\delta = 1$. □

As a corollary, we can give a necessary and sufficient condition for free codes to satisfy $\delta = 1$ which only requires us to know the minimum compressed distance of the code and the minimum Hamming distance of its projection, as opposed to the minimum Hamming distance of the code itself.

COROLLARY 5.33. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a free nonzero code of length n. Then $\delta = 1$ if and only if $d(\pi^n(C)) = \check{d}(C)$.*

Proof. " $\Rightarrow$ ": Assume that $\delta = 1$. It follows directly from Proposition 5.27 that $d(\pi^n(C)) = \check{d}(C)$.
" $\Leftarrow$ ": Assume that $d(\pi^n(C)) = \check{d}(C)$. Then we immediately obtain that $\delta = 1$ by combining Theorem 5.32 and Proposition 5.30. □

5.5. Further Results about the cH-ratio.

It seems difficult to generally say much about the cH-ratio. Recall that Corollary 4.43 implies that any free code C satisfies $d_H(C) = d(\pi^n(C))$. So, if we assume a code to be free, we obtain the following result.

PROPOSITION 5.34. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a free nonzero code of length n. Then we have that $\check{d}(C) = \delta d(\pi^n(C))$.*

Proof. We have that

$$\check{d}(C) = \delta d_H(C) = \delta d_H(\pi^n(C))$$

where the first equality holds by definition of δ and the second equality follows from Corollary 4.43. □

REMARK 5.35. Note that this result generalizes Corollary 5.33.

The following lemma locates vectors of minimal Hamming weight for $\delta > 1$.

LEMMA 5.36. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n and assume that its cH-ratio δ satisfies $\delta > 1$. Let $v \in C \setminus \{0\}$ with $d_H(v, 0) = d_H(C)$. Then $v \in p(\mathbb{Z}/p^s\mathbb{Z})^n$.*

Proof. This statement is the contraposition of one of the implications in Lemma 5.24. □

NOTATION 5.37. Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n. We denote with $U(C)$ the set defined as

$$U(C) := \{v = (v_i)_{i=1}^n \in C \mid \text{there exists } j \in \{1, ..., n\} \text{ such that } v_j \in (\mathbb{Z}/p^s\mathbb{Z})^*\}.$$

If $\delta < 2$, then the nonzero vectors of minimal overweight must lie in $U(C)$.

LEMMA 5.38. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n with cH-ratio δ. Assume that $\delta < 2$. Then*

$$\{v \in C \mid \check{d}(v, 0) = \check{d}(C)\} \subset U(C).$$

Proof. Let v be such that $\check{d}(v, 0) = \check{d}(C)$. Then

$$2d_H(C) > \delta d_H(C) = \check{d}(C) = \check{d}(v, 0) \geq d_H(v, 0) \geq d_H(C).$$

This forces $\check{d}(v, 0) < 2d_H(v, 0)$, so at least one of the entries of v must be in $(\mathbb{Z}/p^s\mathbb{Z})^*$. We conclude that $v \in U(C)$. □

Finally, we consider the case $\delta = 2$. We first observe that if the projection of a nonzero code is trivial, then $\delta = 2$.

Niklas Gassner
niklas.gassner@uzh.ch

LEMMA 5.39. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n. Assume that $\pi^n(C) = \{0\}$. Then $\delta = 2$.*

Proof. Under these assumptions, every $v \in C$ satisfies $v \in p(\mathbb{Z}/p^s\mathbb{Z})^n$, hence for all $v \in C$ we have that $\check{d}(v,0) = 2d_H(v,0)$. Thus, pick $v \in C \setminus \{0\}$ with $\check{d}(v,0) = \check{d}(C)$. Then

$$2d_H(C) \leq 2d_H(v,0) = \check{d}(v,0) = \check{d}(C).$$

Since we always have that $\check{d}(C) \leq 2d_H(C)$, we can conclude that $\delta = 2$. □

Further, we give a necessary and sufficient condition for a code C to satisfy $\delta = 2$ by locating elements v with $\check{d}(C) = \check{d}(v,0)$.

LEMMA 5.40. *Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a nonzero code of length n. Then $\delta = 2$ if and only if there exists a $v \in p(\mathbb{Z}/p^s\mathbb{Z})^n$ with $\check{d}(v,0) = \check{d}(C)$.*

Proof. The case $s = 1$ is tautological since both statements cannot hold, hence we can assume that $s \geq 2$.
" $\Rightarrow$ " : Assume that $\delta = 2$ and pick $v \in C$ with $d_H(v,0) = d_H(C)$. Then we obtain that

$$\check{d}(C) \leq \check{d}(v,0) \leq 2d_H(v,0) = 2d_H(C) = \check{d}(C).$$

This forces $\check{d}(v,0) = 2d_H(v,0)$ which forces $v \in p(\mathbb{Z}/p^s\mathbb{Z})^n$.

" $\Leftarrow$ " : Let $v = (v_i)_{i=1}^n \in p(\mathbb{Z}/p^s\mathbb{Z})^n$ be such that $\check{d}(v,0) = \check{d}(C)$. Our goal is to show that $d_H(v,0) = d_H(C)$.

Let $w = (w_i)_{i=1}^n \in C \setminus \{0\}$ and assume that $d_H(w,0) \leq d_H(v,0)$. Then

$$\check{d}(w,0) = \sum_{i=1}^{n} \mathrm{Wt}(w_i) \leq 2d_H(w,0) \leq 2d_H(v,0) = \check{d}(v,0),$$

where we used in the first inequality that the Hamming distance $d_H(w,0)$ is the number of nonzero entries. But, by the choice of v, we also have that $\check{d}(v,0) \leq \check{d}(w,0)$, hence it follows that $\check{d}(v,0) = \check{d}(w,0)$. This forces that both inequalities are equalities and hence $2d_H(w,0) = 2d_H(v,0)$. We conclude that $d_H(w,0) = d_H(v,0)$ and hence that $d_H(v,0) = d_H(C)$. □

5.6. Relation to $s = 2$.

Our goal in this subsection is to relate the case $s \geq 2$ to the case $s = 2$. Given a code $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ for $s \geq 2$, we will show the existence of a code $\tilde{C} \subset (\mathbb{Z}/p^2\mathbb{Z})^n$ with similar properties. The code $\tilde{C}$ will be explicitly constructed under the assumption that we are given a certain morphism ϕ. Such a morphism always exists, but explicitly finding one is a nontrivial problem.

We first remind the reader of some notation, then state the main result.

Recall that the map π_2 is given by

$$\pi_2 : (\mathbb{Z}/p^s\mathbb{Z}) \to (\mathbb{Z}/p^2\mathbb{Z}),$$

Niklas Gassner
niklas.gassner@uzh.ch

$$x \mapsto (x \bmod p^2).$$

Further, π_2^n is the induced map

$$\pi_2^n : (\mathbb{Z}/p^s\mathbb{Z})^n \to (\mathbb{Z}/p^2\mathbb{Z})^n,$$
$$(x_i)_{i=1}^n \mapsto (\pi_2(x_i))_{i=1}^n = (x_i \bmod p^2)_{i=1}^n.$$

THEOREM 5.41. *Let $s \geq 2$ and $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n. Then there exists a code $\check{C}$ containing C such that $\pi_2^n(\check{C})$ satisfies $d_H(C) = d_H(\pi_2^n(\check{C}))$ and $\check{d}(\pi_2^n(\check{C})) \leq \check{d}(C)$. In particular, if $\delta_C = 1$, equality holds.*

The rest of this subsection will be devoted to the proof of this theorem.

5.6.1. Construction.

We may assume that $C \neq \{0\}$, otherwise we simply take $\check{C} = \{0\}$.

By the classification of finite abelian groups, there exist unique $n_1, ..., n_s$ and a (not necessarily unique) isomorphism

$$\phi : ((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}) \oplus (\mathbb{Z}/p^s\mathbb{Z})^{n_s} \xrightarrow{\sim} C.$$

Note that ϕ is an isomorphism of $\mathbb{Z}$-modules and hence also of $\mathbb{Z}/p^s\mathbb{Z}$-modules.

Fix such ϕ and define

$$F := \phi((\mathbb{Z}/p^s\mathbb{Z})^{n_s}),$$
$$T := \phi((\mathbb{Z}/p\mathbb{Z})^{n_1} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}).$$

By definition we have that F is free as a $(\mathbb{Z}/p^s\mathbb{Z})$-module and that $T \subset p(\mathbb{Z}/p^s\mathbb{Z})$. Further, $C = F \oplus T$, so for all $c \in C$ there exists a unique pair $(f, t) \in F \times T$ such that $c = f + t$. Note that F and T depend on the choice of ϕ, but we will see that the code we will construct in $(\mathbb{Z}/p^2\mathbb{Z})^n$ does not.

Pick a $(\mathbb{Z}/p^s\mathbb{Z})$-basis $f_1, ..., f_m$ of F and nonzero generators $t_1, ..., t_l$ of T satisfying $\sum_{i=1}^l \lambda_i t_i = 0$ for some $\lambda_1, ..., \lambda_l \in \mathbb{Z}/p^s\mathbb{Z}$ if and only if $\lambda_i t_i = 0$ for all $i \in \{1, ..., l\}$. Stated differently, we want our generators $t_1, ..., t_l$ to satisfy $T = \bigoplus_{i=1}^l \langle t_i \rangle$. The existence of such generators will be proved in Lemma 5.42.

Note that necessarily we must have that $t_i \in p(\mathbb{Z}/p^s\mathbb{Z})^n$. For $i \in \{1, ..., l\}$ choose an element $\check{t}_i \in p(\mathbb{Z}/p^s\mathbb{Z})^n$ such that

(1) at least one entry of $\check{t}_i$ is in $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$,
(2) there exists an integer $\tilde{m}_i \geq 0$ with $p^{\tilde{m}_i}\check{t}_i = t_i$.

In particular, if t_i satisfies the first condition, then $\check{t}_i = t_i$.

Define

$$\check{C} := \langle f_1, ..., f_m, \check{t}_1, ..., \check{t}_l \rangle \subset (\mathbb{Z}/p^s\mathbb{Z})^n$$

and

$$C_2 := \pi_2^n(\check{C}) = \langle \pi_2^n(f_1), ..., \pi_2^n(f_m), \pi_2^n(t_1), ..., \pi_2^n(t_l) \rangle \subset (\mathbb{Z}/p^2\mathbb{Z})^n.$$

Note that if $C \neq \{0\}$, then so is C_2.

Our goal is now to show that C_2 is independent of choices and satisfies the properties stated in the theorem.

LEMMA 5.42. *There exist generators $t_1, ..., t_l$ of T such that $\sum_{i=1}^{l} \lambda_i t_i = 0$ if and only if $\lambda_i t_i = 0$ for all $i \in \{1, ..., l\}$.*

Proof. For all $j \in \{1, ..., s-1\}$, let

$$i_j : (\mathbb{Z}/p^j\mathbb{Z})^{n_j} \to (\mathbb{Z}/p\mathbb{Z})^{n_1} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}$$

be the natural inclusion.

Define for all $k \in \{1, ..., n_j\}$ the element

$$e_{j,k} := \begin{pmatrix} 0 & ... & 0 & 1 & 0 & ... & 0 \end{pmatrix} \in (\mathbb{Z}/p^j\mathbb{Z})^{n_j},$$

where the 1 is in the k-th entry.

Define

$$G := \bigcup_{j=1}^{s-1} \{i_j(e_{j,k}) \mid k \in \{1, ..., n_j\}\}.$$

Then we have that

$$(\mathbb{Z}/p\mathbb{Z})^{n_1} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}} = \bigoplus_{j=1}^{s-1} \bigoplus_{k=1}^{n_j} \langle i_j(e_{j,k}) \rangle.$$

Since ϕ is an isomorphism, we obtain that $\phi(G)$ is a generating system of T with the desired properties. □

5.6.2. Independence of Choices of $\check{t}_i$.

Recall, that we constructed $\check{C}$ and C_2 as follows: we pick an isomorphism

$$\phi : ((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}) \oplus (\mathbb{Z}/p^s\mathbb{Z})^{n_s} \xrightarrow{\sim} C,$$

a basis $f_1, ..., f_m$ of

$$F = \phi((\mathbb{Z}/p^s\mathbb{Z})^{n_s})$$

and nonzero generators $t_1, ..., t_l$ of

$$T = \phi((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}})$$

such that $T = \bigoplus_{i=1}^{n} \langle t_i \rangle$.

Then we pick for all $i \in \{1, ..., l\}$ an element $\check{t}_i \in p(\mathbb{Z}/p^s\mathbb{Z})^n$ such that at least one entry of $\check{t}_i$ is in $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$ and that there exists a natural number $\tilde{m}_i \in \mathbb{N}$ such that $p^{\tilde{m}_i}\check{t}_i = t_i$.

Finally, we set $\check{C} = \langle f_1, ..., f_m, \check{t}_1, ..., \check{t}_l \rangle$ and $C_2 = \pi_2^n(\check{C})$, the image of the natural projection π_2^n to $(\mathbb{Z}/p^2\mathbb{Z})^n$.

We will now show that C_2 does not depend on the choices of the generators $\check{t}_1, ..., \check{t}_l$, when given generators $t_1, ..., t_l$.

LEMMA 5.43. *Let $s \geq 2$ and $x, y \in p(\mathbb{Z}/p^s\mathbb{Z})$ such that $p^{\tilde{m}}x = p^{\tilde{m}}y$ for some $\tilde{m} < s-1$. Then $x \equiv y \bmod p^2$.*

Proof. We have that $p^{\tilde{m}}x = p^{\tilde{m}}y$, hence it follows that $p^{\tilde{m}}(x-y) = 0$. Using that $\tilde{m} < s-1$, this forces that $x - y \in p^2(\mathbb{Z}/p^s\mathbb{Z})$, which implies the result. □

COROLLARY 5.44. *C_2 is independent of the choices of the generators $\check{t}_1, ..., \check{t}_l$.*

Proof. For a fixed $i \in \{1, ..., l\}$, let $\check{t}_{i,1} = (a_1)_{i=1}^n$ and $\check{t}_{i,2} = (b_1)_{i=1}^n$ be two elements of $p(\mathbb{Z}/p^s\mathbb{Z})^n$ with at least one entry in $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$ such that there exists an $\tilde{m}$ with $p^{\tilde{m}}\check{t}_{i,1} = p^{\tilde{m}}\check{t}_{i,2} = t_i$.

Since t_i is nonzero we must have that $\tilde{m} < s - 1$. By Lemma 5.43, it follows that $a_i \equiv b_i \bmod p^2$, hence we obtain that $\pi_2^n(\check{t}_{i,1}) = \pi_2^n(\check{t}_{i,2})$. □

5.6.3. Properties.

The following observations will help us to prove the missing claims.

We first notice that the elements $\check{t}_i$ also have the property that the sum $\sum_{i=1}^l \langle \check{t}_i \rangle$ is direct.

LEMMA 5.45. *The elements $\check{t}_1, ..., \check{t}_l$ have the property that $\sum_{i=1}^l \lambda_i \check{t}_i = 0$ for some $\lambda_1, ..., \lambda_l \in (\mathbb{Z}/p^s\mathbb{Z})$ if and only if $\lambda_i \check{t}_i = 0$ for all $i \in \{1, ..., l\}$.*

Proof. " $\Leftarrow$ ": Obvious.
" $\Rightarrow$ ": Assume, by contradiction, that $\sum_{i=1}^l \lambda_i \check{t}_i = 0$ and that $\lambda_i \check{t}_i \neq 0$ for at least one i. Pick $\tilde{m} \in \mathbb{N}$ maximal such that $p^{\tilde{m}}\lambda_i \check{t}_i \neq 0$ for at least one $i \in \{1, ..., l\}$. Let

$$J := \{i \in \{1, ..., l\} \mid p^{\tilde{m}}\lambda_i \check{t}_i \neq 0\}.$$

By choice of $\tilde{m}$ it follows that for all $i \in \{1, ..., l\}$ we have that $p^{\tilde{m}+1}\lambda_i \check{t}_i = 0$, so for all $i \in \{1, ..., l\}$ there exists a $\mu_i \in (\mathbb{Z}/p^s\mathbb{Z})$ such that $p^{\tilde{m}}\lambda_i \check{t}_i = \mu_i t_i$, where we used that t_i is nonzero for all $i \in \{1, ..., n\}$. Further, for all $j \in J$ we must have that $\mu_j t_j \neq 0$. Thus we obtain that

$$0 = p^{\tilde{m}}0 = p^{\tilde{m}} \sum_{i=1}^l \lambda_i \check{t}_i = \sum_{i=1}^l p^{\tilde{m}}\lambda_i \check{t}_i = \sum_{i=1}^l \mu_i t_i = \sum_{j \in J} \mu_j t_j.$$

But since $\mu_j t_j \neq 0$ for all $j \in J$, which is nonempty by the choice of $\tilde{m}$, we get a contradiction to the choice of the generators $t_1, ..., t_l$. □

The following Lemma tells us that any element of C with coefficients divisible by p^2 can be written as p times an element in $\check{C}$. Informally speaking, for any element x in $p^2(\mathbb{Z}/p^s\mathbb{Z})^n \cap C$, there exists an element "$\frac{1}{p}x$" in $\check{C}$.

LEMMA 5.46. *Let $x \in p^2(\mathbb{Z}/p^s\mathbb{Z})^n \cap C$. Then there exists a $y \in \check{C}$ with $py = x$.*

Proof. We write x as linear combination of the generators of C, that is we write

$$x = \lambda_1 f_1 + ... + \lambda_m f_m + \mu_1 t_1 + ... + \mu_l t_l.$$

Claim: For all $i \in \{1, ..., m\}$ we have either $\lambda_i = 0$ or $p^2 | \lambda_i$.
Proof: Since $x \in p^2(\mathbb{Z}/p^s\mathbb{Z})^n$, it follows that $p^{s-2}x = 0$. Further, $C = F \oplus T$, hence we have that

$$p^{s-2}(\lambda_1 f_1 + ... + \lambda_m f_m) = 0.$$

The linear independence of $f_1, ..., f_m$ forces that $p^2\lambda_i = 0$ for all i, so either $p^2 | \lambda_i$ or $\lambda_i = 0$, which concludes the claim.

For each $i \in \{1, ..., m\}$, choose a $\check{\lambda}_i \in \mathbb{Z}/p^s\mathbb{Z}$ such that $p\check{\lambda}_i = \lambda_i$.

Using that $C = F \oplus T$, we also have that

$$p^{s-2}(\mu_1 t_1 + ... + \mu_l t_l) = 0.$$

Thus, by the choice of the generators $t_1, ..., t_l$, it follows that $p^{s-2}\mu_i t_i = 0$ for all indices $i \in \{1, ..., l\}$. We observe the following.

(1) If t_i has at least one entry in $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$, then $p^{s-2}t_i \neq 0$. Thus we must have that either $p|\mu_i$ or $\mu_i = 0$.
(2) If not, then $t_i = p^{m_i}\check{t}_i$ for some $m_i \geq 1$.

In both cases, there exists a $\check{\mu}_i \in \mathbb{Z}/p^s\mathbb{Z}$ such that $\mu_i t_i = p\check{\mu}_i\check{t}_i$. Thus, the element

$$y := \check{\lambda}_1 f_1 + ... + \check{\lambda}_m f_m + \check{\mu}_1\check{t}_1 + ... + \check{\mu}_l\check{t}_l \in \check{C}$$

satisfies $py = x$. □

We also notice that every element of $\check{C}$ is of the form "$\frac{1}{p^{\check{m}}}x$" for some element $x \in C \setminus \{0\}$ and some $\check{m} \in \mathbb{N}$.

LEMMA 5.47. *Let $y \in \check{C} \setminus \{0\}$. Then there exists a $x \in C \setminus \{0\}$ and a $\tilde{m} \in \{0, 1, ..., s-1\}$ such that $p^{\tilde{m}}y = x$.*

Proof. We write y as linear combination of the generators of $\check{C}$, that is we write

$$y = \sum_{i=1}^{m} \lambda_i f_i + \sum_{i=1}^{l} \mu_i \check{t}_i.$$

Case 1: $\sum_{i=1}^{l} \mu_i\check{t}_i = 0$.
Then $y = \sum_{i=1}^{m} \lambda_i f_i \in C$, so we can pick $x = y$ and $\tilde{m} = 0$.
Case 2: $\sum_{i=1}^{l} \mu_i\check{t}_i \neq 0$.
Pick $\tilde{m}$ maximal with $p^{\tilde{m}} \sum_{i=1}^{l} \mu_i\check{t}_i \neq 0$. Then we have that $p^{\tilde{m}+1} \sum_{i=1}^{l} \mu_i\check{t}_i = 0$, which implies by Lemma 5.45 that $p^{\tilde{m}+1}\mu_i\check{t}_i = 0$ for all $i \in \{1, ..., l\}$. For all $i \in \{1, .., l\}$ there exists a k_i such that $p^{k_i}\check{t}_i = t_i \neq 0$, so it follows that there exist $\check{\mu}_1, ..., \check{\mu}_l \in (\mathbb{Z}/p^s\mathbb{Z})$ such that $p^{\tilde{m}}\mu_i\check{t}_i = \check{\mu}_i t_i$ for all $i \in \{1, ..., l\}$ and at least one $\check{\mu}_i$ is nonzero. Thus

$$\begin{aligned} p^{\tilde{m}}y &= p^{\tilde{m}}(\sum_{i=1}^{m} \lambda_i f_i + \sum_{i=1}^{l} \mu_i\check{t}_i) \\ &= \sum_{i=1}^{m} p^{\tilde{m}}\lambda_i f_i + \sum_{i=1}^{l} p^{\tilde{m}}\mu_i\check{t}_i \\ &= \sum_{i=1}^{m} p^{\tilde{m}}\lambda_i f_i + \sum_{i=1}^{l} \check{\mu}_i t_i \in C, \end{aligned}$$

which is nonzero since $\sum_{i=1}^{l} \check{\mu}_i t_i \neq 0$ and $C = F \oplus T$. □

Niklas Gassner
niklas.gassner@uzh.ch

5.6.4. Independence of ϕ and the Generators $t_1, ..., t_l$.

We first recall the construction of $\check{C}$ and C_2.

We fix an isomorphism

$$\phi : ((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}) \oplus (\mathbb{Z}/p^s\mathbb{Z})^{n_s} \xrightarrow{\sim} C,$$

pick a basis $f_1, ..., f_m$ of

$$F = \phi((\mathbb{Z}/p^s\mathbb{Z})^{n_s})$$

and nonzero generators $t_1, ..., t_l$ of

$$T = \phi((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}})$$

such that $T = \bigoplus_{i=1}^{n} \langle t_i \rangle$.

Then, we manipulate the generators $t_1, ..., t_l$ to obtain generators $\check{t}_1, ..., \check{t}_l$ and define $\check{C} = \langle f_1, ..., f_m, \check{t}_1, ..., \check{t}_l \rangle$ and $C_2 = \pi_2^n(\check{C})$.

We will now show that C_2 is independent of the choice of the isomorphism ϕ and the choice of generators.

Proposition 5.48. *C_2 is independent of the isomorphism*

$$\phi : ((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}) \oplus (\mathbb{Z}/p^s\mathbb{Z})^{n_s} \xrightarrow{\sim} C$$

and the choice of generators $f_1, ..., f_m, t_1, ..., t_l$.

Proof. Let

$$\psi : ((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}) \oplus (\mathbb{Z}/p^s\mathbb{Z})^{n_s} \xrightarrow{\sim} C$$

be another isomorphism and denote by

$$G := \psi((\mathbb{Z}/p^s\mathbb{Z})^{n_s}),$$

$$U := \psi((\mathbb{Z}/p\mathbb{Z})^{n_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{n_2} \times ... \times (\mathbb{Z}/p^{s-1}\mathbb{Z})^{n_{s-1}}).$$

Pick a $\mathbb{Z}/p^s\mathbb{Z}$-basis $g_1, ..., g_m$ of G and generators $u_1, ..., u_l$ of U satisfying $\sum_{i=1}^{l} \lambda_i u_i = 0$ if and only if $\lambda_i u_i = 0$ for all $i \in \{1, ..., l\}$. Note that the cardinality of the basis and the number of such generators must indeed coincide with the cardinality of the basis of F (in fact $m = n_s$) and the cardinality of the generating set of T by uniqueness of $n_1, ..., n_{s-1}$. Let $\check{u}_1, ..., \check{u}_l \in p(\mathbb{Z}/p^s\mathbb{Z})^n$ be chosen according to our construction, that is for all $i \in \{1, ..., l\}$ we have that $\check{u}_i$ has at least one entry in $p(\mathbb{Z}/p^s\mathbb{Z})$ and for each $i \in \{1, ..., l\}$ there exists an $\check{m}_i \in \mathbb{N}$ such that $p^{\check{m}_i}\check{u}_i = u_i$.

Claim 1: $\langle \pi_2^n(g_1), ..., \pi_2^n(g_m), \pi_2^n(\check{u}_1), ..., \pi_2^n(\check{u}_l) \rangle \subset C_2$.

Proof: Since $\langle \pi_2^n(g_1), ..., \pi_2^n(g_m), \pi_2^n(\check{u}_1), ..., \pi_2^n(\check{u}_l) \rangle$ is the smallest group containing all $\pi_2^n(g_i)$ and $\pi_2^n(\check{u}_i)$'s, we need to check that $\pi_2^n(g_i) \in C_2$ and $\pi_2^n(\check{u}_j) \in C_2$ for all indices $i \in \{1, ..., m\}$ and all $j \in \{1, ..., l\}$. In fact, for all $i \in \{1, ..., m\}$ we have that $g_i \in C \subset \check{C}$, so in particular $\pi_2^n(g_i) \in \pi_2^n(\check{C}) = C_2$.

Now, pick an $i \in \{1, ..., l\}$ and consider $\check{u}_i$. By construction, $\check{u}_i \in p(\mathbb{Z}/p^s\mathbb{Z})^n$ and there exists a $\tilde{m}$ such that $p^{\tilde{m}}\check{u}_i = u_i \in C$.

Case 1: $\tilde{m} = 0$.

In this case we have that $\check{u}_i \in C \subset \check{C}$, hence it follows that $\pi_2^n(\check{u}_i) \in \pi_2^n(\check{C}) = C_2$.
Case 2: $\tilde{m} \geq 1$.

Since $u_i \in C \cap p^2(\mathbb{Z}/p^s\mathbb{Z})^n$, by Lemma 5.46 we have that there exists a $v_i \in \check{C}$ such that $pv_i = u_i$. Inductively, there exists a $\check{v}_i \in \check{C} \cap p(\mathbb{Z}/p^s\mathbb{Z})$ with at least one entry in $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$ and a $k \in \mathbb{N}$ such that $p^k\check{v}_i = u_i$.

Subclaim: $k = \check{m}$.

Proof: Let r be maximal with $u_i \in p^r(\mathbb{Z}/p^s\mathbb{Z})$. Then we must have that $k = r - 1 = \check{m}$. It follows that $p^{\check{m}}\check{v}_i = p^{\check{m}}\check{u}_i$. From Lemma 5.43 we obtain that $\pi_2^n(\check{v}_i) = \pi_2^n(\check{u}_i)$, which concludes the claim.

Claim 2: $C_2 \subset \langle \pi_2^n(g_1), ..., \pi_2^n(g_m), \pi_2^n(\check{u}_1), ..., \pi_2^n(\check{u}_l)\rangle$.

Proof: Lemma 5.46 and Lemma 5.43 also hold for $\langle \pi_2^n(g_1), ..., \pi_2^n(g_m), \pi_2^n(\check{u}_1), ..., \pi_2^n(\check{u}_l)\rangle$ since it is also constructed as described in Subsection 5.6.1. Hence, by exchanging the roles of C_2 and $\langle \pi_2^n(g_1), ..., \pi_2^n(g_m), \pi_2^n(\check{u}_1), ..., \pi_2^n(\check{u}_l)\rangle$ we get the claim. □

5.6.5. Behaviour of the Distances.

We prove that the constructed code C_2 satisfies $d_H(C_2) = d_H(C)$ and $\check{d}(C_2) \leq \check{d}(C)$ and then conclude Theorem 5.41 by combining all results on the way.

Proposition 5.49. *We have that $d_H(C_2) = d_H(C)$.*

Proof. "$\leq$": Pick $v \in C \setminus \{0\}$ with $d_H(v, 0) = d_H(C)$. By Lemma 5.25, there exists a $k \in \mathbb{N}$ such that all nonzero entries of v are in $p^k(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{k+1}(\mathbb{Z}/p^s\mathbb{Z})$. We split the proof into three cases.

> Case 1: $k = 0$.
> We can set $\check{v} := v$. Then we have that $d_H(v, 0) = d_H(\pi_2^n(\check{v}), 0)$ since all entries of v are either zero or a unit and π_2 sends units to units.
> Case 2: $k = 1$.
> We can again set $\check{v} := v$. Since π_2 sends elements of $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$ to nonzero elements, we must get that $d_H(v, 0) = d_H(\pi_2^n(\check{v}), 0)$.
> Case 3: $k \geq 2$.
> By Lemma 5.46, there exists a $\check{v} \in \check{C}$ with $p^{k-1}\check{v} = v$. Necessarily, $\check{v} \in p(\mathbb{Z}/p^s\mathbb{Z})$ and has exactly $d_H(v, 0)$ entries in $p(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$. So these $d_H(v, 0)$ entries are exactly the entries which do not lie in $\mathrm{Ker}(\pi_2)$, hence $d_H(v, 0) = d_H(\check{v}, 0)$.

In all three cases we conclude that

$$d_H(C_2) \leq d_H(\check{v}, 0) = d_H(v, 0) = d_H(C).$$

" $\geq$": Let $w = (w_i)_{i=1}^n \in \check{C}$ with $\pi_2^n(w) \neq 0$. Necessarily there exists an $i \in \{1, ..., n\}$ such that $w_i \in (\mathbb{Z}/p^s\mathbb{Z}) \setminus p^2(\mathbb{Z}/p^s\mathbb{Z})$.

Let $\check{m} \in \{0, 1\}$ be maximal with $w \in p^{\check{m}}(\mathbb{Z}/p^s\mathbb{Z})$.

> Claim: At least $d_H(C)$ entries of w are in $p^{\check{m}}(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{\check{m}+1}(\mathbb{Z}/p^s\mathbb{Z})$.

Niklas Gassner
niklas.gassner@uzh.ch

Proof: By Lemma 5.47, we have that $p^{s-1-\check{m}}w \in C \setminus \{0\}$. Thus it follows that $d_H(p^{s-1-\check{m}}w, 0) \geq d_H(C)$ and since all w_i are in $p^{\check{m}}(\mathbb{Z}/p^s\mathbb{Z})$ we have that

$$p^{s-1-\check{m}}w_i \neq 0 \Leftrightarrow w_i \in p^{\check{m}}(\mathbb{Z}/p^s\mathbb{Z}) \setminus p^{\check{m}+1}(\mathbb{Z}/p^s\mathbb{Z}).$$

It follows that $d_H(\pi_2^n(w), 0) \geq d_H(C)$. We conclude since w is arbitrary. □

Proposition 5.50. *The compressed distance satisfies* $\check{d}(C_2) \leq \check{d}(C)$.

Proof. We split the proof into three cases, one where $\delta_C = 1$, one where $\delta_C = 2$ and the remaining case where $1 < \delta_C < 2$.
Case 1: $\delta_C = 1$.

Then, by Lemma 5.24, there exists a $v \in C$ such that $d_H(v, 0) = d_H(C)$ such that all nonzero entries of v are units. In this case, we have that

$$\check{d}(\pi_2^n(v)) = d_H(\pi_2^n(v), 0) = d_H(v, 0)$$

and hence

$$\check{d}(C_2) \leq \check{d}(\pi_2^n(v), 0) = d_H(v, 0) = d_H(C) = \check{d}(C),$$

where we used that $\delta_C = 1$ in the last equality.
Case 2: $\delta_C = 2$.

This case follows directly from the inequality

$$\check{d}(C_2) \leq 2d_H(C_2) = 2d_H(C) = \check{d}(C).$$

Case 3: $1 < \delta_C < 2$.

Pick $v \in C$ with $\check{d}(v, 0) = \check{d}(C)$. By Lemma 5.38, at least one of the entries of v is a unit, hence it follows that $\pi_2^n(v) \neq 0$. Further, we have that $\check{d}(\pi_2^n(v), 0) \leq \check{d}(v, 0)$. Therefore we conclude with

$$\check{d}(C_2) \leq \check{d}(\pi_2^n(v), 0) \leq \check{d}(v, 0) = \check{d}(C).$$

□

We will now prove Theorem 5.41 by referring to the relevant results. We repeat that the theorem requires that $\pi_2^n(\check{C})$ satisfies $d_H(C) = d_H(\pi_2^n(\check{C}))$ and $\check{d}(\pi_2^n(\check{C})) \leq \check{d}(C)$ and further states that if $\delta_C = 1$, equality holds.

Proof. Given a code C, let $\check{C}$ be a code constructed according our instructions. As before, we write C_2 for $\pi_2^n(\check{C})$.

By Proposition 5.49, we have that $d_H(C_2) = d_H(C)$.

Proposition 5.50 states that $\check{d}(C_2) \leq \check{d}(C)$.

Finally, assume that $\delta_C = 1$. Then, using Proposition 5.50, we get that

$$d_H(C_2) \leq \check{d}(C_2) \leq \check{d}(C) = d_H(C) = d_H(C_2),$$

where we used Proposition 5.49 in the last equality. This forces $\check{d}(C_2) = d_H(C)$. □

Niklas Gassner
niklas.gassner@uzh.ch

5.7. Constructing first Examples.

We will give some examples of linear codes, that reach bounds for fixed values. Let's start by defining generator matrices, which will make our notation much more compact.

Definition 5.51. Let $C \subset (\mathbb{Z}/p^s\mathbb{Z})^n$ be a code of length n that can be generated by k elements as $\mathbb{Z}/p^s\mathbb{Z}$-module. A generator matrix of C is a $k \times n$ matrix with entries in $\mathbb{Z}/p^s\mathbb{Z}$ whose rows generate C as $\mathbb{Z}/p^s\mathbb{Z}$-module.

We start to give a code C with the parameters $p^2 = 4$, $n = 8$ and $\check{d}(C) = 10$.

Using Corollary 5.21, the Plotkin bound for the compressed distance, we have that C satisfies

$$|C| \leq \frac{10}{10-8} = 5.$$

Since $|C|$ must also divide $|(\mathbb{Z}/4\mathbb{Z})^8| = 4^8$, we have that $|C|$ is a power of two.

Thus we obtain that $|C| \leq 4$.

Example 5.52. Let C_1 be the code with generating matrix

$$M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 \end{pmatrix}.$$

Then $|C_1| = 4$ and $\check{d}(C_1) = 10$.

Example 5.53. Let C_2 be the code with generating matrix

$$M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 \end{pmatrix}.$$

This code also satisfies $|C_2| = 4$ and $\check{d}(C_2) = 10$.

5.8. A Nontrivial Example.

We fix the values $p^2 = 4$, $n = 9$ and $\check{d}(C) = 10$.

We use Corollary 5.21 to obtain that any linear code C with these parameters must satisfy

$$|C| \leq \frac{10}{10-9} = 10.$$

We also must have that $|C|$ divides $|(\mathbb{Z}/4\mathbb{Z})^8| = 4^8$, so $|C|$ must be a power of 2. It follows that $|C| \leq 8$.

Example 5.54. Denote with C_3 the code with generating matrix

$$M_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 2 \end{pmatrix}.$$

We will now show that C_3 is indeed a code achieving the Plotkin bound.

Lemma 5.55. *C_3 is a code of cardinality 8.*

Proof. Denote by

$$A_1 = \langle \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 0 \end{pmatrix} \rangle$$

and

$$A_2 = \langle \begin{pmatrix} 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 2 \end{pmatrix} \rangle.$$

The intersection of A_1 and A_2 is $\{0\}$, hence we have that

$$C_3 = A_1 \oplus A_2,$$

which implies that

$$|C_3| = |A_1| \cdot |A_2| = 4 \cdot 2 = 8.$$

□

LEMMA 5.56. *The code C_3 satisfies that $\check{d}(C_3) = 10$.*

Proof. " $\leq$ ": The element $v_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 0 \end{pmatrix}$ satisfies $\check{d}(v_1, 0) = 10$.
" $\geq$ ": For any element v of C_1, there exist $a, b \in \mathbb{Z}/4\mathbb{Z}$ such that

$$v = \begin{pmatrix} a & a & a & a+2b & a+2b & a+2b & 2a & 2a+2b & 2b \end{pmatrix}.$$

Assume that $v \neq 0$. If $a = 0$ or $b \in \{0, 2\}$, then clearly $\check{d}(v, 0) \geq 10$. Hence we can assume that $a \neq 0$ and $b \in \{1, 3\}$.
Case 1: $a \in \{1, 3\}$.
In this case, v has six entries in $\{1, 3\} = (\mathbb{Z}/4\mathbb{Z})^*$ and two entries that equal two. Hence $\check{d}(v, 0) = 10$.
Case 2: $a = 2$.
Since we assumed that $b \in \{1, 3\}$, it follows that $2b = 2$. Thus we get that

$$v = \begin{pmatrix} 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}$$

and $\check{d}(v, 0) = 10$. □

COROLLARY 5.57. *The code C_3 satisfies that $\delta = 2$.*

Proof. Since $\check{d}(C_3) = 10$, we must have $d_H(C_3) \geq 5$.
Now, set $v = \begin{pmatrix} 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 & 2 \end{pmatrix}$. Then we conclude, since

$$d_H(C_3) \leq d_H(v, 0) = 5.$$

□

5.9. A More Sophisticated Example.

We fix the parameters $p^s = 25$, $n = 5$ and $\check{d} = 5$.
Let $|C|$ be a code with these parameters. From Proposition 5.16, we have that

$$|B_{2,\check{d}}(x)| = \sum_{k=0}^{1} \sum_{m=0}^{2-2k} \binom{5}{k} (5-1)^k \binom{5-k}{m} (25-5)^m = 4121.$$

Niklas Gassner
niklas.gassner@uzh.ch

Thus, from Corollary 5.17, the sphere-packing bound for the compressed distance, we obtain that

$$|C| \leq \frac{25^5}{4121} \approx 2370.$$

Further, $|C|$ divides 25^5, we must have that $|C| \leq 625$.

EXAMPLE 5.58. Let C_4 be the code with generating matrix

$$M_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 5 & 0 & 0 & 5 & 10 \\ 5 & 15 & 20 & 0 & 0 \end{pmatrix}.$$

LEMMA 5.59. *The code C_4 satisfies $|C_4| = 625$.*

Proof. We consider the groups

$$A_1 = \langle \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix} \rangle,$$
$$A_2 = \langle \begin{pmatrix} 5 & 0 & 0 & 5 & 10 \end{pmatrix}, \begin{pmatrix} 5 & 15 & 20 & 0 & 0 \end{pmatrix} \rangle.$$

Both of its generators are of order 5, and we cannot obtain one generator by multiplying the other with a unit, hence we get that $|A_2| = 5^2 = 25$.

For each element $v \in A_2$, there exist $a, b \in \mathbb{Z}/25\mathbb{Z}$ such that

$$v = \begin{pmatrix} 5a+5b & 15b & 20b & 5a & 10a \end{pmatrix}.$$

So we see that $A_1 \cap A_2 = \{0\}$. Hence $C_4 = A_1 \oplus A_2$ and thus we can conclude since

$$|C_4| = |A_1| \cdot |A_2| = 25 \cdot 5^2 = 625.$$

□

LEMMA 5.60. *The code C_4 satisfies $\check{d}(C_4) = 5$.*

Proof. " $\leq$ " We observe that $\check{d}(C_4) \leq 5$, since the element $v_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ satisfies $\check{d}(v, 0) = 5$.
" $\geq$ ": Let $v \in C_4 \neq \{0\}$.
Case 1: $v \in A_1 \setminus \{0\}$.
In this case we have that $\check{d}(v, 0) \geq 5$.
Case 2: $v \in A_2 \setminus \{0\}$.
If we assume that $v \in A_2 \setminus \{0\}$, then there exist $a, b \in \mathbb{Z}/25\mathbb{Z}$ such that

$$v = \begin{pmatrix} 5a+5b & 15b & 20b & 5a & 10a \end{pmatrix}.$$

We see immediately that at least 3 entries of v must be nonzero. Since all entries are in $5(\mathbb{Z}/25\mathbb{Z})$, we obtain that $\check{d}(v, 0) \geq 6$.
Case 3: $v = v_1 + v_2$ for $v_1 \in A_1 \setminus \{0\}$ and $v_2 \in A_2 \setminus \{0\}$.
There exist $a, b, c \in \mathbb{Z}/25\mathbb{Z}$ such that

$$v = \begin{pmatrix} 5a+5b+c & 15b+c & 20b+c & 5a+c & 10a+c \end{pmatrix}.$$

Subcase 3.1: $v \in (\mathbb{Z}/25\mathbb{Z})^*$.
Then all of v's entries are units, hence $\check{d}(v, 0) = 5$.

Niklas Gassner
niklas.gassner@uzh.ch

Subcase 3.2: $v \in 5(\mathbb{Z}/25\mathbb{Z})$.

We claim that every such element has at least 3 nonzero entries. To prove this, we show that no element of $A_2 \setminus \{0\}$ does have the same entry thrice or more.

Consider an element $v_2 \in A_2$. We can write

$$v_2 = \begin{pmatrix} 5a+5b & 15b & 20b & 5a & 10a \end{pmatrix}.$$

The cases $a \in 5(\mathbb{Z}/25\mathbb{Z})$ or $b \in 5(\mathbb{Z}/25\mathbb{Z})$ are clear, so we assume that $a, b \in (\mathbb{Z}/25\mathbb{Z})^*$. We can also assume that $b = 1$ and $a \in \{1, 2, 3, 4\}$, since for every $a \in (\mathbb{Z}/25\mathbb{Z})^*$, $a + 5$ yields the same vector v_2. Then we get that

$$v_2 = \begin{pmatrix} 5a+5 & 15 & 20 & 5a & 10a \end{pmatrix}.$$

So setting $a = 1, 2, 3, 4$, we see that the statement holds true.

It follows that for any $r \in 5(\mathbb{Z}/25\mathbb{Z})$, we have that

$$v = r \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix} - v_2$$

has at least 3 nonzero entries, which lie $5(\mathbb{Z}/25\mathbb{Z})$. Hence we obtain that $\check{d}(v, 0) \geq 6$, which yields the conclusion.

□

Corollary 5.61. *C_4 satisfies $\delta = \frac{5}{3}$.*

Proof. We have that $d_H(C_4) \geq 3$ as otherwise $\delta > 2$, which is impossible.

Note also that

$$v_2 = \begin{pmatrix} 10 & 15 & 20 & 5 & 10 \end{pmatrix} \in A_2$$

and that

$$10 \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix} - v_2 = \begin{pmatrix} 0 & 20 & 15 & 5 & 0 \end{pmatrix} \in C_4.$$

It follows that $d_H(C_4) \leq 3$. □

References.

[GO04] Marcus Greferath and Michael E. O'Sullivan. "On bounds for codes over Frobenius rings under homogeneous weights". In: *Discrete Mathematics* 289 (2004), pp. 11–24. ISSN: 0012-365X. DOI: 10.1016/j.disc.2004.10.002.

[CH97] Ioana Constantinescu and Werner Heise. "A metric for codes over residue class rings". In: *Problemy Peredachi Informatsii* 33.3 (1997), pp. 22–28.

[Rot06] Ron Roth. *Introduction to coding theory*. Cambridge University Press, 2006. ISBN: 978-0521845045.

[Sin64] R. Singleton. "Maximum distance q-nary codes". In: *IEEE Transactions on Information Theory* 10.2 (1964), pp. 116–118. DOI: 10.1109/TIT.1964.1053661.

[Lin82] J.H. van Lint. *Introduction to Coding Theory*. Graduate texts in mathematics. Springer-Verlag, 1982. ISBN: 978-3-662-08000-9.

[Gil52] E. N. Gilbert. "A comparison of signalling alphabets". In: *The Bell System Technical Journal* 31.3 (1952), pp. 504–522. DOI: 10.1002/j.1538-7305.1952.tb01393.x.

[Var57] R. R Varshamov. "Estimate of the number of signals in error correcting codes". In: *Dokl. Akad. Nauk SSSR* 117 (1957), pp. 739–741.

[Plo60] M. Plotkin. "Binary codes with specified minimum distance". In: *IRE Transactions on Information Theory* 6.4 (1960), pp. 445–450. DOI: 10.1109/TIT.1960.1057584.

[Gab12] Ernst Gabidulin. "A brief survey of metrics in coding theory". In: *Mathematics of Distances and Applications* 66 (2012), pp. 66–84.

[AH13] Tim L. Alderson and Svenja Huntemann. "On maximum Lee distance codes". In: *Journal of Discrete Mathematics* (2013). DOI: 10.1155/2013/625912.