Classification of lower bounds on the minimum distance of cyclic codes

Claus Jensby Madsen

AALBORG UNIVERSITET

Institut for Matematiske Fag
Frederik Bajers Vej 7G, 9220 Aalborg Ø
Telefon 99 40 99 40
Fax 98 15 81 29
http://www.math.aau.dk/

Titel:

Classification of lower bounds on the minimum distance of cyclic codes

Projektperiode:
Forårssemesteret 2010

Deltagere:
Claus Jensby Madsen

Vejleder:
Olav Geil

Oplagstal: 6

Sidetal: 63

Bilagsantal og –art: 0

Afsluttet den 10. juni 2010

Synopsis:

This paper provides a framework of lower bounds on the minimum distance of cyclic codes.
Root bounds depends solely on the defining set and the length of a cyclic code, and the BCH Bound, the Hartmann-Tzeng Bound, Bound A and several Boston Bounds are sown to belong to this family. Border bounds furthermore depends on the defining set of cyclic subcodes as well. The Schaub Bound, the Singleton Bound and the van Lint-Wilson Bound are shown to belong to this class. Furthermore are the Schaub Bound and Singleton Bound shown to be equivalent and the van Lint-Wilson Bound shown to share the same independece-check procedure with the two others.

Resumé

I denne rapport opstilles rammer, som danner grundlag for en samling af nedre grænser for minimumsafstanden af cykliske koder. Disse bliver delt op i grænser, som kun afhænger af kodens definerende mængde og længde, og grænser, som derudover også afhænger af de definerende mængder af de cykliske subkoder.

Først introduceres nogle vigtige begreber, som bruges til at bevise resultaterne, bl.a. lineær kompleksitet, diskrete Fourier-transformationer, og i særdeleshed singletons, som benyttes til at lave nedre grænser for rangen af matricer, som man kun har delvist information om.

Et større begrebsapparat for de såkaldte rodgrænser introduceres, og en række af kendte grænser (de BCH-lignende grænser) vises at tilhøre denne familie af grænser – og i flere tilfælde en bestemt delfamlie kaldet stærke rodgrænser.

Rodgrænserne udvides til kantgrænserne, og Schaub-grænsen og van Lint-Wilson-grænsen vises begge at være kantgrænser, men også at de er baseret på samme uafhængighedstjekprocedure.

Contents

Chapter 1

Preliminaries

In order to lay the foundation of the following chapters we will briefly summarize some important concepts and results from algebraic coding theory as well as introduce notation used throughout the paper.

We denote by $\mathbb{N}_0$ the set $\mathbb{N} \cup \{0\}$, by $\overline{\mathbb{N}}$ the set $\mathbb{N} \cup \{\infty\}$, by $\mathcal{P}_k$ the set of all polynomials of degree less than k, and by $\mathcal{P}(S)$ the power set of S. I denote by $\overline{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$.

Given the integers $N \in \mathbb{N}_0$ and $n \in \mathbb{N}$, we denote by $(N)_n$ the remainder of division of N by n. We also denote by $\ \mathrm{rem}\ $ the infix modulo operator.

Let $n \in \mathbb{N}$. We denote by $\mathbb{Z}_n^*$ the set $\{x \in \mathbb{N} \mid 1 \leq x \leq n-1, \gcd(x,n) = 1\}$.

We denote by S_n the symmetric group of an n-dimensional vector space.

Definition 1.0.1 (Associated matrix)**.** Let $n \in \mathbb{N}$ and $a \in (a_1, \ldots, a_n)$ be a vector of vector space $\mathbb{F}^n$. Then the associated matrix $M(a)$ is an $\mathbb{F}^{n \times n}$ matrix given by cyclic shifting the rows, i.e.

$$M(a) = \begin{bmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \\ a_2 & a_3 & \ldots & a_n & a_1 \\ \vdots & & & \vdots & \\ a_n & a_1 & \ldots & a_{n-2} & a_{n-1} \end{bmatrix}.$$

Definition 1.0.2 (Field)**.** Let $\mathbb{F}$ be a set with the compositions $+$ and $\cdot$. If $\mathbb{F}$ is a communitative group with respect to addition, $\mathbb{F}\backslash\{0\}$ is a commutative group with respect to multiplication and multiplication distributes over addition, then $\mathbb{F}$ is a field.

The order of $\mathbb{F}$ is the number of elements in $\mathbb{F}$. The characteristic of $\mathbb{F}$ is smallest number p such that $\sum_{i=1}^{p} 1 = 0$.

$\mathbb{F}$ is a finite field if the order of $\mathbb{F}$ is finite.

Throughout this paper $\mathbb{F}_q$ will denote a field of order q.

Definition 1.0.3 (nth root of unity)**.** Let $\alpha \in \overline{\mathbb{F}}_q$. If $\alpha^n = 1$, then α is called an nth root of unity. If furthermore there does not exist a $k \in \{0, \ldots, n-1\}$ such that $\alpha^k = 1$, then α is a primitive nth root of unity.

Proposition 1.0.4. *Let $n \in \mathbb{N}$ and q be a prime power. If $\gcd(n, q) = 1$, then there exists a primitive nth root of unity.*

Proof. There exists a t such that all the zeros of $x^n - 1$ is in $\mathbb{F}_{q^t}$ because every time you encounter a non-linear factor of $x^n - 1$ that can't be factorized, you extend the field by creating a new splitting field with respect to this factor. □

1.1 Algebraic coding theory

First we will quickly recap some fundamentals of abstract coding theory.

Definition 1.1.1 (Linear code)**.** Let $n, q \in \mathbb{N}$. Let $\mathbb{F}_q$ denote a finite field with q elements, and let $\mathbb{F}_q^n$ denote the n-dimensional vector space over $\mathbb{F}_q$. Any subspace $C \subseteq \mathbb{F}_q^n$ is called a linear code. The elements of C are called code words. We denote by $\mathcal{L}_q$ the set of linear codes over $\mathbb{F}_q$ and by $\mathcal{L}$ the set $\cup_q \mathcal{L}_q$.

Definition 1.1.2 (Minimum distance)**.** The distance $d(\vec{x}_1, \vec{x}_2)$ between two vectors is the number of components of the vectors, where the components differ. The minimum distance $d(C)$ of a code C is the lower limit of the distance of any two code words in C. For linear codes the minimum distance of a code equals the minimum weight of the set of all non-zero codewords.

There exists a vector space isomorphism $\phi : \mathbb{R}^n \to \mathcal{P}_n$ with the definition $(x_1, \ldots, x_n) \mapsto x_1 + \ldots + x_n z^{n-1}$. Due to this isomorphism the code words can be represented by a vector as well as a polynomial and these representations will be used interchangably.

Definition 1.1.3 (Cyclic code)**.** A cyclic code is a linear code, in which for all codewords their cyclic shifts are also codewords. We denote by $\mathcal{C}_q$ the set of cyclic codes over $\mathbb{F}_q$ and by $\mathcal{C}$ the set $\cup_q \mathcal{C}_q$. A cyclic subcode C' of a cyclic code C is a cyclic code, where $C' \subseteq C$.

From now on we will implicitly assume $\gcd(n, q) = 1$ for all cyclic codes of order q and length n.

The generator polynomial plays a crucial role for the study of cyclic codes.

Definition 1.1.4 (Generator polynomial)**.** Let C be a cyclic code, and let $g(x)$ be a monic polynomial of minimal degree in $C \backslash \{0\}$. Then $g(x)$ is called a generator polynomium.

Proposition 1.1.5. *The generator polynomium is unique.*

Proof. Asumme $g(x)$ and $h(x)$ are both generator polynomials of the same cyclic code. Let $k(x) = g(x) - h(x)$. By Definition 1.1.4 we know that $g(x)$ and $h(x)$ are monic, which means the degree of $k(x)$ is strictly smaller than the degree of $g(x)$ and $h(x)$. But this is a contradiction, since by Definition 1.1.4 we have that $g(x)$ and $h(x)$ should be of minimal degree. □

Proposition 1.1.6. *Let C be a cyclic code with generator polynomial $g(x)$ and let $c(x) \in C$. Then $g(x) \mid c(x)$.*

Proof. We know that $c(x) = a(x)g(x) = r(x)$ where $\deg(r(x)) < \deg(g(x))$[1, Proposition 4.2.4]. Since $\deg(c(x)) = a(x)g(x)$ then $a(x)g(x) \in C$. Since C is a linear code, then it implies that $r(x)$ is also a codeword. Since $\deg(r(x)) < \deg(g(x))$ then $r(x)$ has to be the zero polynomial, which proves the claim. □

Proposition 1.1.7. *Let C and C' be a cyclic codes, such that $C' \subseteq C$. Let $g(x)$ and $g'(x)$ be the generator polynomials of C and C' respectively. Then $g(x) \mid g'(x)$.*

Proof. Since $g'(x) \in C'$ and $C' \subseteq C$ then $g'(x) \in C$. This means there exists a polynomial $a(x)$ such that $g'(x) = a(x)g(x)$. Thus $g(x) \mid g'(x)$. □

Proposition 1.1.8. *Let C be an (n, k) cyclic code with generator polynomial $g(x) = \sum_{i=0}^{n-k} g_i x^i$. Then*

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & \dots & & 0 & g_0 & g_1 & \dots & g_{n-k} \end{bmatrix}$$

is a generator matrix for C.

Proof. The first row of G is $g(x)$ and the other rows are cyclic shifts if the first row. Thus all rows are in C. All rows have different degrees (viewed as polynomials), which means they are linearly independent.

Furthermore there is precisely k rows. Therefore are the rows of G a basis of C. □

Definition 1.1.9 (Defining set)**.** Let $C \in \mathcal{C}$ be a cyclic code og length n, let g be the generator polynomial of C and let α be a primitive n-th root of unity. We denote by $S_{C,\alpha}$ the defining set of C with respect to α, i.e.

$$S_{C,\alpha} = \{i \in \{0, \dots, n-1\} \mid g(\alpha^i) = 0\}.$$

The defining set will play an extremely important role throughout the following chapters.

1.2 Equivalence of cyclic codes

In this section we briefly introduce the a notion of equivalence of cyclic codes, i.e. we define natural equivalence.

Definition 1.2.1 (The set S)**.** We denote by S the subset of $\mathbb{N} \times \mathbb{N}$, where $(q, n) \in S$ if and only if p is a prime, $m \in \mathbb{N}$, $q = p^m$ and $\gcd(n, p) = 1$.

Definition 1.2.2 (The map ζ)**.** We denote by Z the set of all functions $\zeta : S \to \cup_{p \text{ prime}} \overline{\mathbb{F}}_p$ so that $\zeta(p^m, n)$ returns a primitive n-th root of unity over $\mathbb{F}_p$.

Definition 1.2.2 might not seem well-defined, but it is well-defined enough for our usage. Whenever we take ζ from Z in order to get a primitive n-th root of unity, it doesn't matter which root of unity we get.

Definition 1.2.3 (Natural equivalence)**.** Let $C_1, C_2 \in \mathcal{C}_{q,n}$. We say that C_1 and C_2 are naturally equivalent if there are two primitive nth roots of unity over $\mathbb{F}_q$, α and β, so that $S_{C_1,\alpha} = S_{C_2,\beta}$.

Proposition 1.2.4. *Let C_1 and C_2 be naturally equivalent cyclic codes. Then $d(C_1) = d(C_2)$.*

Furthermore, let C_1 be in $\mathcal{C}_{q,n}$. Let α and β be primitive nth roots of unity. Then there is a unique code C_2 so that $S_{C_1,\alpha} = S_{C_2,\beta}$.

This proposition is taken from [2, Theorem 2.4].

Chapter 2

Linear complexity

In this chapter we introduce the concept of linear complexity, which is a useful concept that we will be needing some of these results later in the paper.

Throughout this chapter we will utilize the following notation:

- b^n will denote a finite sequence $(b_0, b_1, \ldots, b_{n-1})$ of some field $\mathbb{F}$.
- b^0 will denote the empty sequence.
- b^∞ will denote a semi-infinite sequence $(b_0, b_1, \ldots)$ of some field $\mathbb{F}$.
- 0^n will denote the sequence of zeros of length n.

2.1 Introduction

We start with the definition of linear complexity:

Definition 2.1.1 (Linear complexity)**.** Let $n \in \mathbb{N}_0$, and let b^n be a finite or semi-finite sequence over $\mathbb{F}$. The linear complexity $\Lambda(b^n)$ of b^n is the smallest nonnegative integer L such that there exists $c_1, \ldots, c_L \in \mathbb{F}$ for which

$$b_j + c_1 b_{j-1} + \cdots + c_L b_{j-L} = 0 \qquad \text{for all } L \leq j < n. \tag{2.1}$$

Note that $\Lambda(b^n) = n$ is possible, as $L = n$ implies no j within $L \leq j < n$.

This concept is a measure for how complex a pattern a sequence has as illustrated in the following example.

Example 2.1.2. Here follows a few simple examples of calculation of linear complexity.

- Consider the alternating sequence $(1, -1, 1, -1, 1, -1, \ldots)$. This sequence has a linear complexity of 1, since

$$b_j + b_{j-1} = 0 \qquad 1 \leq j < n.$$

- Now consider the sequence of Fibonacci numbers $(1, 1, 2, 3, 5, 8, \ldots)$. This sequence has by construction a linear complexity of 2, since

$$b_j - b_{j-1} - b_{j-2} = 0 \qquad\qquad 2 \leq j < n$$

by the definition of Fibonacci numbers.

Proposition 2.1.3. *Let $n \in \mathbb{N}$. $\Lambda(b^n) = n$ if and only if $b^{n-1} = 0^{n-1} \wedge b_{n-1} \neq 0$.*

Proof. Assume $\Lambda(b^n) = n$. This means that $b_{n-1} \neq 0$ – otherwise would $\Lambda(b^n) < n$. Furthermore does $b^{n-1} = 0^{n-1}$ have to hold, since otherwise would $\Lambda(b^n) < n$ as well.

Assume $b^{n-1} = 0^{n-1} \wedge b_{n-1} \neq 0$. Since b_{n_1} cannot be written as any linear combination of the preceding values, then $\Lambda(b^n) = n$. □

We will now state some basic properties of linear complexity.

Proposition 2.1.4. *$\Lambda(b^n) = 0$ if and only if $b^n = 0^n$.*

Proof. This claim is a direct consequence of Definition 2.1.1. □

Proposition 2.1.5. *For all $n \in \mathbb{N}$ then $\Lambda(b^{n+1}) \geq \Lambda(b^n)$ holds. Furthermore, if $\Lambda(b^{n+1}) > \Lambda(b^n)$, then $\Lambda(b^{n+1}) = n + 1 - \Lambda(b^n)$.*

Proof. $\Lambda(b^{n+1}) \geq \Lambda(b^n)$ must hold, since the $\Lambda(b^{n+1})$ coefficients found for b^{n+1} can also be used for b^n.

Assume $\Lambda(b^{n+1}) > \Lambda(b^n)$. In this case the $n+1$th element disturbs the pattern of the preceding n elements, because the complexity increases.

Let $L_n = \Lambda(b^n)$ and $L_{n+1} = \Lambda(b^{n+1})$. This means that for the first n elements in the sequence is a linear combination of the previous L_n elements, i.e. $x_i = c_{i-1}x_{i-1} + \cdots + c_{i-L_n}x_{i-L_n}$. Isolating x_{i-L_n} we get that it can be written as a linear combination of the next L_n elements in the sequence.

Take the last element $x_{n+1} = d_n x_n + \cdots + d_1 x_1 + d_0 x_0$. The first $x_0, \ldots, x_{L_n - 1}$ can be substituted with a linear combinations of the later elements of the sequence. Thus $\Lambda(b^{n+1}) = n + 1 - \Lambda(b^n)$.

□

This proposition is consistent with Proposition 2.1.3: let $b^n = 0^n$. By Proposition 2.1.4 $\Lambda(b^n) = 0$. Then by Proposition 2.1.5 we get $\Lambda(b^{n+1}) = n + 1 - \Lambda(b^n) = n + 1$.

Proposition 2.1.6. *Let $n, m \in \mathbb{N}$ so that $n \leq m$. Let b^n be a subsequence of a^m, i.e. there exists an integer i such that $b_j = a^{j+i}$ for $0 \leq j \leq n-1$. Then $\Lambda(b^n) \leq \Lambda(a^m)$.*

Proof. $\Lambda(b^n) > \Lambda(a^m)$ cannot be true, since the coefficients found for a^m at $a_i, \ldots, a_{i+n-1}$ can be used for b^n as well because $b_j = a^{j+i}$ for $0 \leq j \leq n-1$. Therefore can b^n not have a larger linear complexity (i.e. needs more coefficients) than a^m when the coefficients from a^m suffice. □

2.2 Periodic sequences

In this section we will deal with periodicity of semi-infinite sequences.

Definition 2.2.1 (Periodicity)**.** A sequence b^∞ is said to be periodic with period $N \in \mathbb{N}$ when

$$b_j = b_{j+N} \qquad \text{for all } j \in \mathbb{N}_0.$$

Furthermore is the smallest period of a sequence called the fundamental period.

The first period of the sequence, denoted by b^N, is $(b_0, b_1, \ldots, b_{N-1})$.

Example 2.2.2. Consider once again the alternating sequence $(1, -1, 1, -1, 1, -1, \ldots)$. All even integers are periods of this sequence, and it's fundamental period is 2.

A property of periodic sequences is that every periodic sequence is completely characterized by it's first period, i.e. if you have the first period, you everything about the sequence, since you can in principle reconstruct the whole sequence.

Definition 2.2.3 (Cyclic left-shift operator)**.** Let $n \in \mathbb{N}$. Let $S : \mathbb{F}^n \to \mathbb{F}^n$ be a map, such that

$$S(b^n) = (b_1, b_2, \ldots, b_{N-1}, b_0).$$

Then S is called the cyclic left-shift operator. Let S^{-1} denote it's inverse map, i.e. the cyclic right-shift operator.

Let $n \in \mathbb{Z}$.

- If $n > 0$ then let S^n denote the compound of n S maps.
- If $n < 0$ then let S^n denote the compound of $|n|$ S^{-1} maps.
- If $n = 0$ then let S^n denote the no operation operator, i.e. the identity map.

The cyclic left-shift operator has a number of nice properties. It is apparent that S is a linear operator over the vector space $\mathbb{F}^n$, is bijective, and satisfy the usual laws of exponents.

If b^∞ is periodic with period N, then Equation (2.1) will be equivalent to

$$b_j + c_1 b_{j-1} + \cdots + c_L b_{j-L} = 0 \qquad \text{for all } L \leq j < L + N. \tag{2.2}$$

Equation (2.2) can in turn be rewritten using the cyclic left-shift operator as

$$S^L(b^N) + c_1 S^{L-1}(b^N) + \cdots + c_L b^N = 0^N. \tag{2.3}$$

This leads us to the definition of the characteristic polynomial:

Definition 2.2.4 (Characteristic polynomial)**.** Let

$$c(x) = x^L + c_1 x^{L-1} + \cdots + c_L,$$

where $c_1, \ldots, c_L$ are the coefficients of Equation (2.3). Then $c(x)$ is called the characteristic polynomial.

Now we will walk through some properties of periodic sequences regarding linear complexity.

Proposition 2.2.5. *If b^∞ is periodic with period N, then $\Lambda(b^\infty) \leq N$.*

Proof. Take any subsequence of b^∞ of length N. By definition and by Equation (2.2) it's linear complexity cannot be larger than N. Thus $\Lambda(b^\infty) \leq N$. □

Recall that $M(v)$ denotes the circulant matrix of the vector v.

Proposition 2.2.6. *Let b^∞ be a periodic sequence with period N. Then $\Lambda(b^N) = \operatorname{rank}(M(b^N))$.*

Proof. Consider Equation (2.3), which holds for b^N. The vectors of this equation corresponds to the first $L+1$ rows of $M(b^N)$. The equation yields that the $L+1$th row is a linear combination of the preceing L rows, i.e. the first L rows are linearly independent.

Note that Equation (2.3) also implies that

$$S^{L+i}(b^N) + c_1 S^{L+i-1}(b^N) + \cdots + c_L S^i(b^N) = 0^N \tag{2.4}$$

for all $i \in \mathbb{N}_0$, which means that any row of $M(b^N)$ is a linear combination of the preceding L rows.

This implies that $\operatorname{rank}(M(v)) = L = \Lambda(b^N)$. □

2.3 The discreet Fourier transforms

Later we will need the discreet Fourier transforms, so we will now introduce it to the reader.

Definition 2.3.1. Let $\mathbb{F}$ be a field and α be a primitive Nth root of unity of $\mathbb{F}$. The discreet Fourier transform of a sequence b^N of length N is another sequence B^N of length N, where

$$B_i = \sum_{j=0}^{N-1} b_j \alpha^{ij}.$$

Note that if we formulate the sequences in terms of polynomials, then the notation of Definition 2.3.1 is greatly reduced to $B_i = b(\alpha^i)$.

Proposition 2.3.2. *Let $\mathbb{F}$ be a field, $k \in \mathbb{F}$ and α be a primitive Nth root of unity of $\mathbb{F}$. Then*

$$\sum_{i=0}^{N-1} \alpha^{ki} = \begin{cases} N & N \mid k \\ 0 & N \nmid k \end{cases}.$$

Proof. Assume N divides k. Then there exists a c such that $cN = k$. This implies

$$\begin{aligned} \sum_{i=0}^{N-1} \alpha^{ki} &= \sum_{i=0}^{N-1} (\alpha^N)^{ci} \\ &= \sum_{i=0}^{N-1} 1 \\ &= N. \end{aligned}$$

Assume N does not divide k. This implies that $\alpha^k \neq 1$ and therefore $\alpha^k - 1 \neq 0$. Then we calculate

$$\begin{aligned} (\alpha^k - 1) \sum_{i=0}^{N-1} \alpha^{ki} &= \sum_{i=0}^{N-1} \alpha^{k(i+1)} - \sum_{i=0}^{N-1} \alpha^{ki} \\ &= \sum_{i=1}^{N} \alpha^{ki} - \sum_{i=0}^{N-1} \alpha^{ki} \\ &= a^{Nk} - 1 \\ &= (a^N)^k - 1 \\ &= 0. \end{aligned}$$

By the zero-product rule we get that $\sum_{i=0}^{N-1} \alpha^{ki} = 0$. □

Using Definition 2.3.1 and Proposition 2.3.2 we can get the inverse discreet Fourier transform

$$\begin{aligned} \frac{1}{N} \sum_{i=0}^{N-1} B_i \alpha^{-ij} &= \frac{1}{N} \left(\alpha^{-0\cdot j} \sum_{k=0}^{N-1} b_k \alpha^{0\cdot k} + \cdots + \alpha^{-(N-1)\cdot j} \sum_{k=0}^{N-1} b_k \alpha^{(N-1)\cdot k} \right) \\ &= \frac{1}{N} \Big(b_0 (\alpha^{0-0\cdot j} + \alpha^{1\cdot j} + \cdots + \alpha^{-(N-1)\cdot j}) + \cdots + \\ &\quad b_j (\overbrace{\alpha^{0-0\cdot j} + \alpha^{j-\cdot j} + \cdots + \alpha^{(N-1)-(N-1)\cdot j}}^{=N}) + \cdots + \\ &\quad b_{n-1} (\alpha^{0-0\cdot j} + \alpha^{1-1\cdot j} + \cdots + \alpha^{(N-1)-(N-1)\cdot j}) \Big). \end{aligned}$$

By Proposition 2.3.2 only the $j+1$st term yields a non-zero value, so

$$\frac{1}{N}\sum_{i=0}^{N-1} B_i \alpha^{-ij} = \frac{1}{N}(b_j N) = b_j.$$

Note that

$$\begin{aligned} B_{i+N} &= \sum_{j=0}^{N-1} \alpha^{i+N} j \\ &= \sum_{j=0}^{N-1} \alpha^{i} j \\ &= B_i \end{aligned}$$

and

$$\begin{aligned} b_{j+N} &= \frac{1}{N}\sum_{i=0}^{N-1} B_i \alpha^{-i(j+N)} \\ &= \frac{1}{N}\sum_{i=0}^{N-1} B_i \alpha^{-ij} \\ &= b_j \end{aligned}$$

So both b^∞ and B^∞ is periodic with the same period N.

Recall that $w(x)$ denotes the Hamming weight of x. We now have sufficient groundwork to prove Blahut's Theorem:

Theorem 2.3.3 (Blahut's Theorem)**.** *Let b^∞ be periodic with period N. Then $\Lambda(b^\infty) = w(B^N)$ and $\Lambda(B^\infty) = w(b^N)$*

Proof. Let A_j^∞ be the periodic sequence with the first period of

$$A_j^N = (1, \alpha^j, \alpha^{2j}, \ldots, \alpha^{(N-1)j}). \tag{2.5}$$

It is not hard to see that $\alpha^j A_j^N = S(A_j^N)$, and therefore that for any polynomial $p(X)$ that $p(\alpha^j)A_j^N = p(S)(A_j^N)$ holds.

If $b^N = 0^N$ then by Definition 2.3.1 $B^N = 0$, and thus Blahut's Theorem holds trivially in this special case.

Suppose $b^N \neq 0^N$. Then let $b_{n(j)}$ for $j \in \{1, 2, \ldots, W(b^N)\}$ be the nonzero components of b^N. Then by Definition 2.3.1 and Equation (2.5) we have that

$$B^N = \sum_{j=1}^{w(b^N)} b_{n(j)} A_{n(j)}^N.$$

This equation comes directly from Definition 2.3.1 rewritten to handle a whole sequence at once instead of only a single value, as well as discarding all the zero terms and formulate the α in terms of A_j^N. This furthermore implies

$$\begin{aligned} p(S)B^N &= p(S)\sum_{j=1}^{w(b^N)} b_{n(j)}A_{n(j)}^N \\ &= \sum_{j=1}^{w(b^N)} b_{n(j)}p(S)A_{n(j)}^N \\ &= \sum_{j=1}^{w(b^N)} b_{n(j)}p(\alpha^{n(j)})A_{n(j)}^N. \end{aligned} \tag{2.6}$$

Consider the polynomial

$$c(x) = \prod_{j=1}^{w(b^N)} (x - \alpha^{n(j)}).$$

Note that $c(\alpha^{n(j)}) = 0$ for $j \in \{1, 2, \ldots, w(b^N)\}$, which implies that Equation (2.6) yields zero if $p(\alpha^{n(j)}) = c(\alpha^{n(j)})$.

If $p(\alpha^{n(j)}) \neq 0$ for some $j \in \{1, 2, \ldots, w(b^N)\}$, then $p(S)B^N \neq 0^N$, which can be seen by the following:

Assume $p(S)B^N = 0^N$. Let $w = w(b^N)$. Equation (2.6) can be rewritten as

$$\begin{aligned} p(S)B^N = {} & (b_{n(1)}p(\alpha^{n(1)}) \cdot 1, b_{n(1)}p(\alpha^{n(1)})\alpha^{n(1)}, \ldots, b_{n(1)}p(\alpha^{n(1)})\alpha^{(N-1)n(1)}) + \\ & (b_{n(2)}p(\alpha^{n(2)}) \cdot 1, b_{n(2)}p(\alpha^{n(2)})\alpha^{n(2)}, \ldots, b_{n(2)}p(\alpha^{n(2)})\alpha^{(N-1)n(2)}) + \\ & \cdots + \\ & (b_{n(w)}p(\alpha^{n(w)}) \cdot 1, b_{n(w)}p(\alpha^{n(w)})\alpha^{n(w)}, \ldots, b_{n(w)}p(\alpha^{n(w)})\alpha^{(N-1)n(w)}). \end{aligned}$$

Let

$$Q(x) = b_{n(1)}p(\alpha^{n(1)})x^{n(1)} + \cdots + b_{n(w)}p(\alpha^{n(w)})x^{n(w)}.$$

Then $p(S)B^N = (Q(1), Q(\alpha), \cdots, Q(\alpha^{N-1}))$. Notice that $Q(1) = Q(\alpha) = \cdots = Q(\alpha^{N-1}) = 0$. This means $Q(x)$ has N zeros. But since $n(w) < N$ then $Q(x) \equiv 0$. Since $b^N \neq 0^N$ and powers of α cannnot be zero, then $\alpha^{n(j)} = 0$. By the law of contraposition we then get that if $p(\alpha^{n(j)}) \neq 0$ for some $j \in \{1, 2, \ldots, w(b^N)\}$, then $p(S)B^N \neq 0^N$.

Therefore is $c(x)$ the characteristic polynomial of B^∞, since they have exactly the same zeros. Then we can calculate the linear complexity:

$$\Lambda(B^\infty) = \deg c(x) = w(b^N).$$

The other half of Blahut's Theorem is proved analougously interchanging b^∞ and B^∞. □

Theorem 2.3.4 (Zero-Location Theorem)**.** *The minimum distance d of an (N, K) cyclic code generated by $g(x)$ is equal to the minimum linear complexity $\Lambda(B^\infty)$ among all periodic sequences B^∞, whose first period B^N is a non-zero N-tuple with a 0 in each component where G^N contains a 0.*

Proof. In this proof we will switch between sequence notation and polynomial notation implicitly to make the proof more concise and readable.

Let $b(x)$ be a codeword in the cyclic code generated by $g(x)$, i.e. $b(x) = g(x)a(x)$ for a polynomial $a(x)$ of degree less than K.

We now consider the discreet Fourier transform of $b(x)$, which with polynomial notation is $B_i = A_i G_i$ for all $i \in \mathbb{N}_0$, and A^∞ is the periodic sequence, where A^N is the discreet Fourier transform of a^N and likewise with G and g.

The set of polynomials $a(x)$ of degree less than K forms a K-dimensional vector space. This is also true for the set of Fourier-transformed codewords B^N.

Therefore it must be the K-dimensional space of all N-tuples B^N with zero in the exact same locations as the zeros of $g(x)$.

Theorem 2.3.3 gives us that $w(b^N) = \Lambda(B^N)$. When $\Lambda(B^N)$ is minimal, then so is $w(b^N)$, i.e. you have the minimum distance. □

Chapter 3

The set U

In this chapter we will introduce the set U, which is a handy construction to utilize in situations where we only have partial information about the values of some placeholders.

Definition 3.0.5. By U we denote the set $\{0, \Delta, \Delta^+\}$. Addition and multiplication of elements of U is defined as stated in table 3.1.

(a) Addition table.

$+$	0	Δ	Δ^+
0	0	Δ	Δ^+
Δ	Δ	Δ	Δ
Δ^+	Δ^+	Δ	Δ

(b) Mutiplication table.

$\cdot$	0	Δ	Δ^+
0	0	0	0
Δ	0	Δ	Δ
Δ^+	0	Δ	Δ^+

Table 3.1: The addition table and multiplication tables of the set U.

We will interpret the symbols of U as following: let $\mathbb{F}$ be a field and $x \in \mathbb{F}$. If x is non-zero, we say it is Δ^+, and if zero we sat it is 0. If we have no information about x we say it is Δ, i.e. it can be zero or it can be non-zero.

The addition and multiplication tables in table 3.1 reflect the the possible conservation of information by adding and multiplying field elements we do not know for certain. For example adding two non-zero field elements can be zero or can be non-zero. Thus the sum of two Δ^+ elements is a Δ element.

Notice that though it has many similarities, U is not a field. In fact $(U, +)$ is not even a group, since not all elements of U has inverse elements (e.g. no element of U added to Δ^+ is able to yield 0). Nevertheless U retains most of the other properties of fields; it for instance obeys the law of association with respect to addition as well as multiplication, and it obeys the law of distribution. Therefore it is quite "field-like" and shares a lot of properties with fields.

Since U is not a field U^n is not a vector space for an $n \in \mathbb{N}$, but they

still closely resembles them respectively, we will to use the same terminology keeping in mind we do not work in fields and vector spaces.

Definition 3.0.6. Let $n, m \in \mathbb{N}$ and $u \in U^n$. Then u is a vector. All the elements of $U^{n\times m}$ are matrices. The associated matrix of the vector u is defined completely analogous to definition 1.0.1.

Linear dependency is an extremely useful concept of linear algebra, so we wish to have a counterpart for this concept for U.

Definition 3.0.7 (Linear dependency in U)**.** Let $s, n \in \mathbb{N}$. Let $v_1, \ldots, v_s \in U^n$, where $v_j = (v_{j,1}, \ldots, v_{j,n})$ for $1 \leq j \leq s$.

We say that $v_1, \ldots, v_s$ are linearly dependent if there is a field $\mathbb{F}$, field elements $\lambda_1, \ldots, \lambda_s \in \mathbb{F}$ and $\tilde{v}_{j,i} \in \mathbb{F}$ for $1 \leq j \leq s$ and $1 \leq i \leq n$ so that

1. $(\lambda_1, \ldots, \lambda_s) \neq (0, \ldots, 0)$,
2. $\sum_{j=1}^{s} \lambda_j \tilde{v}_{j,i} = 0$ for $1 \leq i \leq n$,
3. If $v_{j,i} = 0$, then $\tilde{v}_{j,i} = 0$ and if $v_{j,i} = \Delta^+$, then $\tilde{v}_{j,i} \neq 0$.

Otherwise they are linearly independent.

If any v_j is so that no subset of $\{v_1, \ldots, v_s\}$ containing v_j is linearly dependent, then we say that v_j is linearly independent from the others.

It shows that definition 3.0.7 is quite similar to the conventional definition of linear dependence in linear algebra. Notice in bullet (3) that the case of $v_{j,i} = \Delta$ wasn't mentioned. This merely reflects the fact that $\tilde{v}_{j,i}$ can be chosen without restrictions.

Having the linear dependency definition we can introduce a definition of rank analogous to linear algebra.

Definition 3.0.8 (Rank)**.** Let M be a matrix over U. We denote by $\operatorname{rank}(M)$ the rank of M, i.e. the largest $r \in \mathbb{N}$ so that there exists a set of r linearly independent rows.

Proposition 3.0.9. *Let $r, s \in \mathbb{N}$. Let $M = (m_{i,j})$ be an $r \times s$ matrix over a field $\mathbb{F}$. Let $\hat{M} = (\hat{m}_{i,j})$ be the $r \times s$ matrix over U so that if $m_{i,j} = 0$ then $\hat{m}_{i,j} = 0$ otherwise $\hat{m}_{i,j} = \Delta^+$. Then* $\operatorname{rank}(\hat{M}) \leq \operatorname{rank}(M)$.

Proof. Let $r = \operatorname{rank}(\hat{M})$. By Definition 3.0.8 we have the largest $r \in \mathbb{N}$ so that there exists a set of r linearly independent rows in $\hat{M}$. This cannot possibly be larger than the rank of M, because M is one of the matrices $\hat{M}$ represents. □

Example 3.0.10. Here is an example illustrating both $\operatorname{rank}(\hat{M}) = \operatorname{rank}(M)$ and $\operatorname{rank}(\hat{M}) < \operatorname{rank}(M)$ is possible. Consider the matrix over U

$$\hat{M} = \begin{bmatrix} \Delta^+ & \Delta^+ \\ \Delta^+ & \Delta^+ \end{bmatrix}, \tag{3.1}$$

which have rank 1. Now consider the matrices over a field, say $\mathbb{F}_2$, which both can be represented by $\hat{M}$:

$$M_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$
$$M_2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$

Here $\text{rank}(M_1) = 1$ and $\text{rank}(M_2) = 2$.

We introduce a convenient map called A, which is used to retrieve all possible combinations of a vector in U, which has no Δ symbols.

Definition 3.0.11. (The map A) Let $n \in \mathbb{N}$ and $(v_1, \ldots, v_n) \in U^n$. We denote by $A(v)$ the set of vectors $(u_1, \ldots, u_n) \in U^n$ so that

- if $v_i = 0$ then $u_i = 0$,
- if $v_i = \Delta^+$ then $u_i = \Delta^+$,
- if $v_i = \Delta$ then $u_i = 0$ or $u_i = \Delta^+$.

Example 3.0.12.

$$A\Big((\Delta^+, \Delta, 0, \Delta)\Big) = \Big\{(\Delta^+, 0, 0, 0), (\Delta^+, \Delta^+, 0, 0), (\Delta^+, 0, 0, \Delta^+), (\Delta^+, \Delta^+, 0, \Delta^+)\Big\}.$$

Definition 3.0.13 (The map R)**.** Let $n \in \mathbb{N}$ and $S \subseteq \{1, \ldots, n\}$.

We denote by $R(n, S)$ the vector $(u_1, \ldots, u_n)$ in U^n such that if $i \in S$ then $u_i = 0$, otherwise $u_i = \Delta$.

We denote by $\hat{R}(n, S)$ the vector $(u_1, \ldots, u_n)$ in U^n such that if $i \in S$ then $u_i = 0$, otherwise $u_i = \Delta^+$.

3.1 Singletons

Determining a rank of a matrix in U is a complex problem in the sense that the algorithm suggested by definition 3.0.7 has a large complexity.

This section introduces the concept of singletons with an algorithm, which is useful in determining a lower bound for the ranks and much faster than utilizing the definition.

For this section we will use the following notation: let M be a matrix over either U or a field $\mathbb{F}$. Then $M[j]$ denotes the j-th column of M and $M[i, j]$ denotes the i, j-th entry of M.

Definition 3.1.1 (Singleton)**.** Let M be a matrix over U and $j \in \mathbb{N}$. We say that $M[j]$ is a singleton if there exists an $i \in \mathbb{N}$ so that $M[i, j] = \Delta^+$ and $M[l, j] = 0$ for $i \neq j$. The i-th row of M is called the row corresponding to the singleton.

Example 3.1.2. Consider the matrix

$$M = \begin{bmatrix} \Delta & \Delta^+ & 0 \\ \Delta^+ & 0 & 0 \end{bmatrix}. \tag{3.2}$$

The 2nd column is a singleton, and the 1st row is the row corresponding to that singleton.

These two small lemmas provides the justification of the following algorithm.

Lemma 3.1.3. *Let M be a matrix over U and $M[j]$ be one of it's columns. If $M[j]$ is a singleton, then the corresponding row is linearly independent from the others.*

Proof. This claim holds, because in every matrix represented my M the corresponding row is the only row with a non-zero value in the j-th entry due to the singleton. □

Lemma 3.1.4. *Let M be a matrix over U and $M[j]$ be one if it's columns. Suppose $M[j]$ is a singleton and let row i be it's corresponding row. Let M' be the matrix obtained from M by erasing column j and row i. Then M has full rank if and only if M' has full rank.*

Proof. Assume M has full rank, i.e. all it's rows are linearly independent. Deleting row i will retain linear independence of the remaining rows. Deleting column j will also retain linear independence of the rows, because that column only contains zeros after deletion of row j. Thus M' has full rank.

Assume M' has full rank, i.e. all it's rows are linearly independent. Before deleting row i and column j then row i was linearly independent to all the other rows due to lemma 3.1.3. Thus M all rows of M are linearly independent and thus M has full rank. □

Algorithm 3.1.5 (The singleton procedure)**.** Let $r, n \in \mathbb{N}$ with $r \leq n$ and $A_r \in U^{r \times n}$.

Search for a singleton in A_r. Assume the singleton $A_r[j]$ is found. Delete the singleton and it's corresponding row obtaining the $(r-1) \times (n-1)$ matrix A_{r-1}. Due to lemma 3.1.4 A_{r-1} has full rank if and only if A_r has full rank.

If possible repeat these steps with the new matrix until it has only one row left, i.e. is a $1 \times (n - r + 1)$ matrix A_1. If A_1 contains at least one Δ^+, then A_1 has full rank and therefore A_r also has full rank. In this case the singleton procedure is said to be successful.

However, if the algorithm fails to find a singleton in a matrix A_i, $1 < i \leq r$ then the singleton procedure is said to not be successful and cannot say anything conclusive about the rank of A_r.

Example 3.1.6. Demonstration of the singleton procedure:

$$A_3 = \begin{bmatrix} 0 & \Delta^+ & \Delta & 0 \\ 0 & 0 & \Delta^+ & \Delta^+ \\ \Delta^+ & 0 & 0 & \Delta \end{bmatrix}, \qquad \text{column 1 is a singleton}$$

$$A_2 = \begin{bmatrix} 0 & \Delta^+ & \Delta^+ \\ \Delta^+ & 0 & \Delta \end{bmatrix}, \qquad \text{column 1 is a singleton}$$

$$A_1 = \begin{bmatrix} \Delta^+ & \Delta^+ \end{bmatrix}.$$

A_1 contains a Δ^+, and therefore the singleton procedure is successful and A_3 has full rank.

The following lemmas establish a relationship between the ranks of different matrices.

Definition 3.1.7 (Reflection)**.** Let $n \in \mathbb{N}$ and $u \in U^n$. We denote by $\hat{u}$ the reflection of u, i.e. the vector in U where $u_i = \hat{u}_{n-i+1}$ for $1 \leq i \leq n$.

Let M be a matrix over U. We denote by $\hat{M}$ the reflection of M, i.e. the $M \in U^{n \times n}$ matrix so that $M[j,i] = \hat{M}[j, n-i+1]$ for $1 \leq i \leq n$.

Lemma 3.1.8. *Let $n \in \mathbb{N}$ and $u, v \in U^n$. Let $m \in \mathbb{N}$. If u is obtained from a cyclic shift of v, then* $\operatorname{rank}(M(u)) = \operatorname{rank}(M(v))$.

Proof. By definition 1.0.1 the rows of $M(u)$ and $M(v)$ are the same, but in another order. Thus they have the same rank. □

Lemma 3.1.9. *Let $n \in \mathbb{N}$ $\sigma \in S_n$ be a permutation. Let $M \in U^{n \times n}$ and let M' be the matrix obtained by applying σ to the rows of M. Then* $\operatorname{rank}(M) = \operatorname{rank}(M')$.

Proof. The permutation of M only change the order of the columns of M, and thus the rank of the matrix is unchanged. □

Lemma 3.1.10. *For any $M \in U^{n \times n}$ we have* $\operatorname{rank}(M) = \operatorname{rank}(\hat{M})$.

Proof. The reflection of a vector is a permutation, and thus by lemma 3.1.9 the claim holds. □

Lemma 3.1.11. *For any $u \in U^n$ we have* $\operatorname{rank}(M(u)) = \operatorname{rank}(M(\hat{u}))$.

Proof. The reflection of the matrix associated to u is identicial to the matrix associated to the reflection of u, except another order of the rows, so $\operatorname{rank}(M(\hat{u})) = \operatorname{rank}(\hat{M}(u))$ must hold. The application of lemma 3.1.10 then yields the desired result. □

The following proposition gives an interesting lower rank bound for matrices of a certain form, which will prove useful later:

Proposition 3.1.12. *Let $A = M(v) \in U^n$ and let $r \in \mathbb{N}_0$. If v has the form*

$$v = (\overbrace{0, \ldots, 0}^{r}, \Delta^+, ?, \ldots, ?),$$

where ? denotes any element of U, then $\operatorname{rank}(A) \geq r + 1$.

Proof. Let $A_{r+1} \in U^{(r+1)\times n}$ be the matrix obtained by the first $r+1$ rows of $M(v)$. The objective is to show that A_{r+1} has full rank using the fact that the singleton procedure is successful. This is proven by induction over r.

Let $r = 0$. Then A_1 consist of one row identical to v, where the first entry is Δ^+. Thus the singleton procedure is successful.

Let $r > 0$. Then the matrix A_{r+1} will have the following form:

$$A_{r+1} = \begin{bmatrix} 0 & \ldots & 0 & \Delta^+ & ? & \ldots \\ ? & 0 & \ldots & 0 & \Delta^+ & ? \\ & \ddots & & & & \ddots \\ ? & \ldots & ? & 0 & \ldots & \end{bmatrix}.$$

The $r+1$-th column is a singleton with the 1st row as the corresponding row.

Then erase the first row and the $r+1$-th column. This operation yields A_r, which is the resulting matrix containing exactly the first r rows of $M(v')$ where

$$v' = (\overbrace{0, \ldots, 0}^{r-1}, \Delta^+, ?, \ldots, ?).$$

By the induction hypothesis the singleton procedure is successful for A_r. Thus it's also successful for A_{r+1}. □

3.2 Blocks

In this section we will introduce a practical notation for constructing elaborate patterns of elements from U. Inspired by the notation of exponentiation we will define blocks as following:

Let $i \in \mathbb{N}$. We denote by $(0)^i$, $(\Delta)^i$ and $(\Delta^+)^i$ the vectors of U^i given by

$$(0)^i = (\overbrace{0, \ldots, 0}^{i}),$$

$$(\Delta)^i = (\overbrace{\Delta, \ldots, \Delta}^{i}),$$

$$(\Delta^+)^i = (\overbrace{\Delta^+, \ldots, \Delta^+}^{i}).$$

Blocks can also be constructed from other blocks, by repeating the blocks the number of times the exponent dictates.

Example 3.2.1. An example of resolving the vector built by blocks:

$$\begin{aligned}(\Delta^+)^2\big((\Delta)^4(0)^2\big)^3 &= (\Delta^+,\Delta^+)\big(\Delta,\Delta,\Delta,\Delta,0,0\big)^3\\ &= (\Delta^+,\Delta^+,\Delta,\Delta,\Delta,\Delta,0,0,\Delta,\Delta,\Delta,\Delta,0,0,\Delta,\Delta,\Delta,\Delta,0,0).\end{aligned}$$

Notice that the elements of U can be thought of as vectors of U^1 and thus can also be considered blocks themselves. So it's possible to make the definition more compact by using recursivity.

Definition 3.2.2 (Contains with overlapping)**.** Let $n, m \in \mathbb{N}$ where $n \geq m$. Let $v = (v_1, \ldots, v_n) \in U^n$ and $u = (u_1, \ldots, u_m) \in U^m$. Let w be v concatenated with itself, i.e. $w = (v_1, \ldots, v_n, v_1, \ldots, v_n) = (w_1, \ldots, w_{2n})$.

We say that $u \subset v$ or v contains with overlapping u when

$$w = (v_1, \ldots, w_j, \overbrace{u_1, \ldots, u_m}^{m}, w_{j+m+1}, \ldots, w_{2n}).$$

for some $0 \leq j \leq 2n - m - 1$.

Chapter 4

Root bounds

In this chapter we will introduce root bounds and study their properties.

4.1 Introduction

First we need some definitions to lay a foundation. These definitions are very convenient, as they will come in handy later.

Definition 4.1.1. We denote by D the set

$$D = \Big\{(n, S) \in \mathbb{N} \times \mathcal{P}(\mathbb{N}) \mid S \subseteq \{1, \ldots, n\}\Big\}.$$

Definition 4.1.2. Let $(n, S) \in D$. Let $S = \{i_1, \ldots, i_m\}$. We denote by $(n, S)^{\#}$ the set

$$(n, S)^{\#} = \{S_1, \ldots, S_r\},$$

where $r = |\mathbb{Z}_n^*|$ and for all $l \in \mathbb{Z}_n^*$ there is a j such that $S_j = \{(li_h)_n | 1 \leq h \leq m\}$.

A couple of interesting facts can be derived from this definition. Notice that if $l = 1$, there exists an element S_j of $(n, S)^{\#}$ such that

$$S_j = \{(li_h)_n | i \leq h \leq m\} = \{(i_h)_n | i \leq h \leq m\} = \{i_h | i \leq h \leq m\} = S.$$

Thus $S \in (n, S)^{\#}$ always holds.

Definition 4.1.3. We denote by χ the map $\chi : \mathcal{C} \to \mathbb{N}$ such that $\chi(C) = p$, where p is the characteristic of the field C is over.

Definition 4.1.4. Let $\zeta \in Z$. We denote by ϕ_ζ the map $\phi_\zeta : \mathcal{C} \to D$ such that $\phi_\zeta(C) = (n, S_{C,\alpha})$, where $\alpha = \zeta(\chi(C), n)$.

Proposition 4.1.5. *For any $\zeta \in Z$, the map ϕ_ζ is surjective.*

Proof. The proof is done by taking an arbitrary $(n, S) \in D$ and showing you can always find a cyclic code C that ϕ_ζ maps to (n, S).

Let $\zeta \in Z$. Take any pair $(n, \{i_1, \ldots, i_m\}) \in D$ and take any prime p. Let $\alpha = \zeta(p, n)$ and let $\mathbb{F} \subseteq \overline{\mathbb{F}}_p$ be a finite field containing α.

Let C be the cyclic code over $\mathbb{F}$ with length n and is generated by the generator polynomial $g(x) = (x-\alpha^{i_1}) \cdots (x-\alpha^{i_m})$. Thus $S_{C,\alpha} = \{i_1, \ldots, i_m\}$, which implies $\phi_\zeta(C) = (n, \{i_1, \ldots, i_m\})$. Therefore ϕ_ζ is surjective. □

Definition 4.1.6. [Root function] A root function is a map $f : D \to \overline{\mathbb{N}}$ such that $\forall \zeta \in Z, \forall C \in \mathcal{C}, f \circ \phi_\zeta(C) \leq d(C)$. We denote by R the set of all root functions.

Given $f \in R$, then f is said to be invariant if $\forall T \in (n, S)^\#, f(n, S) = f(n, T)$.

Furthermore we denote by $f^\#$ the map $f^\#(n, S) = \max_{T \in (n,S)^\#} f(n, T)$.

Definition 4.1.7. [Root bound] For any $\zeta \in Z$ and any $f \in R$, the composite map $f_{D,\zeta} = f \circ \phi_\zeta : \mathcal{C} \to \overline{\mathbb{N}}$ is called the root bound associated to f and ζ. If f is invariant, then $f_{D,\zeta}$ is called invariant. We denote by R_D the set of all root bounds.

It is evident from Definition 4.1.6 and 4.1.7 that root bounds are indeed lower bounds for the minimum distance of the code.

The root functions have some intuitive properties:

Proposition 4.1.8. *For any $f \in R$, it holds that $f^\# \in R$, $f^\#$ is invariant and $f \leq f^\#$.*

Proof. By Definition 4.1.6 $f^\#(n, S) = f(n, T)$ for a $T \in \{n, S\}^\#$. Thus $f^\# \in R$.

By Definition 4.1.6 and $S \in (n, S)^\#$ it is true, that $\max_{U \in (n,S)^\#} f(n, U) = \max_{U \in (n,T)^\#} f(n, U)$ for $T \in \{n, S\}^\#$, which implies $\forall T \in (n, S)^\#, f^\#(n, S) = f^\#(n, T)$. Thus $f^\#$ is invariant.

By Definition 4.1.6 and $S \in (n, S)^\#$ it holds that
$f(n, S) \leq \max_{T \in (n,S)^\#} f(n, T) = f^\#(n, S)$. □

Notice that the root bounds only depends on the length and the defining set of a code.

Lemma 4.1.9. *Let $C_1 \in \mathcal{C}_{q_1,n}$ and $C_2 \in \mathcal{C}_{q_2,n}$. Let $\zeta \in Z$. If $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ and $\phi_\zeta(C_1) = \phi_\zeta(C_2)$ then $d(C_1) = d(C_2)$.*

Proof. Since $\phi_\zeta(C_1) = \phi_\zeta(C_2)$ then the codes has an identical defining set with respect to ζ.

This implies that if you construct two semi-infinite sequences b_1^∞ and b_2^∞ such that b_1^n has zeros the same positions as g_1^n and b_2^n has zeros the same positions as g_2^n, then b_1^∞ and b_2^∞ has zeros in the exact same positions.

Using Theorem 2.3.4 then proves the claim. □

Theorem 4.1.10. *Let $C_1 \in \mathcal{C}_{q_1,n}$ and $C_2 \in \mathcal{C}_{q_2,n}$. Let $\zeta \in Z$. If $\chi(C_1) = \chi(C_2)$ and $\phi_\zeta(C_1) = \phi_\zeta(C_2)$ then $d(C_1) = d(C_2)$.*

Proof. Let $p = \chi(C_1)$. Then $q_1 = p^{r_1}$ and $q_2 = p^{r_2}$ for some $r_1, r_2 \in \mathbb{N}$.

Let $Q = p^{q_1 q_2}$. Thus $\mathbb{F}_{q_1}, \mathbb{F}_{q_2} \subseteq \mathbb{F}_Q$. Let $C_3 \in \mathcal{C}_{Q,n}$ so that $\phi_\zeta(C_3) = \phi_\zeta(C_1)$. Thus by Lemma 4.1.9 $d(C_3) = d(C_1)$ and $d(C_3) = d(C_2)$. □

Definition 4.1.11 (Monotonicity)**.** Let f be a root function. f is said to be monotone if for any (n, S) and (n, S') in D, where $S \subseteq S'$, then $f(n, S) \leq f(n, S')$.

All root bounds associated with monotone root functions are called monotone root bounds.

Theorem 4.1.12. *Let δ be a monotone root bound. Let C be a cyclic code and C' be a cyclic subcode of C. Then $\delta(C) \leq \delta(C')$.*

Proof. Since δ is a monotone root bound, we have some $\delta = f \circ \phi_\zeta$, where f is a monotone root function and $\zeta \in Z$.

Assume $\phi_\zeta(C) = (n, S)$ and $\phi_\zeta(C') = (n, S')$. By Proposition 1.1.7 we know that the generator polynomial g of C must divide the generator polynomial g' of C' because $C' \subseteq C$ and thus $g'(x) = a(x)g(x)$ for some $a(x)$. Therefore the zeros of g are also zeros of g' and thus $S \subseteq S'$.

Ergo, by Definition 4.1.11 $f(n, S) \leq f(n, S')$ holds, and thus $\delta(C) \leq \delta(C')$. □

We introduce a number of relevant properties of some root functions and root bounds, which we will use later.

Definition 4.1.13 (Strong root function)**.** A strong root function is a map $f : D \to \mathbb{N}$ such that

$$\forall (n, S) \in D, \qquad f(n, S) \leq \min\left\{\operatorname{rank}\big(M(u)\big) \mid u \in A\big(R(n, S)\big)\right\}.$$

We denote by R^S the set of all strong root functions.

Definition 4.1.14 (Strong root bound)**.** If δ is a root bound associated to a strong root function we say that δ is a strong root bound.

We denote by R_D^S the set of all strong root bounds.

Definition 4.1.15 (Lower and upper bounds)**.** A map $\delta : \mathcal{L} \to \overline{\mathbb{N}}$ is called

- a lower bound on $\mathcal{L}$ if $\delta(C) \leq d(C)$ for all $C \in \mathcal{L}$.
- an upper bound on $\mathcal{L}$ if $\delta(C) \geq d(C)$ for all $C \in \mathcal{L}$.

Analogously for a map $\delta : \mathcal{C} \to \overline{\mathbb{N}}$.

Definition 4.1.16 (Tight bounds)**.** Let $C \in \mathcal{C}$ and $\mathcal{F} \subseteq \mathcal{C}$. Let δ be a lower or upper bound on C. We say that

- δ is tight on C if $\delta(C) = d(C)$.
- δ is tight on $\mathcal{F}$ if $\delta(C) = d(C)$ for all $C \in \mathcal{F}$.

Definition 4.1.17 (Sharp bounds)**.** Let $C \in \mathcal{C}$ and $\mathcal{F} \subseteq \mathcal{C}$. Let δ_1 and δ_2 be lower or upper bounds on C. We say that

- δ_1 is sharper than δ_2 on C if $\delta_1(C) \geq \delta_2(C)$.
- δ_1 is sharper than δ_2 on $\mathcal{F}$ if $\delta_1(C) \geq \delta_2(C)$ for all $C \in \mathcal{F}$.

4.2 Maximal root functions and root bounds

In this section we introduce a variety of notions for a maximal root function. We start with f^*:

Definition 4.2.1. Let $f \in R$. We denote by f^* the map

$$f^*(n, S) = \max_{S' \subseteq S} f(n, S').$$

f^* also has a variety of properties:

Proposition 4.2.2. *Let $f \in R$. Then f^* is a monotone root function, $f \leq f^*$ and if g is any monotone root function so that $f \leq g$ then $f^* \leq g$.*

Proof. Let $C \in \mathcal{C}_{q,n}$ and $\zeta \in Z$. The goal is to prove that $(f^* \circ \phi_\zeta)(C) \leq d(C)$.

Let $\mathbb{F}_Q$ be the splitting field of $z^n - 1$ over $\mathbb{F}_q$. Let $\tilde{C} \in \mathcal{C}_{Q,n}$ such that $\phi_\zeta(\tilde{C}) = \phi_\zeta(C)$. Since $\mathbb{F}_Q$ is the splitting field of $\mathbb{F}_q$ then $\chi(\tilde{C}) = \chi(C)$ and then by Theorem 4.1.10 $d(\tilde{C}) = d(C)$. Since $\chi(\tilde{C}) = \chi(C)$ and $d(\tilde{C}) = d(C)$ then it is enough to prove that $(f^* \circ \phi_\zeta)(\tilde{C}) \leq d(\tilde{C})$.

Let $(n, S) = \phi_\zeta(\tilde{C})$. By Definition 4.2.1 we have $f^*(n, S) = f(n, S')$ for an $S' \subseteq S$. Let $C' \in \mathcal{C}_{Q,n}$ so that $\phi_\zeta(C') = (n, S')$.

Since $S' \subseteq S$ then $g'(x) | g(x)$ where $g(x)$ is the generator polynomial of $\tilde{C}$ and $g'(x)$ the generator polynomial of C'. Thus all codewords that can be generated by $g(x)$ can also be generated by $g'(x)$ and thus $\tilde{C} \subseteq C'$. Since the minimum distance of a code cannot possibly increase when adding codewords, then $d(C') \leq d(\tilde{C})$ must hold.

Taking advantage of the fact that f is a root function the arguments of the proof is summarized in the following inequality:

$$(f^* \circ \phi_\zeta)(C) = f^*(n, S) = f(n, S') \leq d(C') \leq d(\tilde{C}) = d(C).$$

Thus by Definition 4.2.1 f^* is a root function.

If $S \subseteq T$ then $\mathcal{P}(S) \subseteq \mathcal{P}(T)$ and therefore

$$\max_{T' \subseteq T} f(n, T') \geq \max_{S' \subseteq S} f(n, S'),$$

which by Definition 4.2.1 is

$$f^*(n,T) \geq f^*(n,S),$$

which by Definition 4.1.11 implies that f^* is monotone.

$f \leq f^*$ holds due to Definition 4.2.1.

Let $(n,S) \in D$. For any $S' \subseteq S$ $g(n,S) \geq g(n,S') \geq f(n,S')$ holds. This implies

$$g(n,S) \geq \max_{S' \subseteq S} f(n,S') = f^*(n,S).$$

□

f^* is a maximal root function with respect to S. Next we define another notion of a maximal root function, where we take the maximal root function for a fixed S and let f vary.

Definition 4.2.3. We denote by $f_{\max} : D \to \overline{\mathbb{N}}$ the map

$$f_{\max}(n,S) = \max_{f \in R} f(n,S).$$

We can immediately prove a set of basic properties for $f_{\max}$ from the definition.

Proposition 4.2.4. *The map $f_{\max}$ is a monotone root function, which is maximal in R and invariant, as well as $f^*_{\max} = f_{\max}$ and $f^{\#}_{\max} = f_{\max}$.*

Proof. We need to prove that $(f_{\max} \circ \phi_\zeta)(C) \leq d(C)$ for all $C \in \mathcal{C}$. Let $(n,S) = \phi_\zeta(C)$. By Definition 4.2.3 there exists an $f \in R$ so that $f_{\max}(n,S) = f(n,S)$. Thus

$$(f_{\max} \circ \phi_\zeta)(C) = f_{\max}(n,S) = f(n,S) = (f \circ \phi_\zeta)(C) \leq d(C). \tag{4.1}$$

Therefore is $f_{\max}$ a root function.

For any $(n,S) \in D$ and for any $f \in R$ we have by Definition 4.2.3 $f_{\max}(n,S) \geq f(n,S)$. Thus $f_{\max}$ is maximal in R.

Now consider $f^*_{\max}$. By Proposition 4.2.2 $f^*_{\max}$ is a monotone root function and $f^*_{\max} \geq f_{\max}$. Since $f_{\max}$ is maximal then $f^*_{\max} \leq f_{\max}$ must hold. Thus $f^*_{\max} = f_{\max}$ and thus $f_{\max}$ is monotone.

Now consider $f^{\#}_{\max}$. By Proposition 5.1.12 we have $f^{\#}_{\max} \geq f_{\max}$. Since $f_{\max}$ is maximal then $f^{\#}_{\max} \leq f_{\max}$ must hold. Thus $f^{\#}_{\max} = f_{\max}$ and thus $f_{\max}$ is invariant. □

It is straightforward to apply Proposition 4.2.4 on the corresponding root bound.

Corollary 4.2.5. *The map $f_{\max,D}$ is a monotone invariant root bound, which is maximal in R_D.*

Proof. $f_{\max,D}$ is a monotone invariant root bound due to Proposition 4.2.4 and Definition 4.1.7 and 4.1.11.

Since $f_{\max}$ by Proposition 4.2.4 is maximal in R, then $f_{\max,D}$ is maximal in R_D. □

4.3 Alternative formulation of the maximal root bound

This section introduces another equivalent way of expressing the maximal root bound. First we introduce some definitions and lemmas to lay the foundation.

Definition 4.3.1. For any $\zeta \in Z$ and any $(n, S) \in D$, we define the sets $V^{\zeta}_{(n,S)} \in \mathcal{C}$ and $T^{\zeta}_{(n,S)} \in \mathbb{N}$ so that

$$V^{\zeta}_{(n,S)} = \{C \mid C \in \mathcal{C}, \phi_{\zeta}(C) = (n, S)\},$$
$$T^{\zeta}_{(n,S)} = \{d(C) \mid C \in \mathcal{C}, \phi_{\zeta}(C) = (n, S)\}.$$

It follows from Proposition 4.1.5 that for any $\zeta \in Z$ and any $(n, S) \in D$ that $V^{\zeta}_{(n,S)} \neq \emptyset$ and $T^{\zeta}_{(n,S)} \neq \emptyset$.

Lemma 4.3.2. *For any $\zeta, \zeta' \in Z$ and any $(n, S) \in D$ we have $V^{\zeta}_{(n,S)} = V^{\zeta'}_{(n,S)}$ and $T^{\zeta}_{(n,S)} = T^{\zeta'}_{(n,S)}$*

Proof. Let $C \in V^{\zeta}_{(n,S)}$. Then $C \in \mathcal{C}_{q,n}$ for a field $\mathbb{F}_q$. By Proposition 1.2.4 there is a naturally equivalent code $C' \in \mathcal{C}_{q,n}$ so that $\phi_{\zeta'}(C') = (n, S)$ and $d(C) = d(C')$.

Define the maps $\rho(C) : V^{\zeta}_{(n,S)} \to V^{\zeta'}_{(n,S)}$ and $\hat{\rho} : V^{\zeta'}_{(n,S)} \to V^{\zeta}_{(n,S)}$ so that

$$\rho(C) = C' \qquad \hat{\rho}(C') = C.$$

They satisfy the equations

$$\begin{aligned}
\rho \circ \hat{\rho} &= 1_{V^{\zeta}_{(n,S)}}, \\
\hat{\rho} \circ \rho &= 1_{V^{\zeta'}_{(n,S)}}, \\
d(C) &= d(\rho(C)), && C \in V^{\zeta}_{(n,S)}, \\
d(C') &= d(\hat{\rho}(C)), && C' \in V^{\zeta'}_{(n,S)},
\end{aligned}$$

where the 1s are the identity maps of the respective sets. Thus the claim holds. □

Definition 4.3.3. We denote by g the map $g : D \to \overline{\mathbb{N}}$ by choosing an arbitrary $\zeta \in Z$ and setting

$$g(n, S) = \min T^{\zeta}_{(n,S)}.$$

Definition 4.3.3 is well-defined because Lemma 4.3.2 states that $T^{\zeta}_{(n,S)}$ does not depend on the choice of ζ.

Notice that $T^{\zeta}_{(n,S)}$ was defined as the set of all possible minimum distances of all cyclic codes with length n and defining set S. The map g takes the smallest possible minimum distance for a cyclic code with length n and defining set S. In other words g is an upper bound of the minimum distance, i.e. g tells what is the worst minimum distance we can possibly get.

Lemma 4.3.4. *$g \in R$.*

Proof. Let $C \in \mathcal{C}$ and $\zeta \in Z$. Let $(n,S) \in \phi_\zeta(C)$. $C \in V^{\zeta}_{(n,S)}$, which implies $d(C) \in T^{\zeta}_{(n,S)}$. By Definition 4.3.3 we have $g(n,S) = \min T^{\zeta}_{(,S)}$. Therefore $g(n,S) \leq d(C)$ which implies $(g \circ \phi_\zeta)(C) \leq d(C)$ and therefore is g a root function. □

Now we are ready to present the alternative way of expressing the maximal root function $f_{\max}$.

Theorem 4.3.5. *$g = f_{\max}$.*

Proof. $f_{\max}$ is a maximal in R and by Lemma 4.3.4 $g \in R$, which implies $f_{\max} \geq g$.

We need to show $f_{\max} \leq g$ for all (n,S). Assume to the contrary that there exists an $(n,S) \in D$ so that $f_{\max}(n,S) > g(n,S)$.

Let $\zeta \in Z$. Let $C \in V^{\zeta}_{(n,S)}$ so that $d(C) = \min T^{\zeta}_{(n,S)}$. By Proposition 4.1.5 such a C exists. This implies

$$d(C) = \min T^{\zeta}_{(n,S)} = g(n,S) < f_{\max}(n,S) = (f_{\max} \circ \phi_\zeta)(C),$$

which contradicts the fact that $f_{\max}$ is a root function. Thus $g = f_{\max}$. □

Corollary 4.3.6. *For any $\zeta \in Z$ and $C \in \mathcal{C}$ we have*

$$f_{\max,D,\zeta}(C) = \min\{d(C') \mid C' \in \mathcal{C}, \phi_\zeta(C') = \phi_\zeta(C)\} \tag{4.2}$$

$$f_{\max,D,\zeta}(C) = f_{\max,D}(C) \tag{4.3}$$

$$= \max_{\zeta' \in Z} f_{\max,D,\zeta'}(C) \tag{4.4}$$

$$= \max_{1 \leq i \leq r} \Big\{ \min\{d(C') \mid C' \in \mathcal{C}, S_{C',\beta} = S_{C,\alpha_i}, \alpha_i = \zeta(\chi(C),n), \beta = \zeta(\chi(C'),n)\}\Big\}. \tag{4.5}$$

Proof. Equation (4.2) is given by Theorem 4.3.5 and Definition 4.1.7 and 4.3.3:

$$\begin{aligned} f_{\max,D,\zeta}(C) &= (f_{\max} \circ \phi_\zeta)(C) = (g \circ \phi_\zeta)(C) \\ &= \min\{d(C') \mid C' \in \mathcal{C}, \phi_\zeta(C') = \phi_\zeta(C)\}. \end{aligned}$$

By Lemma 4.3.2 $T^{\zeta}_{(n,S)} = T^{\zeta'}_{(n,S)}$ for any $\zeta, \zeta' \in Z$. Therefore

$$\min\{d(C') \mid C' \in \mathcal{C}, \phi_{\zeta}(C') = \phi_{\zeta}(C)\} = \min\{d(C') \mid C' \in \mathcal{C}, \phi_{\zeta'}(C') = \phi_{\zeta'}(C)\}$$

and this means that $f_{\max,D,\zeta} = f_{\max,D,\zeta'}$, which means $f_{\max,D,\zeta}$ doesn't depend on ζ and the ζ subscript can be discarded. This gives equation (4.3).

When $f_{\max,D,\zeta}$ doesn't depend on the choice of ζ we can just as well choose the ζ which "maximizes" $f_{\max,D,\zeta}$. Thus equation (4.4).

Equation (4.2) inserted in (4.4) yields (4.5). □

Theorem 4.3.7. *$f_{\max,D} \neq d$.*

Proof. The goal is to prove that there exists a $C \in \mathcal{C}$ so that $f_{\max,D}(C) \neq d(C)$. First we show that if there exists two codes with certain properties this statement holds. Next we explicitly find such two codes.

Consider the two fields $\mathbb{F}_{q_1}$ and $\mathbb{F}_{q_2}$ with characteristics p_1 and p_2 respectively so that $p_1 \neq p_2$.

Assume $n, r \in \mathbb{N}$ so that $\alpha_1, \ldots, \alpha_r$ are all the primitive nth roots of unity over $\mathbb{F}_{q_1}$ and $\beta_1, \ldots, \beta_r$ are all the primitive nth roots of unity over $\mathbb{F}_{q_2}$.

We take any $\zeta_1, \ldots, \zeta_r \in Z$ so that $\zeta_i(p_1, n) = \alpha_i$ and $\zeta_i(p_2, n) = \beta_i$ for $1 \leq i \leq r_1$. This is possible because Z contains all possible ζs, and it's just a matter of picking the right ones, which suit our needs.

Furthermore let $C_1 \in \mathcal{C}_{q_1,n}$ and $C_2 \in \mathcal{C}_{q_2,n}$ so that

$$d(C_1) < d(C_2), \tag{4.6}$$

$$S_{C_1,\alpha_i} = S_{C_2,\beta_i}, \qquad 1 \leq i \leq r. \tag{4.7}$$

Notice that since both codes are of length n and by equation (4.7) the defining sets are equal for all i, then $\phi_{\zeta_i}(C_1) = \phi_{\zeta_i}(C_2)$ for all i.

By Corollary 4.3.6 we have

$$\begin{aligned} f_{\max,D}(C_2) &= \max_{1\leq i\leq r} \Big\{ \min\{d(C') \mid C' \in \mathcal{C}, S_{C',\beta} = S_{C_2,\alpha_i}, \alpha_i = \zeta(\chi(C_2), n), \\ &\qquad \beta = \zeta(\chi(C'), n)\}\Big\}. \\ &= \max_{1\leq i\leq r} \{\min T^{\zeta_i}_{(n,S_i)}\} \end{aligned} \tag{4.8}$$

where $S_i = S_{C_2,\alpha_i}$. By equation (4.7) we have that for any i C_1 also has the defining set S_i and therefore $C_1 \in V^{\zeta_i}_{(n,S_i)}$ and $d(C_1) \in T^{\zeta_i}_{(n,S_i)}$, which implies

$$\min T^{\zeta_i}_{(n,S_i)} \leq d(C_1). \tag{4.9}$$

By Equation (4.6), (4.8) and (4.9) we have

$$f_{\max,D}(C_2) = \max_{1\leq i\leq r} \{\min T^{\zeta_i}_{(n,S_i)}\} \leq \max_{1\leq i\leq r} (d(C_1)) = d(C_1) < d(C_2),$$

which shows that $f_{\max,D}(C_2) < d(C_2)$.

Now we will find two codes satisfying the assumptions in the previous part of the proof.

Let $q_1 = 2$, $q_2 = 17$ and $n = 31$. Since 31 is a prime number, then there are $r = \phi(31) = 31 - 1 = 30$ primitive nth roots of unity, where ϕ is Euler's ϕ-function.

Then we take two codes C_1 and C_2 both with the defining set

$$S = \{3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30\}.$$

S can with the help of Maple be used to construct generator polynomials $g_1(x)$ and $g_2(x)$:

$$\begin{aligned}
g(x) &= (x-3)(x-6)(x-11)\cdots(x-29)(x-30) \\
&= x^{15} - 279x^{14} + 35836x^{13} - 2808476x^{12} + 150033118x^{11} - 5780426594x^{10} \\
&\quad + 165699263988x^9 - 3592868139068x^8 + 59299066476681x^7 \\
&\quad - 743231577708495x^6 + 6995910714581736x^5 - 48385986918631056x^4 \\
&\quad + 236860438567939200x^3 - 769576057605655632x^2 \\
&\quad + 1469916529769413440x - 1226781977195174400, \\
g_1(x) &= g(x) \text{ rem } 2 = x^{15} + x^{14} + x^7 + x^6, \\
g_2(x) &= g(x) \text{ rem } 17 \\
&= x^{15} + 10x^{14} + 9x^{12} + 9x^{11} + 4x^{10} + 12x^9 + 16x^8 + 4x^7 + x^6 + 10x^5 \\
&\quad + 13x^4 + 14x^3 + 6x^2 + 6x.
\end{aligned}$$

Then 31×16 generator matrices can be constructed by cyclic shifting $g_1(x)$ and $g_2(x)$.

These codes have the minimum distances $d(C_1) = 7$ and $d(C_2) = 12$ and thus satisfies the criteria of the first part of the proof. □

The consequences of Theorem 4.3.7 are interesting. A root bound only depends on the information given by the defining set of a code. This theorem states that it is impossible to find a root bound that is equal to the minimum distance for all possible cyclic codes.

4.4 Reformulation of known bounds

In this section we list some known lower bounds and by reformulating them into the framework of this paper showing these bounds are root bounds.

Theorem 4.4.1. *Let C be a cyclic code. Then*

$$d(C) = \min\left\{\operatorname{rank}\big(M(\mathrm{DFT}(c))\big) \;\middle|\; c \in C, c \neq 0\right\}$$

Proof. Let b be a codeword in C of length n. Let b^∞ be the semi-inifinite sequence of period n, whose first period is $b^n = b$. Let $B^\infty = \mathrm{DFT}(b^\infty)$.

By Proposition 2.2.6 and Theorem 2.3.3 we have that $\mathrm{rank}(M(B^n)) = \Lambda(B^n) = \Lambda(B^\infty) = w(b^n)$. In other words for a codeword b we have that $\mathrm{rank}(M(\mathrm{DFT}(b))) = w(b)$. Taking the minimum weight of all non-zero codewords we get the minimum distance. □

Theorem 4.4.2. *Let C be a cyclic code of length n, defining set S and minimum distance d. Then*

$$\min\big\{\mathrm{rank}\big(M(u)\big) \;\mid\; u \in A\big(R(n,S)\big)\big\} \leq d. \tag{4.10}$$

Proof. The zero entries of a codeword c are preserved in a discreet Fourier transformation $\mathrm{DFT}(c)$.

Proposition 4.4.1 we have an expression of d, which is equivalent to the U representation on the right side of Inqeuality (4.10). By Proposition 3.0.9 we get Inqeuality (4.10). □

The following proposition justifies calling Definition 4.1.13 a root function.

Proposition 4.4.3. *A strong root function is a root function.*

Proof. Let f be a strong root function. We then have to verify it satisfies Definition 4.1.6.

Let $\zeta \in Z$ and $C \in \mathcal{C}$ of length n. Let $p = \chi(C)$ and $\alpha = \zeta(p,n)$. We have

$$(f \circ \phi_\zeta)(C) = f(n, S_{C,\alpha}).$$

Since f is a strong root function we have by Definition 4.1.13 that

$$f(n, S_{C,\alpha}) \leq \min\big\{\mathrm{rank}\big(M(u)\big) \mid u \in A\big(R(n, S_{C,\alpha})\big)\big\}.$$

By Theorem 4.4.2 we have $f(n, S_{C,\alpha}) \leq d(C)$, which implies f is a root function. □

The strong root bounds can be used to introduce yet another notion of maximality.

Definition 4.4.4. We denote by $f^S_{\max}$ the map $f^S_{\max} : D \to \overline{\mathbb{N}}$ as

$$f^S_{\max}(n,S) = \max_{f \in R^S} f(n,S).$$

Proposition 4.4.5. *The map $f^S_{\max}$ is a strong root function, which is maximal in R^S, monotone and invariant.*

Proof. Let $(n, S) = \phi_\zeta(C)$. By Definition 4.4.4 there exists an $f \in R^S$ so that $f^S_{\max}(n, S) = f(n, S)$. Therefore is $f^S_{\max}$ a strong root function.

For any $(n, S) \in D$ and for any $f \in R^S$ we have by Definition 4.4.4 $f^S_{\max}(n, S) \geq f(n, S)$. Therefore $f^S_{\max}$ is maximal in R^S.

Now consider $f^{S,*}_{\max}$. By Proposition 4.2.2 $f^{S,*}_{\max}$ is a monotone root function and $f^{S,*}_{\max} \geq f^S$. Since $f^S_{\max}$ is maximal then $f^{S,*}_{\max} \leq f^S_{\max}$ must hold. Thus $f^{S,*}_{\max} = f^S_{\max}$ and thus $f^S_{\max}$ is monotone.

Now consider $f^{S,\#}_{\max}$. By Proposition 5.1.12 we have $f^{S,\#}_{\max} \geq f^S_{\max}$. Since $f^S_{\max}$ is maximal then $f^{S,\#}_{\max} \leq f^S_{\max}$ must hold. Thus $f^{S,\#}_{\max} = f^S_{\max}$ and thus $f^S_{\max}$ is invariant. □

With the help of the strong root functions we can derive an explicit expression for $f^S_{\max}$.

Theorem 4.4.6. $f^S_{\max}(n, S) = \min\{\operatorname{rank}(M(u)) \mid u \in A(R(n, S))\}$.

Proof. By Proposition 4.4.5 we have that $f^S_{\max}$ is a strong root function and thus by Definition 4.1.13

$$f^S_{\max}(n, S) \leq \min\{\operatorname{rank}(M(u)) \mid u \in A(R(n, S))\} \tag{4.11}$$

holds. Since $f^S_{\max}$ is maximal in R^S by Proposition 4.4.5, it is sufficient to show that there exists an $f \in R^S$ such that $f(n, S) = \min\{\operatorname{rank}(M(u)) \mid u \in A(R(n, S))\}$.

Let $f_0(n, S) = \min\{\operatorname{rank}(M(u)) \mid u \in A(R(n, S))\}$. Since f_0 is well-defined, then the theorem must hold. □

4.4.1 BCH Bound

One of the perhaps most well-known bounds are the BCH Bound.

Theorem 4.4.7 (BCH Bound)**.** *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n, k, d]$ cyclic code over $\mathbb{F}_q$ with generator polynomial g.*

If there exists $i, l \in \{0, \ldots, n-1\}$ such that

$$g(\alpha^{i+j}) = 0, \qquad 0 \leq j \leq l-1,$$

then $d \geq l + 1$.

Definition 4.4.8 (BCH root function)**.** We denote by f_{BCH} the map $f_{\mathrm{BCH}} : D \to \mathbb{N}$

$$f_{\mathrm{BCH}}(n, S) = \max\{i \in \mathbb{N} \mid (0)^i \subseteq R(n, S)\} + 1.$$

Definition 4.4.8 says in plain words that f_{BCH} returns the largest number of consecutive numerals in S.

Theorem 4.4.9. *f_{BCH} is a strong root function.*

Proof. Suppose $f_{\mathrm{BCH}}(n,S) = l+1$, which implies that $(0)^l \subseteq R(n,S)$. We need to show that for any $v \in A(R(n,S))$ we have that $\mathrm{rank}(M(v)) \geq l+1$.

Since $(0)^l \subseteq R(n,S)$, then any $v \in A(R(n,S))$ must necessarily contain a block $(0)^j$, where $j \geq l$. By Lemma 3.1.8 we can without loss of generality assume that this block is located in the beginning of v, i.e.

$$v = (\overbrace{0,\ldots,0}^{j},\Delta^+,*,\ldots,*), \qquad\qquad j \geq l,$$

where $*$ denotes any element of U. Then by Proposition 3.1.12 we have $\mathrm{rank}(M(v)) \geq j+1 \geq l+1$.

Then is the inequality of Definition 4.1.13 satisfied and thus is f_{BCH} a strong root function. □

Corollary 4.4.10. *The BCH Bound is a strong root bound and is the bound associated to* f_{BCH}.

Proof. Let δ be the root bound associated with f_{BCH}. By Theorem 4.4.9 and Definition 4.1.14 we have that the δ is a strong root bound.

If $(0)^l \subseteq R(n,S)$ then there exist an $i \in \{0,\ldots,n-l+1\}$ such that $(i,i+1,\ldots,i+l-1) \subseteq S$, which implies the BCH Bound. □

4.4.2 Hartmann-Tzeng Bound

The Hartmann-Tzeng Bound is a generalisation of the BCH Bound, which suggests it might also be a root bound.

Theorem 4.4.11 (Hartmann-Tzeng Bound)**.** *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$ with generator polynomial g.*

If there exists $i,l,r,s \in \{0,\ldots,n-1\}$ such that $\gcd(r,n) < l$ and

$$g(\alpha^{i+j+kr}) = 0 \qquad\qquad 0 \leq j \leq l-1, 0 \leq k \leq s-1,$$

then $d \geq l+s$.

Definition 4.4.12 (Hartmann-Tzeng root function)**.** For any r,s,n we denote by $\rho = \rho(r,s,n)$ the quotient of rs divided by n and increased by 1, and we denote by $R(n,S)^\rho$ the vector obtained by concatenating $R(n,S)$ with itself ρ times.

Let f_{HT} be the map $f_{\mathrm{HT}} : D \to \mathbb{N}$ so that

$$f_{\mathrm{HT}}(n,S) = \max\{i \in \mathbb{N} \mid i = l+s\},$$

where l,s are such that there exist $r \in \mathbb{N}$, $\gcd(r,n) < l$, for which

$$((0)^l(\Delta)^{r-l})^s \subseteq R(n,S)^\rho.$$

The following proofs involves a lot of different values, so we start with a brief example, which we will relate to throughout this subsection.

Example 4.4.13 (Hartmann-Tzeng Bound example)**.** Let C be a binary cyclic code of length $n = 17$ with the defining set $S = \{1,2,5,6,8,9,15,16\}$. We notice that $B = ((0)^2(\Delta)^5)^3 \subseteq R(n,S)^\rho$. We can without any problems assume that B is located at the beginning of v.

Let

$$v = (0,0,1,1,0,0,1,0,0,1,1,1,1,1,0,0,1).$$

This yields the matrix

$$M(v) = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

It is clear that the first 3 rows of $M(v)$ are linearly independent, which corresponds to the BCH Bound. In the Hartmann-Tzeng Bound on the other hand we exploit the fact that we have a pattern of several intervals of consecutive zeros, which ultimately yields an even better bound. By constructing a submatrix of row 1, 2, 5, 13 and 16,

$$T = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

it it clear that the singleton procedure is successful on T, which means $M(v)$ has rank at least 5, which is a better bound than the BCH Bound.

We will need a few definitions and lemmas. From now on we will assume that v is beginning with zeros.

Lemma 4.4.14. *Let $n, r, s, l \in \mathbb{N}$ such that $\gcd(r, n) < l$. Then for any $i \in \{0, \ldots, n-1\}$ there is a $k \in \mathbb{N}$ and a $0 \leq t \leq l-1$ such that*

$$i \equiv (s+k)r + t \pmod{n}. \tag{4.12}$$

Proof. Let $i \in \{0, \ldots, n-1\}$ and let $\lambda = \gcd(r, n)$. Assume $\lambda < l$. Let t be such that

$$i \equiv t \pmod{\lambda}, \qquad 0 \leq t \leq l-1. \tag{4.13}$$

Congruence (4.13) implies that $\lambda | i - t$. Congruence (4.12) can be rewritten as

$$\begin{aligned} i &\equiv (s+k)r + t \pmod{n}, \\ i - t &\equiv (s+k)r \pmod{n}, \\ \frac{i-t}{\lambda} &\equiv (s+k)\frac{r}{\lambda} \pmod{\frac{n}{\lambda}}. \end{aligned} \tag{4.14}$$

Thus we need to search for a k satisfying Congruence (4.14). Let $y = s + k$. Then we have

$$\frac{i-t}{\lambda} \equiv y\frac{r}{\lambda} \pmod{\frac{n}{\lambda}}. \tag{4.15}$$

Since $\lambda = \gcd(r, n)$ then $\frac{n}{\lambda}$ and $\frac{r}{\lambda}$ must be integers and $\gcd(\frac{r}{\lambda}, \frac{n}{\lambda}) = 1$. Then the Extended Euclidean Algorithm yields an u and v such that

$$u\frac{r}{\lambda} + v\frac{n}{\lambda} = \gcd(\frac{r}{\lambda}, \frac{n}{\lambda}) = 1.$$

Multiplying with $\frac{i-t}{\lambda}$ yields

$$\left(\frac{i-t}{\lambda}u\right)\frac{r}{\lambda} + \left(\frac{i-t}{\lambda}v\right)\frac{n}{\lambda} = \frac{i-t}{\lambda}.$$

It shows that $\frac{i-t}{\lambda}u$ is a solution to Congruence (4.15).

If we let $k = \frac{i-t}{\lambda}u - s$, then we then have a k and t, which satisfies Congruence (4.12). □

Definition 4.4.15 (Primary pivot)**.** Let $n \in \mathbb{N}$ and $v \in (U \backslash \{\Delta\})^n$ such that $v \neq 0$. Let $i \in \{0, \ldots, n-1\}$ such that

$$i = \min\{h \mid v[h] = \Delta^+\}.$$

Then is i called the primary pivot of v.

In Example 4.4.13 we see that 2 is the primary pivot of v. The purpose of the primary pivot is to supply us with l linearly independent rows in $M(v)$, where l is the number of consecutive zeros. Next we introduce the secondary pivot, which is responsible for the remaining s independent rows.

Definition 4.4.16 (Secondary pivot)**.** Let $n, r, s, l \in \mathbb{N}$ such that $\gcd(r, n) < l$ and let $v \in (U \backslash \{\Delta\})^n$ such that $v \neq 0$. Let B be a block, where $B \subseteq v^\rho$. Let $i \in \{0, \ldots, n-1\}$ such that

1. $v[i] = \Delta^+$,
2. $i \equiv (s+k)r + t \pmod{n}$,

3. $v[i'] = 0$ for any i' so that

$$i' \equiv (s + k')r + j \pmod{n},$$

where $k' \in \{0, \ldots, k-1\}$ and $j \in \{0, \ldots, l-1\}$.

Then is i called the secondary pivot of v with respect to B.

Proposition 4.4.17. *Let $n \in \mathbb{N}$. For all $v \in (U\backslash\{\Delta\})^n$ such that $v \neq 0$ there exists a secondary pivot i.*

Proof. Since $v \neq 0$ there exists an i such that $v[i] = \Delta^+$. By Theorem 4.4.14 any such i would satisfy $i \equiv (s+k)r + t \pmod{n}$.

If this i satisfy item 3, then the proof is done. Assume i doesn't satisfy item 3. Then assign the new values $i := i'$, $k := k'$ and $t := j$ for some smaller i'. These new values satisfy item 1 and 2. If item 3 isn't satisfied, repeat the procedure. □

The secondary pivot can be understood in the following way: start at the left most value of v, i.e. at index 0. That is the first zero of the first interval of consecutive zeros. Then go rs forward. Then you are at the first value right after the block B (the subblock of size r repeated s times). The interval here corresponding to the interval of zeros of the subblocks might or might not all be zero. As long as they are all zero continue r steps more ahead. Then you have eventually advanced $(s+k)r$ steps total and found an interval, which contains a non-zero value. Go further t forward to reach that non-zero value. This is a secondary pivot.

Example 4.4.18. This is a continuation of Example 4.4.13.

We will now calculate a secondary pivot i of v with respect to $((0)^2(\Delta)^5)^3$. We have that $n = 17$, $r = 7$, $s = 3$ and $l = 2$. $i = 11$ is a secondary pivot, since $v[11] = 1$ and yields $t = 0$ and $k = 1$, where it can be shown that item 3 is satisfied for $k' = 0$ and $j \in \{0, 1\}$.

We will now relate this example to the above description of the secondary pivot. Start at index 0. Since $((0)^2(\Delta)^5)^3$ is in the beginning of v we can move $sr = 21$ forward (notice for every 7 steps the first two are zeros). Now we are at position 4. Since 4 and 5 are zeros, we can move 7 more ahead once (because $k = 1$), but at 11 we see that not both 11 and 12 are zeros We just pick 11 to be our secondary pivot (thus offset $t = 0$ – if we picked 12 then $t = 1$).

This observation leads to the following lemma:

Lemma 4.4.19. *Let $n, r, s, l \in \mathbb{N}$ such that $\gcd(r, n) < l$ and let $v \in (U\backslash\{\Delta\})^n$ such that $v \neq 0$ and $((0)^l(*)^{r-l})^s \subseteq v^\rho$ where $*$ denotes either 0 or Δ^+. Let i be the secondary pivot of v with respect to $B = ((0)^l(\Delta)^{r-l})^s$. Then $v[i - zr] = 0$ for $z \in \{1, \ldots, s-1\}$.*

Proof. We look at two cases and prove the claim for both.

Since i is a secondary pivot, then

$$i - zr \equiv (s + k - z)r + t \pmod{n}.$$

First assume $z \leq k$. Then let $k' = k - z$. Since $k' \in \{0, \ldots, k-1\}$ $t \in \{0, \ldots, l-1\}$ then by item 3 of Definition 4.4.16 we have that $v[i - zr] = 0$.

Next assume $z > k$. Let $s' = s + k - z$. Then $s' < s$, which means the index s' is inside the block B. Since $t \in \{0, \ldots, l-1\}$ and by construction of B we have that $v[s'r + t] = 0$ and therefore $v[i - zr] = 0$. □

We are now ready for the major results of this subsection.

Theorem 4.4.20. *f_{HT} is a strong root function.*

Proof. Let $(n, S) \in D$. By Definition 4.4.12 we have l, s, r such that $f_{\mathrm{HT}}(n, S) = l + s$ and l, s, r satisfy the definition. Let $v \in A(R(n, S))$ and let $m = rs$.

By Definition 4.1.13 and theorem 4.4.11 we just need to show that the singleton procedure is successful for $l + s$ rows of the matrix $M(v)$. The strategy is to carefully pick $l + s$ rows of $M(v)$ in a way, that the singleton procedure will be successful when applied to a matrix consisting of these rows. To accomplish this we will exploit the properties of the primary and secondary pivots.

Let j be the primary pivot of v. If $j > rs$ then $(0)^{rs} \subseteq v$ and then Definition 4.4.8 and Theorem 4.4.9 gives that $\operatorname{rank}(M(v)) \geq rs + 1 \geq l + s$ and then is f_{HT} a strong root function.

Suppose $j \leq rs$. Let i be the secondary pivot of v with respect to the block $((0)^l(\Delta)^{r-l})^s$.

We have to choose $l + s$ rows of $M(v)$ so that we can sucessfully apply the singleton procedure. First we take the first l rows:

$$\begin{bmatrix}
0 & \ldots & 0 & \Delta^+ & 0 & \ldots & 0 & * & \ldots & * & \ldots & \\
* & 0 & \ldots & 0 & \Delta^+ & 0 & \ldots & 0 & * & \ldots & * & \ldots \\
\vdots & & \vdots & & & & & & & & & \\
* & \ldots & * & 0 & \ldots & \Delta^+ & 0 & \ldots & 0 & * & \ldots & *
\end{bmatrix}$$

Next we append the $((s-z)r + j)$th row of $M(v)$ for all $z \in \{1, \ldots, s\}$, thus obtaining

$$T = \begin{bmatrix}
0 & \ldots & 0 & \Delta^+ & 0 & \ldots & 0 & * & \ldots & * & \ldots & & \\
* & 0 & \ldots & 0 & \Delta^+ & 0 & \ldots & 0 & * & \ldots & * & \ldots & \\
\vdots & & \vdots & & & & & & & & & & \\
* & \ldots & * & 0 & \ldots & \Delta^+ & 0 & \ldots & 0 & * & \ldots & * & \\
* & \ldots & * & 0 & \ldots & 0 & * & \ldots & & & & & \\
* & \ldots & * & 0 & \ldots & 0 & * & \ldots & * & 0 & \ldots & 0 & * \\
\vdots & & \vdots & & & & & & & & & & \\
* & \ldots & * & 0 & \ldots & 0 & * & \ldots & * & 0 & \ldots & 0 & *
\end{bmatrix}$$

We then have the $(l+s) \times n$ matrix T, which is a submatrix of $M(v)$. We will now apply the singleton procedure on T.

By picking the last s rows that way we ensure that the s intervals of consecutive zeros will be aligned under the upper triangular matrix in the first l rows: for $z = 1$ we get the jth row, which is just the first row shifted j to the right, and afterwards we shift multipla of r for each other interval of zeros.

Therefore the l rows are immediately erased, because they are rows associated to the singletons. Afterwards we have the last s rows of T:

$$T' = \begin{bmatrix} * & \dots & * & 0 & \dots & 0 & * & \dots & * & \dots & \Delta^+ & * & \dots & \\ * & \dots & * & 0 & \dots & 0 & * & \dots & * & 0 & \dots & 0 & * & \dots \\ \vdots & & \vdots & & & & & & & & & & & \\ * & \dots & * & 0 & \dots & 0 & * & \dots & * & 0 & \dots & 0 & * & \dots \end{bmatrix}$$

All the rows have at least one Δ^+ because of the presence of the secondary pivot in each row.

By construction of T, we know that T' consists of rows, which are r-cyclic shifts of each other, i.e. $T'[a+1, h] = T'[a, h-r]$.

Let $i' = i - (s-k)r + j - 1$. This is the secondary pivot of the first row of T'.

Then by Definition 4.4.16 item (1) we have that $T'[1, i'] = \Delta^+$. We need to determine that the i'th column is a singleton. As a matter of fact it is, because

$$T'[z, i'] = T'[1, i' - (z-1)r] = 0, \qquad z \in \{2, \dots, s\}, \tag{4.16}$$

where we exploit that the rows are r-cyclic and use Lemma 4.4.19. We then delete that column and the first row, and repeat the procedure.

In this way we will get a singleton with the 1st row as a corresponding row in each step, and thus we will end up with a single row containing a Δ^+. Thus is the singleton procedure successful, and then is T of full rank, and then is $\text{rank}(M(v)) \geq l + s$.

□

Corollary 4.4.21. *The Hartmann-Tzeng Bound is a strong root bound and it is the bound associated to* f_{HT}.

Proof. Let δ be the root bound associated with f_{HT}. By Theorem 4.4.20 and Definition 4.1.14 we have that the δ is a strong root bound.

The conditions of Theorem 4.4.11 corresponds to having a block of length $m = rs$ of the form $((0)^l(\Delta)^{r-l})^s$. Thus this bound corresponds to f_{HT}. □

4.4.3 Bound A

Bound A is a relatively new and not wellknown bound discovered around 2005 by Emanuele Betti & Massimiliano Sala.

Theorem 4.4.22. *Let* α *be an primitive nth root of unity over* $\mathbb{F}_q$ *and let* C *be an* $[n, k, d]$ *cyclic code over* $\mathbb{F}_q$. *Let* S *be the complete defining set of* C *with respect to* α.

Suppose there are $m, l \in \mathbb{N}$ *and* $i_0 \in \{0, \ldots, n-1\}$ *such that*

1. $(i_0 + j)_n \in S$, *for all* $j \in \{0, \ldots, ml - 1\}$,
2. $(i_0+j)_n \in S$, *for all* $j \in \{(m+h)l+1, \ldots, (m+h)l+l-1\}$, $0 \leq h \leq m$,

or such that

1. $(i_0 + j)_n \in S$, *for all* $j \in \{hl, \ldots, hl + l - 2\}$, $0 \leq h \leq m$,
2. $(i_0 + j)_n \in S$, *for all* $j \in \{(m + 1)l, \ldots, (2m + 1)l - 1\}$,

then

$$d \geq ml + l.$$

Definition 4.4.23 (Bound A root function)**.** Let f_A be the map $f_A : D \to \mathbb{N}$ so that

$$f_A(n, S) = \max\{i \in \mathbb{N} \mid i = ml + l\},$$

where m and l are so that either

$$((0)^l)^m(\Delta(0)^{l-1})^{m+1} \subseteq R(n, S) \tag{4.17}$$

or

$$((0)^{l-1}\Delta)^{m+1}((0)^l)^m \subseteq R(n, S). \tag{4.18}$$

Theorem 4.4.24. *The map* f_A *is a strong root function.*

Proof. Consider f_A. By definition either (4.17) or (4.18) holds. By Lemma 3.1.11 we can assume (4.17) holds.

We need to show that for any $v \neq 0$ so that $((0)^l)^m(\Delta(0)^{l-1})^{m+1}$ we have that $\operatorname{rank}(M(v)) \geq ml + l$. As usual we construct a submatrix of $M(v)$ by wisely choosing $ml + l$ rows such that the singleton procedure is successful.

Let T be the submatrix of $M(v)$ formed by the first $ml+l$ rows. By Lemma 3.1.8 we can safely assume that the block is located in the beginning of v. We look at the the value of $v[ml+1]$; either $v[ml+1] = 0$ or $v[ml+1] = \Delta^+$.

Assume $v[ml + 1] = 0$. Then $(0)^{j_0} \subseteq v$ for a $j_0 \geq ml + l$ because at least the first $ml + l$ entries of v will be 0. Thus applying Proposition 3.1.12 we have $\operatorname{rank}(M(v)) \geq ml + l + 1 \geq ml + l$.

Assume $v[ml + 1] = \Delta^+$. This implies v starts with the block $((0)^l)^m\Delta^+(0)^{l-1}(\Delta(0)^{l-1})^m$. We will consider the columns $T[(m + i)l + j]$, where j is decreasing from l to 1 and for every fixed j i is increasing from 0 to m. We want to prove that at every step that column is a singleton.

By the circularity of T we have that

$$\begin{aligned} T[il + j, (m + i)l + j] &= T[il + j - 1, (m + i)l + j - 1] \\ &= \dots \\ &= T[2, ml + 2] \\ &= T[1, ml + 1] = v[ml + 1] = \Delta^+. \end{aligned}$$

Suppose there is an $s \in \{2, \dots, ml + l\}$ such that $T[s, (m + i)l + j] = \Delta^+$. This implies by circularity that $v[(m + i)l + j - s] = \Delta^+$. By assumption of v we have that $(m + i)l + j - s = (m + h)l$, $h \in \mathbb{N}_0$. Isolating s we get

$$s = (i - h)l + j, \qquad\qquad h \in \mathbb{N}_0.$$

If $h = 0$ then $s = il + j$, which implies $u[m + 1] = \Delta^+$, which holds by assumption. If $h > 0$ then we have $s = i'l + j$, where $i' < i$ (since $i' = i - h$). The sth row has already been erased by a previous step. Thus is $T[l(m+i)+j]$ a singleton.

Therefore is the singleton procedure successful, and $\operatorname{rank}(M(v)) \geq \operatorname{rank}(T) = ml + l$. Then by Definition 4.4.23 and 4.1.13 we have that f_{B4} is a strong root function. □

Corollary 4.4.25. *Bound A is a strong root bound and it is the bound associated with the strong root function f_A.*

Proof. First consider condition 1 of Theorem 4.4.22. If $i_0 + ml - 1 \leq n - 1$, then S contains ml consecutive intgers, and if not, then there are two blocks of consecutive integers in the start and the end, "wrapping around". We can still view the latter case as having ml consecutive integers. We will refer to this block as the "large block".

Next consider condition 2. It says that for any h we have $l-1$ consecutive integers in S, which we will call a "small block". It also says that between

any two small blocks we have an integer $i' = i_0 + ((m+h)l)_n$ so that we do not know if $i' \in S$ (because the theorem mentions nothing about those values) and that there is an integer $i'' = (ml)_n$ so that we do not know if $i'' \in S$. In other words, condition 1 and 2 is equivalent to stating that $((0)^l)^m(\Delta(0)^{l-1})^{m+1} \subseteq R(n,S)$.

A similar argument can be made that condition 3 and 4 are equivalent to stating that $((0)^{l-1}\Delta)^{m+1}((0)^l)^m \subseteq R(n,S)$.

Since f_A is a strong root function, then Bound A must be a strong root bound. □

4.4.4 Boston Bounds

The Boston Bounds comes in different varieties.

Theorem 4.4.26 (Boston Bound 1). *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$. Let S be the complete defining set of C with respect to α.*

If $3 \nmid n$ and $\{0,1,3,4\} \subseteq S$ then $d \geq 4$.

Theorem 4.4.27 (Boston Bound 2). *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$. Let S be the complete defining set of C with respect to α.*

If $\{0,1,3,5\} \subseteq S$ then $d \geq 4$.

Theorem 4.4.28 (Boston Bound 3). *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$. Let S be the complete defining set of C with respect to α.*

If $3 \nmid n$ and $\{0,1,3,4,6\} \subseteq S$ then $d \geq 5$.

Theorem 4.4.29 (Boston Bound 4). *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$. Let S be the complete defining set of C with respect to α.*

If $4 \nmid n$ and $\{0,1,2,4,5,6,8\} \subseteq S$ then $d \geq 6$.

Theorem 4.4.30 (Boston Bound V). *Let α be an primitive nth root of unity over $\mathbb{F}_q$ and let C be an $[n,k,d]$ cyclic code over $\mathbb{F}_q$. Let S be a complete defining set of C with respect to α.*

If $3 \nmid n$ and $\{0,1,3,4,6,7\} \subset S$, then $d \geq 6$.

Then we will define the root functions.

Definition 4.4.31 (Boston root functions). Let $f_{\mathrm{B1}}, f_{\mathrm{B2}}, f_{\mathrm{B3}}, f_{\mathrm{B4}}, f_{\mathrm{B5}}$ be the

maps $f_{\mathrm{B1}}, f_{\mathrm{B2}}, f_{\mathrm{B3}}, f_{\mathrm{B4}}, f_{\mathrm{B5}} : D \to \mathbb{N}$ such that

$$f_{\mathrm{B1}}(n,S) = \begin{cases} 4 & (0,0,\Delta,0,0) \subseteq R(n,S) \wedge 3 \nmid n, \\ 1 & \text{otherwise} \end{cases}$$

$$f_{\mathrm{B2}}(n,S) = \begin{cases} 4 & (0,0,\Delta,0,\Delta,0) \subseteq R(n,S), \\ 1 & \text{otherwise} \end{cases}$$

$$f_{\mathrm{B3}}(n,S) = \begin{cases} 5 & (0,0,\Delta,0,0,\Delta,0) \subseteq R(n,S) \wedge 3 \nmid n, \\ 1 & \text{otherwise} \end{cases}$$

$$f_{\mathrm{B4}}(n,S) = \begin{cases} 6 & (0,0,0,\Delta,0,0,0,\Delta,0) \subseteq R(n,S) \wedge 4 \nmid n, \\ 1 & \text{otherwise} \end{cases}$$

$$f_{\mathrm{B5}}(n,S) = \begin{cases} 6 & R(n,S) = (0,0,\Delta,0,0,\Delta,0,0,\ldots) \wedge 3 \nmid n, \\ 1 & \text{otherwise} \end{cases}$$

Theorem 4.4.32. *f_{B1} is a strong root function.*

Proof. This is merely a special case of f_{HT} with $l = 2$ and $s = 2$.

By Theorem 4.4.20 we have that f_{HT} is a strong root function, and therefore is f_{B1} also a strong root function. □

Corollary 4.4.33. *Boston Bound 1 is a strong root bound and it is implied by f_{B1}.*

Proof. Let δ be the root bound associated with f_{B1}. By Theorem 4.4.32 and Definition 4.1.14 we have that the δ is a strong root bound.

If $(0,0,\Delta,0,0) \subseteq R(n,S)$ then there exist an $i \in \{0,\ldots,n-4\}$ such that $(i,i+1,i+2,i+3) \subseteq S$, which implies Boston Bound 1. □

Remark 4.4.34. Notice that in Corollary 4.4.33 we didn't just prove Boston Bound 1 but have also generalised it slightly. This can be done in the same manner with the remaining Boston Bounds.

Theorem 4.4.35. *f_{B2} is a strong root function.*

Proof. We need to show that for any $v \neq 0$ such that $(0,0,\Delta,0,\Delta,0) \subseteq v$ we have $\operatorname{rank}(M(v)) \geq 4$. By lemma 3.1.8 we can assume that the block is located in the beginning of v.

The two cases

1. $(0,0,0,0,\Delta,0) \subseteq v$,
2. $(0,0,\Delta^+,0,\Delta,0) \subseteq v$,

necessarily covers all possibilities, so it suffice to show $\operatorname{rank}(M(v)) \geq 4$ for each case.

Assume $(0,0,0,0,0,\Delta,0) \subseteq v$. This implies that $(0)^4 \subseteq v$. This is a special case of f_{BCH} and thus gives that $\operatorname{rank}(M(v)) \geq 5 \geq 4$.

Next assume $(0,0,\Delta^+,0,0,\Delta,0) \subseteq v$. Let A_4 be the submatrix formed by the 1st, 2nd, 3rd and last row of $M(v)$, i.e.

$$A_4 = \begin{bmatrix} 0 & 0 & \Delta^+ & 0 & \Delta & 0 & * & \dots \\ * & 0 & 0 & \Delta^+ & 0 & \Delta & 0 & \dots \\ * & * & 0 & 0 & \Delta^+ & 0 & \Delta & \dots \\ 0 & \Delta^+ & 0 & \Delta & 0 & * & * & \dots \end{bmatrix},$$

where * denotes any element of U.

It is quite straightforward that the singleton procedure is successful for A_4. Thus is $\operatorname{rank}(M(v)) \geq 4$ for this case too.

Then by Definition 4.4.31 and 4.1.13 we have that f_{B2} is a strong root function. □

Corollary 4.4.36. *Boston Bound 2 is a strong root bound and it is implied by f_{B2}.*

Proof. Let δ be the root bound associated with f_{B2}. By Theorem 4.4.32 and Definition 4.1.14 we have that the δ is a strong root bound.

If $(0,0,\Delta,0,\Delta,0) \subseteq R(n,S)$ then there exist an $i \in \{0,\dots,n-5\}$ such that $(i,i+1,i+3,i+5) \subseteq S$, which implies Boston Bound 2. □

Theorem 4.4.37. *f_{B3} is a strong root function.*

Proof. We need to show that for any $v \neq 0$ such that $(0,0,\Delta,0,0,\Delta,0) \subseteq v$ and $3 \nmid n$ we have $\operatorname{rank}(M(v)) \geq 5$. By lemma 3.1.8 we can assume that the block is located in the beginning of v.

The four cases

1. $(0,0,0,0,0,\Delta,0) \subseteq v$,
2. $(0,0,\Delta^+,0,0,0,0) \subseteq v$,
3. $(0,0,\Delta^+,0,0,\Delta^+,0,0) \subseteq v$,
4. $(0,0,\Delta^+,0,0,\Delta^+,0,\Delta^+) \subseteq v$,

necessarily covers all possibilities, so it suffice to show $\operatorname{rank}(M(v)) \geq 5$ for each case.

Assume $(0,0,0,0,0,\Delta,0) \subseteq v$. This implies that $(0)^5 \subseteq v$. This is a special case of f_{BCH} and thus gives that $\operatorname{rank}(M(v)) \geq 6 \geq 5$.

Assume $(0,0,\Delta^+,0,0,0,0) \subseteq v$. This implies that $(0)^4 \subseteq v$. This is a special case of f_{BCH} and thus gives that $\operatorname{rank}(M(v)) \geq 5$.

Assume $(0,0,\Delta^+,0,0,\Delta^+,0,0) \subseteq v$. Since $3 \nmid n$ then $n \geq 10$. Thus we have that $((0)^2\Delta)^3 \subseteq v$. Therefore we have another special case of f_{HT} with $l = 2$ and $s = 3$ (since $3 \nmid n$ and 3 is a prime then $\gcd(3,n) = 1 < l$), which yields $\operatorname{rank}(M(v)) \geq 2 + 3 = 5$.

Assume $(0,0,\Delta^+,0,0,\Delta^+,0,\Delta^+) \subseteq v$. Let A_5 be the submatrix of $M(v)$ formed by the first three and last two rows, i.e.

$$A_5 = \begin{bmatrix} 0 & 0 & \Delta^+ & 0 & 0 & \Delta^+ & 0 & \Delta^+ & * & \dots \\ * & 0 & 0 & \Delta^+ & 0 & 0 & \Delta^+ & 0 & \Delta^+ & \dots \\ * & * & 0 & 0 & \Delta^+ & 0 & 0 & \Delta^+ & 0 & \dots \\ 0 & \Delta^+ & 0 & 0 & \Delta^+ & 0 & \Delta^+ & * & * & \dots \\ \Delta^+ & 0 & 0 & \Delta^+ & 0 & \Delta^+ & * & * & * & \dots \end{bmatrix},$$

where * denotes any element of U.

It is quite straightforward that the singleton procedure is successful for A_5. Thus is $\operatorname{rank}(M(v)) \geq 5$ for the fourth case too.

Then by Definition 4.4.31 and 4.1.13 we have that f_{B3} is a strong root function. □

Corollary 4.4.38. *Boston Bound 3 is a strong root bound and it is implied by f_{B3}.*

Proof. Let δ be the root bound associated with f_{B3}. By Theorem 4.4.32 and Definition 4.1.14 we have that the δ is a strong root bound.

If $(0,0,\Delta,0,0,\Delta,0) \subseteq R(n,S)$ then there exist an $i \in \{0,\dots,n-6\}$ such that $(i,i+1,i+3,i+4,i+6) \subseteq S$, which implies Boston Bound 3. □

Theorem 4.4.39. *f_{B4} is a strong root function.*

Proof. We need to show that for any $v \neq 0$ such that $(0,0,0,\Delta,0,0,0,\Delta,0) \subseteq v$ and $4 \nmid n$ we have $\operatorname{rank}(M(v)) \geq 6$. By lemma 3.1.8 we can assume that the block is located in the beginning of v.

The four cases

1. $(0,0,0,0,0,0,0,\Delta,0,\Delta,\Delta) \subseteq v$,
2. $(0,0,0,\Delta^+,0,0,0,\Delta,0,0,0) \subseteq v$,
3. $(0,0,0,\Delta^+,0,0,0,\Delta,0,\Delta^+,\Delta) \subseteq v$,
4. $(0,0,0,\Delta^+,0,0,0,\Delta,0,0,\Delta^+) \subseteq v$,

necessarily covers all possibilities, so it suffice to show $\operatorname{rank}(M(v)) \geq 6$ for each case.

Assume $(0,0,0,0,0,0,0,\Delta,0,\Delta,\Delta) \subseteq v$. This implies that $(0)^7 \subseteq v$. This is a special case of f_{BCH} and thus gives that $\operatorname{rank}(M(v)) \geq 8 \geq 6$.

Assume $(0,0,0,\Delta^+,0,0,0,\Delta,0,0,0) \subseteq v$. This implies $((0)^3\Delta)^3 \subseteq v$, and thus we have special case of f_{HT} with $l=3$ and $s=3$ (since $4 \nmid n$ then $\gcd(4,n) \leq 2 < l$), which yields $\operatorname{rank}(M(v)) \geq 3+3=6$.

Assume $(0,0,0,\Delta^+,0,0,0,\Delta,0,\Delta^+,\Delta) \subseteq v$. Let A_6 be the submatrix of $M(v)$ formed by the first four and last two rows, i.e.

$$A_6 = \begin{bmatrix} 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & \Delta^+ & \Delta & \dots \\ * & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & \Delta^+ & \dots \\ * & * & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & \dots \\ * & * & * & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & \dots \\ 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & \Delta^+ & \Delta & * & \dots \\ 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & \Delta^+ & \Delta & * & * & \dots \end{bmatrix},$$

where * denotes any element of U.

It is quite straightforward that the singleton procedure is successful for A_6. Thus is $\text{rank}(M(v)) \geq 6$ for this case.

Lastly assume $(0,0,0,\Delta^+,0,0,0,\Delta,0,0,\Delta^+) \subseteq v$. Let A_6 be the submatrix of $M(v)$ formed by the first four and last two rows, i.e.

$$A_6 = \begin{bmatrix} 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & 0 & \Delta^+ & \dots \\ * & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & 0 & \dots \\ * & * & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & \dots \\ * & * & * & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & \dots \\ 0 & 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & 0 & \Delta^+ & * & \dots \\ 0 & \Delta^+ & 0 & 0 & 0 & \Delta & 0 & 0 & \Delta^+ & * & * & \dots \end{bmatrix},$$

where * denotes any element of U.

It is quite straightforward that the singleton procedure is successful for A_6. Thus is $\text{rank}(M(v)) \geq 6$ for this case too.

Then by Definition 4.4.31 and 4.1.13 we have that f_{B4} is a strong root function. □

Corollary 4.4.40. *Boston Bound 4 is a strong root bound and it is implied by f_{B4}.*

Proof. Let δ be the root bound associated with f_{B4}. By Theorem 4.4.32 and Definition 4.1.14 we have that the δ is a strong root bound.

If $(0,0,0,\Delta,0,0,0,\Delta,0)$ then there exist an $i \in \{0,\dots,n-8\}$ such that $(i,i+1,i+2,i+4,i+5,i+6,i+8) \subseteq S$, which implies Boston Bound 4. □

Theorem 4.4.41. *The map f_{B5} is a root function and the Boston Bound V is the root bound associated with it.*

Proof. f_{B5} is a root function, because by Theorem 4.4.30 $f_{\text{Roos}}(n,S) \leq 6 \leq d$.

The definition of f_{B5} is merely a rewriting of the conditions of Theorem 4.4.30. Therefore is Boston Bound V the root bound associated with f_{B5}. □

An interesting observation is that the Boston Bound 5 cannot be proved using the singleton procedure[2, theorem 3.84]. This can be done by a computer by traversing all possible combinations of submatrices and show the singleton and show the singleton procedure fails for all of them. It's important to note, however, that we don't conclude whether or not Boston Bound 5 actually is strong or not.

Chapter 5

Border bounds

We wish to be able to improve on the root bounds by utilizing more information than merely the length and the defining set of the code, which was all we used with the root bounds.

In this chapter we will introduce border bounds, which in addition take advantage of the knowlegde of the defining sets of the cyclic subcodes of the codes, which means that these bounds – contrary to root bounds – depends on the internal structure of the fields.

5.1 Introduction

First we will introduce some preliminary definitions and claims.

Definition 5.1.1 (Border codeword)**.** A non-zero codeword c of a cyclic code C is called a border codeword for C if it is not contained in any proper cyclic subcode of C.

We denote by $\hat{C}$ the set of all border codewords of C.

Definition 5.1.2 (Border distance)**.** We denote by $\hat{d}(C)$ the border distance of C, i.e.

$$\hat{d}(C) = \min_{c \in \hat{C}} w(c).$$

Example 5.1.3. $C = \mathbb{F}_2^4$ is a cyclic code, and it's proper cyclic subcodes are $C_1 = \{0000, 1010, 0101, 1111\}$, $C_2 = \{0000, 1111\}$ and $C_3 = \{0000\}$. Therefore is e.g. $0100 \in \hat{C} = C \backslash (C_1 \cup C_2 \cup C_3)$ a border codeword. The border distance is then 1.

Lemma 5.1.4. *Let $C \in \mathcal{C}$ and let $c \in C$, $c \neq 0$. Then c is a border codeword for unique cyclic subcode D of C. The generator polynomial of D is the greatest common divisor of c and $x^n - 1$.*

Proof. Take a $c \in C$, $c \neq 0$. If c is a border codeword for C then the claim is trivially satisfied. Assume c is not a border codeword for C. This implies that there exists a proper cyclic subcode $C' \subset C$, where $c \in C'$. If c is a border codeword of C' then the claim is proven, otherwise repeat the procedure of finding a proper cyclic subcode, which c belongs to.

Since the cyclic subcodes found are proper, then their size will always be strictly smaller than the previous cyclic codes, and therefore the above algorithm is bound to end eventually.

Suppose c is a border codeword for D. Let $c = g_D \cdot c_1 \cdots c_s$, $s \in \mathbb{N}_0$ and g_D is the generator polynomial of D. Since c is a border codeword then it is not contained in any proper cyclic subcodes of D, i.e. none of the generator polynomials of these cyclic subcodes divides c. This implies that $g_D = \gcd(c, x^n - 1)$. This also proves uniqueness of D. □

Corollary 5.1.5. *Let $C \in \mathcal{C}$. Then*

$$C\backslash\{0\} = \bigcup_{D \subseteq C, D \in \mathcal{C}} \hat{D}, \tag{5.1}$$

$$d(C) = \min_{D \subseteq C, D \in \mathcal{C}} \hat{d}(D). \tag{5.2}$$

Proof. Let $c \in C\backslash\{0\}$. Then by Lemma 5.1.4 there exists a cyclic subcode D such that c is a border codeword for D, i.e. $c \in \hat{D}$. Thus $c \in \cup_{D \subset C, D \in \mathcal{C}} \hat{D}$.

Let $c \in \cup_{D \subseteq C, D \in \mathcal{C}} \hat{D}$. This implies there is a cyclic subcode D of C such that c is a border codeword for D. Since c by Definition 5.1.1 is non-zero, then $c \in C\backslash\{0\}$. This proves Equation (5.1).

Using Definition 5.1.2 we get

$$\begin{aligned}
\min_{D \subseteq C, D \in \mathcal{C}} \hat{d}(D) &= \min_{D \subseteq C, D \in \mathcal{C}} \min_{c \in \hat{D}} w(c), \\
&= \min_{D \subseteq C, D \in \mathcal{C}, c \in \hat{D}} w(c), \\
&= \min_{c \in C\backslash\{0\}} w(c), \\
&= d(C),
\end{aligned}$$

which proves Equation (5.2). □

Using this result we can reformulate Theorem 4.4.1.

Proposition 5.1.6. *Let $C \in \mathcal{C}$. Let* $\mathrm{DFT}(C)$ *be the code formed by the discreet Fourier transforms of the codewords of C. Then the minimum distance of C is*

$$d(C) = \min_{D \subset C, D \in \mathcal{C}} \{\min_{c \in \hat{D}} \mathrm{rank}(M(\mathrm{DFT}(c)))\}.$$

Proof. By Corollary 5.1.5 and Theorem 4.4.1 we get

$$\begin{aligned} d(C) &= \min_{D \subseteq C, D \in \mathcal{C}} \hat{d}(D) \\ &= \min_{D \subset C, D \in \mathcal{C}} \{\min_{c \in \hat{D}} \operatorname{rank}(M(DFT(c)))\}. \end{aligned}$$ □

We will now expand on the framework of root functions. First we define a set ϵ, which will serve the purpose of border functions equivalent to that of D for root functions.

Definition 5.1.7. We denote by ϵ the set

$$\epsilon = \Big\{(n, S, \mathcal{S}) \in \mathbb{N} \times \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathcal{P}(\mathbb{N})) \mid (n, S) \in D, \mathcal{S} = T_1, \ldots, T_s \\ S \subseteq T_h \subset \{1, \ldots, n\}, T_h \neq T_k, 1 \leq h, k \leq s, h \neq k\Big\}$$

Definition 5.1.8. Let $(n, S, \mathcal{S}) \in \epsilon$, $\mathcal{S} = \{T_1, \ldots, T_s\}$, where $s \in \mathbb{N}$. We denote by $(n, S, \mathcal{S})^{\#}$ the set

$$(n, S, \mathcal{S})^{\#} = \big\{(S_1, \mathcal{S}_1), \ldots, (S_r, \mathcal{S}_r)\big\},$$

where $r = |\mathbb{Z}_n^*|$, $\mathcal{S}_i = \{T_{i,1}, \ldots, T_{i,s}\}$ and for any $l \in \mathbb{Z}_n^*$ there is an i so that $S_i = \{(lt)_n \mid t \in S\}$ and $T_{i,j} = \{(lt)_n \mid t \in T_j\}$ for any j.

Notice that if $l = 1$, there exists an element $(S_j, \mathcal{S}_j) \in (n, S, \mathcal{S})^{\#}$ such that

$$\begin{aligned} S_j &= \{(lt)_n \mid t \in S\} = \{(t)_n \mid t \in S\} = \{t \mid t \in S\} = S \\ T_{i,j} &= \{(lt)_n \mid t \in T_j\} = \{t \mid t \in T_j\} = T_j \\ \mathcal{S}_j &= \{T_{j,1}, \ldots, T_{j,s}\} = \{T_1, \ldots, T_s\} = \mathcal{S} \end{aligned}$$

and therefore $(S, \mathcal{S}) \in (n, S, \mathcal{S})^{\#}$ always holds.

Next we introduce a border function pendant to ϕ_ζ:

Definition 5.1.9. Let $\zeta \in Z$. We denote by φ_ζ the map $\varphi_\zeta : \mathcal{C} \to \epsilon$ such that $\varphi_\zeta(C) = (n, S_{C,\alpha}, \mathcal{S})$, where $\alpha = \zeta(\chi(C), n)$ and $\mathcal{S} = \{S_{D,\alpha} \mid D \subseteq C, D \in \mathcal{C}\}$.

Notice that D cannot be the null cyclic subcode in the above definition, because the null cyclic subcode would yeild the defining set $\{1, \ldots, n\}$, which was excluded in the definition of ϵ.

We are not ready to define the border function, which is quite analougous to root functions, but extended using the previosuly defined concepts.

Definition 5.1.10 (Border function)**.** A border function is a map $f : \epsilon \to \overline{\mathbb{N}}$ such that $\forall \zeta \in Z, \forall C \in \mathcal{C}, f \circ \varphi_\zeta(C) \leq d(C)$. We denote by B the set of all border functions.

Given $f \in B$, then f is said to be invariant if $\forall (S', \mathcal{S}') \in (n, S, \mathcal{S})^{\#}, f(n, S, \mathcal{S}) = f(n, S', \mathcal{S}')$.

Furthermore we denote by $f^{\#}$ the map

$$f^{\#}(n, S, \mathcal{S}) = \max_{(S', \mathcal{S}') \in (n, S, \mathcal{S})^{\#}} f(n, S', \mathcal{S}').$$

Definition 5.1.11 (Border bound)**.** For any $\zeta \in Z$ and any $f \in B$, the composite map $f_{\epsilon,\zeta} = f \circ \varphi_{\zeta} : \mathcal{C} \to \overline{\mathbb{N}}$ is called the border bound associated to f and ζ. If f is invariant, then $f_{\epsilon,\zeta}$ is called invariant. We denote by B_{ϵ} the set of all root bounds.

It is evident from Definition 5.1.10 and 5.1.11 that border bounds are lower bounds for the minimum distance of the code.

Proposition 5.1.12. *For any $f \in B$, it holds that $f^{\#} \in B$, $f^{\#}$ is invariant and $f \leq f^{\#}$.*

Proof. By Definition 5.1.10 $f^{\#}(n, S, \mathcal{S}) = f(n, S', \mathcal{S}')$ for a $(S', \mathcal{S}') \in \{n, S, \mathcal{S}\}^{\#}$. Thus $f^{\#} \in B$.

By definition 5.1.10 and $(S', \mathcal{S}') \in \{n, S, \mathcal{S}\}^{\#}$ it is true, that $\max_{(U,\mathcal{U}) \in (n,S,\mathcal{S})^{\#}} f(n, U, \mathcal{U}) = \max_{(U,\mathcal{U}) \in (n,T,\mathcal{T})^{\#}} f(n, U, \mathcal{U})$ for $(T, \mathcal{T}) \in \{n, S, \mathcal{S}\}^{\#}$, which implies $\forall (T, \mathcal{T}) \in (n, S, \mathcal{S})^{\#}, f^{\#}(n, S, \mathcal{S}) = f^{\#}(n, T, \mathcal{T})$. Thus $f^{\#}$ is invariant.

By definition 5.1.10 and $(S, \mathcal{S}) \in (n, S, \mathcal{S})^{\#}$ it holds that

$$f(n, S, \mathcal{S}) \leq \max_{(T,\mathcal{T}) \in (n,S,\mathcal{S})^{\#}} f(n, T, \mathcal{T}) = f^{\#}(n, S, \mathcal{S}). \qquad \square$$

It is clear that root functions are a generalization of border function, since root functions can be regarded as border functions by disregarding $\mathcal{S}$ as the following definition and proposition illustrates.

Definition 5.1.13. Let $f \in R$. We denote by $\overline{f} : \epsilon \to \overline{\mathbb{N}}$ such that

$$\overline{f}(n, S, \mathcal{S}) = f(n, S).$$

Proposition 5.1.14. *Let $f \in R$. Then $\overline{f} \in B$.*

Proof. The claim follows from Definition 4.1.6 and 5.1.10. $\square$

Using this trick every root function can in principle be regarded as a border function and thus every root bound can be regarded as a border bound.

By analogy to root functions we now define strong border functions:

Definition 5.1.15 (Localization)**.** Let f be a border function. A function $\hat{f} : D \to \overline{\mathbb{N}}$ such that

$$f(n, S, \mathcal{S}) = \min_{T \in \mathcal{S}} \hat{f}(n, T), \qquad \hat{f}(n, T) \leq \min\{\mathrm{rank}(M(\hat{R}(n, T)))\}$$

is called the localization of f.

Definition 5.1.16 (Strong border function)**.** A border function is called a strong border function if there exists a localization of it.

We denote by B^S the set of all strong border functions.

Definition 5.1.17 (Strong border bound)**.** A border bound associated to a strong border function is called a strong border bound.

We denote by B_ϵ^S the set of all strong border bounds.

Proposition 5.1.18. *Let $f \in R^S$. Then $\overline{f} \in B^S$.*

Proof. The claim follows from Definition 4.1.13 and 5.1.16. □

We now formally introduce an algorithm framework to assist us in estimating lower bounds of the border bounds.

Definition 5.1.19 (Independence-check procedure)**.** Let $n, m \in \mathbb{N}$. Let ϵ be an algorithm that admits as input any matrix $A \in U^{n \times m}$ and that returns either true or false. We say that ϵ is an independence-check procedure if any time it returns true, then A has full rank, i.e. $\text{rank}(A) = \min(n, m)$.

Given an independence-check procedure ϵ, we are able to construct algorithms, which are lower bounds on the rank of a matrix over U. We call these rank-bounding algorithms. Here we introduce two of them:

Algorithm 5.1.20 (First rank-bounding algorithm from ϵ)**.** Input: A matrix A over U. Output: A natural number. Initialization: Let S be a finite sequence of rows of A containing the first row of A. Cycle: Construct a matrix of the rows of S and evaluate it with ϵ. If false, then remove the last row from S. If there exists a row of A, which hasn't been added to S yet, then add it and repeat the cycle. Otherwise return the length of S.

Algorithm 5.1.21 (Second rank-bounding algorithm from ϵ)**.** Input: A matrix A over U. Output: A natural number. Initialization: Let $l = 1$. Cycle: Construct every combination of matrices formed by taking l rows of A and evaluate them all with ϵ. If they all return true and $l < n$ then set $l := l + 1$ and repeat the cycle. If they all return true and $l = n$ then return n. Otherwise return $l - 1$.

Definition 5.1.22 (First and second realization)**.** Let f be a strong border function and $\hat{f}$ be it's localization, and let ϵ be an independence-check procedure, $\dot{\epsilon}$ be it's first rank-bounding algorithm and $\tilde{\epsilon}$ be it's second rank-bounding algorithm.

We say that f (or $\hat{f}$) is the first realization of ϵ if $\hat{f}(n, T) = \dot{\epsilon}(M(\hat{R}(n, T)))$ for any $(n, T) \in D$.

Likewise we say that f (or $\hat{f}$) is the second realization of ϵ if $\hat{f}(n, T) = \tilde{\epsilon}(M(\hat{R}(n, T)))$ for any $(n, T) \in D$.

In both cases we say that f is based on ϵ.

5.2 Reformulation of known bounds

Analogous to the root bound section of the same name, we will now reformulate some bounds within the new framework and thus show they are border bounds.

5.2.1 Schaub Bound

In this subsection we will introduce an independence-check procedure, whose first realization is equivalent ot the Schaub Bound.

Algorithm 5.2.1 (Schaub independence-check procedure)**.** Input: A matrix A over U, whose rows are n-dimensional vectors of U^n and form the set $R = \{r_1, \ldots, r_h\}$. Initialization: Let $i = 0$ and let $c_1, \ldots, c_{h-1} \in U$. Cycle: For column i of A we will consider

$$r_h[i] = \sum_{j=1}^{h-1} c_j r_j[i]. \tag{5.3}$$

Find the possible values of $c_1, \ldots, c_{h-1}$ satisfying Equation (5.3) and also satisfying the equations from earlier cycles. If it yields a contradiction and $i < n$, then let $i := i + 1$ and repeat the cycle. If it yields a contradiction, then return true. If not and $i < n$, then let $i := i + 1$ and repeat the cycle. If not and $i = n$, then return false. Output: true or false. Initialization:

Example 5.2.2. Let

$$T = \begin{bmatrix} \Delta^+ & \Delta^+ & 0 & 0 & \Delta^+ & 0 & \Delta^+ & \Delta^+ \\ 0 & 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 \\ 0 & 0 & \Delta^+ & \Delta^+ & 0 & 0 & \Delta^+ & 0 \\ \Delta^+ & \Delta^+ & 0 & 0 & 0 & \Delta^+ & 0 & 0 \\ 0 & 0 & 0 & \Delta^+ & \Delta^+ & 0 & 0 & \Delta^+ \\ 0 & 0 & \Delta^+ & \Delta^+ & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \Delta^+ & 0 & 0 & 0 \end{bmatrix}.$$

Let $r_1, \ldots, r_7$ be the rows of T.

We want to estimate $\operatorname{rank}(T)$ by invoking the Schaub independence-check procedure several times.

- T contains Δ^+s, so $\operatorname{rank}(T) \geq 1$.
- We apply the procedure on the first two rows. We want to find out if the second row is a linear combination of the first row, which is essentially what the Schaub independence-check procedure is about. Let $c_1 \in U$ so that $r_2 = c_1 r_1$. 1st column yields $r_2[0] = c_1 r_1[0]$, which yields $0 = c_1 \Delta^+$, i.e. $c_1 = 0$. 2nd to 4th column yields no additional restrictions. From now on we will not mention the columns, which

doesn't add additional restrictions or add restrictions we don't use in our argument. The 5th column yields $r_2[4] = c_1 r_1[4]$, which yields $\Delta^+ = 0 \cdot 0$, which is a contradiction. Thus $\text{rank}(T) \geq 2$.

- We want to check if r_3 is linearly dependent on $\{r_1, r_2\}$. 1st column yields $r_3[0] = c_1 r_1[0] + c_2 r_2[0]$, which yields $0 = c_1\Delta^+ + c_2 \cdot 0$, i.e. $c_1 = 0$. 3rd column yields $r_3[2] = c_1 r_1[2] + c_2 r_2[2]$, which yields $\Delta^+ = 0 \cdot 0 + c_2 \cdot 0$, which is impossible. Thus $\text{rank}(T) \geq 3$.

- We continue in the same pattern as the previous bullets, but less verbose. 1st column yields $c_1 = \Delta^+$. 3rd column yields $c_3 = 0$. 5th column yields $\Delta^+ = 0$, which is a contradiction. Thus $\text{rank}(T) \geq 4$.

- 3rd column yields $c_3 = 0$. By 7th column this implies $c_1 = 0$, and this creates a contradiction in the 5th column.

- 3rd column yields $c_3 = \Delta^+$. 6th column yields $c_1 = \Delta^+$. 7th column yields $c_5 = \Delta^+$. 1st column yields $c_4 = \Delta^+$. 5st column yields $c_2 = \Delta^+$. No contradiction with 2nd, 4th and 8th column, so we discard r_6.

- Remembering we discarded r_6 we need to examine $r_7 = \sum_{j=1}^{5} c_j r_j$. 3rd column yields $c_3 = 0$. 4th column yields $c_5 = 0$. 5th column yields $c_1 = \Delta^+$. 1st column yields $c_4 = \Delta^+$. 6th column yields $c_2 = \Delta^+$. 7th column then contains a contradiction. Thus $\text{rank}(T) \geq 6$.

What we have done in Example 5.2.2 is actually the first rank-bounding algorithm of the Schaub independence-check procedure. By Definition 5.1.22

By using this procedure we get the first realization and by Definition 5.1.22 view it as the localisation of a strong root function. We will name this root function the Schaub function. The Schaub bound is the border bound associated to the Schaub function[2, page 45].

5.2.2 The Singleton-procedure Bound

In this subsection we consider the singleton procedure described in chapter 3. This is by Definition 5.1.19 actually an independence-check procedure.

Definition 5.2.3 (Singleton-procedure function)**.** Let ϵ be the singleton procdure, and let h be the first realization of ϵ. Then h is a singleton-procedure function.

Definition 5.2.4 (Singleton-procedure bound)**.** The bound associated with the singleton-procedure function is called the Singleton-procedure Bound.

We will now illustrate this algorithm. For the sake of comparison with Schaub independence-check procedure we use the same input as Example 5.2.2.

Example 5.2.5. We consider the matrix T of Example 5.2.2.

- r_1 contains a Δ^+, so $\text{rank}(T) \geq 1$.
- The submaxtrix consisting of rows $\{r_1, r_2\}$ contains a singleton in the first column, and erasing yields a non-zero row, thus $\text{rank}(T) \geq 2$.
- The submaxtrix consisting of rows $\{r_1, r_2, r_3\}$ has singletons at column 1 and afterwards column 3. Thus $\text{rank}(T) \geq 3$.
- The submaxtrix consisting of rows $\{r_1, r_2, r_3, r_4\}$ has singletons at column 3 and then column 5 and then column 1. Thus $\text{rank}(T) \geq 4$.
- The submaxtrix consisting of rows $\{r_1, r_2, r_3, r_4, r_5\}$ has singletons at column 3, then 4, then 5, then 1. Thus $\text{rank}(T) \geq 5$.
- The submaxtrix consisting of rows $\{r_1, r_2, r_3, r_4, r_5, r_6\}$ has no singletons, so we discard r_6 and still have $\text{rank}(T) \geq 5$.
- The submaxtrix consisting of rows $\{r_1, r_2, r_3, r_4, r_5, r_7\}$ has singletons at column 3, then 7, then 8, then 5, then 1. Thus $\text{rank}(T) \geq 6$.

5.2.3 Equivalence of the bounds

In this subsection we will show that the Schaub Bound and the Singleton-procedure Bound are equivalent.

This result requires a little preparation in form of a few lemmas and definitions for convenience.

Definition 5.2.6 ($\mathcal{M}_T$ and $\mathcal{Q}_T$)**.** Let $h, n \in \mathbb{N}$, such that $2 \leq h \leq n$, and let T be an $h \times n$ matrix over U.

We denote by $\mathcal{M}_T$ the logical statement "we can prove that the rows of T are linearly dependent by applying the Schaub procedure."

We denote by $\mathcal{Q}_T$ the logical statement "we can prove that the rows of T are linearly dependent by applying the singleton procedure."

Lemma 5.2.7. *If $\mathcal{M}_T$, then there is at least one singleton in T.*

Proof. By the law of contraposition the claim is equivalent to the claim "if there are no singletons, then $\mathcal{M}_T$ is false." So we assume that there are no singletons and must prove that $\mathcal{M}_T$ cannot hold, i.e. we must find $c_1, \ldots, c_{h-1} \in \{0, \Delta^+\}$ such that the last row of T may be a linear combination of the others with $c_1, \ldots, c_{h-1}$ as coefficients.

Let $c_i = \Delta^+$ for $1 \leq i \leq h-1$. We will show that this choice of coefficients will not lead to any contradiction.

Let i be a column index $1 \leq j \leq n$. We have that

$$r_h(i) = \sum_{j=1}^{h-1} c_j r_j(i).$$

Since the $r_j(i)$, which yields zero doesn't contribute to the sum, we can disregard those. We then let $A_i = \{k \in \mathbb{N} \mid r_k(i) \neq 0\}$ and then we have

$$\begin{aligned} r_h(i) &= \sum_{j=1}^{h-1} c_j r_j(i) \\ &= \sum_{j \in A_i} c_j r_j(i) \\ &= \sum_{j \in A_i} \Delta^+ \Delta^+ \\ &= \sum_{j \in A_i} \Delta^+. \end{aligned}$$

There are three possible outcomes of this expression:

1. if $|A_i| = 0$ then $\sum_{j \in A_i} \Delta^+ = 0$,
2. if $|A_i| = 1$ then $\sum_{j \in A_i} \Delta^+ = \Delta^+$,
3. if $|A_i| > 1$ then $\sum_{j \in A_i} \Delta^+ = \Delta$.

In the first case all entries 1 to $h-1$ of column i are zeros except possibly the last entry h. There will be a contradiction if $r_h(i) = \Delta^+$, but this cannot be the case, because we assumed T contained no singletons.

In the second case exact one entry of the first $h-1$ entries is Δ^+. Here there will be a contradiction only if $r_h(i) = 0$, but this cannot be the case either, because then the column would be a singleton.

In the third case $r_h(i) = \Delta$, which doesn't make any restictions on the values, and is thus incapable of creating a contradiction. □

Lemma 5.2.8. *Let T' be the matrix obtained by T by erasing a singleton and it's corresponding row. Then $\mathcal{M}_T \Leftrightarrow \mathcal{M}_{T'}$.*

Proof. We can without loss of generality assume the singleton of T is the first column. This gives the following setting:

$$T = \begin{bmatrix} \Delta^+ & \Delta & \dots & \Delta \\ 0 & & & \\ 0 & & T' & \\ 0 & & & \end{bmatrix}.$$

Let t_i denote the ith row of T and $t_i(j)$ denot the jth entry of t_i. Analogous with t' and T'. Notice $t_i(j) = t'_i(j)$ for $2 \leq i \leq h$ and $2 \leq j \leq n$.

By the law of contraposition the claim is equivalent to $\neg\mathcal{M}_T \Leftrightarrow \neg\mathcal{M}_{T'}$.

$\neg\mathcal{M}_T$ means that there are $h-1$ elements $\{c_1^T, \dots, c_{h-1}^T\}$ in $\{0, \Delta^+\}$ such that the last row in T may be a linear combination of the other rows, i.e.

$$t_h = \sum_{i=1}^{h-1} c_i^T t_i. \tag{5.4}$$

$\neg\mathcal{M}_{T'}$ means that there are $h-2$ elements $\{c_2^{T'},\ldots,c_{h-1}^{T'}\}$ in $\{0,\Delta^+\}$ such that the last row in T' may be a linear combination of the other rows, i.e.

$$t'_h = \sum_{i=2}^{h-1} c_i^{T'} t'_i.$$

First we will prove $\mathcal{M}_T \Leftarrow \mathcal{M}_{T'}$. We merely construct $\{c_1^T,\ldots,c_{h-1}^T\}$ such that $c_1^T = 0$ and $c_j^T = c_j^{T'}$ for $2 \le j \le h-1$.

Then we will prove $\mathcal{M}_T \Rightarrow \mathcal{M}_{T'}$. From Equation (5.4) we have in particular that $t_h(1) = \sum_{i=1}^{h-1} c_i^T t_i(1)$. Since $t_1(1) = \Delta^+$ and $t_j(1) = 0$ for $2 \le j \ne h$ then

$$\begin{aligned}
0 &= t_h(1) \\
&= \sum_{i=1}^{h-1} c_i^T t_i(1) \\
&= c_1^T t_1(1) + \sum_{i=2}^{h-1} c_i^T t_i(1) \\
&= c_1^T t_1(1) + \sum_{i=2}^{h-1} c_i^T \cdot 0 \\
&= c_1^T t_1(1) \\
&= c_1^T \cdot \Delta^+,
\end{aligned}$$

which implies $c_1^T = 0$. This means that the last row of T may be a linear combination of the last $h-2$ rows, which are the rows of T'.

In other words, we construct $\{c_2^{T'},\ldots,c_{h-1}^{T'}\}$ such that $c_i^{T'} = c_i^T$ for $2 \le i \le h-1$. □

Theorem 5.2.9. *The localization of the Schaub function and the localization of the singleton-procedure function are the first relization of the same independence-check procedure.*

Proof. First we realize, that the claim can be rephrased to $\mathcal{Q}_T \Leftrightarrow \mathcal{M}_T$.

$\mathcal{Q}_T \Rightarrow \mathcal{M}_T$ holds, because if T can be proven to be linearly independent by the singleton procedure, then it is quite straightforward to prove the same by finding contradictions when trying to find coefficients in the Schaub independence-check procedure.

$\mathcal{Q}_T \Leftarrow \mathcal{M}_T$ is proven by induction on n. For $n = 1$ it is obvious.

Suppose $n > 1$. By Lemma 5.2.7 we know that T contains a singleton. Assume column i is a singleton. We then erase the singleton and it's corresponding row and obtain matrix T'. The erasure was a step in the singleton procedure, so $\mathcal{Q}_{T'} \Leftrightarrow \mathcal{Q}_T$.

By the induction hypothesis we have that $\mathcal{M}_{T'} \Rightarrow \mathcal{Q}_{T'}$. Combined with Lemma 5.2.8 we have that

$$\mathcal{M}_T \Leftrightarrow \mathcal{M}_{T'} \Rightarrow \mathcal{Q}_{T'} \Leftrightarrow \mathcal{Q}_T. \qquad \square$$

This result is interesting, because it implies that the associated border bounds are equivalent, i.e. equal for any choice of $\zeta \in Z$.

5.2.4 The van Lint-Wilson Shifting Bound

This subsection describes the van Lint-Wilson Shifting Bound in the framework of this paper. First we will need a definition.

Definition 5.2.10 (Independence from S)**.** Let $S \subset \mathbb{N}$ and $A \subseteq S$. We say that A is independent from S if one of the following holds:

1. $A = \emptyset$.
2. A is a shift of a set B, where B is independent from S.
3. $A = B \cup \{a\}$, where B is independent from S, $B \subseteq S$ and $a \notin S$.

Repeated use of this definition can be used to construct independent sets as illustrated in the following example.

Example 5.2.11. Let $S = \{1, 3, 4\}$.

By item 1 $\emptyset$ is independent from S and since $\emptyset \subseteq S$ and $5 \notin S$, then by item 3 $\emptyset \cup \{5\} = \{5\}$ is independent from S.

By item 2 the independent set $\{5\}$ can be shifted to $\{3\}$ and still be independent. Then by item 3 $\{3\} \cup \{6\} = \{3, 6\}$ is also independent.

Using item 2 then $\{1, 4\}$ is independent as well, and by item 3 so is $\{1, 4, 5\}$, etc.

Algorithm 5.2.12 (van Lint-Wilson Shifting Bound)**.** Input: A cyclic code $C \in \mathcal{C}_{q,n}$ and α, where α is a primitive nth root of unity over $\mathbb{F}_q$.

Cycle: For any cyclic subcode D of C:

- Compute the defining set S of D with respect to α.
- Compute the length $\lambda(D)$ of the largest set independent from S.

Afterwards return $\min\{\lambda(D) \mid C \subseteq D, D \text{ cyclic subcode}\}$.

It is clear that the van Lint-Wilson Shifting Bound is a border bound, since it uses information about the cyclic subcodes.

A lot more can be said about the bound though. But to prove that we first need to introduce some lemmas.

Lemma 5.2.13. *Let A, S be non-empty sets. If A is independent from S, then there is another set B and an element $a \notin S$ such that A is a shift of $B \cup \{a\}$ and B is independent from S, but $B \subset S$.*

Proof. This claim is implied by Definition 5.2.10. The only way to add elements it by item 3, and since A is an arbitrary independent set from S, then an arbitrary shift can have been applied to it as well. □

For the remainder of this subsection when we deal with integers a we implicitly mean $(a)_n$ to avoid overburdening the reader with heavy notation.

Lemma 5.2.14. *Let $S \subseteq \{0, \ldots, n-1\}$ such that $S \neq \emptyset$. Let $w = \hat{R}(n, S)$ and $M = M(w)$. Let v be the first column of M.*

Then for any $0 \leq i \leq n-1$ we have $v[i] = w[n-i]$.

Proof. This is a consequence of Definition 1.0.1. □

Lemma 5.2.15. *Let $T, S \subset \{0, \ldots, n-1\}$ be non-empty sets. Assume $T = \{t_1, \ldots, t_r\}$ and $S = \{s_1, \ldots, s_h\}$. Let $a \notin S$, and let $M = M(\hat{R}(n, S))$ be formed by the rows $M_1, \ldots, M_n$. Let M' be a submatrix of M consisting of the rows $M_{n-a}, M_{n-t_1}, \ldots, M_{n-t_r}$.*

Then the first column of M' is a singleton if and only if $T \subset S$.

Proof. Let $M' = (m'_{i,j})$ and $M = (m_{i,j})$. Let v be the first column of M, v' be the first column of M' and $w = \hat{R}(n, S)$.

We have that $m'_{1,j} = m_{n-a,j}$ for any $0 \leq j \leq n-1$, $m'_{i+1,j} = m_{n-t_i,j}$ for $0 \leq j \leq n-1$ and $0 \leq i \leq r-1$. Thus we also have that $v[0] = v[n-a]$ and $v[i+1] = v[n-t_i]$ for $0 \leq i \leq r-1$.

Since $a \notin S$ then there must be an Δ^+ in the ath entry of w. By Lemma 5.2.14 it holds that $v[0] = w[n-a] = \Delta^+$. Therefore v' is a singleton if and only if $m'_{2,1} = m'_{3,1} = \cdots = m'_{r+1,1} = 0$, i.e. if and only if $m_{n-t_1,1} = m_{n-t_2,1} = \cdots = m_{n-t_r,1} = 0$, which by Lemma 5.2.14 is true if and only if $w[t_1] = w[t_2] = \cdots = w[t_r] = 0$. By Definition 3.0.13 this is true if and only if $t_1, t_2, \ldots, t_r \in S$, i.e. $T \subset S$. □

Lemma 5.2.16. *Let $T \subset S \subset \{0, \ldots, n-1\}$ such that $T, S \neq \emptyset$ and let $a \notin S$. Assume $T = \{t_1, \ldots, t_r\}$. Let $M = M(\hat{R}(n, S))$ be formed by the rows $M_1, \ldots, M_n$. Let M' be a submatrix of M consisting of the rows $M_{n-a}, M_{n-t_1}, \ldots, M_{n-t_r}$.*

Then the singleton independence-check procedure is successful on M' if and only if T is independent from S.

Proof. The claim is proven by induction on $|T|$.

Assume $|T| = 1$. Then $T = \{t_1\}$. By Definition 5.2.10 any such T is independent from S (by applying item 1, 3 and 2 in that order). M' contains two non-zero rows, and by Lemma 5.2.15 then the first column is a singleton. Then it is trivial to realize that the singleton procedure is successful on M'.

Assume $|T| = l + 1$. By Lemma 5.2.15 M' has a singleton. Erasing the singleton and it's corresponding row we obtain a matrix M''. By Lemma 5.2.13 we have that for some I, J then T is a shift of $I = J \cup \{b\}$, where J is independent from S, $J \subset S$ and $b \notin S$. By the induction hypothesis then the independence-check procedure is successful on M''. Since T is obtained

by a shift if I, which means that the zeros of w is shifted accordingly, which implies that the rows of M' (except the corresponding row of the first singleton) is shifted accordingly. All this implies that the columns of M' are cyclic permutations of M'', which means the singleton independence-check procedure is successful on M' if and only if it is on M''. □

Proposition 5.2.17. *Let $C \in \mathcal{C}$ and $\zeta \in Z$. Let S be it's defining set with respect to $\alpha = \zeta(\chi(C), n)$. Let λ be the size of the largest set independent from S. Let $r = \tilde{\epsilon}(M(\hat{R}(n, S)))$. Then*

$$r = \lambda.$$

Proof. This claim holds by Lemma 5.2.16 and Algorithm 5.1.21. □

Lemma 5.2.18.

Proof. If c is contained in the cyclic code D □

Theorem 5.2.19. *The van Lint-Wilson Shifting Bound is a strong border bound.*

The localization of it's strong border function is identical to the second realization of the singleton procedure.

Proof. This is a consequence of Proposition 5.2.17. □

Chapter 6

Final remarks

In this last chapter we will briefly recapitulate some of the major results presented in this paper.

Cyclic codes are a type of codes of great interest, because they are easy to encode (e.g. by using shift registers) and they include famous and important codes like BCH codes and Reed Solomon-codes, which are widely used in practice. This has spawned a lot of research and different bounds has been discovered with different approaches: the BCH-like bounds, the van Lint-Wilson shifting bound, etc.

The defining set of a cyclic code contains a vast amount of information. You can for example construct the generator polynomial of the code from the defining set, which again provides access to a lot of information about the code.

From this point of view it is natural to build a framework for bounds, which solely depends on the defining set and the length of the code. This was called root bounds. This framework was further developed by incorporating the defining sets of cyclic subcodes as well, resulting in border bounds. Obviously border bounds provide better estimations than root bounds, since they contain the same information as the root bounds as well as additional information. The downside is, that the root bounds usually are of polynomial-time complexity, but border bounds are exponential-time complexity.

The framework of root bounds and border bounds presented in this paper has to some extent categorized a range of known bounds into root bounds and border bounds, and several of the known root bounds are shown to be strong root bounds.

It it not surprising that the BCH-like bounds are closely related, but the fact that the Schaub bound and the van Lint-Wilson shifting bound are quite closely related as well is by no means trivial or obvious. Not only are they both border bounds, but they are also shown to share the same independence-check procedure, namely the singleton procedure.

Bibliography

[1] Niels Lauritzen. *Concrete Abstract Algebra.* Cambridge University Press, 2003.

[2] Emanuele Betti & Massimiliano Sala. A theory for distance bounding cyclic codes. `http://www.bcri.ucc.ie/BCRI_63.pdf`.