ON THE ABSOLUTE STATE COMPLEXITY OF ALGEBRAIC GEOMETRIC CODES

by

SALİHA PEHLİVAN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabanci University
Spring 2008

ON THE ABSOLUTE STATE COMPLEXITY OF ALGEBRAIC GEOMETRIC CODES

APPROVED BY

Assist. Prof. Cem Güneri .....
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu .....

Prof. Dr. Henning Stichtenoth .....

Prof. Dr. Albert Kohen Erkip .....

Assoc. Prof. Erkay Savaş .....

DATE OF APPROVAL: June 30, 2008

Aileme...

Acknowledgements

I would like to express my gratitude and deepest regards to my supervisor Assist. Prof. Cem Güneri for his motivation, guidance and encouragement throughout this thesis.

I also would like to thank all my friends for their invaluable friendship and encouragement.

My special thanks to my family for their endless support in every step I take throughout my life.

ON THE ABSOLUTE STATE COMPLEXITY OF ALGEBRAIC GEOMETRIC CODES

Saliha Pehlivan

Mathematics, Master of Science Thesis, 2008

Thesis Supervisor: Assist. Prof. Cem Güneri

Keywords: trellis of a code, absolute state complexity, algebraic geometric code, function field, gonality.

Abstract

A trellis of a code is a labeled directed graph whose paths from the initial to the terminal state correspond to the codewords. The main interest in trellises is due to their applications in the decoding of convolutional and block codes.

The absolute state complexity of a linear code C is defined in terms of the number of vertices in the minimal trellises of all codes in the permutation equivalence class of C. In this thesis, we investigate the absolute state complexity of algebraic geometric codes. We illustrate lower bounds which, together with the well-known Wolf upper bound, give a good idea about the possible values of the absolute state complexities of algebraic geometric codes. A key role in the analysis is played by the gonality sequence of the function field that is used in code construction.

CEBİRSEL GEOMETRİ KODLARININ MUTLAK DURUM KARMASIKLIGI ÜZERİNE

Saliha Pehlivan

Matematik, Yüksek Lisans Tezi, 2008

Tez Danışmanı: Yard. Doç Dr. Cem Güneri

Anahtar Kelimeler: kod kafesi, mutlak durum karmaşıklığı, cebirsel geometri kodu, fonksiyon cismi, gonalite.

Özet

Başlangıç ve bitiş durumları arasındaki yolları bir kodun elemanlarına denk gelen etiketlenmiş yönlü çizgeye o kodun kafesi denir. Kafesler, evrişimli ve blok kodların çözümlemelerindeki uygulamaları sebebiyle ilgi uyandıran konulardır.

Doğrusal bir kodun mutlak durum karmaşıklığı, o kodun permütasyon denklik sınıfındaki tüm kodların minimal kafeslerindeki köşe sayıları cinsinden tanımlanır. Bu tezde cebirsel geometri kodlarının mutlak durum karmaşıklığı araştırılmıştır. İyi bilinen Wolf üst sınırıyla birlikte cebirsel geometri kodlarının mutlak durum karmaşıklığının alabileceği değerleri anlamamıza yarayan alt sınırlar gösterilmiştir. Yapılan analizlerde kod inşasında kullanılan fonksiyon cisminin gonalite dizisi önemli bir rol oynamıştır.

Contents

Acknowledgements **v**

Abstract **vi**

Özet **vii**

1 TRELLIS STATE COMPLEXITY OF LINEAR CODES **1**

1.1 Codes and Trellises 1

1.2 Minimal Proper Trellises 5

1.3 Minimal Trellises For Linear Codes 10

1.4 Absolute State Complexity 14

2 A GOPPA-LIKE BOUND ON THE ABSOLUTE STATE COMPLEXITY OF AG CODES **19**

2.1 Algebraic Geometric Codes 19

2.2 Gonality Sequence of Algebraic Function Fields 20

2.3 A Goppa-like Bound on the ASC of AG Codes 24

2.4 Further Lower Bounds on the ASC of AG Codes 28

3 IMPROVEMENTS FOR A CLASS OF AG CODES **33**

3.1 The Numerical Function $R(N)$ 33

3.2 An Improvement on the ASC of Hermitian Codes 39

Bibliography **44**

List of Figures

1.1 A graph that is a trellis and a graph that is not. 3

1.2 An improper and proper trellises over $\mathbb{F}_2$ which are one-to-one. 3

1.3 An improper trellis for the code $C = \{000, 100, 101, 111\}$ 6

1.4 The minimal proper trellis for the code $C = \{000, 011, 100, 111\}$. 7

1.5 Minimal proper trellis and improper minimal trellis for the same code . 9

1.6 Two nonisomorphic minimal trellises for the code $C = \{00, 10, 11\}$. . . 10

1.7 A minimal BCJR trellis for the code $C = \{0000, 1001, 0110, 1111\}$. . . . 12

1.8 Minimal trellis for [6,3,2] linear code. 15

1.9 Minimal trellis for the permuted binary [6,3,2] linear code 16

List of Tables

2.1 Bounds on $s[C_m]$ for codes on the Hermitian function field where $q = 2, 3, 4, 5, 7, 8$. 32

3.1 Bounds on $s[C_m]$ for Hermitian codes over $\mathbb{F}_{q^2}$ for $q = 2, 3, 4, 5, 7, 8$. . . 43

CHAPTER 1

TRELLIS STATE COMPLEXITY OF LINEAR CODES

This chapter is devoted to the introduction of the main topic of this thesis: trellises. After some basic definitions and properties, we obtain the main (upper) bound on the trellis complexity of codes, namely the Wolf bound. We also show the existence of a minimal trellis for linear codes, which will be frequently used in the following chapters. Our main reference is the chapter of A. Vardy in the Handbook of Coding Theory ([11]).

1.1 Codes and Trellises

In this section, we start with reviewing some basic notions of coding theory. We will then introduce some definitions and concepts from the trellis theory that will be used throughout the thesis.

Let $\mathbb{F}_q$ be a finite field with q elements. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ the *Hamming distance* on $\mathbb{F}_q^n$ is defined as

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

The *weight* of $x \in \mathbb{F}_q^n$ is given by

$$w(x) := | \{i \mid x_i \neq 0\} | = d(x, 0).$$

A *block code* over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ while a *linear code* is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. In the latter case, we call the $k = \dim_{\mathbb{F}_q}(C)$ the *dimension* of the code. An element of a code C is called a *codeword* and the number n is called the *length* of C. The *minimum distance* $d(C)$ of a code C is defined as

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

It is easy to see that the minimum distance of a linear code corresponds to the minimum weight of a nonzero codeword. A linear code of length n, dimension k, and minimum distance d is called an $[n, k, d]$ code.

The *dual code* of C is the code $C^{\perp}$ defined as

$$C^{\perp} := \{x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid \langle x, y \rangle = 0, \ \forall y \in C\}$$

where $\langle x, y \rangle := \sum_{i=1}^{n} x_i y_i$ is the usual inner product on $\mathbb{F}_q^n$

A *generator matrix* of a linear code C is a $k \times n$ matrix whose rows form a basis of C whereas a *parity check matrix* for C is a generator matrix of $C^{\perp}$.

Definition 1.1.1. Let C be an $[n, k, d]$ linear code and i be a positive integer with $1 \leq i \leq k$. We define the *i-th generalized Hamming weight of* C as

$$d_i(C) := \min\{|\ supp(D)\ | \mid \text{D is a subcode of C, } \dim(D) \geq i\}$$

where support of D is defined as

$$supp(D) := \{i \mid \exists (x_1, \ldots, x_n) \in D \ s.t. \ x_i \neq 0\}$$

The sequence $\{d_i(C) : i = 1, \ldots, k\}$ is called the *generalized Hamming weight hierarchy* of C. Note that $d_1(C) = d$.

Proposition 1.1.1. (Singleton Bound). *For an $[n, k, d]$ linear code over $\mathbb{F}_q$ we have*

$$k + d \leq n + 1$$

A code whose parameters satisfy the equality in the above proposition is called an MDS (*maximum distance separable*) code.

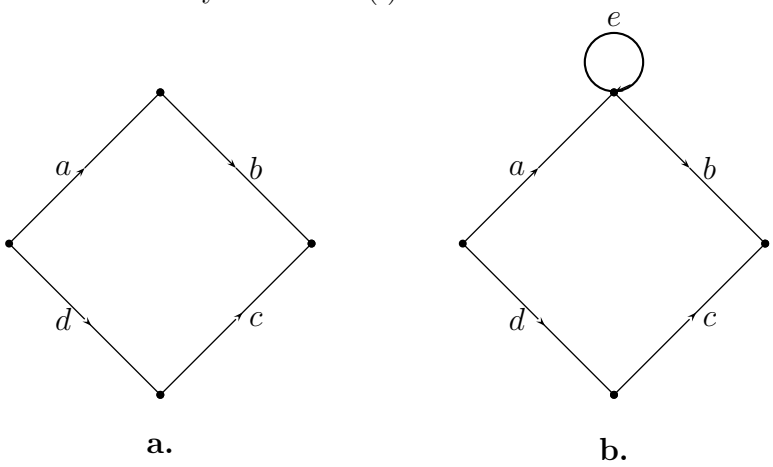
An *edge-labeled directed graph* consists of a set V of *vertices*, a finite set A called the *alphabet*, and a set E of ordered triples (v, v', α) where $v, v' \in V$ and $\alpha \in A$. An element of E is called an *edge* of the graph, and we say that an edge $(v, v', \alpha) \in E$ begins at v, ends at v', and has label α.

Definition 1.1.2. A *trellis* $T = (V, E, A)$ *of depth* n is an edge-labeled directed graph where V is the union of $(n + 1)$ disjoint subsets $V_0, V_1, \ldots, V_n$, such that

(i) every edge in T that begins at a vertex in V_i, ends at a vertex in V_{i+1}

(ii) every vertex in T lies on some path from a vertex in V_0 to a vertex in V_n.

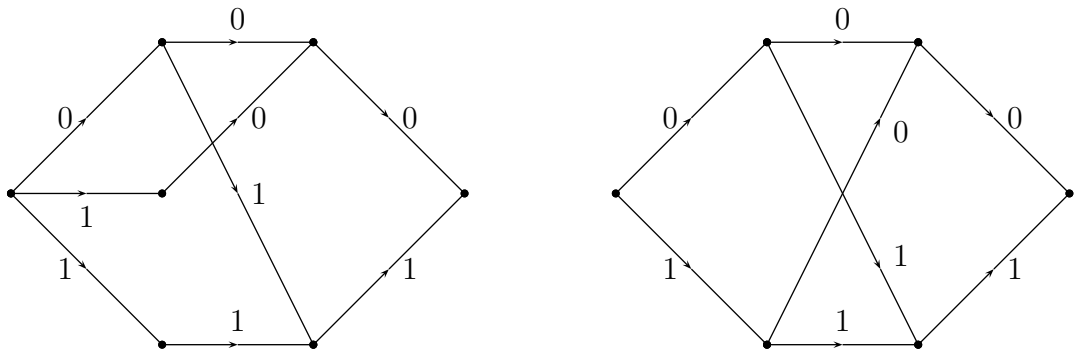
An example of a trellis is shown in Figure 1.1a. The graph in Figure 1.1b is not a trellis since it does not satisfy condition (i) above.



a. **b.**

Figure 1.1: A graph that is a trellis and a graph that is not.

Throughout this thesis, we will assume that V_0 and V_n have single vertex, called the *root* and the *toor*, respectively. The ordered index set $I = \{0, 1, \ldots, n\}$ induced by the partiton of V is called the *time axis* for T. We call V_i the set of vertices at time i. The partition of the vertex set V induces the corresponding partition of edge set E into disjoint n subsets $E_1, \ldots, E_n$ where E_i is the set of edges that end at a vertex in V_i.



a. **b.**

Figure 1.2: An improper and proper trellises over $\mathbb{F}_2$ which are one-to-one.

Definition 1.1.3. Let $T = (V, E, A)$ be a trellis of depth n.

(i) If all paths of length n in a trellis T are labeled distinctly, T is called *one-to-one* (Figure 1.2).

(ii) If the edges beginning at the same vertex of a trellis T are labeled distinctly, T is called *proper* (Figure 1.2b). Otherwise, T is said to be *improper* (Figure 1.2a).

From the above definition we see that the set of one-to-one trellises includes the set of proper trellises, since V_0 has only one element.

Definition 1.1.4. Let $T = (V, E, A)$ be a trellis of depth n. For a path of length n

$$v_0 \stackrel{\alpha_1}{\rightarrow} v_1 \stackrel{\alpha_2}{\rightarrow} \ldots \stackrel{\alpha_n}{\rightarrow} v_n,$$

consider the n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ over A. We say that T *represents* a block code C of length n over A if the set of all paths of length n yields exactly the set of codewords of C.

Two trellises $T = (V, E, A)$ and $T' = (V', E', A)$ are said to be *isomorphic* if there is a one-to-one correspondence ψ from V to V' such that $\psi(V_i) = V_i'$ (for all i), and (v, v', α) is an edge in E if and only if $(\psi(v), \psi(v'), \alpha)$ is an edge in E'. Note that isomorphic trellises represent the same code.

It is obvious that every trellis T represents a unique code. On the other hand, there can be many nonisomorphic trellises for the same code. A natural question is given any two nonisomorphic trellises for C which one is 'better'? The answer to this question should be 'whichever yields a simpler trellis representation for C'. To measure simplicity, we can define several trellis complexity measures and prefer the trellis that minimizes these complexity measures.

Let C be a block code of length n over the finite field $\mathbb{F}_q$, and $T = (V, E, \mathbb{F}_q)$ be a trellis of length n that represents C. We define the following complexity measures for T:

$$\textit{state cardinality profile}: \quad \text{the ordered sequence } |V_0|, |V_1|, \ldots, |V_n| \tag{1.1}$$

$$\textit{maximum number of states}: \quad S_{max} = \max\{|V_0|, |V_1|, \ldots, |V_n|\} \tag{1.2}$$

In section 3, we will see that if C is a linear code over $\mathbb{F}_q$ and T is 'the minimal trellis' for C, the cardinality of V_i is a power of q. Then complexity measures of T are

$$\textit{state complexity profile}: \quad \text{the ordered sequence } s_0, s_0, \ldots, s_n \tag{1.3}$$

$$\textit{state complexity} \ : \ \ s = \max\{s_0, s_0, \ldots, s_n\} \tag{1.4}$$

where $s_i = \log_q |V_i|$.

We can define similar complexity measures based on the number of edges in the trellis. However, such complexity measures are closely related to the state complexity s in (1.4) and a trellis that minimizes one complexity measure often minimizes other measures too. Since a state complexity is more common to study, we will just concantrate on this.

To minimize the state complexity of a trellis for any given block code C, we need to construct a simple trellis representing the code C. This leads to the notion of *minimal* trellises.

1.2 Minimal Proper Trellises

Now, we start by defining the minimal proper trellis and proceed by constructing such a trellis for any block code.

Definition 1.2.1. Let T be a proper trellis for a code C of length n. If any proper trellis T' for C satisfies $|V_i| \leq |V_i'|$ for each $i = 0, 1, \ldots, n$, then we say that T is a *minimal proper trellis* for C.

T is said to be a *minimal trellis* for C if T is a trellis that minimizes the number of vertices at each time i among all possible (not just among proper) trellis representations for C.

Theorem 1.2.1. *Every block code has a minimal proper trellis which is unique up to isomorphism.*

This theorem will be proved via three propositions (Propositions 1.2.1, 1.2.2, and 1.2.3). For this purpose, we proceed by defining two equivalence relations one of which is defined by a proper trellis T for C and the other is defined by the code C itself. To introduce these equivalence relations, we will give the following definitions.

Definition 1.2.2. Let C be a code of length n over a finite alphabet A. The codes $\mathcal{P}_i^*$ and $\mathcal{F}_i^*$, known as the *projection of C on the past,* respectively*, future* at time i, are defined as

$$\mathcal{P}_i^* = \{(c_1, c_2, \ldots, c_i) : \ (c_1, c_2, \ldots, c_i, c_{i+1}, \ldots, c_n) \in C\} \tag{1.5}$$

$$\mathcal{F}_i^* = \{(c_{i+1}, c_{i+2}, \ldots, c_n) : \ (c_1, c_2, \ldots, c_i, c_{i+1}, \ldots, c_n) \in C\}. \tag{1.6}$$

We have $\mathcal{P}_n^* = \mathcal{F}_0^* = C$ and $\mathcal{P}_0^* = \mathcal{F}_n^* = \emptyset$.

T-equivalence relation. Let T be a proper trellis for a code C of length n. Given a codeword $c \in \mathcal{P}_i^*$ and a path $P = e_1, e_2, \ldots, e_i$ beginning at the root of T, we say that P *corresponds* to c if $c = (\alpha(e_1), \alpha(e_2), \ldots, \alpha(e_i))$ where $\alpha(e_i)$ denotes the label of edge e_i. Note that T is proper only if the correspondence between paths of length i in T and codewords in $\mathcal{P}_i^*$ is one-to-one for all $i = 1, \ldots, n$. Let c and c' be any two codewords in $\mathcal{P}_i^*$. If the paths P_c and $P_{c'}$ corresponding to these codewords end at the same vertex in V_i, we say that c and c' are *T-equivalent* and denote it by $c \sim_T c'$. From the definition, we can say that the number of T-equivalence classes in $\mathcal{P}_i^*$ equals to the number of vertices at time i in T.

Remark 1.2.1. If T is not proper, the relation defined above may not be an equivalance relation since transitivity may fail. For example, in the improper trellis in Figure 1.3, we have $00 \sim_T 10$, $10 \sim_T 11$, but, $00 \nsim_T 11$.

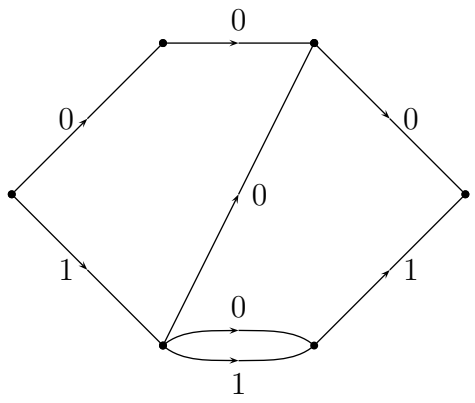


Figure 1.3: An improper trellis for the code $C = \{000, 100, 101, 111\}$

Future equivalance relation. For each $c \in \mathcal{P}_i^*$, we define the *future* of c in C as the set

$$F(c) := \{x \in A^{n-i} : (c, x) \in C\}.$$

Let c and c' be any two codewords in $\mathcal{P}_i^*$. We say that c and c' are *future-equivalent* if $F(c) = F(c')$ and denote it by $c \sim c'$.

Proposition 1.2.1. Let T be a proper trellis for C and let $c, c' \in \mathcal{P}_i^*$. If $c \sim_T c'$, then $c \sim c'$.

Proof. Since T is a proper trellis for C, there is exactly one path of length i that corresponds to each of c and c' in T. Since these codewords end at the same vertex v in V_i, futures of c and c' correspond to the paths of length $n-i$ from v. □

It follows from Prop 1.2.1 that the number of future equivalence classes in $\mathcal{P}_i^*$ is less than or equal to the number of T-equivalence classes in $\mathcal{P}_i^*$. Since the latter number is equal to $|V_i|$, we have

$$|V_i^*| \leq |V_i|, \text{ for all } i = 1, 2, \ldots, n, \tag{1.7}$$

where $|V_i^*|$ denotes the number of future equivalence classes in $\mathcal{P}_i^*$. Recall that the future equivalence relation is independent of the proper trellis representing the code C. Hence, we consider a trellis $T^* = (V^*, E^*, A)$ for C whose vertices in V_i^* are in one-to-one correspondence with the future equivalence classes in $\mathcal{P}_i^*$ (for all i). Note that $|V_0^*| = |V_n^*| = 1$ since $\mathcal{P}_0^* = \emptyset$ and $\mathcal{P}_n^* = C$. Let $v \in V_i^*$ and $v' \in V_{i+1}^*$ be two vertices of T^*. Then v and v' are connected by an edge (in E_{i+1}^*) if and only if v and v' correspond to the classes $(c_1, c_2, \ldots, c_i) \in \mathcal{P}_i^*$ and $(c_1, c_2, \ldots, c_{i+1}) \in \mathcal{P}_{i+1}^*$. In this case, the label of the edge joining v to v' is c_{i+1}.

Example 1.2.1. Consider the binary linear code $C = \{000, 011, 100, 111\}$ together with its proper trellis representation in Figure 1.2b. Future equivalence classes for C at time $i = 1, 2$ are

$$\begin{aligned} F(0) = \{00, 11\} = F(1) &\Rightarrow 0 \sim 1 \; in \; \mathcal{P}_1^* \\ F(00) = \{0\} = F(10) &\Rightarrow 00 \sim 10 \; in \; \mathcal{P}_2^* \\ F(01) = \{0\} = F(11) &\Rightarrow 01 \sim 11 \; in \; \mathcal{P}_2^* \end{aligned}$$

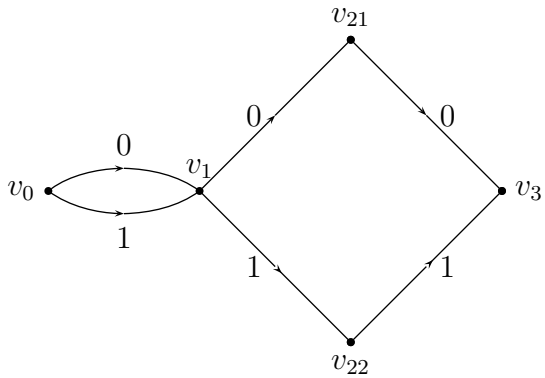


Figure 1.4: The minimal proper trellis for the code $C = \{000, 011, 100, 111\}$.

Then we have

$$V_1^* = \{\{0,1\}\} = \{v_1\}$$

$$V_2^* = \{\{00,10\},\{01,11\}\} = \{v_{21}, v_{22}\}.$$

The correspondng minimal proper trellis for C is shown in Figure 1.4.

Proposition 1.2.2. *T^* is a minimal proper trellis for C.*

Proof. Minimality of T^* follows from (1.7). So, we need to show that T^* is proper and represents C. Let $e_1 = (v, v', \alpha)$ and $e_2 = (v, v'', \alpha)$ be two edges in T^* from $v \in V_i^*$ with the same label. Then there are codewords $c = (c_1, c_2, \ldots, c_i, \alpha, \ldots)$, $d = (d_1, d_2, \ldots, d_i, \alpha, \ldots) \in C$ with $(c_1, c_2, \ldots, c_i) \in v$, $(d_1, d_2, \ldots, d_i) \in v$, $(c_1, c_2, \ldots, c_i, \alpha) \in v'$, and $(d_1, d_2, \ldots, d_i, \alpha) \in v''$. Since

$$(c_1, c_2, \ldots, c_i) \sim (d_1, d_2, \ldots, d_i)$$

it follows from the construction of T^* that

$$(c_1, c_2, \ldots, c_i, \alpha) \sim (d_1, d_2, \ldots, d_i, \alpha)$$

Therefore $v' = v''$.

It remains to show that T^* represents C. Since we used the codewords of C to define the edges of T^*, it is clear that C is contained in the trellis code of T^*. To prove that the code corresponding to T^* is contained in C, we show by induction on i that every path of length i starting at the root of T^* corresponds to a codeword of $\mathcal{P}_i^*$. For $i = 0$, the statement is trivial. Assume that the statement is true for $i = k$ and we are given a path of length $k+1$, $P = e_1, e_2, \ldots, e_{k+1}$, that begins at the root of T^* and $e_{k+1} = (v, v', \alpha)$. By induction there is a codeword $c \in C$, such that $(c_1, c_2, \ldots, c_k) \in \mathcal{P}_k^*$ corresponds to the first k edges of the path. From the construction of T^*, there is a codeword $d \in C$ such that $(d_1, d_2, \ldots, d_k) \in v$, $(d_1, d_2, \ldots, d_k, d_{k+1}) \in v'$ and $\alpha(e_{k+1}) = \alpha$. Since $(c_1, c_2, \ldots, c_k)$ and $(d_1, d_2, \ldots, d_k)$ end at the same vertex, they have the same future. Then, $(c_1, c_2, \ldots, c_k, d_{k+1}, \ldots, d_n) \in C$. It follows that $(c_1, c_2, \ldots, c_k, \alpha)$ is a codeword of $\mathcal{P}_{k+1}^*$. □

Proposition 1.2.3. *Any minimal proper trellis for C is isomorphic to T^*.*

Proof. Let T be a minimal proper trellis for C, and $c \in \mathcal{P}_i^*$. Let $v(c)$ be the T-equivalence class of c, and $v'(c)$ be the T^*-equivalence class of c, which is also future-equivalence class of c. By Proposition 1.2.1, $v(c) \subseteq v^*(c)$ for any $c \in \mathcal{P}_i^*$. Since T is minimal, it does not have more equivalence classes than T^*. Thus, $v(c) = v^*(c)$. This leads to a one-to-one correspondence between V_i and V_i^*. For any $v \in V_i$, choose a codeword $c \in v$, and let $\psi(v) = v^*(c)$ where $v^*(c) \in V_i^*$.

If $v \in V_i$ and (v, v', α) is an edge in T, there exists a codeword $c \in C$ whose path includes α. From the construction of T^*, $((c_1, c_2, \ldots, c_i), (c_1, c_2, \ldots, c_{i+1}), \alpha)$ is an edge of T^*, which is $(\psi(v), \psi(v'), \alpha)$. On the other hand, if

$$((c_1, c_2, \ldots, c_i), (c_1, c_2, \ldots, c_{i+1}), \alpha)$$

is an edge of T^*, there must be an edge $(v(c_1, c_2, \ldots, c_i), v'(c_1, c_2, \ldots, c_{i+1}), \alpha)$ in T; otherwise the codeword c would not be in the trellis code of T. Therefore, ψ is an isomorphism between T and T^*.

□

Remark 1.2.2. The minimal proper trellis for C may not be minimum over all trellises of C. Consider the nonlinear code $C = \{000, 100, 101, 111\}$ whose minimal proper trellis is shown in Figure 1.6a. Note that the improper trellis in Figure 1.6b for the same code has less vertices at time 2.

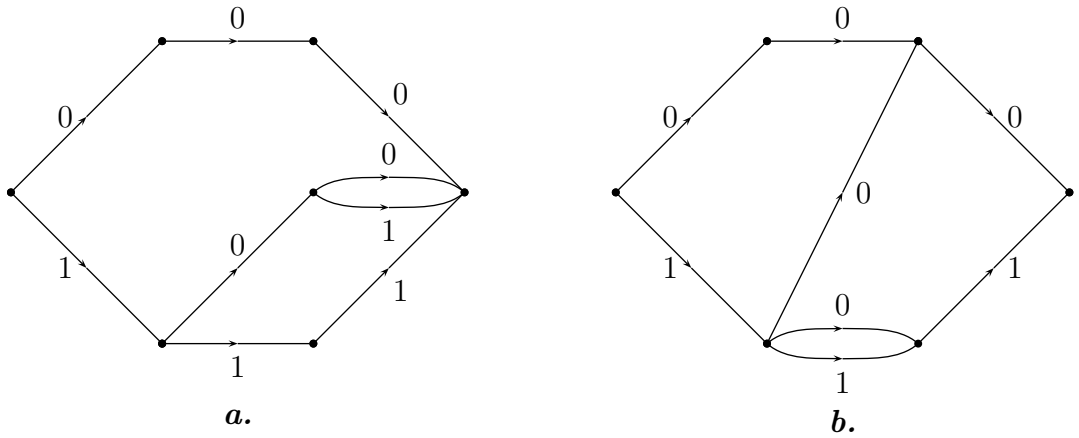


Figure 1.5: Minimal proper trellis and improper minimal trellis for the same code

.

Remark 1.2.3. The minimal trellis for C may not be unique like the minimal proper trellis. Consider the nonlinear code $C = \{00, 10, 11\}$. As we can see in Figure 1.6, the code has two nonisomorphic minimal trellis representations for C.

A natural question one might ask is when is the minimal proper trellis a minimal trellis for C. We will address this question in the following section.

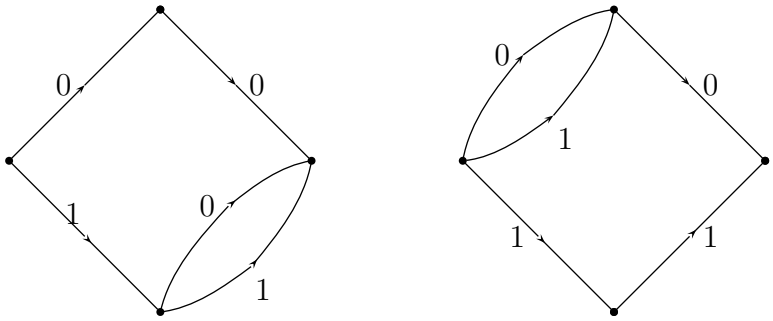


Figure 1.6: Two nonisomorphic minimal trellises for the code $C = \{00, 10, 11\}$.

1.3 Minimal Trellises For Linear Codes

There are alternative ways to construct minimal trellises for linear codes. In this section, we will introduce two of these methods which are commonly used.

Proposition 1.3.1. *If C is a linear code, then a minimal proper trellis for C is also a minimal trellis for C. Furthermore, any minimal trellis for C is proper.*

Proof. Let c be a codeword in C and H be a parity check matrix of C. Note that an $(n-i)$-tuple $(x_{i+1}, \ldots, x_n)$ is a tail of $(c_1, \ldots, c_i) \in \mathcal{P}_i^*$ if and only if

$$(c_1, \ldots, c_i, 0, \ldots, 0)H = -(0, \ldots, 0, x_{i+1}, \ldots, x_n)H.$$

Hence, two codewords $(c_1, \ldots, c_i)$ and $(d_1, \ldots, d_i) \in \mathcal{P}_i^*$ have a common tail if and only if

$$(c_1, \ldots, c_i, 0, \ldots, 0)H = (d_1, \ldots, d_i, 0, \ldots, 0)H.$$

In this case they have same futures, i.e. $(c_1, \ldots, c_i) \sim (d_1, \ldots, d_i)$. From this argument, we see that if T is any trellis for C, and any two codewords in $\mathcal{P}_i^*$end at the same vertex at time i, then their futures are equal. Moreover, such codewords end at the same vertex in T^* at time i. Hence, T^* does not have more vertices for each time $i = 1, \ldots, n$ than T does, i.e., a minimal proper trellis is a minimal trellis for C. In the above argument if we let T be a proper trellis for C, then we conclude that any minimal trellis for C must be proper.

□

Bahl-Cocke-Jelinek-Raviv construction (BCJR). Let C be a code of length n over $\mathbb{F}_q$. Let $H = [h_1, h_2, \ldots, h_n]$ be a parity check matrix for C, where $h_1, h_2, \ldots, h_n$ are the columns of H. Vertices of BCJR trellis at time i are defined by

$$V_i = \{c_1h_1 + c_2h_2 + \cdots + c_ih_i : (c_1, \ldots, c_i) \in \mathcal{P}_i^*\} \tag{1.8}$$

with $V_0 = \{\mathbf{0}\} = V_n$. There is an edge $e = (v, v', \alpha)$ in $T = (V, E, \mathbb{F}_q)$ with $v \in V_i$ and $v' \in V_{i+1}$ if and only if there is a codeword $c \in C$ such that

$$\begin{aligned} c_1h_1 + c_2h_2 + \cdots + c_ih_i &= v, \\ c_1h_1 + \cdots + c_ih_i + c_{i+1}h_{i+1} &= v', \\ \alpha &= c_{i+1}. \end{aligned}$$

Note that the vertex set at time i is a linear space for all i. Thus, V_i is the image of C under the linear mapping $\sigma_i : C \to V_i$ defined by

$$\sigma_i(c) = c_1h_1 + c_2h_2 \cdots + c_ih_i \tag{1.9}$$

with $c = (c_1, c_2, \ldots, c_n)$, while the edge set E_i, which is also a linear space for all i, is the image of C under the linear mapping τ_i defined by

$$\tau_i(c) = (\sigma_i(c), \sigma_{i+1}(c), c_{i+1}). \tag{1.10}$$

We denote the dimensions of the vertex space V_i and the edge space E_i by

$$\begin{aligned} s_i &= \dim V_i = \log_q |V_i|, \quad \text{for } i = 0, 1, \ldots, n \\ b_i &= \dim E_i = \log_q |E_i|, \quad \text{for } i = 1, 2, \ldots, n. \end{aligned}$$

Remark 1.3.1. Note that V_i is the row space of $G_iH_i^T$ i.e., $s_i = \text{rank}(\ G_iH_i^T)$, where G_i and H_i are the matrices that consist of the first i columns of G and H, respectively.

Example 1.3.1. Consider the self-dual (i.e. $C = C^\perp$) binary linear code C defined by the following generator and parity-check matrices:

$$G = H = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Then we know by the BCJR construction that $V_0 = V_4 = \{\mathbf{0}\}$ while V_1, V_2, V_3 can be, respectively, represented as the row-spaces of the following matrices:

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

In other words,

$$V_1 = \big\{(0,0),(0,1)\big\} = \{v_{11}, v_{12}\},$$
$$V_2 = \big\{(0,0),(1,0),(0,1),(1,1)\big\} = \{v_{21}, v_{22}, v_{23}, v_{24}\},$$
$$V_3 = \big\{(0,0),(0,1)\big\} = \{v_{31}, v_{32}\}$$

The state complexity profile of T is given by $\{s_0, s_1, s_2, s_3, s_4\} = \{0, 1, 2, 1, 0\}$ and the resulting BCJR trellis is shown in Figure 1.7.

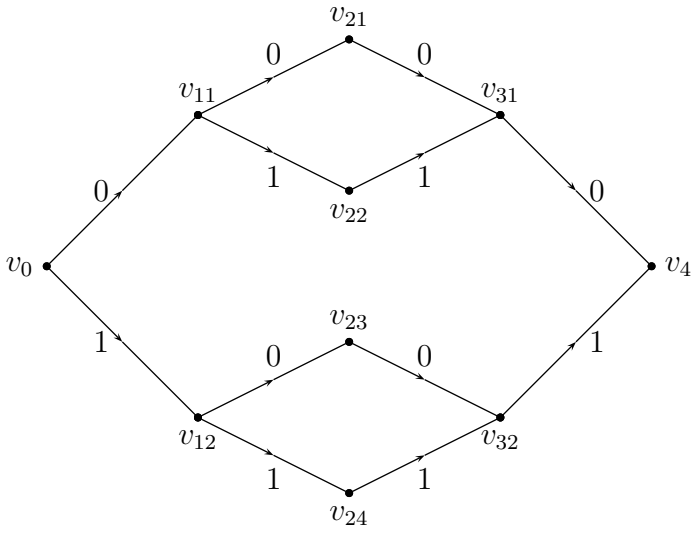


Figure 1.7: A minimal BCJR trellis for the code $C = \{0000, 1001, 0110, 1111\}$.

Proposition 1.3.2. *BCJR trellis $T = (V, E, \mathbb{F}_q)$ represents the linear code C.*

Proof. Since codewords of C define the edge set of T, every codeword corresponds to a path of length n in T. We have to show that every path of length n produces a codeword. For any path $e_1, \ldots, e_n$ of length n, we have $0 = v_n = \alpha(e_1)h_1 + \cdots + \alpha(e_n)h_n$. Hence, $(\alpha(e_1), \ldots, \alpha(e_n)) \in C$. □

Theorem 1.3.1. *The BCJR construction produces a minimal trellis.*

Proof. Let T be any trellis and T^* be a minimal trellis for C. We know from the proof of Proposition 1.3.1 that if any two codewords c and c' in $\mathcal{P}_i^*$ end at the same vertex at time i in T, then they have common futures. To establish the minimality of BCJR trellis, it is enough to show that if two codewords of $\mathcal{P}_i^*$ are future equivalent then

they end at the same vertex at time i in T. Let $c, c' \in \mathcal{P}_i^*$ be future equivalent and let $x = (x_{i+1}, \ldots, x_n)$ be a common tail of c and c'. Then $(c, x)H^T = (c', x)H^T = \mathbf{0}$. This implies that

$$c_1h_1 + \cdots + c_ih_i = -x_{i+1}h_{i+1} + \cdots + x_nh_n = c'_1h_1 + \cdots + c'_ih_i.$$

Then, from the definition of V_i, we say that the paths in T corresponding to c and c' end at the same vertex at time i.

□

By Propositions 1.2.3, 1.3.1 and 1.3.2, and Theorem 1.3.1, we obtain the following.

Theorem 1.3.2. *Every linear code has a minimal trellis which is unique up to isomorphism.*

Forney construction. Let C be a code of length n over $\mathbb{F}_q$. We define the *past* and, respectively, *future* subcodes of C as

$$\mathcal{P}_i = \{(c_1, \ldots, c_i) : \ (c_1, \ldots, c_i, 0 \ldots, 0) \in C\} \subseteq \mathbb{F}_q^i \tag{1.11}$$

$$\mathcal{F}_i = \{(c_{i+1}, \ldots, c_n) : \ (0 \ldots, 0, c_{i+1}, \ldots, c_n,) \in C\} \subseteq \mathbb{F}_q^{n-i} \tag{1.12}$$

with $\mathcal{P}_n = \mathcal{F}_0 = C$ and $\mathcal{P}_0 = \mathcal{F}_n = \{\mathbf{0}\}$. Clearly, the direct sum $\mathcal{P}_i \oplus \mathcal{F}_i$ is a linear subcode of C. The Forney trellis $T = (V, E, \mathbb{F}_q)$ for C is constructed by identifying the vertices in V_i with the cosets of $\mathcal{P}_i \oplus \mathcal{F}_i$ in C, that is,

$$V_i := C/\mathcal{P}_i \oplus \mathcal{F}_i \tag{1.13}$$

for $i = 0, 1, \ldots, n$. We have $\mathcal{P}_0 \oplus \mathcal{F}_0 = \mathcal{P}_n \oplus \mathcal{F}_n = C$ so that V_0 and V_n consist of a single coset. There is an edge $e = (v, v', \alpha)$ in $T = (V, E, \mathbb{F}_q)$ from $v \in V_i$ to $v' \in V_{i+1}$ if and only if there is a codeword $c \in C$ such that c lies in the intersection of the cosets of v and v' and whose $(i+1)$st coordinate is α.

Theorem 1.3.3. *Forney construction produces a minimal trellis.*

Proof. Let H be a parity check matrix for C and let $c \in C$. Consider the mapping σ_i in (1.9). Then, $c \in \mathcal{P}_i \oplus \mathcal{F}_i$, with $(c_1, \ldots, c_i, 0, \ldots, 0) \in \mathcal{P}_i$ and $(0, \ldots, 0, c_{i+1}, \ldots, c_n) \in \mathcal{F}_i$, if and only if $\sigma_i(c) = \mathbf{0}$. This shows that $\mathcal{P}_i \oplus \mathcal{F}_i$ is the kernel of σ_i. Thus,

$$\dim \sigma_i(C) = \dim C - \dim(\mathcal{P}_i \oplus \mathcal{F}_i).$$

Hence, the number of vertices in the BCJR trellis is equal to the number of vertices in the Forney trellis for each time. Then, the Forney trellis is minimal since the BCJR trellis is so. □

Example 1.3.2. Consider again the linear code C of Example 1.3.1. The past subcodes of C are $\mathcal{P}_0 = \mathcal{P}_1 = \mathcal{P}_2 = \{\mathbf{0}\}$, $\mathcal{P}_3 = \{\mathbf{0}, 011\}$, and $\mathcal{P}_4 = C$ whereas the future subcodes of C are $\mathcal{F}_0 = C$, $\mathcal{F}_1 = \{\mathbf{0}, 110\}$, and $\mathcal{F}_2 = \mathcal{F}_3 = \mathcal{F}_4 = \{\mathbf{0}\}$. Thus the direct sum subcodes are

$$\mathcal{P}_1 \oplus \mathcal{F}_1 = \{0000, 0110\},$$
$$\mathcal{P}_2 \oplus \mathcal{F}_2 = \{0000\},$$
$$\mathcal{P}_3 \oplus \mathcal{F}_3 = \{0000, 0110\}.$$

Then, $C/(\mathcal{P}_i \oplus \mathcal{F}_i)$ are

$$V_1 = \big\{\{0000, 0110\}, \{1001, 1111\}\big\} = \{v_{11}, v_{12}\},$$
$$V_2 = \big\{\{0000\}, \{0110\}, \{1001\}, \{1111\}\big\} = \{v_{21}, v_{22}, v_{23}, v_{24}\},$$
$$V_3 = \big\{\{0000, 0110\}, \{1001, 1111\}\big\} = \{v_{31}, v_{32}\}.$$

The resulting Forney trellis, which is identical to the BCJR trellis, is shown in Figure 1.7.

1.4 Absolute State Complexity

We start by defining the notion of permutation equivalence for codes. Two codes are said to be **permutation equivalent**, if one of them is obtained by permuting the coordinates in the other. In coding theory, permutation equivalent codes are viewed as essentially the same. However, the following example shows that two permutation equivalent codes can have significantly different minimal trellis representations.

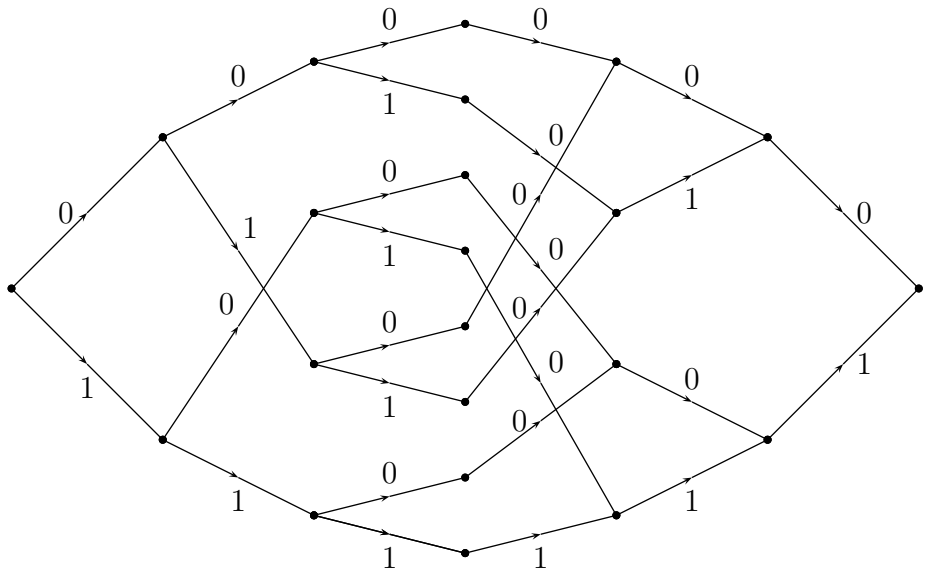


Figure 1.8: Minimal trellis for [6,3,2] linear code.

Example 1.4.1. Consider the binary $[6, 3, 2]$ linear code C, generated by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

A minimal trellis for C is shown in Figure 1.8. Now, permute the time axis of the minimal trellis for C with the permutation $\pi = (2, 3, 6)$. The resulting code C' is generated by the following matrix,

$$G' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

The corresponding minimal trellis is shown in Figure 1.9.

Motivated by this example, we introduce the following notions of state complexity for codes. Let C be a linear code of length n over $\mathbb{F}_q$. If T is a trellis representation of C, recall that we defined the state complexity of T as

$$s_T(C) := \max\{s_0, \ldots, s_n\}$$

where $s_i(T) = \log_q |V_i|$ for all i. If T^* is a minimal trellis for C, then we define the *state complexity of the code* C as $s(C) := s_{T^*}(C)$. As seen in Example 1.4.1, $s(C)$ may change if one considers permutation equivalent codes to C. Let us denote by $[C]$ the set of codes that are permutation equivalent to C. Then we define the *absolute state complexity of* C as

$$s[C] := \min\{s(C') : C' \in [C]\}.$$

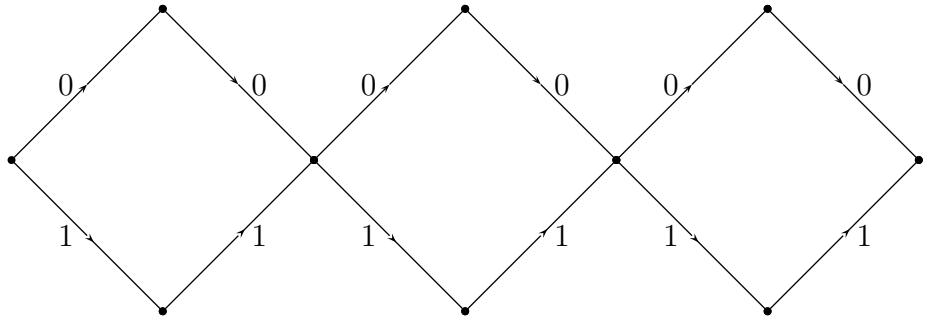


Figure 1.9: Minimal trellis for the permuted binary [6,3,2] linear code .

From now on, we will be interested in the absolute state complexity of linear codes. Our intent in the rest of this chapter is to estimate the state and absolute state complexities of linear codes. Let us start with a simple fact.

Proposition 1.4.1. *The minimal trellis $T = (V, E, \mathbb{F}_q)$ for a linear code C of length n and the minimal trellis $T^\perp = (V^\perp, E^\perp, \mathbb{F}_q)$ for its dual code $C^\perp$ have identical state complexities.*

Proof. Let G and H denote the generator and parity check matrices of C, respectively. By Remark 1.3.1, we know that $\dim(V_i)$ is equal to the rank of $G_i H_i^T$. Similarly, we have $\dim(V_i^\perp)$ =rank$(H_i G_i^T)$ for the dual trellis. Then, the two dimensions are clearly the same. □

For a linear $[n, k, d]$ code C over $\mathbb{F}_q$, we denote the dimensions of the past and future subcodes (cf. (1.11) and (1.12)) of C by $p_i = dim\mathcal{P}_i$ and $f_i = dim\mathcal{F}_i$. It is clear that the sequence $p_1, \ldots, p_n$ is nondecreasing while the sequence $f_1, \ldots, f_n$ is nonincreasing. From the Forney construction (cf. (1.13)), we have

$$s_i(C) = k - \triangle_i(C),$$

where $\triangle_i = \triangle_i(C) := p_i + f_i,$ for each $i = 0, 1, \ldots, n$. Hence, the state complexity of the code is

$$s(C) = k - \triangle(C),$$

where $\triangle = \triangle(C) :=\min\{\triangle_0, \triangle_1, \ldots, \triangle_n\}$. Let us also define $\triangle[C] :=\max\{\triangle(C') : C' \in [C]\}$.

Remark 1.4.1. By definition of the minimum distance d of C, we have

(i) $\mathcal{P}_i = \{\mathbf{0}\}$ for $0 \leq i \leq d-1$. In particular, $\min\{\triangle_0, \ldots, \triangle_{d-1}\} = \triangle_{d-1}$.

(ii) $\mathcal{F}_i = \{\mathbf{0}\}$ for $n-d+1 \leq i \leq n$. In particular $\min\{\triangle_{n-d+1}, \ldots, \triangle_n\} = \triangle_{n-d+1}$.

Proposition 1.4.2. *For a linear [n,k,d] code C, we have*

$$s(C) = \begin{cases} k & \text{if } 2d \geq n+2 \\ k - \min\{\triangle_{d-1}, \ldots, \triangle_{n-d+1}\} & \text{otherwise} \end{cases}$$

Proof. If $2d \geq n+2$, then there exists an integer i such that $n-d+1 \leq i \leq d-1$. Then the result follows from Remark 1.4.1. □

Theorem 1.4.1. (Wolf bound) *Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. Then the state complexity of C is upper bounded by*

$$s(C) \leq w(C) := \min(k, n-k).$$

Proof. We know that $s_i(C) = k - \triangle_i(C) \leq k$ for all i so that $s(C) \leq k$. Since C and $C^\perp$ have identical state complexities, $s_i(C) = s_i^\perp(C) \leq n-k$, which implies that $s(C) \leq n-k$. Then the result follows. □

The Wolf bound holds for any permutation of the time axis of the minimal trellis for an $[n, k, d]$ linear code C, i.e., $s[C] \leq w(C)$.

We will finish this chapter with two crucial propositions, due to Munuera and Torres, that reduce the estimation of the absolute state complexity to estimations at weights of a code. These two results will play key roles in Chapters 2 and 3.

Proposition 1.4.3. *Let t be a non-negative integer. Then $s[C] \geq w(C) - t$ if either $2d \geq n+2-t$, or $2d^\perp \geq n+2-t$.*

Proof. We know that $\mathcal{P}_{d-1} = \{\mathbf{0}\}$. Now, let us assume that $2d \geq n + 2 - t$. If $\mathcal{F}_{d-1} = \{\mathbf{0}\}$, then $s_{d-1}(C) = k$ which implies that $s(C) \geq s_{d-1}(C) = k$. On the other hand, if $\mathcal{F}_{d-1} \neq \{\mathbf{0}\}$, then $\mathcal{F}_{d-1}$ is a subcode of C of length $(n-d+1)$ whose minimum distance is at least d. From the Singleton bound, we get

$$f_{d-1} \leq n_{\mathcal{F}_{d-1}} - d_{\mathcal{F}_{d-1}} + 1 \leq (n - d + 1) - d + 1 = n - 2d + 2 \leq t.$$

Thus, $s(C) \geq s_{d-1}(C) \geq k - t$.

If we assume that $2d^{\perp} \geq n + 2 - t$ and if we apply the above argument to the dual code of C, then we obtain $s(C^{\perp}) \geq n - k - t$. From Proposition 1.4.1 and the Wolf bound, we conclude that $s(C) \geq w(C) - t$. Since the dimension and the length of C do not depend on the coordinate permutation, $s[C] \geq w(C) - t$. □

Remark 1.4.2. For an MDS code, if $n \geq 2k$ then we get $2d = 2n + 2 - 2k \geq n + 2$. Otherwise, we have $2d^{\perp} = 2k + 2 \geq n + 2$ (we used the fact that the dual of an MDS code is also MDS). Thus it always holds that $\max(2d, 2d^{\perp}) \geq n + 2$ for MDS codes. This implies, with Proposition 1.4.2, the well known result that MDS codes attain the Wolf bound.

Proposition 1.4.4. *Let i be a positive integer with $1 \leq i \leq k$. Then $s[C] \geq w(C) - i + 1$ provided that either $d_i(C) \geq n + 2 - d$ or $d_i(C^{\perp}) \geq n + 2 - d^{\perp}$ where $d_i(C)$ is the ith generalized Hamming weight.*

Proof. Assume that $d_i(C) \geq n + 2 - d$. Since $\mathcal{F}_{d-1}$ has length $n - d + 1$, we have $|Supp(\mathcal{F}_{d-1})| \leq n - d + 1$. Then $|Supp(\mathcal{F}_{d-1})| < d_i(C)$ by the assumption. From the definition of $d_i(C)$, $f_{d-1} < i$ so that $s(C) \geq s_{d-1}(C) \geq k - i + 1$. If $d_i(C^{\perp}) \geq n + 2 - d^{\perp}$, by applying a similar argument to $C^{\perp}$, we obtain $s(C^{\perp}) \geq n - k - i + 1$. Therefore, $s(C) \geq w(C) - i + 1$. Noting that the lower bound does not depend on the coordinate permutation of C, the result follows. □

CHAPTER 2

A GOPPA-LIKE BOUND ON THE ABSOLUTE STATE COMPLEXITY OF AG CODES

In this chapter we investigate the absolute state complexity (ASC) of algebraic geometric (AG) codes. In the previous chapter we proved a general upper bound on ASC of linear codes (Wolf bound). Here, we will obtain lower bounds for the ASC of AG codes. A major role will be played by the gonality sequence of a function field which is used in the construction of the code. Our main reference in this chapter is an article of Munuera and Tores [5]. However, we state and prove some of their results in a different form since it is not clear whether some results of [5] are completely correct or not (cf. Propositions 2.3.1, 2.3.2, Theorem 2.3.1 and Corollaries 2.3.1, 2.3.2). When the so-called abundance of the code and its dual are the same, our statements match theirs.

For an introduction to AG codes, we refer to Stichtenoth's book [10].

2.1 Algebraic Geometric Codes

Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and $P_1, P_2 \ldots, P_n$ be a set of pairwise distinct rational places of F/K. Let D and G be divisors of F/K such that $D = P_1 + P_2 + \cdots + P_n$ and the supports of G and D are disjoint. For a divisor A of F/K, we define the vector space $\mathcal{L}(A)$ as

$$\mathcal{L}(A) := \{f \in F \mid (f) + A \geq 0\} \cup \{0\}$$

where (f) is the principal divisor of f. We denote the degree and the dimension of $\mathcal{L}(A)$ over K by $\deg A$ and $\ell(A)$, respectively. The *algebraic geometric (AG) code* $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is the image of the following $\mathbb{F}_q$-linear map

$$\begin{aligned} \phi : \mathcal{L}(G) &\rightarrow \mathbb{F}_q^n & (2.1) \\ f &\mapsto (f(P_1), f(P_2), \ldots, f(P_n)). & (2.2) \end{aligned}$$

Let us note that the dual code is also an AG code. Namely, $C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D,H)$, where $H = W - (G - D)$ for some canonical divisor W.

The code $C_{\mathcal{L}}(D,G)$ is an $[n,k,d]$ code over $\mathbb{F}_q^n$ with the parameters

$$k = \ell(G) - \ell(G - D), \tag{2.3}$$

$$d \geq n - \deg G \text{ (Goppa bound)}. \tag{2.4}$$

We denote the dimension of kerϕ (i.e. $\ell(G-D)$) by a and call it the *abundance* of the code. We will assume throughout that $G - D$ is special (i.e. $i(G-D) = \ell(W-(G-D)) \neq 0$). If not, it is easy to see that G is also nonspecial and hence

$$k = \ell(G) - \ell(G-D) = (\deg G + 1 - g) - (\deg(G-D) + 1 - g) = n,$$

i.e. $C_{\mathcal{L}}(D,G) = \mathbb{F}_q^n$ is a trivial code.

2.2 Gonality Sequence of Algebraic Function Fields

For every positive integer i, we define the *i-th gonality* of the function field F/K as

$$\gamma_i := \min\{\deg A \mid A \in \mathrm{Div}(F/K) \text{ and } \ell(A) \geq i\}. \tag{2.5}$$

The sequence $GS(F/K) := (\gamma_i : i \in \mathbf{N})$ is called the *gonality sequence* of F/K. If we choose A in (2.5) as the zero divisor of F/K, we see that the first element of the gonality sequence is 0.

Lemma 2.2.1. *Let*

$$\gamma = \min\{[F : K(x)] \mid x \in F \setminus K\}.$$

Then, $\gamma = \gamma_2$.

Proof. Choose an element $x \in F \setminus K$ and consider the divisor $A := (x)_\infty$. Since 1 and x are linearly independent in $\mathcal{L}(A)$, we have $\ell(A) \geq 2$. Thus, for any $x \in F \setminus K$, we have

$$\gamma_2 \leq \deg A = [F : K(x)].$$

Therefore, $\gamma_2 \leq \gamma$. On the other hand, let A be a divisor with deg A=γ_2 and $\ell(A) \geq 2$. There is a positive divisor B with $B \sim A$ so that deg B=deg A and $\ell(B) = \ell(A)$. For $x \in \mathcal{L}(B) \setminus K$ note that $(x)_\infty \leq B$ since B is effective. Hence,

$$[F : K(x)] = \deg(x)_\infty \leq \deg B = \gamma_2.$$

This implies that $\gamma_2 \geq \gamma$ and the proof is concluded. □

Remark 2.2.1. The number γ in Lemma 2.2.1 is the (usual) gonality of F/K.

Lemma 2.2.2. *Let F/K be an algebric function field of genus g and suppose that F/K has a rational place. Then*

(i) The gonality sequence of F/K is strictly increasing.

(ii) $\gamma_i = g + i - 1$ for any i with $i \geq g + 1$.

(iii) $\gamma_i \geq 2(i-1)$ for any i with $1 \leq i \leq g$.

(iv) $\gamma_g = 2g - 2$.

Proof. (i) Let A be a divisor of degree γ_i with $\ell(A) \geq i$. If we show the existence of a divisor B with deg $B < \gamma_i$ and $\ell(B) \geq i - 1$ then the proof follows. Let $B := A - P$ where P is a rational place. We know that $\ell(A) - \ell(B) \leq$ deg $A -$deg B=1 ([10, Lemma 1.4.8]). Hence, $\ell(B) \geq \ell(A) - 1 \geq i - 1$.

(ii) Let A be a divisor with deg $A = i + g - 1 \geq 2g$. For a canonical divisor W, we have $\ell(W - A) = 0$ since $\deg(W - A) < 0$. By Riemann-Roch Theorem, we have $\ell(A) =$deg $A + 1 - g = i$. Thus, $\gamma_i \leq g + i - 1$. Now, let B be a divisor with deg $B < i + g - 1$. There exists a divisor D such that $B \leq D$ and deg $D = i + g - 2$. By assumption on i, we have deg $D \geq 2g - 1$. Hence, $\ell(D) =$deg $D + 1 - g = i - 1$. This shows that if deg $B < i + g - 1$, then $\ell(B) < \ell(D) < i$. Therefore, $\gamma_i = i + g - 1$ in this case.

(iii-iv) Let W be a canonical divisor so that deg $W = 2g - 2$ and $\ell(W) = g$. Then, by the definition of gonality numbers, we have

$$\gamma_g \leq 2g - 2. \tag{2.6}$$

Since there is no negative gonality number, we have $0 \leq \gamma_i \leq 2g-2$ for $i \leq g$. Consider a divisor A with deg$A = \gamma_i$ and $\ell(A) \geq i$. By Clifford's theorem, $\ell(A) \leq 1 + (1/2)$deg $A = 1 + \gamma_i/2$. Hence, we have $i \leq 1 + \gamma_i/2$, i.e. $\gamma_i \geq 2i - 2$ if $i \leq g$. If $i = g$, then $\gamma_g \geq 2g - 2$. This implies, together with (2.6), that $\gamma_g = 2g - 2$. □

Example 2.2.1. Consider the Hermitian function field $H = \mathbb{F}_{q^2}(x, y)$ defined by

$$y^q + y = x^{q+1}.$$

The genus of H is $q(q-1)/2$ and it has q^3+1 rational places (see [10, Lemma 6.4.4]). The gonality sequence of H is exactly known. Namely, if k is a positive integer of the form $k = \frac{1}{2}(j+1)(j+2) - i$ (for $0 \leq i \leq j$), then

$$\gamma_k = \begin{cases} j(q+1) - i & \text{if } 1 \leq k \leq g \\ k + g - 1 & \text{if } k > g \end{cases} \tag{2.7}$$

In fact, we can compute the gonality sequence of any smooth plane curve by Pellikaan's work [9, Corollary 2.4]. Below, we list the gonality sequences of the Hermitian function field over various square finite fields:

$GS(H/\mathbb{F}_4) = \{0, 2, \rightarrow\}$

$GS(H/\mathbb{F}_9) = \{0, 3, 4, 6, \rightarrow\}$

$GS(H/\mathbb{F}_{16}) = \{0, 4, 5, 8, 9, 10, 12 \rightarrow\}$

$GS(H/\mathbb{F}_{25}) = \{0, 5, 6, 10, 11, 12, 15, 16, 17, 18, 20 \rightarrow\}$

$GS(H/\mathbb{F}_{49}) = \{0, 7, 8, 14, 15, 16, 21, 22, 23, 24, 28, 29, 30, 31, 32, 35, 36, 37, 38, 39, 40,$
$42, \rightarrow\}$

$GS(H/\mathbb{F}_{64}) = \{0, 8, 9, 16, 17, 18, 24, 25, 26, 27, 32, 33, 34, 35, 36, 40, 41, 42, 43, 44, 45,$
$48, 49, 50, 51, 52, 53, 54, 56 \rightarrow\}.$

We proceed by results that will be used to prove a lower bound for the ASC of AG codes.

Lemma 2.2.3. *Consider $C = C_{\mathcal{L}}(D, G)$ of abundance a. Then the i-th generalized Hamming weight d_i of C satisfies*

$$d_i \geq n - \deg G + \gamma_{a+i} \tag{2.8}$$

where $\gamma_a + i$ is the $(a+i)$-th element of the gonality sequence of F/K.

Proof. We first show the following claim:

$d_i \leq t$ if and only if there exists $(n-t)$ pairwise distinct places in $\mathrm{supp}(D)$, say $P_{t+1}, \ldots, P_n$ without loss of generality, such that $\ell(G - P_{t+1} - \cdots - P_n) \geq a + i$.

If $d_i \leq t$, then there is a subcode V_i of C such that $\dim V_i = i$ and $|supp(V_i)| \leq t$. Let V_i be generated by $\phi(f_1), \ldots, \phi(f_i)$, where $f_1, \ldots, f_i \in \mathcal{L}(G)$. Then, $f_1, \ldots, f_i$ are linearly independent functions which have zeros at at least $(n-t)$ distinct places, say $P_{t+1}, \ldots, P_n$. Then, $f_1, \ldots, f_i \in \mathcal{L}(G - P_{t+1} - \cdots - P_n) \setminus \mathcal{L}(G - D)$. If $\{g_1, \ldots, g_a\}$ is a

basis of $\mathcal{L}(G-D)$, then the set $\mathcal{B}=\{f_1,\ldots,f_i,g_1,\ldots,g_a\}\subseteq\mathcal{L}(G-P_{t+1}-\cdots-P_n)$ is linearly independent. Hence, $\ell(G-P_{t+1}-\cdots-P_n)\geq a+i$.

On the other hand, assume that $\{g_1,\ldots,g_a\}$ is a basis of $\mathcal{L}(G-D)$. We can extend it to a basis $\mathcal{B}=\{g_1,\ldots,g_a,f_1,\ldots,f_i,\ldots\}$ of $\mathcal{L}(G-P_{t+1}-\cdots-P_n)$. Let the set $\{\phi(f_1),\ldots,\phi(f_i)\}$ generate a subcode V_i of C. Since $f_1,\ldots,f_i$ are zero at $P_{t+1},\ldots,P_n$, we have $|supp(V_i)|\leq t$. This implies that $d_i\leq t$.

Using the above claim, we have

$$\begin{aligned} d_i(C) &= \min\{\deg D' \mid 0\leq D'\leq D, \ell(G-D+D')\geq a+i\} \\ &= \min\{n-\deg D'' \mid 0\leq D''\leq D, \ell(G-D'')\geq a+i\} \end{aligned}$$

for every i, $1\leq i\leq k$, where k is the dimension of C. Now, let $A\leq D$ be an effective divisor such that $d_i(C)=n-\deg A$ and $\ell(G-A)\geq a+i$. By definition of $(a+i)$-th element of the gonality sequence, we have

$$\gamma_{a+i}\leq \deg(G-A)=\deg G-n+d_i(C).$$

Then, $d_i(C)\geq n-\deg G+\gamma_{a+i}$. □

Corollary 2.2.1. (Improved Goppa Bound) *For any AG code $C_{\mathcal{L}}(D,G)$ of abundance a, we have*

$$d\geq n-\deg G+\gamma_{a+1}. \tag{2.9}$$

Proof. Letting $i=1$ in Lemma 2.2.3, the result follows. □

Note that if the abundance is zero, then $d\geq n-\deg G$ in (2.9), which is nothing but the Goppa bound (2.4). Since the gonality sequence is increasing, by Lemma 2.2.1 Equation (2.9) improves the Goppa bound in general.

We finish this section with one more lower bound on the minimum distance of AG codes.

Corollary 2.2.2. *For an AG code $C_{\mathcal{L}}(D,G)$ of abundance a, we have*

$$d\geq (n-k+1)-(g-a). \tag{2.10}$$

Proof. Note that $k=\ell(G)-a$ satisfies $k\geq \deg G+1-g-a$ by the Riemann-Roch Theorem. Then, Corollary 2.2.1 implies that

$$d\geq (n-k+1)-g-a+\gamma_{a+1}.$$

It is sufficient to show that $a \leq g$ since we then have $\gamma_{a+1} \geq 2a$ from Lemma 2.2.1. If $a = 0$, this is clear. Assume that $a \geq 1$. Since the divisor $G - D$ is assumed to be special we have $\deg(G - D) \leq 2g - 2$. Then, by Clifford's theorem we have

$$a = \ell(G - D) \leq 1 + \frac{1}{2}\deg(G - D) \leq g.$$

□

Note that (2.10) can be rewritten as $d \geq s(C) - (g - a)$, where $s(C) = n - k + 1$ is the Singleton bound for linear codes (cf. Prop. 1.1.1).

2.3 A Goppa-like Bound on the ASC of AG Codes

We will give the proof of the main Theorem (a lower bound on $s[C]$) in this section, next two statements are the applications of Propositions 1.4.2 and 1.4.3, and they help us to estimate how far an AG code is from the Wolf bound.

Proposition 2.3.1. *For $C = C_{\mathcal{L}}(D, G)$, if one of the following holds*

(1) $\deg(G) < \lfloor n/2 \rfloor + \gamma_{a+1}$,

(2) $\deg(G) > \lceil n/2 \rceil + 2g - 2 - \gamma_{a^\perp+1}$,

then we have $s[C] = w(C)$.

Proof. If (1) is satisfied, from the improved Goppa bound (2.9), we have

$$\begin{aligned} d &\geq n - \deg G + \gamma_{a+1} && \text{(by (2.9))} \\ &> \lfloor n/2 \rfloor && \text{(by assumption (1))} \end{aligned}$$

Thus, $d \geq n/2 + 1$ and $2d \geq n + 2$. Then, from Proposition 1.4.2, we have $s[C] \geq w(C)$. The result follows from Wolf bound being an upper bound of $s[C]$. If (2) is satisfied, then we apply the same idea to the dual code $C^\perp = C_{\mathcal{L}}(D, W - G + D)$. We have

$$\begin{aligned} d^\perp &\geq n - \deg(W - G + D) + \gamma_{a^\perp+1} && \text{(by (2.9))} \\ &= n - (2g - 2) + \deg G - n + \gamma_{a^\perp+1} \\ &> \lfloor n/2 \rfloor && \text{(by assumption (2))} \end{aligned}$$

Hence $d^\perp \geq n/2 + 1$ and $2d^\perp \geq n + 2$. The result again follows from Proposition 1.4.2. □

Proposition 2.3.2. *Let i be a positive integer with $1 \leq i \leq k$. If either*

(1) $\gamma_{a+i} \geq 2\deg G - n - \gamma_{a+1} + 2$, *or*

(2) $\gamma_{a^\perp+i} \geq n + 2(2g-2) - 2\deg G - \gamma_{a^\perp+1} + 2$

holds, then $s[C] \geq w(C) - i + 1$.

Proof. Suppose that (1) is satisfied. Then we have

$$\begin{aligned} d_i &\geq n - \deg G + \gamma_{a+i} && \text{(by Lemma 2.2.3)} \\ &\geq \deg G - \gamma_{a+1} + 2 && \text{(by assumption (1))} \\ &\geq n + 2 - d && \text{(by Corollary 2.2.1)} \end{aligned}$$

The result follows from Proposition 1.4.3.

Now, assume that (2) is satisfied and apply the argument above to the dual code $C^\perp = C_{\mathcal{L}}(D, W - G + D)$. We have:

$$\begin{aligned} d_i^\perp &\geq n - \deg(W - G + D) + \gamma_{a^\perp+i} && \text{(by Lemma 2.2.3)} \\ &= n - (2g-2) + \deg G - n + \gamma_{a^\perp+i} \\ &\geq \deg G - (2g-2) + (n + 2(2g-2) - 2\deg G - \gamma_{a^\perp+1} + 2) && \text{(by assumption (1))} \\ &= n - \deg G + (2g-2) - \gamma_{a^\perp+1} + 2 \\ &= \deg(W - G + D) - \gamma_{a^\perp+1} + 2 \\ &\geq n - d^\perp + 2 && \text{(by Corollary 2.2.1)} \end{aligned}$$

Again, we have the desired result by Proposition 1.4.3. □

Now we prove the following simple and general bound for the ASC of AG codes.

Theorem 2.3.1. *For an AG code $C = C_{\mathcal{L}}(D, G)$, we have*

$$s[C] \geq w(C) - g + \min\{a, a^\perp\}, \tag{2.11}$$

where a and $a^\perp$ denote the abundances of C and $C^\perp$, respectively.

Proof. Let $i = g + 1 - a$. We know from the proof of Corollary 2.2.2 that $a \leq g$, so that $i \geq 1$. Furthermore, we have $\gamma_{g+1} = 2g$ by Lemma 2.2.1(ii). Then,

$$\gamma_{a+i} = \gamma_{g+1} = 2g \geq 2\deg G - n - \gamma_{a+1} + 2 \Leftrightarrow 2\deg G \leq n + 2g - 2 + \gamma_{a+1}.$$

Now let $\widetilde{i} = g + 1 - a^\perp$. Then,

$$\gamma_{a^\perp+\widetilde{i}} = \gamma_{g+1} = 2g \geq n+2(2g-2)-2\deg G-n-\gamma_{a^\perp+1}+2 \Leftrightarrow 2\deg G \geq n+2g-2-\gamma_{a^\perp+1}.$$

Since 2deg G must satisfy one of the inequalities above, we have that either hypothesis (1) in Proposition 2.3.2 is satisfied with $i = g+1-a$ or the hypothesis (2) in the same Proposition is satisfied with $\widetilde{i} = g + 1 - a^{\perp}$. Then, we have

$$s[C] \geq w(C) - (g + 1 - a) + 1 = w(C) - g + a$$

or

$$s[C] \geq w(C) - (g + 1 - a^{\perp}) + 1 = w(C) - g + a^{\perp}.$$

□

Remark 2.3.1. The bound in Theorem 2.3.1 is in general sharp. Consider an AG code $C = C_{\mathcal{L}}(D, G)$ constructed using the rational function field. Note that the abundance $a = 0$ since $\deg(G - D) \leq 2g - 2 = -2$. Hence, we have

$$s[C] \geq w(C) - (g - a) = w(C).$$

In fact, any AG code on the rational function field is MDS [10, Page 44]. Hence, the fact that they reach the Wolf bound also follows from Remark 1.4.2.

Corollary 2.3.1. *Consider the AG code $C_{\mathcal{L}}(D, G)$.*

(i) If $a \leq a^{\perp}$ and $\deg G \geq \lfloor n/2 \rfloor + \gamma_{a+1}$, then

$$s[C] \geq w(C) - \left(\deg G + 1 - a - \left\lfloor \frac{n + \gamma_{a+1}}{2} \right\rfloor \right).$$

(ii) If $a \geq a^{\perp}$ and $\deg G \leq \lceil n/2 \rceil + 2g - 2 - \gamma_{a^{\perp}+1}$, then

$$s[C] \geq w(C) - \left(2g - 1 - \deg G - a^{\perp} + \left\lceil \frac{n - \gamma_{a^{\perp}+1}}{2} \right\rceil \right).$$

Proof. (i) By assumption the bound from Theorem 2.3.1 is

$$s[C] \geq w(C) - g + a. \tag{2.12}$$

Let $\alpha := \deg G + 1 - a - \lfloor (n + \gamma_{a+1})/2 \rfloor$. Our claim is to show that $s[C] \geq w(C) - \alpha$. If $g - a \leq \alpha$, then the result follows from (2.12). Hence, assume that $g - a \geq \alpha + 1$

and let $i = \alpha + 1$. Note that $i \geq 1$ by the following:

$$\begin{aligned} i &= \deg G + 2 - a - \left\lfloor \tfrac{n+\gamma_{a+1}}{2} \right\rfloor \\ &\geq \left\lfloor \tfrac{n}{2} \right\rfloor + \gamma_{a+1} + 2 - a - \left\lfloor \tfrac{n+\gamma_{a+1}}{2} \right\rfloor \qquad \text{(by assumption)} \\ &\geq \left\lfloor \tfrac{n}{2} \right\rfloor + \gamma_{a+1} + 2 - a - \tfrac{n+\gamma_{a+1}}{2} \\ &\geq \left\lfloor \tfrac{n}{2} \right\rfloor - \tfrac{n}{2} + \tfrac{\gamma_{a+1}}{2} - a + 2 \\ &\geq \left\lfloor \tfrac{n}{2} \right\rfloor - n/2 + 2 \qquad \text{(by Lemma 2.2.2)} \\ &\geq 1 \end{aligned}$$

Since $g \geq a + i$, we also have the following by Lemma 2.2.2:

$$\begin{aligned} \gamma_{a+i} \geq 2(a+i-1) &= 2\deg G + 2 - 2\left\lfloor \frac{n+\gamma_{a+1}}{2} \right\rfloor \\ &\geq 2\deg G + 2 - n - \gamma_{a+1}. \end{aligned} \tag{2.13}$$

Then, the result follows from Proposition 2.3.2(i).

Part (ii) is proved similarly. Let $\beta = 2g - 1 - \deg G - a^{\perp} + \left\lceil \frac{n-\gamma_{a^{\perp}+1}}{2} \right\rceil$. The claim is to show that $s[C] \geq w(C) - \beta$. If $g - a^{\perp} \leq \beta$, then the result follows from Theorem 2.3.1, since $a \geq a^{\perp}$ by assumption. Therefore, assume that $g - a^{\perp} \geq \beta + 1 = j$. As above, we can show that $j \geq 1$ by the hypothesis on deg$G$ and Lemma 2.2.1. Then, it follows that

$$\gamma_{a^{\perp}+j} \geq n - \gamma_{a^{\perp}+1} - 2\deg G + 4g - 2, \tag{2.14}$$

by Lemma 2.2.2. The proof is concluded by using Proposition 2.3.2(ii). □

Corollary 2.3.2. *(i) Under the hypothesis of Corollary 2.3.1(i), we have*

$$s[C] \geq \left\lfloor \frac{n+\gamma_{a+1}}{2} \right\rfloor - g.$$

(ii) Under the hypothesis of Corollary 2.3.1(ii), we have

$$s[C] \geq g + n - \left\lceil \frac{n+\gamma_{a^{\perp}+1}}{2} \right\rceil.$$

Proof. (i) Set $i = \alpha + 1$, where α is as in the proof of Corollary 2.3.1(i). Then

$$\begin{aligned} d_i - n + \deg G &\geq \gamma_{a+i} && \text{(by (2.8))} \\ &\geq 2\deg G + 2 - n - \gamma_{a+1} && \text{(by (2.13))} \\ &\geq \deg G + 2 - d && \text{(by (2.9))} \end{aligned}$$

Hence, $d_i \geq n + 2 - d$. From the proof of Proposition 1.4.3, we have

$$s[C] \geq k - i + 1 = k - \deg G - 1 + a + \left\lfloor \frac{n + \gamma_{a+1}}{2} \right\rfloor.$$

Since $k = \ell(G) - a \geq \deg G + 1 - g - a$, the result follows.

(ii) The proof follows similarly. Set $j = \beta + 1$, where β is as in the proof of Corollary 2.3.1(ii). Then

$$\begin{aligned} d_j^\perp - n + \deg(W - G + D) &\geq \gamma_{a^\perp + j} && \text{(by (2.8))} \\ &\geq n - \gamma_{a^\perp + 1} - 2\deg G + 4g - 2 && \text{(by (2.14))} \\ &= \deg(W - G + D) - \gamma_{a^\perp + 1} - \deg G + 2g \\ &\geq n - d^\perp - \deg G + 2g && \text{(by (2.9))} \end{aligned}$$

Hence,

$$d_j^\perp \geq 2n - \deg(W - G + D) - d^\perp - \deg G + 2g = n - d^\perp + 2.$$

From the proof of Proposition 1.4.3, we have

$$s[C] \geq (n - k) - j + 1 = (n - k) - \left(2g - 1 - \deg G - a^\perp + \left\lceil \frac{n - \gamma_{a^\perp + 1}}{2} \right\rceil \right).$$

Note that

$$\begin{aligned} n - k = \dim(C^\perp) &= \ell(W - G + D) - a^\perp \\ &\geq \deg(W - G + D) + g + 1 - a^\perp \\ &= (2g - 2 - \deg G + n) + g + 1 - a^\perp \end{aligned}$$

Hence,

$$\begin{aligned} s[C] &\geq (2g - 2 - \deg G + n + g + 1 - a^\perp) - \left(2g - 1 - \deg G - a^\perp + \left\lceil \frac{n - \gamma_{a^\perp + 1}}{2} \right\rceil \right) \\ &= g + n - \left\lceil \frac{n - \gamma_{a^\perp + 1}}{2} \right\rceil \end{aligned}$$

□

2.4 Further Lower Bounds on the ASC of AG Codes

We will end this chapter with two more lower bounds on the ASC of AG codes. Forney's construction of the minimal trellis will play a key role here.

Observe that the i-th past $\mathcal{P}_i$ and the i-th future $\mathcal{F}_i$ subcodes of C in Forney's construction of minimal trellis are, respectively,

$$\mathcal{P}_i = C(D - P_{i+1} - \cdots - P_n, G - P_{i+1} - \cdots - P_n) \tag{2.15}$$

$$\mathcal{F}_i = C(D - P_1 - \cdots - P_i, G - P_1 - \cdots - P_i). \tag{2.16}$$

Let $A_i := G - P_1 - \cdots - P_i$ and $B_i := G - P_{i+1} - \cdots - P_n$. We then have

$$\begin{aligned} s_i(T) &= \dim(C) - \dim(\mathcal{P}_i) - \dim(\mathcal{F}_i) \\ &= \ell(G) - a - [\ell(B_i) - a] - [\ell(A_i) - a] \\ &= \ell(G) + a - \ell(A_i) - \ell(B_i). \end{aligned} \tag{2.17}$$

Proposition 2.4.1. *For $C = C_{\mathcal{L}}(D, G)$ we have*

$$s[C] \geq k + 2a - \ell(2G - D) - 1. \tag{2.18}$$

Proof. Let $0 \leq i \leq n$. If $\ell(A_i) \geq 1$ and $\ell(B_i) \geq 1$ for some i, then by ([10, Prop 1.4.14]) we have

$$\ell(A_i) + \ell(B_i) \leq \ell(A_i + B_i) + 1. \tag{2.19}$$

The claim follows if we use (2.19) in (2.17). Now, assume that either $\ell(A_i) = 0$ or $\ell(B_i) = 0$ for all i. Since $(G - D) \leq (G - A_i)$ and $(G - D) \leq (G - B_i)$, the abundance is zero. Further, $\min\{\ell(A_i) + \ell(B_i) : \text{for } 0 \leq i \leq n\} \leq 1$. Therefore,

$$s(C) \geq k - 1 \geq k - \ell(2G - D) - 1.$$

□

Proposition 2.4.2. *Let $0 \leq i \leq n$ and $j \in \mathbb{N}$ such that $\deg G - \gamma_j < \min(i, n - i)$. Then*

$$s[C] \geq k - 2(j - 1 - a). \tag{2.20}$$

Proof. Note that, by assumption, $\deg A_i < \gamma_j$ and $\deg B_i < \gamma_j$, since

$$\begin{aligned} \deg A_i + i - \gamma_j &= \deg G - \gamma_j < i \\ \deg B_i + n - i - \gamma_j &= \deg G - \gamma_j < n - i. \end{aligned}$$

Then by the definiton of the i-th gonality number, we have

$$\ell(A_i) \leq j-1 \qquad and \qquad \ell(B_i) \leq j-1.$$

Thus, by (2.17), we have

$$s_i(T) \geq k + 2a - 2(j-1).$$

□

Now, we will present an example which shows the behavior of the bounds we have stated so far.

Example 2.4.1. Consider the Hermitian functio field H over $\mathbb{F}_{q^2}$. Let Q_∞ denote the place at infinity and $Q_1, \ldots, Q_{q^3}$ denote all other rational places of H. The AG code C_m defined over H is

$$C_m := C_{\mathcal{L}}(D, mQ_\infty),$$

where $D := \sum_{i=1}^{q^3} Q_i$. These codes are called Hermitian codes. We refer to [10, Chapter 7] for more information on these codes. We will use some properties of C_m from this reference in the following.

Note that if $m < 0$, $\mathcal{L}(mQ_\infty) = \{0\}$ and hence $C_m = \{0\}$. If, on the other hand, $m > n + 2g - 2$, then $k = \ell(G) - \ell(G - D) = n$ by the Riemann-Roch Theorem. Hence, $C_m = \mathbb{F}_{q^2}^n$ in this case. Therefore, it is natural to restrict to $m \in [0, n + 2g - 2]$. Furthermore, we can assume that $m \in \left[\frac{n-1}{2}, \frac{n-3}{2} + 2g\right]$ since, otherwise, $s[C] = w(C)$ by Proposition 2.3.1.

A final natural restriction on m is due to the dual code. Namely, $C_m^\perp = C_{\mathcal{L}}(D, m^\perp Q_\infty)$ where $m^\perp = n + 2g - 2 - m$ ([10, Proposition 7.4.2]). It is not difficult to note that $m \in \left[\frac{n-1}{2} + g, \frac{n-3}{2} + 2g\right]$ iff $m^\perp \in \left[\frac{n-1}{2}, \frac{n-3}{2} + g\right]$. Since $s(C) = s(C^\perp)$, we finally restrict our attention to Hermitian codes C_m with $m \in \left[\frac{n-1}{2}, \frac{n-3}{2} + g\right]$.

Observe that

$$\deg(G - D) = m - q^3 \leq \frac{q^3 - 3}{2} + g - q^3 = -\frac{q^3}{2} - \frac{3}{2} + \frac{q(q-1)}{2}.$$

Hence, for any q, we have $\deg(G - D) < 0$ (i.e. $a = 0$). Similarly, one can show that $\deg(W - G) < 0$ (i.e. $a^\perp = 0$). Therefore, the dimension of C_m is

$$k = \ell(G) = \deg G + 1 - g.$$

In the following table, we list various lower bounds on $s[C_m]$ for $q \in \{2, 3, 4, 5, 7, 8\}$. There are the Wolf bound and the bounds obtained in Corollary 2.3.2, Propositions 2.3.2, 2.4.1, and 2.4.2. We use the gonality sequences of H (over various finite fields) obtained in Example 2.2.1. To compute $\ell(2G - D)$ in Proposition 2.4.1, we use exact formulas for C_m's (for all m) in [10, Proposition 7.4.3]. Namely, we have

$$k = \dim C_{2m} = \ell(2G) - \ell(2G - D).$$

The right hand side is found in [10, Proposition 7.4.3] and $\ell(2G)$ can be exactly computed by the Riemann-Roch Thorem since by the restricted interval for m,

$$\deg 2G = 2m \geq n - 1 = q^3 - 1 \geq 2g - 2, \text{ for any} q.$$

The bold face entries are the best lower bound obtained in this way.

q															
2	m	4													
	Wolf	4													
	C.2.3.2	**3**													
	P.2.3.2	**3**													
	P.2.4.1	2													
	P.2.4.2	2													
3	m	13	14	15											
	Wolf	11	12	13											
	C.2.3.2	**10**	10	10											
	P.2.3.2	**10**	**11**	10											
	P.2.4.1	**10**	10	10											
	P.2.4.2	9	10	**11**											
4	m	32	33	34	35	36	37								
	Wolf	27	28	29	30	31	32								
	C.2.3.2	**26**	26	26	26	26	26								
	P.2.3.2	**26**	**27**	**27**	27	**28**	**27**								
	P.2.4.1	25	26	26	26	26	25								
	P.2.4.2	25	26	**27**	**28**	27	26								
5	m	62	63	64	65	66	67	68	69	70	71				
	Wolf	53	54	55	56	57	58	59	60	61	62				
	C.2.3.2	**52**	52	52	52	52	52	52	52	52	52				
	P.2.3.2	**52**	**53**	**54**	53	54	**54**	**53**	**54**	53	52				
	P.2.4.1	**52**	52	53	53	53	**54**	**53**	53	53	52				
	P.2.4.2	51	52	53	**54**	**55**	**54**	**53**	**54**	**55**	**56**				
7	m	171	172	173	174	175	176	177	178	179	180				
	Wolf	151	152	153	154	155	156	157	158	159	160				
	C.2.3.2	**150**	150	150	150	150	150	150	150	150	150				
	P.2.3.2	**150**	**151**	**152**	**153**	152	153	154	**154**	153	**154**				
	P.2.4.1	**150**	150	151	152	152	152	153	**154**	**154**	153				
	P.2.4.2	149	150	151	152	**153**	**154**	**155**	**154**	153	**154**				
	m	181	182	183	184	185	186	187	188	189	190	191			
	Wolf	161	162	163	164	165	166	167	168	169	170	171			
	C.2.3.2	150	150	150	150	150	150	150	150	150	150	150			
	P.2.3.2	**155**	154	153	154	154	153	152	153	152	151	150			
	P.2.4.1	154	154	153	153	154	153	152	152	152	151	150			
	P.2.4.2	**155**	**156**	**157**	**158**	**157**	**156**	**155**	**156**	**157**	**158**	**159**			
8	m	256	257	258	259	260	261	262	263	264	265	266	267	268	269
	Wolf	229	230	231	232	233	234	235	236	237	238	239	240	241	242
	C.2.3.2	**228**	228	228	228	228	228	228	228	228	228	228	228	228	228
	P.2.3.2	**228**	**229**	**230**	**231**	230	231	232	233	232	**232**	**233**	**234**	233	232
	P.2.4.1	227	228	229	230	230	230	231	232	232	231	232	233	233	232
	P.2.4.2	227	228	229	230	**231**	**232**	**233**	**234**	**233**	**232**	**233**	**234**	**235**	**236**
	m	270	271	272	273	274	275	276	277	278	279	280	281	282	283
	Wolf	243	244	245	246	247	248	249	250	251	252	253	254	255	256
	C.2.3.2	228	228	228	228	228	228	228	228	228	228	228	228	228	228
	P.2.3.2	233	234	233	232	232	233	232	231	230	231	230	229	228	228
	P.2.4.1	232	233	233	232	231	232	232	231	231	230	230	229	228	227
	P.2.4.2	**237**	**238**	**237**	**236**	**235**	**236**	**237**	**238**	**239**	**240**	**239**	**238**	**237**	**236**

Table 2.1: Bounds on $s[C_m]$ for codes on the Hermitian function field where $q = 2, 3, 4, 5, 7, 8$.

CHAPTER 3

IMPROVEMENTS FOR A CLASS OF AG CODES

Blackmore and Norton in [2] introduced a lower bound on $s[C]$ for an AG code C, called the *second gonality bound*. In this chapter, we will improve the previous lower bounds on $s[C]$ for a class of an AG code C by introducing a numerical function $R(N)$, and we will derive a result that is similar to the second gonality bound.

Our main reference will be another article of Munuera and Tores ([6]). For comparison we will also refer to two articles of Blackmore and Norton ([1] and [2])

3.1 The Numerical Function $R(N)$

Throughout the chapter we assume that the algebraic function field F/K has a rational place (cf. Proposition 3.1.1) and we consider $GS(F/K)$ as a subset of $\mathbf{N}' := \{-1\} \cup \mathbf{N}_0$. We will call an element in $\mathbf{N}' \setminus GS(F/K)$ as a *gap* of F/K. By Lemma 2.2.1, there are exactly $g+1$ gaps and the biggest of them is $2g-1$.

Proposition 3.1.1. *Suppose that F/K has a rational place.*

(i) Let a be an integer. Then $a \in GS(F/K)$ iff $2g-1-a \notin GS(F/K)$.

(ii) For $i = 1, \ldots, g$,

$$\gamma_{g-\gamma_i+i-1} < 2g-1-\gamma_i < \gamma_{g-\gamma_i+i}. \tag{3.1}$$

Proof. (i) If $a < 0$ then $a \notin GS(F/K)$. Since $2g-1-a \geq 2g$, by Lemma 2.2.1(ii), $2g-1-a \in GS(F/K)$. If $a > 2g-1$, the result follows similarly. Now, assume that $0 \leq a \leq 2g-1$. There are exactly g gonality numbers of F/K in the interval $[0, 2g-1]$ (cf. Lemma 2.2.1). Thus, if we show that $2g-1-\gamma_i \neq \gamma_j$ for each $i, j \in [1, \ldots, g]$, then the proof is complete. Let A be a divisor of F/K with $\deg A = \gamma_i$ and $\ell(A) \geq i$,

and let W be a canonical divisor of F/K. Then, we have $\ell(W-A) \geq g-\gamma_i+i-1$ by Riemann-Roch Theorem.

(1) Let $j \leq g-\gamma_i+i-1$. Then, $\gamma_j \leq \deg(W-A) = 2g-2-\gamma_i$ so that $\gamma_j < 2g-1-\gamma_i$.

(2) Let $j \geq g-\gamma_i+i$ and assume that $2g-1-\gamma_i = \gamma_j$. Let B be a divisor of F/K with $\deg B = \gamma_j$ and $\ell(B) \geq j$. By the Riemann-Roch Theorem

$$\begin{aligned} \ell(W-B) &\geq j+g-\gamma_j-1 \\ &= j-g+\gamma_i \\ &\geq i \end{aligned} \tag{3.2}$$

Since $\deg(W-B) = 2g-2-\gamma_j = \gamma_i-1$, this contradicts with (3.2) by definition of gonality numbers.

(ii) Let $1 \leq i \leq g$. There are precisely γ_i-i+1 nongonality numbers in the interval $[0,\gamma_i]$. By (i), the interval $[2g-1-\gamma_i, 2g-1]$ has γ_i-i+1 gonality numbers. Taking the fact that $2g-1 \notin GS(F/K)$ and $\gamma_g = 2g-2$ into account, we obtain the first gonality number which is $\gamma_{g-\gamma_i+i}$. Since $2g-1-\gamma_i \notin GS(F/K)$, the proof concludes. □

Lemma 3.1.1. *The AG code $C = C_{\mathcal{L}}(D,G)$ is non-abundant and $2\deg G - n \leq 2g-2$ provided that $2k \leq n$ and $n > 2g$.*

Proof. Suppose that $\ell(G-D) \geq 1$. If $G-D$ is non-special, then

$$k = \ell(G) - (\deg(G-D)+1-g) \geq (\deg G+1-g) - (\deg(G-D)+1-g) = n$$

which is not possible by the hypothesis. So, $G-D$ is a special divisor. Then by Clifford's theorem we have

$$\ell(G-D) \leq \frac{\deg G - n}{2} + 1.$$

Thus,

$$k \geq (\deg G+1-g) - \frac{\deg G-n}{2} - 1 = \frac{\deg G+n-2g}{2}.$$

From the hypothesis, $n \geq 2k \geq \deg G+n-2g$ which implies $2g \geq \deg G$. Since, $\deg(G-D) \geq 0$ (as $\ell(G-D) \geq 1$), we have $2g \geq \deg G \geq n$. This contradicts the hypothesis that $n > 2g$. Taking into account the fact that

$$\frac{n}{2} \geq k = \ell(G) \geq \deg G+1-g,$$

the second statement follows. □

Let $\widetilde{\ell} = \widetilde{\ell}_{F/K} : \mathbf{N}' \to \mathbf{N}_0$ be the numerical function defined by

$$\widetilde{\ell}(a) := \max\{i \in N : \gamma_i \leq a\} \qquad \text{and} \qquad \widetilde{\ell}(-1) := 0.$$

By Lemma 2.2.1, we conclude that $\widetilde{\ell}$ is a nondecreasing function with $\widetilde{\ell}(2g-2) = g$ and $\widetilde{\ell}(2g-1+i) = g+i$ for $i \geq 1$. In addition, if $a+1 \notin GS(F/K)$, then $\widetilde{\ell}(a+1) = \widetilde{\ell}(a)$, and if $a+1 \in GS(F/K)$ then $\widetilde{\ell}(a+1) = \widetilde{\ell}(a)+1$. In particular, $\widetilde{\ell}(a+1) \leq \widetilde{\ell}(a)+1$.

Lemma 3.1.2. *For a divisor M of $\deg M \geq -1$, we have $\ell(M) \leq \widetilde{\ell}(\deg M)$.*

Proof. If $\deg M = -1$, then $\ell(M) = 0 = \widetilde{\ell}(-1)$. Now assume that $\deg M \geq 0$ and let $i \in \mathbf{N}_0$ be such that $\gamma_i \leq \deg M < \gamma_{i+1}$ so that $\widetilde{\ell}(\deg M) = i$. From the definition of gonality number, we have $\ell(M) \leq i$. □

Let $R = R_{F/K} : \mathbf{N}' \cap [-1, 2g-2] \to \mathbf{N}$ be the numerical function defined by

$$R(N) := \min\{\widetilde{\ell}(a) + \widetilde{\ell}(b) : a, b \in \mathbf{N}' \text{ with } a+b = N\}.$$

In the following result, we will use the notation introduced in Chapter 1 that was used in Forney's construction (cf. Page 16).

Theorem 3.1.1. *Let $C = C_{\mathcal{L}}(D, G)$ be an AG code with $2k \leq n$ and $n > 2g$. If $m := \deg G$, then*

$$\triangle[C] \leq R(2m-n). \tag{3.3}$$

In particular, $s[C] \geq w(C) - R(2m-n)$.

Proof. It is sufficient to show that $\triangle(C) \leq R(2m-n)$ since the function R depends only on the function field where C is defined. By the hypothesis, $w(C) = k$. We can assume that $2d < n+2$ by Proposition 1.4.1, since we have $s(C) = k$ otherwise. Then, by the Goppa bound,

$$n + 2 > 2d > 2n - 2m,$$

which implies that $2m - n \geq 1$. Let us consider the i-th past $\mathcal{P}_i$ and the i-th future $\mathcal{F}_i$ subcodes of C in the Forney's construction which are given in (2.15) and (2.16) ,respectively, for an AG code. By Lemma 3.1.1, the code C is non-abundant so that the i-th element of the state complexity profile of C is

$$s_i = s_i(C) = k - \triangle_i$$

where $\triangle_i = \ell(G - P_1 - \cdots - P_i) + \ell(G - P_{i+1} - \cdots - P_n)$. Then, by Proposisition 1.4.1 and since $d \geq n - m$, we have $s(C) = w(C) - \triangle(C)$, where

$$\triangle(C) = \min\{\triangle_{d-1}, \ldots, \triangle_n\} = \min\{\triangle_{n-m-1}, \ldots, \triangle_{m+1}\}.$$

Let $i \in \mathbb{Z}$ with $n - m - 1 \leq i \leq m + 1$, then

$$\deg(G - P_1 - \cdots - P_i) \geq -1, \text{ and } \deg(G - P_{i+1} - \cdots - P_n) \geq -1.$$

Therefore, by Lemma 3.1.2 we have

$$\triangle_i \leq \widetilde{\ell}(\deg(G - P_1 - \cdots - P_i)) + \widetilde{\ell}(\deg(G - P_i + 1 - \cdots - P_n)).$$

Now, by the definition of the function R and since $2m - n \leq 2g - 2$, we have

$$\triangle = \min_{i=1,\ldots,n} \triangle_i \leq \widetilde{\ell}(m - i) + \widetilde{\ell}(m - (n - i)) = R(2m - n) \leq R(2g - 2).$$

Thus, the proof is complete. □

In the remaining parts of this section, we will explore the function R.

Lemma 3.1.3. *Let $N \in \mathbf{N}' \cap [-1, 2g - 2]$.*

(i) R is a non-decreasing function such that $R(N) \leq R(N + 1) \leq R(N) + 1$,

(ii) $1 \leq R(N) \leq i - 1$, if $N < \gamma_i - 1$,

(iii) $R(N) \leq \lfloor (N + 1)/2 \rfloor + 1$,

(iv) There is a gap $a = a(N)$ of F/K with $a \leq N/2$ such that $R(N) = \widetilde{\ell}(a) + \widetilde{\ell}(N - a)$.

Proof. By definition of R, we have $R(-1) = 1$ since $R(-1) = \widetilde{\ell}(-1) + \widetilde{\ell}(0)$.

(i) Assume that $R(N + 1) = \widetilde{\ell}(a) + \widetilde{\ell}(b)$ with $a + b = N + 1$ and $a \leq b$. Since $\widetilde{\ell}$ is a non-decreasing function, we have

$$R(N) \leq \widetilde{\ell}(a) + \widetilde{\ell}(b - 1) \leq \widetilde{\ell}(a) + \widetilde{\ell}(b) = R(N + 1).$$

Thus, we have $R(N) \geq 1$. Let $R(N) < R(N + 1)$ and $R(N) = \widetilde{\ell}(a') + \widetilde{\ell}(b')$ where $a' + b' = N$, then

$$\widetilde{\ell}(a') + \widetilde{\ell}(b') = R(N) < R(N + 1) \leq \widetilde{\ell}(a' + 1) + \widetilde{\ell}(b').$$

Therefore $\widetilde{\ell}(a') < \widetilde{\ell}(a'+1)$, which implies that $\widetilde{\ell}(a')+1 = \widetilde{\ell}(a'+1)$. Hence, $R(N+1) = R(N)+1$.

(ii) $R(N) \leq \widetilde{\ell}(N+1)$ where $N = (N+1)-1$. By hypothesis, $N+1 < \gamma_i$, so that $\widetilde{\ell}(N+1) \leq i-1$.

(iii) There exists $i \in \{1,\ldots,g\}$ such that $\gamma_i \leq N+1 < \gamma_{i+1}$, so $R(N) \leq i$ by (ii). Since $2i-2 \leq \gamma_i \leq N+1$, by Lemma 2.2.1 , $R(N) \leq (N+3)/2$.

(iv) Assume that $R(N) = \widetilde{\ell}(a) + \widetilde{\ell}(b)$ where $a \leq b = N-a$ and $a \in GS(F/K)$. Then, $\widetilde{\ell}(a-1) = \widetilde{\ell}(a) - 1$ and $\widetilde{\ell}(b+1) \leq \widetilde{\ell}(b)+1$. Thus,

$$\widetilde{\ell}(a-1)+\widetilde{\ell}(b+1) \leq \widetilde{\ell}(a)+\widetilde{\ell}(b) = R(N) \leq \widetilde{\ell}(a-1)+\widetilde{\ell}(b+1).$$

If $a-1$ is a gap of F/K, the proof is finished. Otherwise we repeat the above argument until we obtain a gap number. □

Remark 3.1.1. Theorem 3.1.1 produces the result obtained in Theorem 2.3.1, which is $s[C] \geq w(C) - g$ whenever $2k \leq n$ and $n > 2g$ since we have $R(N) \leq R(2g-2) \leq g$ for $N \in \mathbf{N}' \cap [-1, 2g-2]$.

Our goal in the rest of this section is to improve Theorem 3.1.1 further.

Lemma 3.1.4. *Let $i \in \mathbf{N}', N \in \mathbf{N}' \cap [-1, 2g-2]$ and $r \in \mathbf{N}$ with $i+r \leq N+1$. We have*

$$\min\{\widetilde{\ell}(a)+\widetilde{\ell}(N-a) : a \in A\} = \{\widetilde{\ell}(i+r)+\widetilde{\ell}(N-i-r)\},$$

provided that $A = \{i, i+1, \ldots, i+r\} \subset \mathbf{N}'$ is a set of $r+1$ consecutive integers where $i+1,\ldots,i+r$ are gaps of F/K.

Proof. Assume that $a = i+j$ with $1 \leq j \leq r$. Since a is a gap of F/K, $\widetilde{\ell}(a) = \widetilde{\ell}(i)$. To have minimum $\widetilde{\ell}(a)+\widetilde{\ell}(N-a)$, $\widetilde{\ell}(N-a)$ must be minimum. Since $\widetilde{\ell}$ is a nondecreasing function, we choose the largest a in A. □

Proposition 3.1.2. *Let $N \in \mathbf{N}' \cap [-1, 2g-2]$. Then,*

$$R(N) = \min\{\widetilde{\ell}(a)+\widetilde{\ell}(N-a) : a = \lfloor N/2 \rfloor, \text{ or}$$
$$(-1 \leq a \leq N/2 \text{ and } a \text{ is a gap of } F/K \text{ with } a+1 \in GS(F/K))\}$$

Proof. First note that we have , by Lemma 3.1.3(iv), some gap a of F/K that satisfies $R(N) = \widetilde{\ell}(a)+\widetilde{\ell}(N-a)$ where $a \leq N/2$. So, we look for the gaps a with $\leq N/2$. Let $a < \lfloor N/2 \rfloor$. We can assume that each integer a' with $a < a' \leq \lfloor N/2 \rfloor$ is a gap of F/K.

Then $R(N) = \widetilde{\ell}(\lfloor N/2 \rfloor) + \widetilde{\ell}(\lceil N/2 \rceil)$ by Lemma 3.1.3. If a' is not a gap of F/K then we can assume that $a+1 \in GS(F/K)$ by Lemma 3.1.4, and the proof is complete. □

Example 3.1.1. Let $N \in \mathbf{N}' \cap [-1, 2g-2]$ with $\lceil N/2 \rceil < \gamma_2$. From Proposition 3.1.2, we have

$$R(N) = \min\{\widetilde{\ell}(-1) + \widetilde{\ell}(N+1), \widetilde{\ell}(\lfloor N/2 \rfloor) + \widetilde{\ell}(\lceil N/2 \rceil)\}.$$

If $N+1 < \gamma_2$ then $\widetilde{\ell}(N+1) \leq 1$, which implies $R(N) = 1$ since $\widetilde{\ell}(-1) = 0$ and $R(N) \geq 1$. If $N+1 \geq \gamma_2$ then $\widetilde{\ell}(N+1) = 2$. Further, $\widetilde{\ell}(\lfloor N/2 \rfloor) = \widetilde{\ell}(\lceil N/2 \rceil) = 1$, so $R(N) = 2$.

To provide the desired improvement mentioned in Remark 3.1.1, it is effective to compute $R(2g-2)$, which is given in the following statement.

Proposition 3.1.3. $R(2g-2) = g - \max\{\gamma_i - (2i-2) : i = 1, \ldots, g\}$

Proof. By the definition of R and Lemma 3.1.4, we have

$$R(2g-2) = \min\{\widetilde{\ell}(a) + \widetilde{\ell}(2g-2-a) : -1 \leq a \leq 2g-1, a+1 \in GS(F/K)\}.$$

Let $a = \gamma_i - 1$ with $1 \leq i \leq g$. Then,

$$R(2g-2) = \min\{\widetilde{\ell}(\gamma_i - 1) + \widetilde{\ell}(2g - \gamma_i - 1) : i = 1, \ldots, g\}.$$

We have $\widetilde{\ell}(\gamma_i - 1) = i - 1$ and $\widetilde{\ell}(2g - \gamma_i - 1) = g - \gamma_i - 1 + i$, by the definition of the function $\widetilde{\ell}$ and (3.1), respectively. Therefore,

$$R(2g-2) = \min\{g - \gamma_i + 2i - 2 : i = 1, \ldots, g\}.$$

□

Theorem 3.1.2. *Let $C = C_{\mathcal{L}}(D, G)$ be an AG code with $2k \leq n$ and $n > 2g$, where g is the genus of F/K. Then*

$$s[C] \geq w(C) - g + \gamma_2 - 2.$$

Proof. By Lemma 3.1.1 and by Proposition 3.1.3 we have $2m - n \leq 2g - 2$ and $R(2g-2) \leq g - \gamma_2 + 2$. Then, by Theorem 3.1.1, we obtain

$$s[C] \geq w(C) - R(2m-n) \geq w(C) - (g - \gamma_2 + 2).$$

□

3.2 An Improvement on the ASC of Hermitian Codes

In this section, we will study the function R on the Hermitian function field. At the end of the section we will compare the bound we obtain by Theorem 3.1.1 with the bound computed by Blackmore and Norton in [1]

On the Hermitian function field, we can exactly compute the function R since the genus of $H/\mathbb{F}_{q^2}$ is $g = q(q+1)/2$ and its gonality sequence is known (Example 2.2.1).

For an integer $a \in \mathbf{N}_0$, let α and β be the non-negative integers defined by $a = \alpha q + \beta$, $0 \leq \beta < q$. Since $a = \alpha q + \beta = \alpha(q+1) - (\alpha - \beta)$, it is easily seen that $a \in GS(H/\mathbb{F}_{q^2})$ iff $\beta \leq \alpha$ by Example 2.2.1 .

Lemma 3.2.1. *We have*

$$\widetilde{\ell}(a) = \frac{\alpha(\alpha+1)}{2} + \min\{\alpha, \beta\} + 1.$$

Proof. If $a = 0$, then the result holds since $\widetilde{\ell}(0) = 1$. Now, assume $a > 0$. Let $a \in GS(H/\mathbb{F}_{q^2})$ so that $\min\{\alpha, \beta\} = \beta$. Using Example 2.2.1, let k be such that $\gamma_k = a$. Thus,

$$\begin{aligned} k &= \frac{(\alpha+1)(\alpha+2)}{2} - (\alpha - \beta) \\ &= \frac{\alpha(\alpha+1)}{2} + \beta + 1, \end{aligned}$$

since $a = \alpha q + \beta = \alpha(q+1) - (\alpha - \beta)$. If a is a gap of $H/\mathbb{F}_{q^2}$ then $\beta > \alpha$ and $\widetilde{\ell}(a) = \widetilde{\ell}(\alpha q + \alpha)$. Similarly, we find k which satisfies $\gamma_k = \alpha q + \alpha$. Then,

$$k = \frac{(\alpha+1)(\alpha+2)}{2} = \frac{\alpha(\alpha+1)}{2} + \alpha + 1.$$

□

Lemma 3.2.2. *Let $N \in \mathbf{N}' \cap [-1, 2g-2]$ and $a = \alpha q + \beta$ be a gap of $H/\mathbb{F}_{q^2}$ with $\alpha \geq 1$ and $a \leq N/2$. Then*

$$\widetilde{\ell}(a) + \widetilde{\ell}(N-a) \leq \widetilde{\ell}(a-q) + \widetilde{\ell}(N-(a-q)).$$

Proof. Let $a' := a - q = (\alpha - 1)q + \beta$ and $b := N - a = \delta q + \epsilon$ with $0 \leq \epsilon < q$, so $b' = N - a' = (\delta + 1)q + \epsilon$. By Lemma 3.2.1, we have

$$\begin{aligned} \widetilde{\ell}(a) - \widetilde{\ell}(a') &= \frac{\alpha(\alpha+1)}{2} + \alpha + 1 - \left(\frac{\alpha(\alpha-1)}{2} + (\alpha - 1) + 1 \right) \\ &= \alpha + 1 \end{aligned} \tag{3.4}$$

If $b \in GS(H/\mathbb{F}_{q^2})$, then, since $\epsilon \leq \delta$,

$$\begin{aligned} \widetilde{\ell}(b) - \widetilde{\ell}(b') &= \frac{\delta(\delta+1)}{2} + \epsilon + 1 - \left(\frac{(\delta+1)(\delta+2)}{2} + \epsilon + 1 \right) \\ &= -\delta - 1. \end{aligned} \tag{3.5}$$

From the above equations and since a is a gap number, (i.e., $a \leq b = N - a$ which implies $\delta \geq \alpha$), we have

$$\begin{aligned} \widetilde{\ell}(a) + \widetilde{\ell}(b) &= \widetilde{\ell}(a') + \widetilde{\ell}(b') - \delta + \alpha \\ &\leq \widetilde{\ell}(a') + \widetilde{\ell}(b'). \end{aligned} \tag{3.6}$$

Let b be a gap number so that $\epsilon > \delta$. Then

$$\begin{aligned} \widetilde{\ell}(b) - \widetilde{\ell}(b') &= \frac{\delta(\delta+1)}{2} + \delta + 1 - \left(\frac{(\delta+1)(\delta+2)}{2} + \delta + 2 \right) \\ &= -\delta - 2. \end{aligned} \tag{3.7}$$

Thus, the result follows. □

Proposition 3.2.1. *Let $N \in \mathbf{N}_0 \cap [0, 2g-2]$ and assume that α and β are the integers defined by $\lfloor N/2 \rfloor = \alpha q + \beta$ with $0 \leq \beta < q$ and let $\alpha \geq 1$.*

(i) If $\lfloor N/2 \rfloor$ is a gap of $H/\mathbb{F}_{q^2}$, then

$$R(N) = \min\{\widetilde{\ell}(\lfloor N/2 \rfloor) + \widetilde{\ell}(\lceil N/2 \rceil), \widetilde{\ell}(\alpha q - 1) + \widetilde{\ell}(N - \alpha q + 1)\}.$$

(ii) If $\lfloor N/2 \rfloor \in GS(H/\mathbb{F}_{q^2})$, then

$$R(N) = \widetilde{\ell}(\alpha q - 1) + \widetilde{\ell}(N - \alpha q + 1).$$

Proof. Note that $\alpha q - 1 \notin GS(H/\mathbb{F}_{q^2})$ since $\alpha q = \alpha(q+1) - (\alpha + 1)$ and $\alpha + 1 > \alpha$ but $\alpha q \in GS(H/\mathbb{F}_{q^2})$. Then the result follows by Prop 3.8 and Lemma 3.2.2. □

We now define the concept of 'jump' to improve the above result. If $R(N) > R(N-1)$, the integer N with $0 \leq N \leq 2g-2$ is called a *jump* of $H/\mathbb{F}_{q^2}$. The set of jumps of $H/\mathbb{F}_{q^2}$ is denoted by $U(H/\mathbb{F}_{q^2})$ and the number of jumps is equal to $R(2g-2)$, which can be computed via Proposition 3.2.1.

Lemma 3.2.3. *Let $H/\mathbb{F}_{q^2}$ be a Hermitian function field of degree $q+1$. Then*

(1) $|U(H/\mathbb{F}_{q^2})| = \begin{cases} q^2/4 & \text{if } q \text{ is even} \\ (q^2-1)/4 & \text{if } q \text{ is odd} \end{cases}$

(2) $U(H/\mathbb{F}_{q^2}) = \{\alpha q + \beta : 0 \le \alpha \le q-2,\ -1 \le \alpha \le q-2, \text{ and } 2\beta + 2 \le \alpha \text{ or } \beta = q-1\} \setminus \{2g-1\}$.

Proof. (1) We compute $R(2g-2)$. Let q be even. Then

$$g - 1 = \frac{q(q-1)}{2} - 1 = \frac{(q-2)(q+1)}{2} = \frac{(q-2)q}{2} + \frac{q-2}{2}$$

so $g-1 \in GS(H/\mathbb{F}_{q^2})$. By Proposition 3.2.1 we have

$$R(2g-2) = \widetilde{\ell}(\alpha q - 1) + \widetilde{\ell}(2g - 2 - \alpha q + 1)$$

where $\alpha = (q-2)/2$. Note that

$$\alpha q - 1 = \frac{(q-2)}{2}q - 1 = \frac{(q-4)}{2}q + q - 1$$

and

$$2g - 2 - \alpha q + 1 = (q-2)(q+1) - q\frac{(q-2)}{2} + 1 = \frac{(q-2)q}{2} + q - 1.$$

Then by Lemma 3.2.1, we have

$$\widetilde{\ell}(\alpha q - 1) = \frac{(q-4)}{2}\frac{(q-2)}{2}\frac{1}{2} + \frac{q}{2} - 2 + 1 = \frac{q^2}{8} - \frac{q}{4}$$

and

$$\widetilde{\ell}(2g - 2 - \alpha q + 1) = \frac{(q-2)}{2}\frac{q}{2}\frac{1}{2} + \frac{q}{2} = \frac{q^2}{8} + \frac{q}{4}.$$

Hence, the result follows. Similar arguments are applied for an odd q.

(2) Let T be the set on the right hand side of the equality in the item (2). We first show that $|T| = R(2g-2)$. Consider $2\beta + 2 = \alpha = q-2$ so that $1 = q - 3 - 2\beta$ and $\beta = \lfloor (q-4)/2 \rfloor$. Further, the number of elements of T where $\beta = q-1$ is $q-1$ since $2g-1 \notin T$, i.e., for $\alpha = q-2$ we have $\alpha q + \beta = 2g-1$. Thus

$$|T| = \sum_{\beta=0}^{\lfloor (q-4)/2 \rfloor} (q - 3 - 2\beta) + q - 1 = R(2g-2).$$

Since every element in T is a jump of $H/\mathbb{F}_{q^2}$, the proof is finished. □

Example 3.2.1. Consider the Hermitian function field over $\mathbb{F}_{64}$ so that $q = 8$ and $g = 28$. In the following table the bold face entries demonstrate the jumps of $H/\mathbb{F}_{64}$ where the integers range from -1 to 54.

−1	0	1	2	3	4	5	6
7	8	9	10	11	12	13	14
15	**16**	17	18	19	20	21	22
23	**24**	25	26	27	28	29	30
31	**32**	**33**	34	35	36	37	38
39	**40**	**41**	42	43	44	45	46
47	**48**	**49**	**50**	51	52	53	54

Proposition 3.2.2. *Let $H/\mathbb{F}_{q^2}$ be a Hermitian function field and $N \in \mathbf{N}' \cap [-1, 2g-2]$. Let α and β be the integers defined by $N = \alpha q + \beta$ with $0 \leq \alpha \leq q-2$ and $-1 \leq \beta \leq q-2$.*

(1) If $\beta > \lfloor \alpha/2 \rfloor - 1$, then $R(N) = R(\alpha q + \lfloor \alpha/2 \rfloor - 1)$,

(2) If $\beta \leq \lfloor \alpha/2 \rfloor - 1$, then

$$R(N) = \begin{cases} \alpha(\alpha+2)/4 + \beta + 2 & \text{if } \alpha \text{ is even} \\ (\alpha+1)^2/4 + \beta + 2 & \text{if } \alpha \text{ is odd} \end{cases}$$

Proof. (1) The largest jump of $H/\mathbb{F}_{q^2}$ not exceeding N is achieved when $\beta = \left\lfloor \frac{(\alpha-2)}{2} \right\rfloor$, i.e., $2\beta + 2 = \alpha$. Thus the equality holds.

(2) Let us put all the integers from -1 to $2g$-2 in an array according to the values of α and β which, respectively, correspond to the rows and the columns of the array as in the above example. The j-th row of the array contains $\lfloor (j+2)/2 \rfloor$ jumps of $H/\mathbb{F}_{q^2}$ which are exactly in the first $\lfloor (j+2)/2 \rfloor$ columns of the array. Then the number of jumps of $H/\mathbb{F}_{q^2}$ is:

$\beta + 2 + 2(\sum_{i=1}^{\alpha/2} i) = \alpha(\alpha+2)/4$, when α is even, and

$\beta + 2 + 2(\sum_{i=1}^{(\alpha-1)/2} i) + (\alpha+1)/2 = (\alpha+1)^2/4$, when α is odd.

□

We finish the chapter with an example to demonstrate the effect of these results on the bounds of $s[C]$, where C is an AG code on the Hermitian function field.

Example 3.2.2. Let $C = C_{\mathcal{L}}(D, mQ_\infty)$ be a Hermitian code over $\mathbb{F}_{q^2}$. For $q = 2, 3, 4, 5, 7, 8$, the values of m =deg G and the genus g are given in Example 2.4.1. To apply Theorem 3.1.1, m has to satisfy $-1 \leq 2m - n \leq 2g - 2$ which corresponds to the interval used in Example 2.4.1, i.e. $m \in [\frac{n-1}{2}, \frac{n-3}{2} + g]$. Note that $2k \leq n$ and $n > 2g$.

In the following table, the row Wolf and the row Chp2 contains the Wolf upper bound on $s[C]$ and the best lower bound obtained in Chapter 2, respectively. While true values of $s[C]$ which are obtained by Blackmore and Norton [1] are given in the row True, the bounds obtained from Theorem 3.1.1 and Proposition 3.2.2 are demonstrated in the row Thm 3.1.1. The lower bounds that attain the true values of $s[C]$ are in bold face.

q															
2	m	4													
	Wolf	4													
	Chp2	**3**													
	Thm 3.1.1	**3**													
	True	3													
3	m	13	14	15											
	Wolf	11	12	13											
	Chp2	10	**11**	**11**											
	Thm 3.1.1	10	**11**	**11**											
	True	11	11	11											
4	m	32	33	34	35	36	37								
	Wolf	27	28	29	30	31	32								
	Chp2	**26**	**27**	**27**	**28**	**28**	27								
	Thm 3.1.1	**26**	**27**	**27**	**28**	27	**28**								
	True	26	27	27	28	28	28								
5	m	62	63	64	65	66	67	68	69	70	71				
	Wolf	53	54	55	56	57	58	59	60	61	62				
	Chp 2	52	**53**	**54**	**54**	**55**	54	53	54	55	56				
	Thm 3.1.1	52	**53**	**54**	**54**	**55**	55	55	**56**	55	**56**				
	True	53	53	54	54	55	56	56	56	57	56				
7	m	171	172	173	174	175	176	177	178	179	180				
	Wolf	151	152	153	154	155	156	157	158	159	160				
	Chp 2	150	**151**	**152**	**153**	**153**	**154**	**155**	154	154	154				
	Thm 3.1.1	150	**151**	**152**	**153**	**153**	**154**	**155**	155	155	**156**				
	True	151	151	152	153	153	154	155	156	156	156				
	m	181	182	183	184	185	186	187	188	189	190	191			
	Wolf	161	162	163	164	165	166	167	168	169	170	171			
	Chp 2	155	156	**157**	**158**	157	156	155	156	157	158	159			
	Thm 3.1.1	**157**	156	**157**	**158**	158	157	158	**159**	158	158	**159**			
	True	157	158	157	158	159	159	159	159	160	160	159			
8	m	256	257	258	259	260	261	262	263	264	265	266	267	268	269
	Wolf	229	230	231	232	233	234	235	236	237	238	239	240	241	242
	Chp 2	**228**	**229**	**230**	**231**	**231**	**232**	**233**	**234**	233	232	233	234	235	**236**
	Thm 3.1.1	**228**	**229**	**230**	**231**	**231**	**232**	**233**	**234**	233	**234**	**235**	**236**	235	**236**
	True	228	229	230	231	231	232	233	234	234	234	235	236	237	236
	m	270	271	272	273	274	275	276	277	278	279	280	281	282	283
	Wolf	243	244	245	246	247	248	249	250	251	252	253	254	255	256
	Chp 2	**237**	**238**	237	236	235	236	237	238	**239**	**240**	239	238	237	236
	Thm 3.1.1	**237**	**238**	237	237	**238**	**239**	238	238	**239**	**240**	239	238	239	**240**
	True	237	238	239	238	238	239	240	240	239	240	241	241	240	240

Table 3.1: Bounds on $s[C_m]$ for Hermitian codes over $\mathbb{F}_{q^2}$ for $q = 2, 3, 4, 5, 7, 8$.

Bibliography

[1] Blackmore, T., Norton, G., *Determining When the Absolute State Complexity of a Hermitian Code Achieves the DLP Bound*, SIAM J. Discrete Maths. **15**, 14-40, 2001.

[2] Blackmore, T. and Norton, G., *Lower Bounds on the State Complexity of Geometric Goppa Codes*, Des., Codes, Cryptogr. **29**, 95-115, 2002.

[3] McEliece, R. J., *On the BCJR Trellis for Linear Block Codes*, IEEE Trans. Inform. Theory **42**, 10721092, 1996.

[4] Muder, D. J., *Minimal Trellises for Block Codes*, IEEE Trans. Inform. Theory **34**, 1049-1053, 1988.

[5] Munuera, C., Torres, F., *A Goppa-like Bound on the Trellis State Complexity of Algebraic Geometric Codes*, IEEE Trans. Inform. Theory **49**, 733-737, 2003.

[6] Munuera, C., Torres, F., *Bounding the Trellis State Complexity of Algebraic Geometric Codes*, AAECC **15**, 81-100, 2004.

[7] Munuera, C., *On the Generalized Hamming Weights of Geometric Goppa Codes*, IEEE Trans. Inform. Theory **40**, 2092-2099, 1994.

[8] Nori, A. V., *Unifying Views of Tail-Biting Trellises for Linear Block Codes*, Ph.D. Thesis, Indian Institute of Science, 2005.

[9] Pellikaan, R. *On special divisors and the two variable zeta function of algebraic curves over finite fields*, Proceedings AGTC-4, Luminy, Pellikaan, Perret and Vladut, eds., 175-184, 1996.

[10] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

[11] Vardy, A., 'Trellis structure of codes', in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., 1981-2117, 1998.

[12] Wei, V. K., *Generalized Hamming Weights for Linear Codes*, IEEE Trans. Inform. Theory **37**, 1412-1418, 1991.

[13] Yang, K., Kumar, P. V., and Stichtenoth, H., *On the Weight Hierarchy of Geometric Goppa Codes*, IEEE Trans. Inform. Theory **40**, 913-920, 1994.