List Decoding of Lee Metric Codes

Ido Tal

List Decoding of Lee Metric Codes

Research Thesis

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Computer Science

Ido Tal

Submitted to the Senate of
the Technion — Israel Institute of Technology
Tamuz 5763 Haifa July 2003

The research thesis was done under the supervision of Prof. Ronny Roth in the Computer Science Department.

I sincerely thank Prof. Ronny Roth for coming up with an interesting problem for me to pursue, for our discussions which were very helpful in obtaining the research results, for all that I have learned from him, and — last but not least — for his patience and optimism along the way.

A special thank to my wife Smadar for her love and encouragement.

The generous financial help of the Technion is gratefully acknowledged.

Contents

Abstract **1**

Abbreviations and Notations **2**

1 Introduction **3**

1.1 List-ℓ decoders 4

1.2 Hamming and Lee metrics 6

1.3 GRS and alternant codes 7

1.4 List decoding through bivariate polynomials 7

1.5 A Johnson-type bound 10

1.5.1 A Johnson-type bound for the Lee metric 11

1.6 Organization of this work 12

2 A List Decoder for the Lee Metric **13**

2.1 Introduction 13

2.2 Bounding r^* and Δ^* 16

2.3 Maximizing R, for a given Δ 18

2.3.1 An implicit formula for r_Δ 19

2.3.2 Finding λ_Δ 21

2.3.3 Conclusion for fixed Δ 22

2.4 Finding the linear intervals of $R(\theta, \ell)$ 22

2.4.1 Preliminary claims and definitions 24

2.5 Further tightening the bounds 27

2.5.1 Non-tight bounds 28

2.5.2 A tight bound 28

3 Asymptotics **32**

3.1 An implicit formula for w^* 33

3.2 Finding $\Lambda(w^*)$ 35
3.3 Conclusion for the asymptotic case 35

4 Justification for the Score Selection 38

5 Notes 45
5.1 Code and bijection selection 45
5.2 Other decoders 46

A Proof of Proposition 2.16 49
A.1 The $\lambda_\Delta = \lambda_{\Delta+1}$ case 49
A.2 The $\lambda_\Delta = \lambda_{\Delta+1} + 1$ case 50
A.3 The $\lambda_\Delta \geq \lambda_{\Delta+1} + 2$ case 51

B Proof of Lemma A.8 54
B.1 'Mathematica' input for the $\lambda \neq q/2$ case 55
B.2 'Mathematica' input for the $\lambda = q/2$ case 57

Abstract in Hebrew ה

List of Figures

1.1 Generic bivariate polynomial decoding algorithm for $\mathcal{C}$. 9

2.1 Curve $\theta \mapsto R_\Delta(\theta, \ell)$ for $\ell = 5$, $q = 9$, and $\Delta = 1, 2, 3, 4, 5$. . . . 23
2.2 $R(\theta, \ell, r, \Delta, \lambda)$ for different values of r. 25
2.3 Graphical proof of Lemma 2.20. 26
2.4 Graphical proof of Lemma 2.21. 27
2.5 Curve $\theta \mapsto R(\theta, \ell)$ for $q = 9$ and $\ell = 7, 8$. 29
2.6 $x \mapsto r - x\Delta$ versus $x \mapsto r' - x\Delta'$. 30

3.1 Curve $\theta \mapsto R(\theta, \ell)$ and the Johnson bound for $q = 5$ and $\ell = 7, \infty$. 37

4.1 Graph of $\boldsymbol{\mu}$ versus $\boldsymbol{\mu}'$ in Lemma 4.5. 43
4.2 Graph of $\boldsymbol{\mu}$ versus $\boldsymbol{\mu}'$ in Lemma 4.7. 44

5.1 Comparison of decoding radii, for GRS codes. 47
5.2 Comparison of decoding radii, for alternant codes. 48

Abstract

Let F be a finite field and let $\mathcal{C}$ be a subset of F^n, termed a code. A codeword $\mathbf{c} \in \mathcal{C}$ is transmitted over a noisy channel and distorted by an error vector $\mathbf{e}$. We are given $\mathbf{y}$, which is the distorted word ($\mathbf{y} = \mathbf{c} + \mathbf{e}$) and wish to find out what $\mathbf{c}$ was.

A list-ℓ decoder $\mathcal{D} : F^n \to 2^{\mathcal{C}}$ of decoding radius τ with respect to a given metric $\mathsf{d} : F^n \times F^n \to \mathbb{R}$ is a generalization of classical decoding. Given a received word $\mathbf{y}$, the output of the list-ℓ decoder, $\mathcal{D}(\mathbf{y})$, is a list of at most ℓ codewords. This list is guaranteed to contain all codewords in the sphere of radius τ centered at $\mathbf{y}$. Under the assumption that no more than τ errors occurred in $\mathbf{y}$, we are assured that $\mathbf{c}$ is in $\mathcal{D}(\mathbf{y})$, and this is regarded as a decoding success.

In this work, we concentrate on coding for the Lee metric, which appears in applications such as phase shift keying (PSK) modulation. A polynomial-time list decoder in this metric is presented and analyzed for alternant codes, which are subfield sub-codes of generalized Reed-Solomon codes (GRS). We show a formula for the decoding radius as a function of ℓ and the parameters of the underlying GRS code.

We also show that unlike the Hamming metric counterpart, the decoding radius of our list decoder is generally strictly larger than what one gets from the Lee metric version of the Johnson bound.

Abbreviations and Notations

$\mathbb{N}$	—	nonnegative integers (including 0)
$\mathbb{Z}_q$	—	ring of integers modulo q
ℓ	—	maximal list size
$\mathbf{c}$	—	codeword
$\mathbf{y}$	—	received word
$\mathbf{e}$	—	error word
n	—	code length
k	—	dimension of an underlying GRS code
d	—	code minimum distance (in the metric discussed)
$\mathcal{C}$	—	code
$\mathcal{D}$	—	decoder
$\mathrm{GF}(q)$	—	Galois field of size q
$\alpha_1, \alpha_2, \ldots, \alpha_n$	—	code locators of a GRS or alternant code
$v_1, v_2, \ldots, v_n$	—	column multipliers of a GRS or alternant code
F	—	base field of an alternant code
Φ	—	extension field of an underlying GRS code
$\Phi_k[x]$	—	set of all polynomials with degree less than k over Φ
$Q(x, z)$	—	bivariate interpolation polynomial
$\deg_{\mu,\nu} Q(x, z)$	—	(μ, ν)-weighted degree of $Q(x, z)$
$\langle \cdot \rangle$	—	fixed bijection, $\langle \cdot \rangle : F \to \mathbb{Z}_q$
$[n]$	—	the set $\{1, 2, \ldots, n\}$
$\mathcal{M}$	—	multiplicity matrix
$\mathcal{S}_{\mathcal{M}}(\mathbf{c})$	—	the score of codeword $\mathbf{c}$ with respect to $\mathcal{M}$

Chapter 1

Introduction

Suppose we want to transmit information over a noisy channel. The channel typically models a communication line or a storage device. Let F be a finite field. The channel receives as input a vector $\mathbf{x} \in F^n$ and outputs a vector $\mathbf{y} = \mathbf{x} + \mathbf{e} \in F^n$. That is, $\mathbf{y}$ is sometimes a corrupted version of $\mathbf{x}$, where $\mathbf{e}$ — termed the error vector — has a certain probability distribution.

Fix a metric $\mathsf{d} : F^n \times F^n \to \mathbb{N}$, where $\mathbb{N}$ is the set of nonnegative integers. An (n, M, d) (block) code over F is a nonempty subset $\mathcal{C}$ of size M of F^n, where $d = \min_{\mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C}: \mathbf{c}_1 \neq \mathbf{c}_2} \mathsf{d}(\mathbf{c}_1, \mathbf{c}_2)$ is the minimum distance of the code. If $\mathcal{C}$ is a vector space over F, it is termed a linear code with parameters $[n, k, d]$, where $k = \log_{|F|} M$ is the code dimension. Elements of $\mathcal{C}$ are called *codewords.*

A code is used to transmit information over the noisy channel. An *information word* $\mathbf{u}^*$ is encoded via a one-to-one function into a codeword $\mathbf{c}^* \in \mathcal{C}$ and $\mathbf{c}^*$ is sent over the channel. As stated, at the other end of the channel, the output is a received word $\mathbf{y} = \mathbf{c}^* + \mathbf{e}$. Given $\mathbf{y}$, we now need to make an educated guess at the receiving end as to what codeword was sent, and from this — which information word was transmitted.

It is a well-known theorem in coding theory that a sphere in F^n (with respect to the metric d) of radius $(d-1)/2$ that is centered at $\mathbf{y}$ will contain at most one codeword [16, Chapter 1]. Therefore, we may define the function $D : F^n \to \mathcal{C} \cup \{\text{‘e’}\}$ as

$$D(\mathbf{y}) = \begin{cases} \mathbf{c} & \text{if there exists } \mathbf{c} \in \mathcal{C} \text{ such that } \mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \frac{d-1}{2} \\ \text{‘e’} & \text{otherwise} \end{cases} .$$

Note that if $\mathsf{Prob}(\mathsf{d}(\mathbf{c}^*, \mathbf{y}) > (d-1)/2)$ is sufficiently small, we have a reliable means to transmit information over the noisy channel: Upon receiving $\mathbf{y}$, we output $D(\mathbf{y})$, where 'e' is the "decoding-error" symbol. Since $\mathsf{Prob}(\mathsf{d}(\mathbf{c}^*, \mathbf{y}) > (d-1)/2)$ is sufficiently small, $D(\mathbf{y})$ will likely be equal to the transmitted codeword $\mathbf{c}^*$. That is, in most cases, our guess will be correct. We call this method of decoding *classical decoding*.

1.1 List-ℓ decoders

List decoders were introduced by Elias and Wozencraft (see [7]). A list-ℓ decoder $\mathcal{D} : F^n \to 2^{\mathcal{C}}$ of decoding radius τ is a generalization of classical decoding. As before, the input to a list-ℓ decoder is the received word $\mathbf{y}$. However, the output of a list-ℓ decoder is now a set (list) of codewords. This list is guaranteed to contain all codewords in the sphere of radius τ centered at $\mathbf{y}$, namely,

$$\mathcal{D}(\mathbf{y}) \supseteq \{\mathbf{c} \in \mathcal{C} : \mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \tau\} .$$

Also, the list is guaranteed to contain no more than ℓ codewords, i.e.,

$$|\mathcal{D}(\mathbf{y})| \leq \ell .$$

Under the assumption that no more than τ errors occurred in $\mathbf{y}$, we are assured that $\mathbf{c}^* \in \mathcal{D}(\mathbf{y})$.

It will sometimes be convenient to characterize a list-ℓ decoder by its *relative decoding radius* θ. A list-ℓ decoder $\mathcal{D} : F^n \to 2^{\mathcal{C}}$ has a relative decoding radius θ if

$$\mathcal{D}(\mathbf{y}) \supseteq \{\mathbf{c} \in \mathcal{C} : \mathsf{d}(\mathbf{c}, \mathbf{y}) < n\theta\} ,$$

and the list size is at most ℓ. Thus, for a codeword $\mathbf{c} \in \mathcal{C}$, if $\mathsf{d}(\mathbf{y}, \mathbf{c}) < n\theta$, then $\mathbf{c} \in \mathcal{D}(\mathbf{y})$. Note that these two characterizations are essentially equivalent: A list-ℓ decoder has a relative decoding radius θ if and only if it has a decoding radius $\tau = \lceil n\theta \rceil - 1$.

What practical uses do we have for a list-ℓ decoder? To answer this question, let us first define two more decoders. For $\mathbf{y} \in F^n$, define

$$\{D_{\mathrm{NCD}}, D_{\mathrm{MLD}}\} : F^n \to \mathcal{C}$$

as follows:

Nearest Codeword Decoding: $D_{\mathrm{NCD}}(\mathbf{y}) = \mathbf{c}$, where $\mathbf{c} \in \mathcal{C}$ is such that $\mathsf{d}(\mathbf{y}, \mathbf{c})$ is minimal. A nearest codeword decoder is defined in [5, page 10] as a "complete decoder".

Maximum Likelihood Decoding: $D_{\mathrm{MLD}}(\mathbf{y}) = \mathbf{c}$, where $\mathbf{c} \in \mathcal{C}$ is such that $\mathsf{Prob}(\mathbf{y}$ received $\mid \mathbf{c}$ sent$)$ is maximal. For further reference see [8, page 120].

In case of ties, we pick one codeword according to some rule (for instance, the first codeword in some lexicographic order).

Suppose we know the value of $\mathbf{y}$ and the probability distribution of the channel, but nothing else. That is, we have no side information, and thus, $D_{\mathrm{MLD}}(\mathbf{y})$ is the "best guess" as to the value of $\mathbf{c}^*$. We say that the distance function d accurately models the channel if $\mathsf{Prob}(\mathbf{y}$ received $\mid \mathbf{c}$ sent$)$ is a monotonically decreasing function of $\mathsf{d}(\mathbf{y}, \mathbf{c})$. If this is the case, then $D_{\mathrm{NCD}}(\mathbf{y}) = D_{\mathrm{MLD}}(\mathbf{y})$ (for example, this happens when the distance function used is the Hamming metric and the channel is the q-ary symetric channel with crossover probabilty less than $1 - 1/q$). Therefore, an efficient implementation of D_{NCD}, or at least something "close to it" is desirable. Let $\mathcal{D} : F^n \to 2^{\mathcal{C}}$ be a list-ℓ decoder, with decoding radius τ. Define the function $D^{\tau}_{\mathrm{NCD}} : F^n \to \mathcal{C}$ as

$$D^{\tau}_{\mathrm{NCD}}(\mathbf{y}) = \mathbf{c}, \text{ where } \mathbf{c} \in \mathcal{D}(\mathbf{y}) \text{ is such that } \mathsf{d}(\mathbf{c}, \mathbf{y}) \text{ is minimal .}$$

Thus, by the definition of $\mathcal{D}$, we have that $D^{\tau}_{\mathrm{NCD}}(\mathbf{y}) = D_{\mathrm{NCD}}(\mathbf{y})$ whenever $\mathsf{d}(D_{\mathrm{NCD}}(\mathbf{y}), \mathbf{y}) \leq \tau$. Specifically, the latter is true if no more than τ errors occurred in the transmission of $\mathbf{c}^*$.

It might also be the case that we do have some side information. For example, suppose we are transmitting text. In that case, some sequences of codewords results in gibberish, while others do not. A related example: we might know the a posteriori codeword distribution, that is, we know $\mathsf{Prob}(\mathbf{c}$ transmitted$)$ for every $\mathbf{c} \in \mathcal{C}$. A list-$\ell$ decoder could be utilized for these cases as well: we choose from $\mathcal{D}(\mathbf{y})$ the most probable codeword. If d is chosen wisely and the decoding radius τ is large enough, we would generally not be limiting ourselves by considering only the codewords in $\mathcal{D}(\mathbf{y})$, as opposed to all the codewords in $\mathcal{C}$.

1.2 Hamming and Lee metrics

Denote by $[n]$ the set $\{1, 2, \ldots, n\}$. The Hamming distance between two elements x, y in F is simply

$$\mathsf{d}_{\mathcal{H}}(x, y) \triangleq \left\{ \begin{array}{ll} 1 & \text{if } x \neq y \\ 0 & \text{otherwise} \end{array} \right. .$$

Thus, the Hamming distance between two words $\mathbf{x} = (x_i)_{i \in [n]}$ and $\mathbf{y} = (y_i)_{i \in [n]}$ in F^n is simply the number of indexes where the two words are different, that is,

$$\mathsf{d}_{\mathcal{H}}(\mathbf{x}, \mathbf{y}) \triangleq \sum_{i \in [n]} \mathsf{d}_{\mathcal{H}}(x_i, y_i) = |\{i : x_i \neq y_i\}| \ .$$

The Hamming metric is by far the most studied metric in error correcting codes.

A lesser used distance function is the Lee metric [14]. Recall that $F = \mathrm{GF}(q)$, and let $\mathbb{Z}_q$ denote the ring of integers modulo q. Denote by 1 the multiplicative unity in $\mathbb{Z}_q$. The Lee weight of an element $a \in \mathbb{Z}_q$, denoted $|a|$, is defined as the smallest nonnegative integer s such that $s \cdot 1 \in \{a, -a\}$. Fix a bijection $\langle \cdot \rangle : F \to \mathbb{Z}_q$ and define the Lee distance $\mathsf{d}_{\mathcal{L}}$ between two elements x, y in F as

$$\mathsf{d}_{\mathcal{L}}(x, y) \triangleq |\langle x \rangle - \langle y \rangle| \ .$$

The Lee distance between two words $\mathbf{x} = (x_i)_{i \in [n]}$ and $\mathbf{y} = (y_i)_{i \in [n]}$ (over F) is defined as

$$\mathsf{d}_{\mathcal{L}}(\mathbf{x}, \mathbf{y}) \triangleq \sum_{i=1}^{n} \mathsf{d}_{\mathcal{L}}(x_i, y_i) \ .$$

The distance function to be used in a specific case is usually selected based on the characteristics of the channel, as well as the type of modulation used. The Lee metric is a very natural one for an additive white Gaussian noise channel (AWGN), when a phase shift keying modulation is used (PSK) [2, Chapter 8]. One might also consider the Lee metric for use in noisy runlength-limited (RLL) (d, k)-constrained channels, or in channels where spectral-null constraints are desired [22].

1.3 GRS and alternant codes

We will now define the codes which will be used in this work. Fix $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^m)$, and denote by $\Phi_k[x]$ the set of all polynomials over Φ with degree less than k. Hereafter in this work, we fix $\mathcal{C}_{\mathrm{GRS}}$ to be an $[n, k]$ GRS code over Φ with distinct code locators $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Phi$ and nonzero column multipliers $v_1, v_2, \ldots, v_n \in \Phi$, that is,

$$\mathcal{C}_{\mathrm{GRS}} = \{\mathbf{c} = (v_1 u(\alpha_1) \;\; v_2 u(\alpha_2) \;\; \ldots \;\; v_n u(\alpha_n)) \, : \, u(x) \in \Phi_k[x]\} \ .$$

We let $\mathcal{C}_{\mathrm{alt}}$ be the respective alternant code over F, namely, $\mathcal{C}_{\mathrm{alt}} = \mathcal{C}_{\mathrm{GRS}} \cap F^n$.

In the Hamming metric, many efficient classical decoding algorithms are known for GRS and alternant codes [26],[5],[17],[25]. In the Lee metric, a classical decoder for normalized ($v_j = \alpha_j \ , \ j \in [n]$) alternant and normalized GRS codes is presented in [22]. One should also mention the negacyclic codes [2, Chapter 9], introduced by Berlekamp. Berlekamp presented a classical decoding algorithm for negacyclic codes in the Lee metric.

1.4 List decoding through bivariate polynomials

The Welch-Berlekamp algorithm [26] is a classical (list-1) decoder for GRS codes in the Hamming metric, which makes use of bivariate polynomials (see also Berlekamp [3], Blackburn [4], Dabiri and Blake[6], and Ma and Wang [15] for related work). The methods introduced in this section grew out of the 1997 seminal paper by Sudan [24], which generalized the Welch-Berlekamp algorithm. In 1999, Sudan's earlier results were improved by Guruswami and Sudan [10], and further improved in 2000 by Koetter and Vardy [12]. The issue of list decoding for a more general metric is discussed by Koetter and Vardy in [13], which appeared in 2002.

Denote the quantity $(k-1)/n$ as the *modified code rate*. Note that $(k-1)/n$ is approximately the code rate of $\mathcal{C}_{\mathrm{GRS}}$ for large n. However, our discussion will mainly focus on $\mathcal{C}_{\mathrm{alt}}$.

The polynomial-time list-ℓ decoder for $\mathcal{C}_{\mathrm{alt}}$ in [10], [12] is based on the next lemma. Let $\mathcal{M} = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$ be a $q \times n$ matrix over $\mathbb{N}$, whose rows are indexed by the elements of F. The matrix $\mathcal{M}$ is referred to as a *multiplicity matrix*. The *score* of a codeword $\mathbf{c} = (c_j)_{j \in [n]} \in \mathcal{C}_{\mathrm{alt}}$ with respect to $\mathcal{M}$ is defined by

$$\mathcal{S}_{\mathcal{M}}(\mathbf{c}) = \sum_{j=1}^{n} \mathcal{M}_{c_j,j} \ . \tag{1.1}$$

For a nonzero bivariate polynomial $Q(x,z) = \sum_{h,i} Q_{h,i} x^h z^i$ over Φ, let the (μ,ν)-weighted degree of $Q(x,z)$ be given by

$$\deg_{\mu,\nu} Q(x,z) = \max_{h,i \,:\, Q_{h,i} \neq 0} \{ h\mu + i\nu \} \ .$$

Lemma 1.1 *Let ℓ and β be positive integers and $\mathcal{M}$ be a $q \times n$ matrix over $\mathbb{N}$. Suppose there exists a nonzero bivariate polynomial $Q(x,z) = \sum_{h,i} Q_{h,i} x^h z^i$ over Φ that satisfies the degree constraints*

$$\deg_{0,1} Q(x,z) \leq \ell \qquad \textit{and} \qquad \deg_{1,k-1} Q(x,z) < \beta \ , \tag{1.2}$$

and the multiplicity constraints

$$\sum_{h,i} \binom{h}{s}\binom{i}{t} Q_{h,i} \alpha_j^{h-s} (\gamma/v_j)^{i-t} = 0 \ , \quad \gamma \in F \ , \quad j \in [n] \ , \quad 0 \leq s+t < \mathcal{M}_{\gamma,j} \ . \tag{1.3}$$

Then, for every codeword $\mathbf{c} = (v_j u(\alpha_j))_{j \in [n]} \in \mathcal{C}_{\mathrm{alt}}$,

$$\mathcal{S}_{\mathcal{M}}(\mathbf{c}) \geq \beta \qquad \Longrightarrow \qquad (z - u(x)) \,|\, Q(x,z) \ .$$

Also,

$$|\mathbf{c} \in \mathcal{C} \ : \ \mathcal{S}_{\mathcal{M}}(\mathbf{c}) \geq \beta| \leq \ell \ .$$

Equation (1.2) determines the number of significant coefficients in $Q(x,z)$, while Equation (1.3) defines a set of linear homogeneous equations in these coefficients. Clearly, a nonzero solution $Q(x,z)$ exists if the number of coefficients exceeds the number of equations.

Example 1.1 *Let $F = \Phi = \mathrm{GF}(5) = \mathbb{Z}_5$, and fix $\langle\cdot\rangle$ as the identity function. Let $\mathcal{C}$ be an $[n,k]$ GRS code over F, with $n = 4$ and $k = 2$. Fix $\mathbf{y} = (0100)$ as the received word. For $\ell = 6$, we define $Q(x,z)$ by the following $\mathcal{M}$ and β: $\beta = 8$ and*

$$\mathcal{M} = \begin{array}{c} 2 \\ 1 \\ 0 \\ 4 \\ 3 \end{array} \left(\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 3 & 1 & 1 \\ 3 & 1 & 3 & 3 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right) \ .$$

On the one hand, $\mathcal{M}$ *implies* $4 \cdot (\binom{3+1}{2} + \binom{1+1}{2} + \binom{1+1}{2}) = 32$ *linear equations. On the other hand,* $k = 2$*,* $\beta = 8$ *and* $\ell = 6$ *imply* 35 *significant coefficients. Thus, we can construct a nonzero* $Q(x, z)$*.*

Let $\mathbf{c} = (1140)$*. Because* $(\mathcal{S}_{\mathcal{M}}(\mathbf{c}) = 8 \geq \beta)$*, we have that* $\mathbf{c}$ *is in the list.*

Based on Lemma 1.1, the design of a list-ℓ decoder for $\mathcal{C}_{\text{alt}}$ in any given metric can be summarized as follows (see [13]). Find an integer β and a mapping $\mathcal{M} : F^n \to \mathbb{N}^{q \times n}$ such that for the largest possible integer τ, the following two conditions hold for the matrix $\mathcal{M}(\mathbf{y}) = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$ that corresponds to any received word $\mathbf{y}$, whenever a codeword $\mathbf{c} \in \mathcal{C}_{\text{alt}}$ satisfies $\mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \tau$:

(C1) $\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) \geq \beta$.

(C2) The number of coefficients determined by (1.2) exceeds the number of equations in (1.3).

The resulting list-ℓ decoding algorithm is stated in Figure 1.1.

Input: received word $\mathbf{y} \in F^n$, mapping $\mathcal{M} : F^n \to \mathbb{N}^{q \times n}$, constant β, decoding radius τ, list size ℓ.
Output: list of up to ℓ codewords.

1. **Interpolation of $Q(x, z)$:** Find $Q(x, z)$ with coefficients from Φ such that Equations (1.2) and (1.3) are satisfied.

2. **Factorization:** Compute the set U of all polynomials $u(x) \in \Phi_k[x]$ such that $(z - u(x)) | Q(x, z)$.

3. **Output:** Output all $\mathbf{c} \in \mathcal{C}$ such that $\mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \tau$ and there exists $u(x) \in U$ for which $\mathbf{c} = (v_1 u(\alpha_1) \;\; v_2 u(\alpha_2) \;\; v_n u(\alpha_n))$.

Figure 1.1: Generic bivariate polynomial decoding algorithm for $\mathcal{C}$.

Step 1 of the algorithm may be carried out by Gaussian elimination, although more efficient algorithms are known for specific cases [21], [1], [18], [19], [20], [23]. Efficient implementations of Step 2 are known; see for example [21], which takes expected time $O(\ell^2 k(\beta + \log^2 \ell \log(q^m)))$. A straightforward implementation of Step 3 takes $O(\ell k n)$ operations. In this work, we aim at finding β and a mapping $\mathbf{y} \mapsto \mathcal{M}(\mathbf{y})$, such that the decoding radius τ, or alternatively, the relative decoding radius θ, is as large is possible.

1.5 A Johnson-type bound

Fix $F = \mathrm{GF}(q)$ and a distance function d over F^n. For $\mathbf{y} \in F^n$, denote $\mathcal{C}'$ as an $(n, M, d; \theta, \mathbf{y})$ code over F if it is an (n, M, d) code over F, and for every codeword $\mathbf{c} \in \mathcal{C}'$, we have $\mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \theta n$.

We term $\mathcal{J}(M, \theta, q)$ a *Johnson-type bound* [11] for $0 < \theta \leq \chi$ if for every $(n, M, d; \theta, \mathbf{y})$ code over F such that $0 < \theta \leq \chi$,

$$d/n \leq \mathcal{J}(M, \theta, q) \; .$$

We also require that the mapping $\theta \mapsto \mathcal{J}(M, \theta, q)$ is non-decreasing for $0 < \theta \leq \chi$.

We note that such a bound is usually referred to as a *restricted* Johnson bound. It is usually stated for codes $\mathcal{C}'$ such that each codeword $\mathbf{c} \in \mathcal{C}'$ satisfies $\mathsf{d}(\mathbf{c}, \mathbf{y}) = \theta n$. However, we will specify a range $0 < \theta \leq \chi$ such that both the $\leq \theta n$ and the $= \theta n$ bounds are equal.

However, for the $\leq \theta n$ case, the range $0 < \theta \leq \chi$, is usually chosen so that no generality is lost in assuming that $\mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \theta n$. That is, the range of θ is usually chosen such that both bounds are equal.

A Johnson-type bound can also be used to bound from bellow optimal decoding radii.

Proposition 1.2 *Fix $F = \mathrm{GF}(q)$ and a distance function d over F^n. Let $\mathcal{C}$ be an (n, M, d) code over F. Let $\mathcal{J}(M, \theta, q)$ be a Johnson-type bound for $0 < \theta \leq \chi$. For a positive integer $0 < \ell < M$, suppose there exists a smallest $0 < \theta \leq \chi$ such that $d/n = \mathcal{J}(\ell + 1, \theta, q)$, and denote it by θ'. Then, there exists a list-ℓ decoder for $\mathcal{C}$ with relative decoding radius θ'.*

Proof Let θ^* be the largest relative decoding radius attainable by a list-ℓ decoder for $\mathcal{C}$, and let $\mathcal{D}^*$ be the decoder that attains it. If $\theta^* \geq \theta'$ then we are done, since $\mathcal{D}^*$ is the promised decoder.

Assume $\theta^* < \theta'$. From the optimality of θ^*, there exists a received word $\mathbf{y} \in F^n$ such that

$$|\{\mathbf{c} \in \mathcal{C} : \mathsf{d}(\mathbf{y}, \mathbf{c}) \leq \theta^* n\}| \geq \ell + 1 \; .$$

Let $\mathcal{C}'$ be a subset of size $\ell + 1$ of $\{\mathbf{c} \in \mathcal{C} : \mathsf{d}(\mathbf{y}, \mathbf{c}) \leq \theta n\}$. Thus, $\mathcal{C}'$ is an $(n, \ell + 1, d'; \theta^*, \mathbf{y})$ code, where $d' \geq d$. This contradicts the definition of $\mathcal{J}(M, \theta, q)$ and θ'. ■

1.5.1 A Johnson-type bound for the Lee metric

We will now state a Johnson-type bound for the Lee metric. This, in turn, will let us bound the optimal relative decoding radius, θ^*. For the Lee metric, define

$$\chi_{\mathcal{L}}(q) = \begin{cases} q/4 & \text{if } q \text{ is even} \\ (q^2-1)/(4q) & \text{if } q \text{ is odd} \end{cases} , \tag{1.4}$$

and

$$\mathcal{J}_{\mathcal{L}}(M, \theta, q) = \frac{M}{M-1} \cdot \left(2\theta - \frac{\theta^2}{\chi_{\mathcal{L}}(q)} \right) , \quad 0 < \theta \leq \chi_{\mathcal{L}}(q) . \tag{1.5}$$

Notice that $\theta \mapsto \mathcal{J}_{\mathcal{L}}(M, \theta, q)$ is strictly increasing for $0 < \theta \leq \chi_{\mathcal{L}}(q)$. The following is a special case of Lemma 13.62 in [2] (note also Theorem 13.49 therein).

Proposition 1.3 *Fix $F = \mathrm{GF}(q)$, a bijection $\langle \cdot \rangle : F \to \mathbb{Z}_q$, and $\mathsf{d} = \mathsf{d}_{\mathcal{L}}$ as the Lee metric. For $\mathbf{y} \in F^n$ and $0 < \theta \leq \chi_{\mathcal{L}}(q)$, let $\mathcal{C}'$ be an $(n, M, d; \theta, \mathbf{y})$ code over F. Then,*

$$\frac{d}{n} \leq \mathcal{J}_{\mathcal{L}}(M, \theta, q) .$$

For alternant codes we also have the following:

Proposition 1.4 *Fix $F = \mathrm{GF}(q)$, a bijection $\langle \cdot \rangle : F \to \mathbb{Z}_q$, and $\mathsf{d} = \mathsf{d}_{\mathcal{L}}$ as the Lee metric. Let $\mathcal{C}_{\mathrm{GRS}}$ be an $[n, k, d]$ GRS code over $\Phi = \mathrm{GF}(q^m)$, and let $\mathcal{C}_{\mathrm{alt}}$ be the alternant code $\mathcal{C}_{\mathrm{GRS}} \cap F^n$ (over F). Let $\ell > 0$, and suppose $0 < \theta' \leq \chi_{\mathcal{L}}(q)$ is such that*

$$R = \frac{k-1}{n} = 1 - \mathcal{J}_{\mathcal{L}}(\ell + 1, \theta', q) .$$

Then, there exists a list-ℓ decoder for $\mathcal{C}_{\mathrm{alt}}$ with relative decoding radius θ'.

Proof Denote by d' the minimum distance of $\mathcal{C}_{\mathrm{alt}}$. One can easily prove that the minimum Lee distance of a code is always greater than or equal to its minimum Hamming distance. It is a well-known theorem that the minimum Hamming distance of an $[n, k]$ GRS code is $n - k + 1$ [16, page 304]. So, if $\mathsf{d} = \mathsf{d}_{\mathcal{L}}$ and $\mathcal{C}_{\mathrm{GRS}}$ is an $[n, k, d]$ GRS code, then $d' \geq d \geq n - k + 1$. We may now apply Propositions 1.2 and 1.3.

Also, note that for fixed code locators $\alpha_1, \alpha_2, \ldots, \alpha_n$, there exist nonzero column multipliers $v_1, v_2, \ldots, v_n$ such that $d' = d = n - k + 1$. ■

1.6 Organization of this work

In this work, we present a polynomial-time list-ℓ decoder for alternant codes over $F = \mathrm{GF}(q)$ in the Lee metric. For this decoder, we derive a formula for the relative decoding radius θ as a function of the list size ℓ, the code length n, the field size q, and the underlying GRS code dimension k. We also show that unlike the Hamming metric counterpart, the decoding radius of our list decoder is generally strictly larger than what one gets from the Lee metric version of the Johnson bound.

Chapter 2 contains the definition and analysis of our list decoder for the case where ℓ is finite. Chapter 3 is devoted to the asymptotic analysis of the results obtained in Chapter 2, when $\ell \to \infty$. Chapter 3 also contains an asymptotic comparison of the decoding radius obtained by our algorithm and the decoding radius promised by the Lee metric version of the Johnson bound. In Chapter 4, we partially justify the choice of the score matrix made in Chapter 2. Chapter 5 discuses what codes one might choose, and also compares the performance of our decoder to that of other decoders.

Chapter 2

A List Decoder for the Lee Metric

2.1 Introduction

Recall from Section 1.3 that $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^m)$. Define $\mathcal{C}$ as the alternant code:

$$\mathcal{C} = \mathcal{C}_{\mathrm{alt}} = \{\mathbf{c} = (v_1 u(\alpha_1) \;\; v_2 u(\alpha_2) \;\; \ldots \;\; v_n u(\alpha_n)) \,:\, u(x) \in \Phi_k[x]\} \cap F^n \,.$$

We now wish to present a list-ℓ decoder for $\mathcal{C}$ over the Lee metric, based on the general framework outlined in Section 1.4. Let ℓ be the list size, and let r and Δ be positive integers such that $0 < \Delta \le r$. Let $\mathbf{y}$ be the received word. The mapping $\mathbf{y} = (y_j)_{j \in [n]} \mapsto \mathcal{M}(\mathbf{y}) = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$, referred to in Section 1.4, is defined here as

$$\mathcal{M}_{\gamma,j} = \max\{0, r - \mathsf{d}_{\mathcal{L}}(y_j, \gamma) \cdot \Delta\} \,, \quad \gamma \in F \,, \quad j \in [n] \,. \tag{2.1}$$

The choice of this mapping will be justified in Chapter 4. Note that Example 1.1 is consistent with this mapping, for $r = 3$ and $\Delta = 2$

For as yet unspecified parameters λ and θ, define

$$R(\theta, \ell, r, \Delta, \lambda) = \tag{2.2}$$
$$\frac{1}{\binom{\ell+1}{2}} \Big((\ell{+}1)(r{-}\theta\Delta) {-} \tbinom{r+1}{2}(2\lambda{+}1) {+} \tbinom{\lambda+1}{2}\Delta(1{+}2r{-}\tfrac{(2\lambda+1)}{3}\Delta) {+} T \Big) \,,$$

where

$$T = T(r, \Delta, \lambda) = \left\{ \begin{array}{cl} \binom{r-\lambda\Delta+1}{2} & \text{if } \lambda = q/2 \\ 0 & \text{otherwise} \end{array} \right. \,, \tag{2.3}$$

and an expression of the form $\binom{a}{2}$ is shorthand for $a(a-1)/2$ (later on, we wil let the parameters of Equation 2.2 range over the reals). Note that $R(\theta, \ell, r, \Delta, \lambda)$ is a linear function of θ. The following proposition is the basis for our decoder: it provides a choice for β, which, along with the mapping $\mathbf{y} \mapsto \mathcal{M}(\mathbf{y})$ in Equation (2.1), satisfies conditions (C1) and (C2) in Section 1.4.

Proposition 2.1 *For integers $\ell > 0$ and $0 < \Delta \leq r$, define*

$$\Lambda(r, \Delta) = \min\left\{\lfloor r/\Delta \rfloor, \lfloor q/2 \rfloor\right\} , \tag{2.4}$$

and let $\theta = \theta(\ell, r, \Delta)$ be the unique real such that

$$\frac{k-1}{n} = R(\theta, \ell, r, \Delta, \Lambda(r, \Delta)) .$$

Given any nonnegative integer $\tau < n\theta$, conditions (C1) and (C2) are satisfied for

$$\beta = rn - \tau\Delta ,$$

and the mapping $\mathbf{y} = (y_j)_{j \in [n]} \mapsto \mathcal{M}(\mathbf{y}) = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$ defined in Equation (2.1).

Recall that in Example 1.1 we had $\ell = 6$, $q = 5$, $n = 4$, $r = 3$, and $\Delta = 2$. A short calculation shows that $\Lambda(r, \Delta) = 1$, and $\theta(\ell, r, \Delta) = 0.55$. Thus, we choose $\tau = 2 < n\theta$, and $\beta = rn - \tau\Delta = 8$. To sum up, in Example 1.1 we can correct up to 2 errors in the Lee metric.

Note that $\Lambda(r, \Delta)$, and hence $R(\theta, \ell, r, \Delta, \Lambda(r, \Delta))$, are functions of q. However, for the sake of brevity, we will not write this explicitly. The proof of Proposition 2.1 follows from the next three claims.

Claim 2.2 *Fix r, Δ, τ, β, and the mapping $\mathbf{y} = (y_j)_{j \in [n]} \mapsto \mathcal{M}(\mathbf{y}) = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$ as in Proposition 2.1. Let $\mathbf{c} \in \mathcal{C}$ be a codeword and $\mathbf{y} = (y_j)_{j \in [n]}$ be a received word such that $\mathsf{d}_{\mathcal{L}}(\mathbf{c}, \mathbf{y}) \leq \tau$. Then, $\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) \geq rn - \tau\Delta = \beta$.*

Proof Consider the matrix $\mathcal{M}'(\mathbf{y}) = (\mathcal{M}'_{\gamma,j})_{\gamma \in F, j \in [n]}$,

$$\mathcal{M}'_{\gamma,j} = r - \mathsf{d}_{\mathcal{L}}(y_j, \gamma) \cdot \Delta .$$

Obviously, $\mathcal{M}'_{\gamma,j} \leq \mathcal{M}_{\gamma,j}$ for all $\gamma \in F$ and $j \in [n]$, and so $\mathcal{S}_{\mathcal{M}'(\mathbf{y})}(\mathbf{c}) \leq \mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c})$. Notice, however, that $\mathcal{S}_{\mathcal{M}'(\mathbf{y})}(\mathbf{c}) = rn - \mathsf{d}_{\mathcal{L}}(\mathbf{c}, \mathbf{y})\Delta$, and the proof follows. ■

Claim 2.3 *Fix constants r, Δ, and the mapping $\mathbf{y} = (y_j)_{j\in[n]} \mapsto \mathcal{M}(\mathbf{y}) = (\mathcal{M}_{\gamma,j})_{\gamma\in F, j\in[n]}$ as in Proposition 2.1. Let $\lambda = \Lambda(r,\Delta)$ and $T = T(r,\Delta,\lambda)$ be as defined in Equations (2.4) and (2.3), and let $\mathbf{y}$ be a received word. The number of constraints implied by $\mathcal{M}(\mathbf{y})$ in Equation (1.3) is*

$$n\left(\binom{r+1}{2}(2\lambda+1) - \binom{\lambda+1}{2}\Delta(1+2r-\frac{(2\lambda+1)}{3}\Delta) - T\right) . \qquad (2.5)$$

Proof Notice that the number of integer pairs (s,t) such that $0 \le s+t < m$ is $\binom{m+1}{2}$. Thus, the number of constraints implied in Equation (1.3) is

$$\sum_{\gamma\in F,\ j\in[n]} \binom{\mathcal{M}_{\gamma,j}+1}{2} = n\left(\binom{r+1}{2} - T + 2\sum_{i=1}^{\lambda}\binom{r-i\Delta+1}{2}\right) .$$

A straightforward simplification of the sum on the RHS yields the required result. ■

Claim 2.4 *The number of significant coefficients implied by $\beta = rn - \tau\Delta$ in Equation (1.2) is at least*

$$(rn-\tau\Delta)(\ell+1) - (k-1)\binom{\ell+1}{2} . \qquad (2.6)$$

Proof From Equation (1.2) we see that the number of significant coefficients is at least

$$\sum_{i=0}^{\ell}(\beta-(k-1)i) ,$$

and the proof follows. ■

We are now able to prove Proposition 2.1.

Proof of Proposition 2.1 Claim 2.2 ensures that condition (C1) holds. Since $\tau < n\theta$,

$$n\left((r-\theta\Delta)(\ell+1) - \frac{k-1}{n}\binom{\ell+1}{2}\right) \qquad (2.7)$$

is less than Equation (2.6). Note that by the way $\theta = \theta(\ell, r, \Delta)$ is defined, Equation (2.7) is equal to Equation (2.5). Thus, Equation (2.6) is greater than Equation (2.5), and so, condition (C2) holds as well. ■

In light of Proposition 2.1, we now have a method for constructing a list-ℓ decoder for the Lee metric: given the list size ℓ an alternant code $\mathcal{C}$ whose underlying GRS code has modified rate $\frac{k-1}{n}$, pick $0 < \Delta \leq r$ and let θ be such that $\frac{k-1}{n} = R(\theta, \ell, r, \Delta, \Lambda(r, \Delta))$. By Proposition 2.1, we are assured a decoding radius $\tau \geq \lceil n\theta \rceil - 1$. Because we aim at getting a decoding radius that is as large as possible, we will optimize over r and Δ.

We will, however, find it easier to optimize the inverse function, that is, given ℓ and θ, find r and Δ that maximize $R(\theta, \ell, \Delta, \Lambda(r, \Delta))$. The rest of this chapter is devoted to the latter optimization.

Definition 2.1 *For fixed ℓ and θ, we define the pair (r^*, Δ^*), where $r^* = r^*(\theta, \ell)$ and $\Delta^* = \Delta^*(\theta, \ell)$, as the pair (r, Δ) which maximizes the function $R(\theta, \ell, r, \Delta, \Lambda(r, \Delta))$, subject to $0 < \Delta \leq r$. For the sake of uniqueness, in case of ties (several pairs of r and Δ for which the maximum is attained), we pick the pair for which Δ is the smallest, and for that Δ, r is the smallest. Thus, we denote the maximum value of R for given θ and ℓ as*

$$R(\theta, \ell) = R(\theta, \ell, r^*, \Delta^*, \Lambda(r^*, \Delta^*)) \ . \tag{2.8}$$

For the rest of this chapter, let ℓ and θ be fixed. We still need to prove that the above definition is indeed well-defined, i.e., that Δ^* and r^* are bounded. This will follow from the analysis in Section 2.2, where we show that these optimal values satisfy $0 < \Delta^* \leq r^* \leq \ell$. In Section 2.3, we will find a closed formula for the optimal value of r for a *fixed* Δ. This, in turn, will allow us to identify the interval of values of θ for which $\Delta^*(\theta, \ell)$ equals a given value Δ. In particular, we show that $\theta \mapsto R(\theta, \ell)$ is piecewise linear and characterize the intervals where it is linear. Also, in Section 3 we will calculate the asymptotic values of the optimal r and Δ as $\ell \to \infty$.

2.2 Bounding r^* and Δ^*

We will now prove two lemmas, which will lead to the inequality

$$(0 < \Delta^* \leq) \ r^* \leq \ell \ .$$

As a by-product, we will conclude that r^* and Δ^* are indeed well-defined. For fixed ℓ and θ, define $R(r, \Delta, \lambda) = R(\theta, \ell, r, \Delta, \lambda)$.

Lemma 2.5 *Let λ be an integer such that $2 \leq \lambda \leq \lfloor q/2 \rfloor$. Then,*

$$R(r, \Delta, \lambda - 1) \geq R(r, \Delta, \lambda) \ .$$

Proof We have two cases to consider:

Case 1 $\lambda = q/2$: In this case,

$$R(r, \Delta, \lambda - 1) - R(r, \Delta, \lambda) = \frac{2}{\ell(\ell + 1)}(r - \lambda\Delta + 1)(r - \lambda\Delta) \ ,$$

which is negative if and only if $\lambda\Delta - 1 < r < \lambda\Delta$. This completes the proof in this case, since r, Δ, and λ are all integers.

Case 2 $\lambda < q/2$: In this case,

$$R(r, \Delta, \lambda - 1) - R(r, \Delta, \lambda) = \frac{1}{\ell(\ell + 1)}(r - \lambda\Delta + 1)(r - \lambda\Delta) \ .$$

Up to a factor of 2, this is exactly the same expression as in Case 1, and the proof follows.

■

Lemma 2.6 *Let r and Δ be such that $0 < \Delta \leq r$ and $r > \ell$. Then there exist $0 < r' < r$ and $0 < \Delta' \leq \min\{r', \Delta\}$ such that $R(r', \Delta', \Lambda(r', \Delta')) \geq R(r, \Delta, \Lambda(r, \Delta))$, where $\Lambda(\cdot, \cdot)$ is given by Equation (2.4).*

Proof Denote $\lambda = \Lambda(r, \Delta)$, $\lambda' = \Lambda(r', \Delta')$, and $i = r - \ell - 1$. There are two cases to consider:

Case 1 $\Delta \leq r - 1$: Let $r' = r - 1$ and $\Delta' = \Delta$. We will first prove that $R(r', \Delta', \lambda) \geq R(r, \Delta, \lambda)$.

- If $\lambda = q/2$, then

$$\begin{aligned} & R(r', \Delta', \lambda) - R(r, \Delta, \lambda) \\ = \ & \frac{2}{\ell(\ell + 1)}(i + 2i\lambda + \lambda(2 - \Delta + 2\ell - \lambda\Delta)) \\ \geq \ & \frac{2}{\ell(\ell + 1)}(i\lambda + (\lambda - 1) + \ell(\lambda - 1)) \\ \geq \ & 0 \ , \end{aligned}$$

where the first inequality follows from $\lambda\Delta \leq r$.

- On the other hand, if $\lambda < q/2$, then

$$\begin{aligned} & R(r', \Delta', \lambda) - R(r, \Delta, \lambda) \\ = \ & \frac{2}{\ell(\ell+1)}(-1 - \ell + 2(1+i)\lambda + 2\ell\lambda - (1+i+\ell)\lambda) \\ \geq \ & \frac{2}{\ell(\ell+1)}(i\lambda + (\lambda - 1) + \ell(\lambda - 1)) \\ \geq \ & 0 \ . \end{aligned}$$

From the fact that $\lambda' \leq \lambda$ and Lemma 2.5 we conclude that

$$R(r', \Delta', \lambda') \geq R(r', \Delta', \lambda) \geq R(r, \Delta, \lambda) \ .$$

Case 2 $\Delta = r$: Let $r' = r - 1$ and $\Delta' = \Delta - 1$. Note that $\lambda = \lambda' = 1$. Thus,

$$R(r', \Delta', \lambda') - R(r, \Delta, \lambda) = \frac{2}{\ell(\ell+1)}(i + \theta + \ell\theta) \ .$$

This expression is obviously nonnegative, and the proof follows.

■

From Lemma 2.6 we conclude that r^* and Δ^* are indeed well-defined, or, more specifically, that:

Corollary 2.7 *For a specified θ and ℓ, $0 < \Delta^* \leq r^* \leq \ell$.*

Thus, we have a finite search space.

2.3 Maximizing R, for a given Δ

As stated earlier, we wish to maximize $R(r, \Delta, \Lambda(r, \Delta))$, subject to $0 < \Delta \leq r$. Unfortunately, we have no closed formulas for the maximizing values r^* and Δ^*. However, if we *fix* Δ, we can state a "fixed Δ" version of the above-mentioned optimization problem, which we do know how to solve. Since Δ^* is such that $0 < \Delta^* \leq \ell$, we will be able to solve the non-fixed optimization problem (finding Δ^* and r^*) in $O(\ell)$ time. Building on these results, in Section 2.4 we will obtain a full characterization of the linear intervals of the piecewise linear function $R(\theta, \ell)$. This characterization will enable us to solve the non-fixed optimization problem in $O(\log \ell)$ time. The "fixed case" counterpart of the above-mentioned optimization problem is as follows:

Definition 2.2 *For fixed ℓ, θ, and $\Delta > 0$, we define $r_\Delta = r_\Delta(\theta, \ell, \Delta)$ as the value of r that maximizes $R(\theta, \ell, r, \Delta, \Lambda(r, \Delta))$, subject to $0 < \Delta \leq r$. For the sake of uniqueness, in case of ties (several values of r for which the maximum is attained), we pick the smallest value of r.*

Note that by Equation (2.4), $\Lambda(r, \Delta) = \lfloor \frac{q}{2} \rfloor$ for $r \geq \Delta \lfloor \frac{q}{2} \rfloor$. Note also that $R(r, \Delta, \lfloor \frac{q}{2} \rfloor)$ is a convex quadratic polynomial when viewed as a function of r, by Equation (2.2). Therefore, r_Δ is indeed well-defined. Also, note that the above-mentioned "fixed Δ" optimization problem isn't actually affected by the value of θ, again by Equation (2.2).

Suppose for what follows that Δ is fixed. We will find r_Δ and $\lambda_\Delta = \Lambda(r_\Delta, \Delta)$. We will do this in two steps: we will first find the value of λ_Δ, and from this deduce r_Δ. The order of exposition, however, will be reversed: we will first find r_Δ, as a function of λ_Δ; from this derivation of r_Δ, we will deduce λ_Δ.

Lemma 2.8 *Let Δ be such that $\Delta \leq \ell$. Then $r_\Delta \leq \ell$.*

Proof Assume that $r_\Delta > \ell$, the rest of the proof is very much along the same lines as Case 1 of Lemma 2.6. ■

2.3.1 An implicit formula for r_Δ

Fix $\ell \geq 1$, $1 \leq \Delta \leq \ell$, $1 \leq \lambda \leq \lfloor q/2 \rfloor$, and recall that for every r, the function $\theta \mapsto R(\theta, \ell, r, \Delta, \lambda)$ is linear, specifically,

$$R(\theta, \ell, r, \Delta, \lambda) = R(0, \ell, r, \Delta, \lambda) - \frac{2\Delta}{\ell}\theta \; . \tag{2.9}$$

From Equation (2.2) we obtain that the mapping $r \mapsto R(0, \ell, r, \Delta, \lambda)$ is a $\cap$-concave quadratic polynomial. Denote by $\xi_\Delta(\lambda)$ the integer value of r for which $R(0, \ell, r, \Delta, \lambda)$ is maximized (the smallest such integer, in case of ties). From the definition of $\xi_\Delta(\lambda)$ and the $\cap$-concavity of $r \mapsto R(0, \ell, r, \Delta, \lambda)$, we have the following:

Lemma 2.9 *Fix $\ell \geq 1$, $1 \leq \Delta \leq \ell$, $1 \leq \lambda \leq \lfloor q/2 \rfloor$. Let r be an integer. Then,*

$$R(r+1, \Delta, \lambda) \leq R(r, \Delta, \lambda) \iff r \geq \xi_\Delta(\lambda) \; , \tag{2.10}$$

and

$$R(r-1, \Delta, \lambda) < R(r, \Delta, \lambda) \iff r \leq \xi_\Delta(\lambda) \; . \tag{2.11}$$

We can also derive a closed formula for $\xi_\Delta(\lambda)$:

$$\xi_\Delta(\lambda) = \left\{ \begin{array}{cl} \lfloor (\ell + \Delta\lambda^2)/(2\lambda) \rfloor & \text{if } \lambda = q/2 \\ \lfloor (\ell + \Delta(\lambda^2 + \lambda))/(2\lambda + 1) \rfloor & \text{otherwise} \end{array} \right. . \tag{2.12}$$

We will now prove that $r_\Delta = \xi_\Delta(\lambda_\Delta)$, for $0 < \Delta \leq \ell$.

Lemma 2.10 *For $\Delta \geq 1$, we have $r_\Delta \geq \xi_\Delta(\lambda_\Delta)$*

Proof Let $\lambda = \lambda_\Delta$. Define γ as the largest value of r' for which $\lambda = \Lambda(r', \Delta)$. Note that γ might be ∞, namely $\gamma = \infty$ if and only if $\lambda = \lfloor q/2 \rfloor$.

Let $r = r_\Delta$. We will first prove that $R(r + 1, \Delta, \lambda) \leq R(r, \Delta, \lambda)$.

- If $r < \gamma$, then, by the definition of r_Δ, $R(r + 1, \Delta, \lambda) \leq R(r, \Delta, \lambda)$.
- if $r = \gamma$ (namely, $\lambda < \lfloor q/2 \rfloor$ and $r = (\lambda+1)\Delta - 1$), then, by the definition of r_Δ, $R(r+1, \Delta, \lambda+1) \leq R(r, \Delta, \lambda)$. But from Equation (2.2), for any integers r, $\Delta > 0$, and $0 < \lambda < \lfloor q/2 \rfloor$, such that $r = (\lambda + 1)\Delta - 1$, we have that $R(r + 1, \Delta, \lambda) = R(r + 1, \Delta, \lambda + 1)$.

Finally, it follows Equation (2.10) that $r \geq \xi_\Delta(\lambda)$. ■

Lemma 2.11 *For $1 \leq \Delta \leq \ell$, we have $r_\Delta \leq \xi_\Delta(\lambda_\Delta)$.*

Proof Let $\lambda = \lambda_\Delta$. Define β as the smallest value of r' for which $\lambda = \Lambda(r', \Delta)$. We will first prove that $R(r - 1, \Delta, \lambda) < R(r, \Delta, \lambda)$.

- If $r > \beta$, then, by the definition of r_Δ, $R(r - 1, \Delta, \lambda) < R(r, \Delta, \lambda)$.
- If $r = \beta$ and $r > \Delta$ (and so, $\lambda \geq 2$), then, by the definition of r_Δ, $R(r - 1, \Delta, \lambda - 1) < R(r, \Delta, \lambda)$. But from Lemma 2.5 we readily get that $R(r - 1, \Delta, \lambda - 1) \geq R(r - 1, \Delta, \lambda)$.
- If $r = \beta$ and $r = \Delta$ (and so, $\lambda = 1$), then

  $$R(r, \Delta, \lambda) - R(r - 1, \Delta, \lambda) = \frac{2}{\ell(\ell + 1)}(1 + \ell - r) .$$

  From Lemma 2.8 we get that $R(r - 1, \Delta, \lambda) < R(r, \Delta, \lambda)$.

Finally, it follows Equation (2.11) that $r \leq \xi_\Delta(\lambda)$. ■

Proposition 2.12 *For $\Delta \leq \ell$, let $\lambda = \lambda_\Delta$. Then*

$$r_\Delta = \left\{ \begin{array}{cl} \lfloor (\ell + \Delta\lambda^2)/(2\lambda) \rfloor & \textit{if } \lambda = q/2 \\ \lfloor (\ell + \Delta(\lambda^2 + \lambda))/(2\lambda + 1) \rfloor & \textit{otherwise} \end{array} \right. . \tag{2.13}$$

Proof Immediate from Equation (2.12), and Lemmas 2.10 and 2.11. ■

2.3.2 Finding λ_Δ

We will now use Proposition 2.12 to find λ_Δ.

Lemma 2.13 *For every integer $a > 0$ and real x*

$$\left\lfloor \frac{\lfloor x \rfloor}{a} \right\rfloor = \left\lfloor \frac{x}{a} \right\rfloor .$$

Proof This is a special case of Equation (3.11) on page 72 of [9]. ■

Proposition 2.14 *For every $0 < \Delta \le \ell$,*

$$\lambda_\Delta = \min\left\{ \left\lfloor \sqrt{\ell/\Delta} \right\rfloor, \lfloor q/2 \rfloor \right\} .$$

Proof Let $\lambda = \lambda_\Delta$ and $r = r_\Delta$. Define

$$\bar{\lambda} = \lfloor r/\Delta \rfloor ,$$

and recall that $\lambda = \min\left\{\bar{\lambda}, \lfloor q/2 \rfloor\right\}$.

We now have two cases to consider:

Case 1 $\lambda < \lfloor q/2 \rfloor$, and so, $\bar{\lambda} = \lambda$: In this case, $r = \left\lfloor \frac{\ell + \Delta(\lambda^2+\lambda)}{2\lambda+1} \right\rfloor$ and $\lambda = \lfloor r/\Delta \rfloor$. Thus,

$$\lambda = \left\lfloor \frac{\left\lfloor \frac{\ell+\Delta(\lambda^2+\lambda)}{2\lambda+1} \right\rfloor}{\Delta} \right\rfloor$$
$$\Updownarrow$$
$$\lambda = \left\lfloor \frac{\frac{\ell+\Delta(\lambda^2+\lambda)}{2\lambda+1}}{\Delta} \right\rfloor$$
$$\Updownarrow$$
$$\lambda \le \frac{\ell+\Delta(\lambda^2+\lambda)}{\Delta(2\lambda+1)} < \lambda + 1$$
$$\Updownarrow$$
$$\lambda \le \sqrt{\frac{\ell}{\Delta}} < \lambda + 1$$
$$\Updownarrow$$
$$\lambda = \left\lfloor \sqrt{\ell/\Delta} \right\rfloor .$$

Note that the first "if and only if" is explained by Lemma 2.13.

Case 2 $\lambda = \lfloor q/2 \rfloor$, and so, $\bar{\lambda} \geq \lambda$: Note that in this case we have that $r = \left\lfloor \frac{\ell+\Delta(\lambda^2+\lambda)}{2\lambda+1} \right\rfloor$ if q is odd and $r = \left\lfloor \frac{\ell+\Delta\lambda^2}{2\lambda} \right\rfloor$ if q is even. Either way, by a derivation similar to the one in Case 1, we have that the following holds:

$$\lambda \leq \lfloor r/\Delta \rfloor$$
$$\Updownarrow$$
$$\lambda \leq \left\lfloor \sqrt{\ell/\Delta} \right\rfloor .$$

In both Case 1 and Case 2 we have that $\lambda = \min\left\{ \left\lfloor \sqrt{\ell/\Delta} \right\rfloor, \lfloor q/2 \rfloor \right\}$. ■

2.3.3 Conclusion for fixed Δ

Propositions 2.12 and 2.14 lead to the following result.

Proposition 2.15 *For any fixed* $0 < \Delta \leq \ell$*, let*

$$\lambda = \min\left\{ \left\lfloor \sqrt{\ell/\Delta} \right\rfloor, \lfloor q/2 \rfloor \right\} .$$

Then

$$r_\Delta = \begin{cases} \lfloor (\ell + \Delta\lambda^2)/(2\lambda) \rfloor & \textit{if } \lambda = q/2 \\ \lfloor (\ell + \Delta(\lambda^2+\lambda))/(2\lambda+1) \rfloor & \textit{otherwise} \end{cases} \tag{2.14}$$

and

$$\lambda_\Delta = \lambda . \tag{2.15}$$

2.4 Finding the linear intervals of $R(\theta, \ell)$

Recall that

$$R(\theta, \ell) = \max_{r,\Delta} \{ R(\theta, \ell, r, \Delta, \Lambda(r, \Delta)) : 0 < \Delta \leq r \} .$$

Also, for fixed $\Delta > 0$, define $R_\Delta(\theta, \ell) = R(\theta, \ell, r_\Delta, \Delta, \lambda_\Delta)$, where r_Δ and λ_Δ are defined in Equation (2.14) and Equation (2.15), respectively. From Proposition 2.15 we arrive at the following simplification for $R(\theta, \ell)$:

$$R(\theta, \ell) = \max_{\Delta} \{ R_\Delta(\theta, \ell) : 0 < \Delta \leq \ell \} .$$

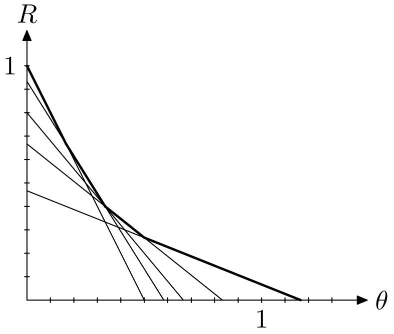

Figure 2.1: Curve $\theta \mapsto R_\Delta(\theta, \ell)$ for $\ell = 5$, $q = 9$, and $\Delta = 1, 2, 3, 4, 5$.

Note that for fixed ℓ, $R_\Delta(\theta, \ell)$ is simply a linear function with slope $-2\Delta/\ell$. Thus, $R(\theta, \ell)$ is a piecewise linear function, with at most ℓ linear intervals. Or, put another way, $R_\Delta(\theta, \ell)$ is the envelope formed by ℓ linear functions. See Figure 2.1 for a graphical representation.

Let ℓ be fixed. A natural question to ask is: For a given $0 < \Delta \leq \ell$, what is the interval $I_\Delta(\ell)$ such that

$$R(\theta, \ell) = R_\Delta(\theta, \ell) \iff \theta \in I_\Delta(\ell) \ .$$

Note that $I_\Delta(\ell)$ might be empty. The set of intervals $I_\Delta(\ell)$ completely defines $R(\theta, \ell)$, in particular, $\Delta^*(\theta, \ell)$ is the smallest Δ for which $\theta \in I_\Delta(\ell)$, and by Proposition 2.15, if we know Δ^*, we know r^* as well (Δ^* and r^* are defined in Definition 2.1). Thus, we would like a fast method for determining the smallest Δ for which $\theta \in I_\Delta$. For fixed ℓ and $0 < \Delta < \ell$, define $\theta_{\Delta,\Delta+1}(\ell)$ as the unique θ for which the two linear functions $\theta \mapsto R_\Delta(\theta, \ell)$ and $\theta \mapsto R_{\Delta+1}(\theta, \ell)$ intersect. This section is devoted to proving the following proposition:

Proposition 2.16 *Let* $1 < \Delta < \ell$. *Then,*

$$\theta_{\Delta,\Delta+1}(\ell) \leq \theta_{\Delta-1,\Delta}(\ell) \ . \tag{2.16}$$

Hence, for $1 < \Delta < \ell$,

$$I_\Delta(\ell) = [\theta_{\Delta,\Delta+1}(\ell), \theta_{\Delta-1,\Delta}(\ell)] \ .$$

Given this, we can find Δ^* by a binary search, which would take $O(\log \ell)$ time. Also, note that we have a closed formula for $\theta_{\Delta,\Delta+1}(\ell)$, and thus one for

$I_\Delta(\ell)$ as well. Therefore, we have an explicit characterization of the piecewise linear function $\theta \mapsto R(\theta, \ell)$. Conversely, we also have an explicit characterization of the inverse function, which maps $\frac{k-1}{n}$ to the optimal relative decoding radius θ.

2.4.1 Preliminary claims and definitions

Fix $\ell \geq 1$, $1 \leq \Delta \leq \ell$, $1 \leq \lambda \leq \lfloor q/2 \rfloor$, and recall the following four facts from Subsection 2.3.1: For every r, the function $\theta \mapsto R(\theta, \ell, r, \Delta, \lambda)$ is linear (Equation (2.9)). The univariate function $r \mapsto R(0, \ell, r, \Delta, \lambda)$ is a $\cap$-concave quadratic polynomial. We've defined $\xi_\Delta(\lambda)$ as the integer value of r for which $R(0, \ell, r, \Delta, \lambda)$ is maximized (the smallest such integer, in case of ties). A formula for $\xi_\Delta(\lambda)$ is given by Equation (2.12).

We denote by $\rho_\Delta(\lambda)$ the real value of r for which $R(0, \ell, r, \Delta, \lambda)$ is maximized. By Equation (2.2),

$$\rho_\Delta(\lambda) = \left\{ \begin{array}{cl} (\ell + \Delta\lambda^2 + 1 - \lambda)/(2\lambda) & \text{if } \lambda = q/2 \\ (\ell + \Delta(\lambda^2 + \lambda) + \frac{1}{2} - \lambda)/(2\lambda + 1) & \text{otherwise} \end{array} \right. . \tag{2.17}$$

Claim 2.17 *Let $\ell \geq 1$, $1 \leq \Delta \leq \ell$, and $1 \leq \lambda \leq \lfloor q/2 \rfloor$. Then*

$$R(0, \ell, \rho_\Delta(\lambda), \Delta, \lambda) \geq R(0, \ell, \xi_\Delta(\lambda), \Delta, \lambda) .$$

Proof By definition, the optimization of R over the integers is a restriction of the more general problem, the optimization of R over the reals. ■

Define $\zeta_\Delta(\lambda) = \rho_\Delta(\lambda) + \frac{1}{2}$,

$$\zeta_\Delta(\lambda) = \left\{ \begin{array}{cl} (\ell + \Delta\lambda^2 + 1)/(2\lambda) & \text{if } \lambda = q/2 \\ (\ell + \Delta(\lambda^2 + \lambda) + 1)/(2\lambda + 1) & \text{otherwise} \end{array} \right. . \tag{2.18}$$

Claim 2.18 *Let $\ell \geq 1$, $1 \leq \Delta \leq \ell$, and $1 \leq \lambda \leq \lfloor q/2 \rfloor$. Then*

$$R(0, \ell, \xi_\Delta(\lambda), \Delta, \lambda) \geq R(0, \ell, \zeta_\Delta(\lambda), \Delta, \lambda) .$$

Proof Recall that $r \mapsto R(0, \ell, r, \Delta, \lambda)$ is a $\cap$-concave quadratic polynomial, which takes its maximum at $r = \rho_\Delta(\lambda)$, and $\xi_\Delta(\lambda)$ is the closest integer to $\rho_\Delta(\lambda)$ (the smaller one, in case of ties). Therefore,

$$|\rho_\Delta(\lambda) - \xi_\Delta(\lambda)| \leq \frac{1}{2} = |\rho_\Delta(\lambda) - \zeta_\Delta(\lambda)| ,$$

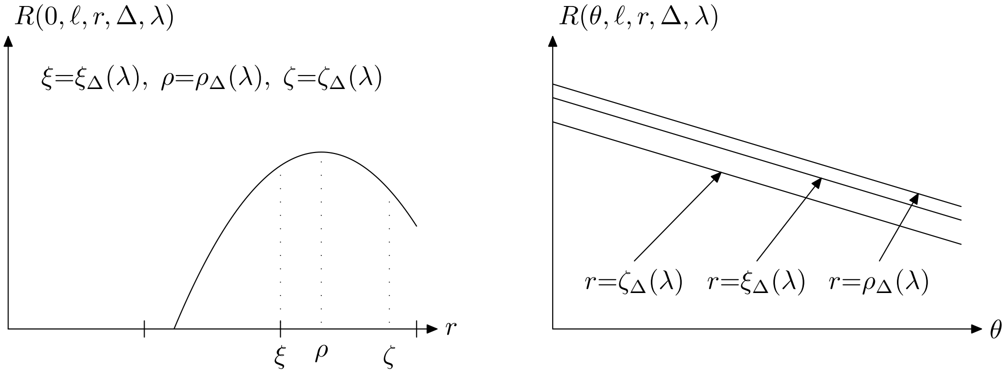

Figure 2.2: Left: R as a function of r, with all other parameters fixed. The tick marks on the r-axis designate integers. Right: Three graphs of R as a function of θ. Each graph has a different r, all other parameters are fixed.

and the proof follows. Claims 2.17 and 2.18 are portrayed in Figure 2.2 (left). Figure 2.2 (right) follows from Claims 2.17 and 2.18, as well as Equation (2.9). ■

Claim 2.19 *Let* $1 \le \Delta \le \ell$ *and* $1 \le \lambda \le \lambda_\Delta$. *Then*

$$R(0,\ell,\xi_\Delta(\lambda),\Delta,\lambda) \ge R(0,\ell,r_\Delta,\Delta,\lambda_\Delta)\ .$$

Proof We have $R(0,\ell,\xi_\Delta(\lambda),\Delta,\lambda) \ge R(0,\ell,r_\Delta,\Delta,\lambda) \ge R(0,\ell,r_\Delta,\Delta,\lambda_\Delta)$, where the second inequality follows from Lemma 2.5. ■

For $\Delta \neq \Delta'$ and $\ell \ge 1$, define $\theta_{\Delta,\Delta'}(\ell,r,r',\lambda,\lambda')$ as the unique real such that

$$\theta = \theta_{\Delta,\Delta'}(\ell,r,r',\lambda,\lambda') \iff R(\theta,\ell,r,\Delta,\lambda) = R(\theta,\ell,r',\Delta',\lambda')\ .$$

Equivalently,

$$\theta_{\Delta,\Delta'}(\ell,r,r',\lambda,\lambda') = \ell \cdot \frac{R(0,\ell,r,\Delta,\lambda) - R(0,\ell,r',\Delta',\lambda')}{2(\Delta-\Delta')}\ . \tag{2.19}$$

Note that under this definition,

$$\theta_{\Delta,\Delta+1}(\ell) = \theta_{\Delta,\Delta+1}(\ell,r_\Delta,r_{\Delta+1},\lambda_\Delta,\lambda_{\Delta+1})\ .$$

Lemmas 2.20 and 2.21 will let us bound $\theta_{\Delta,\Delta+1}(\ell)$ from above and below, respectively. These bounds will subsequently be used in the proof of Proposition 2.16.

Lemma 2.20 *Let $\ell \geq 1$ and $1 \leq \Delta < \ell$. Then*

$$\theta_{\Delta,\Delta+1}(\ell) \leq \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda_\Delta), \rho_{\Delta+1}(\lambda_{\Delta+1}), \lambda_\Delta, \lambda_{\Delta+1}) \ .$$

Proof From Equation (2.19):

$$\begin{aligned}
&\theta_{\Delta,\Delta+1}(\ell) = \theta_{\Delta,\Delta+1}(\ell, r_\Delta, r_{\Delta+1}, \lambda_\Delta, \lambda_{\Delta+1}) && (2.20)\\
&\quad = \frac{\ell}{2}(R(0, \ell, r_{\Delta+1}, \Delta+1, \lambda_{\Delta+1}) - R(0, \ell, r_\Delta, \Delta, \lambda_\Delta)) \\
&\theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda_\Delta), \rho_{\Delta+1}(\lambda_{\Delta+1}), \lambda_\Delta, \lambda_{\Delta+1}) && (2.21)\\
&\quad = \frac{\ell}{2}(R(0, \ell, \rho_{\Delta+1}(\lambda_{\Delta+1}), \Delta+1, \lambda_{\Delta+1}) - R(0, \ell, \zeta_\Delta(\lambda_\Delta), \Delta, \lambda_\Delta)) \ .
\end{aligned}$$

We must now prove that the RHS of Equation (2.20) is less than or equal to the RHS of Equation (2.21). This follows from Claims 2.17 and 2.18. Note that $\xi_\Delta(\lambda_\Delta) = r_\Delta$ and $\xi_{\Delta+1}(\lambda_{\Delta+1}) = r_{\Delta+1}$. For a graphical proof see Figure 2.3. ■

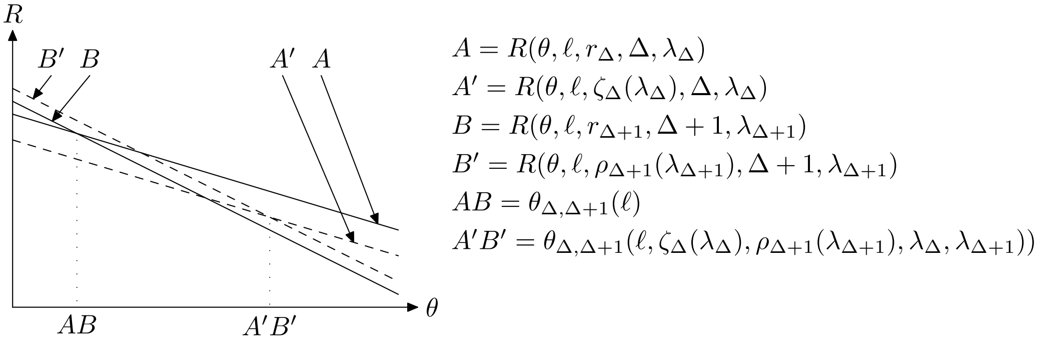
R
B'
B
A'
A
θ
AB
$A'B'$
$A = R(\theta, \ell, r_\Delta, \Delta, \lambda_\Delta)$
$A' = R(\theta, \ell, \zeta_\Delta(\lambda_\Delta), \Delta, \lambda_\Delta)$
$B = R(\theta, \ell, r_{\Delta+1}, \Delta+1, \lambda_{\Delta+1})$
$B' = R(\theta, \ell, \rho_{\Delta+1}(\lambda_{\Delta+1}), \Delta+1, \lambda_{\Delta+1})$
$AB = \theta_{\Delta,\Delta+1}(\ell)$
$A'B' = \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda_\Delta), \rho_{\Delta+1}(\lambda_{\Delta+1}), \lambda_\Delta, \lambda_{\Delta+1}))$

Figure 2.3: Graphical proof of Lemma 2.20.

Lemma 2.21 *Let $\ell \geq 1$ and $1 < \Delta \leq \ell$. Then*

$$\theta_{\Delta-1,\Delta}(\ell) \geq \theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda_\Delta), \zeta_\Delta(\lambda_\Delta), \lambda_\Delta, \lambda_\Delta) \ .$$

Proof From Equation (2.19):

$$
\begin{aligned}
\theta_{\Delta-1,\Delta}(\ell) &= \theta_{\Delta-1,\Delta}(\ell, r_{\Delta-1}, r_{\Delta}, \lambda_{\Delta-1}, \lambda_{\Delta}) && (2.22)\\
&= \frac{\ell}{2}(R(0,\ell,r_{\Delta},\Delta,\lambda_{\Delta}) - R(0,\ell,r_{\Delta-1},\Delta-1,\lambda_{\Delta-1})) \\
\theta_{\Delta-1,\Delta}(\ell,\rho_{\Delta-1}(\lambda_{\Delta}),\zeta_{\Delta}(\lambda_{\Delta}),\lambda_{\Delta},\lambda_{\Delta}) & && (2.23)\\
&= \frac{\ell}{2}(R(0,\ell,\zeta_{\Delta}(\lambda_{\Delta}),\Delta,\lambda_{\Delta}) - R(0,\ell,\rho_{\Delta-1}(\lambda_{\Delta}),\Delta-1,\lambda_{\Delta}))\ .
\end{aligned}
$$

We must now prove that the RHS of Equation (2.22) is greater than or equal to the RHS of Equation (2.23). From Proposition 2.14, $\lambda_{\Delta-1} \geq \lambda_{\Delta}$. The proof follows from Claims 2.17, 2.18, and 2.19. Note that $\xi_{\Delta}(\lambda_{\Delta}) = r_{\Delta}$ and $\xi_{\Delta-1}(\lambda_{\Delta-1}) = r_{\Delta-1}$. For a graphical proof see Figure 2.4. ■

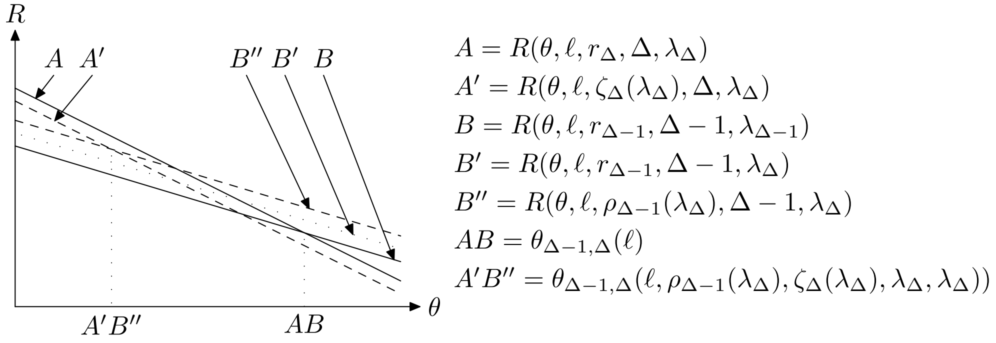

Figure 2.4: Graphical proof of Lemma 2.21.

We defer the proof of Proposition 2.16 to Appendix A. The proof involves three cases, namely: $\lambda_{\Delta} = \lambda_{\Delta+1}$, $\lambda_{\Delta} = \lambda_{\Delta+1} + 1$, and $\lambda_{\Delta} \geq \lambda_{\Delta+1} + 2$. The proof relies on Lemmas 2.20 and 2.21.

2.5 Further tightening the bounds

In this section, we review the bounds used in Section 2.1. In Subsection 2.5.1 we point out that certain bounds are not tight. As we will see, some of this slackness comes with a price (which is not too high). In Subsection 2.5.2 we show that one of the bounds is tight, when we are dealing with optimal values of r and Δ. Thus, Subsection 2.5.1 deals with directions one might choose to take in an attempt to improve the results in this thesis, while Subsection 2.5.2 points out that one direction is a dead-end.

2.5.1 Non-tight bounds

In Claim 2.3 we've bounded from above the number of linear constraints implied by Equation (1.3). Claim 2.3 was subsequently used in the derivation of $R(\theta, \ell, r, \Delta, \Lambda(r, \Delta))$. The number of linear constraints was bounded by

$$\sum_{\gamma \in F,\, j \in [n]} \binom{\mathcal{M}_{\gamma,j} + 1}{2} .$$

Note that this bound might not be tight. The linear equations might be linearly dependent. Moreover, a linear constraint of the form

$$\sum_{h,i} \tbinom{h}{s} \tbinom{i}{t} Q_{h,i} \alpha_j^{h-s}$$

is identically zero for $t > \ell$, as implied by Equation (1.2). Thus, it should not be counted as a linear equation.

On the other hand, in Claim 2.6, which was also used in the derivation of $R(\theta, \ell, r, \Delta, \Lambda(r, \Delta))$, we've bounded from below the number of significant coefficients implied by Equation (1.2). This bound was

$$\sum_{i=0}^{\ell} (\beta - (k-1)i) = (\ell+1)\beta - (k-1)\binom{\ell+1}{2} .$$

Note that if $\beta - (\ell+1)(k+1) < 0$, then the bound is not tight.

We expect $R(\theta, \ell)$ to increase as ℓ grows (every list-$(\ell+1)$ decoder is also a list-ℓ decoder), and this is generally the case. However, because of the non-tight bound on the number of significant coefficients, there are cases where the opposite happens. As an example, take $\theta = 0.8$ and $q = 9$. For these values, $R(\theta, \ell = 7) = 0.164$, as opposed to $R(\theta, \ell = 8) = 0.1611$ (see Figure 2.5).

2.5.2 A tight bound

The following Lemma will show that the bound used in Claim 2.2 is tight for optimal values of r and Δ. If this had not been the case, we might have been able to use this slackness in order to improve the decoding radius.

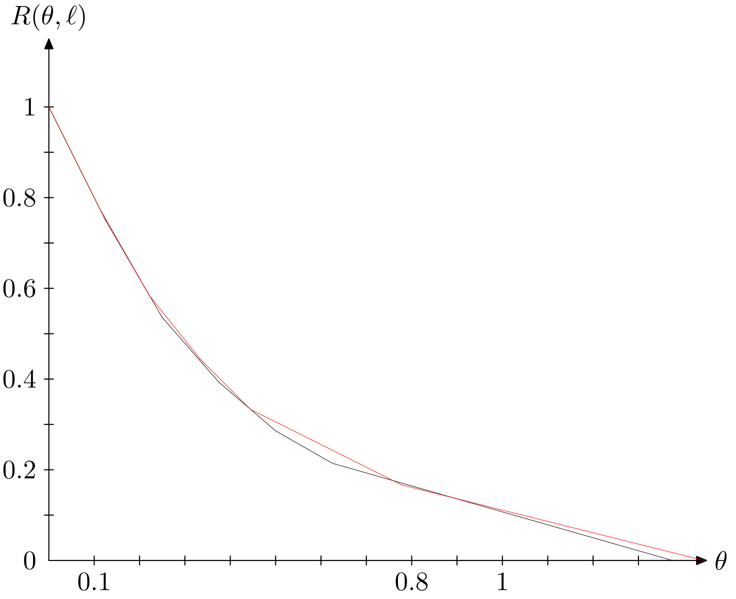

Figure 2.5: Curve $\theta \mapsto R(\theta, \ell)$ for $q = 9$ and $\ell = 7, 8$.

Lemma 2.22 *Fix $\mathcal{C}$ as a length-n alternant code, and let the underlying GRS code have dimension k. Fix ℓ as the list size. Let $\theta(\ell, r, \Delta)$ be as defined in Proposition 2.1, and fix $0 < \Delta \le r \le \ell$ that maximize $\theta(\ell, r, \Delta)$. Let $\theta = \theta(\ell, r, \Delta)$, $\tau = \lceil n\theta \rceil - 1$, and $\beta = rn - \tau\Delta$. Then, for every codeword $\mathbf{c}$ there exists a received word $\mathbf{y}$ such that $\mathsf{d}(\mathbf{c}, \mathbf{y}) = \tau$ and $\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) = \beta$.*

Proof Let $\mathbf{y}$ be such that $\tau - n\lfloor \tau/n \rfloor$ entries of $\mathbf{y}$ are at a distance $\lfloor \tau/n \rfloor + 1$ from the respective entries of $\mathbf{c}$, and the remaining $n - \tau + n\lfloor \tau/n \rfloor$ entries of $\mathbf{y}$ are at a distance $\lfloor \tau/n \rfloor$ from the respective entries of $\mathbf{c}$. By this definition, $\mathsf{d}(\mathbf{c}, \mathbf{y}) = \tau$. We claim that $\mathbf{y}$ is such that $\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) = \beta$.

Assume the contrary, namely, that $\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) > \beta$. Thus, we must have that

$$r - (\lfloor \tau/n \rfloor + 1)\Delta < 0 \ ,$$

and since $\beta > 0$, we must also have that

$$r - \lfloor \tau/n \rfloor \Delta > 0 \ .$$

Define r' and Δ' as the unique integers for which

$$r - \lfloor \tau/n \rfloor \Delta = r' - \lfloor \tau/n \rfloor \Delta' \quad \text{and} \quad r' - (\lfloor \tau/n \rfloor + 1)\Delta' = 0 \ .$$

Note the following facts about r' and Δ' (see also Figure 2.6):

1. r' and Δ' are indeed well-defined.
2. $0 < \Delta' \leq r' \leq \ell$.
3. For $x \leq \lfloor \tau/n \rfloor$ we have $r - x\Delta \geq r' - x\Delta'$.
4. For $x > \lfloor \tau/n \rfloor$ we have $r - x\Delta < r' - x\Delta'$.

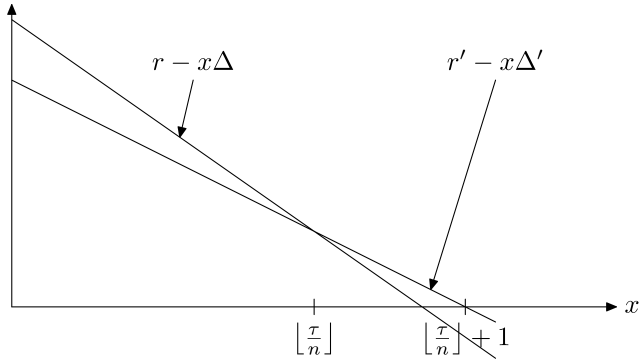

Figure 2.6: $x \mapsto r - x\Delta$ versus $x \mapsto r' - x\Delta'$.

We claim that $\theta(\ell, r', \Delta') > \theta = \theta(\ell, r, \Delta)$, which is a contradiction. We will show this by proving that

$$R(\theta, \ell, r, \Delta, \Lambda(r, \Delta)) < R(\theta, \ell, r', \Delta', \Lambda(r', \Delta')) \ . \tag{2.24}$$

By Fact 3 we have that

$$n \left(\sum_{i=0}^{\lfloor \tau/n \rfloor} \binom{r' - i\Delta'}{2} \right) \leq n \left(\sum_{i=0}^{\lfloor \tau/n \rfloor} \binom{r - i\Delta}{2} \right) \ , \tag{2.25}$$

where the LHS of Equation (2.25) is the number of linear equations implied by r' and Δ', and the RHS is the number of linear equations implied by r and Δ. Note that the number of equations implied by (any) r and Δ is given by Equation (2.5) which, after divided by n and preceded by a minus sign, appears as a sub-expression in Equation (2.2). The other sub-expression inside the outermost parenthesis of Equation (2.2) is $(\ell + 1)(r - \Delta\theta)$. Thus, in order to prove that Equation (2.24) is true, it remains to be shown that $r - \theta\Delta < r' - \theta\Delta'$. This follows from the definition of τ which implies that $\theta > \lfloor \tau/n \rfloor$, and from Fact 4. ■

Chapter 3

Asymptotics

Recall that in the finite ℓ case studied in Chapter 2, we had no closed formula for $\Delta^* = \Delta^*(\theta, \ell)$ (although Equation (2.16) is pretty close). In this chapter, we will take $\ell \to \infty$, and derive a closed asymptotic formula for Δ^*. Therefore, we will also have closed asymptotic formulas for $r^* = r_{\Delta^*}$ and $R(\theta, \ell) = R(\theta, \ell, r^*, \Delta^*, \Lambda(r^*, \Delta^*))$.

For as yet unspecified integer λ and real $w \in [0, 1]$, define

$$\tilde{R}(\theta, w, \lambda) = \left\{ \begin{array}{cc} \frac{3+(6\lambda^2-12\lambda\theta)w-(2\lambda^2+\lambda^4)w^2}{6\lambda} & \text{if } \lambda = q/2 \\ \frac{3+(6\lambda+6\lambda^2-6\theta-12\lambda\theta)w-(\lambda+2\lambda^2+2\lambda^3+\lambda^4)w^2}{6\lambda+3} & \text{otherwise} \end{array} \right. . \tag{3.1}$$

Also, define

$$\Lambda(w) = \left\{ \begin{array}{cc} \min\left\{ \left\lfloor \sqrt{1/w} \right\rfloor, \lfloor q/2 \rfloor \right\} & 0 < w \leq 1 \\ \lfloor q/2 \rfloor & w = 0 \end{array} \right. .$$

Note that $\Lambda(w)$, and hence $\tilde{R}(\theta, r, \Lambda(w))$, are functions of q. However, for the sake of brevity, we will not write this explicitly.

Lemma 3.1 *For $\theta > 0$, $\ell > 0$ and $1 \leq \Delta \leq \ell$, let $w = \Delta/\ell$. Then,*

$$R_\Delta(\theta, \ell) = R(\theta, \ell, r_\Delta, \Delta, \lambda_\Delta) = \tilde{R}(\theta, w, \Lambda(w)) + O(1/\ell) .$$

Proof Note that for $w = \Delta/\ell$, we have $\Lambda(w) = \lambda_\Delta$. Let $\lambda = \lambda_\Delta = \Lambda(w)$ and $r = r_\Delta$. Define $\alpha(\theta, \ell, r, \Delta, \lambda)$ by

$$\alpha(\theta, \ell, r, \Delta, \lambda) = \binom{\ell+1}{2} R(\theta, \ell, r, \Delta, \lambda) .$$

We will soon prove that $R(\theta, \ell, r, \Delta, \lambda) < 1$. But given this we have that $\alpha(\theta, \ell, r, \Delta, \lambda) = O(\ell^2)$, and we can write

$$R(\theta, \ell, r, \Delta, \lambda) = \frac{2}{\ell^2}\alpha(\theta, \ell, r, \Delta, \lambda) + O(1/\ell)\ .$$

We can now replace r by the RHS of Equation (2.13). Removing the floors added by this substitution contributes a factor of $O(1/\ell)$. Rearranging yields the required result.

We will now prove that $R(\theta, \ell, r, \Delta, \lambda) < 1$. By Lemma 2.5 it suffices to prove that $R(\theta, \ell, r, \Delta, 1) < 1$. Since $R(\theta, \ell, r, \Delta, 1)$ is a strictly decreasing function of θ, it suffices to prove that $R(0, \ell, r, \Delta, 1) \leq 1$. If $q = 2$, we have that

$$R(0, \ell, r, \Delta, 1) = \frac{\Delta - \Delta^2 + 2\Delta r + 2\ell r - 2r^2}{\ell + \ell^2}$$

substituting Δ by $r - \bar{r}$ yields

$$R(0, \ell, r, \Delta, 1) = \frac{-r^2 + (2\ell + 1)r - \bar{r} - \bar{r}^2}{\ell + \ell^2}\ . \tag{3.2}$$

Since $\Delta \leq r$, we have $\bar{r} \geq 0$. Substituting the worst case value of 0 for $\bar{r}$ in Equation 3.2 yields

$$\frac{-r^2 + (2\ell + 1)r}{\ell + \ell^2}\ ,$$

which is equal to 1 for $r = \ell, \ell + 1$, and is less than 1 for all other values of r.

The proof for the $q > 2$ case is quite similar. ■

Let us now discard the $O(1/\ell)$ factor and optimize $w \mapsto \tilde{R}(\theta, w, \Lambda(w))$ over w.

3.1 An implicit formula for w^*

Note that the function $w \mapsto \tilde{R}(\theta, w, \Lambda(w))$ is a piecewise quadratic polynomial. One can also easily verify that it is continuous, and has a continuous derivative. Thus, $w \mapsto \tilde{R}(\theta, w, \Lambda(w))$ is $\cap$-concave, and therefore, it attains a (single) maximum for some optimal $0 \leq w^*(\theta) \leq 1$.

We will now find a formula for $w^* = w^*(\theta)$, as a function of $\Lambda(w^*)$ and θ. Recall that $\chi_{\mathcal{L}}(q)$ is defined in Equation (1.4).

Proposition 3.2 *For* $0 < \theta \leq \chi_{\mathcal{L}}(q)$*, let* $\lambda = \Lambda(w^*(\theta))$*. Then,*

$$w^*(\theta) = \begin{cases} \frac{3\lambda-6\theta}{2\lambda+\lambda^3} & \textit{if } \lambda = q/2 \\ \frac{3(\lambda+\lambda^2-\theta-2\lambda\theta)}{\lambda+2\lambda^2+2\lambda^3+\lambda^4} & \textit{otherwise} \end{cases} . \tag{3.3}$$

Proof Fix θ and λ, and denote $w^* = w^*(\theta)$. Consider the function $w \mapsto \tilde{R}(\theta, w, \lambda)$. One can easily prove that the RHS of Equation (3.3) is the value of w for which $\frac{\partial \tilde{R}(\theta,w,\lambda)}{\partial w} = 0$. Note that

$$\left.\frac{\partial \tilde{R}(\theta, w, \lambda)}{\partial w}\right|_{w=w^*} = \left.\frac{\partial \tilde{R}(\theta, w, \Lambda(w))}{\partial w}\right|_{w=w^*} ,$$

because $w \mapsto \tilde{R}(\theta, w, \Lambda(w))$ is continuous, and has a continuous derivative. We have three cases to consider:

Case 1 : In this case,

$$\left.\frac{\partial \tilde{R}(\theta, w, \lambda)}{\partial w}\right|_{w=w^*} = 0 ,$$

and the proof follows.

Case 2 : In this case,

$$\left.\frac{\partial \tilde{R}(\theta, w, \lambda)}{\partial w}\right|_{w=w^*} < 0 .$$

Thus, $w^* = 0$, and therefore, $\lambda = \left\lfloor \frac{q}{2} \right\rfloor$. For $\lambda = \left\lfloor \frac{q}{2} \right\rfloor$, the fact that the RHS of Equation (3.3) is < 0 contradicts the fact that $\theta \leq \chi_{\mathcal{L}}(q)$.

Case 3 : In this case,

$$\left.\frac{\partial \tilde{R}(\theta, w, \lambda)}{\partial w}\right|_{w=w^*} > 0 .$$

Thus, $w^* = 1$, and therefore, $\lambda = 1$. For $\lambda = 1$, the fact that the RHS of Equation (3.3) is > 0 contradicts the fact that $\theta > 0$.

■

3.2 Finding $\Lambda(w^*)$

Equation (3.3) gives us w^*, as a function of $\Lambda(w^*)$ (which is yet unknown) and θ. We will now derive an explicit formula for $\Lambda(w^*)$.

Proposition 3.3 *Let $0 < \theta \leq \chi_{\mathcal{L}}(q)$. Denote by L the unique integer such that $\frac{L^2-1}{3L} \leq \theta < \frac{L+2L}{3(L+1)}$. Then $\Lambda(w^*) = \min\{L, \lfloor q/2 \rfloor\}$.*

Proof Fix $\lambda = \Lambda(w^*)$. There are two cases to consider:

Case 1 $\lambda < \lfloor q/2 \rfloor$: In this case, we have that $\lambda = \left\lfloor \sqrt{1/w^*} \right\rfloor$. By Proposition 3.2, and a straightforward algebraic manipulation, we see that this is equivalent to $\frac{\lambda^2-1}{3\lambda} \leq \theta < \frac{\lambda^2+2\lambda}{3(\lambda+1)}$.

Case 2 $\lambda = \lfloor q/2 \rfloor$: Now we have that $\lambda \leq \left\lfloor \sqrt{1/w^*} \right\rfloor$. A short calculation shows that this yields $\frac{\lambda^2-1}{3\lambda} \leq \theta$.

3.3 Conclusion for the asymptotic case

We can now derive the asymptotic optimal modified rate formula. Inserting Equation (3.3) into Equation (3.1), along with Proposition 3.3, yield the following:

Proposition 3.4 *For $0 < \theta \leq \chi_{\mathcal{L}}(q)$, denote by L the unique integer such that $\frac{L^2-1}{3L} \leq \theta < \frac{L^2+2L}{3(L+1)}$, and let $\lambda = \min\{L, \lfloor q/2 \rfloor\}$. Then,*

$$R(\theta, \infty) = \lim_{\ell \to \infty} R(\theta, \ell) = \begin{cases} \frac{1+2\lambda^2-6\lambda\theta+6\theta^2}{2\lambda+\lambda^3} & \text{if } \lambda = q/2 \\ \frac{\lambda+3\lambda^2+2\lambda^3-6\lambda\theta(1+\lambda)+3\theta^2(1+2\lambda)}{\lambda+2\lambda^2+2\lambda^3+\lambda^4} & \text{otherwise} \end{cases} . \quad (3.4)$$

Proposition 3.4 gives us the asymptotic value of the optimal R, for a given θ. Conversely, we can look at the inverse function of R to derive the asymptotic value of θ, for a given R. Thus, we now have a means to (asymptotically) compare the modified decoding radius obtained by our algorithm to that promised by Proposition 1.4. Define

$$\mathcal{J}_{\mathcal{L}}(\infty, \theta, q) = \lim_{\ell \to \infty} \mathcal{J}_{\mathcal{L}}(\ell, \theta, q) = \left(2\theta - \frac{\theta^2}{\chi_{\mathcal{L}}(q)}\right) , \quad 0 < \theta \leq \chi_{\mathcal{L}}(q) .$$

Proposition 3.5 *For* $0 < \theta \leq \chi_{\mathcal{L}}(q)$*, if* $q = 2$ *or* $q = 3$*, then* $R(\theta, \infty) = 1 - \mathcal{J}_{\mathcal{L}}(\infty, \theta, q)$*. Otherwise,* $R(\theta, \infty) > 1 - \mathcal{J}_{\mathcal{L}}(\infty, \theta, q)$

Proof Define the function $f(\theta, \lambda)$ as the RHS of Equation (3.4). Fix some θ_0, such that $0 < \theta_0 \leq \chi_{\mathcal{L}}(q)$, and let λ be as defined in Proposition 3.4 for $\theta = \theta_0$. Note that λ is fixed.

We have two cases to consider:

Case 1 $\lambda = \lfloor q/2 \rfloor$: If q is even then $\chi_{\mathcal{L}}(q) = \lambda/2$. Otherwise, q is odd, and $\chi_{\mathcal{L}}(q) = (\lambda^2 + \lambda)/(2\lambda + 1)$. If $q = 2$ or $q = 3$, then $\lambda = 1$ and from Equation (3.4) we obtain that $R(\theta_0, \infty) = f(\theta_0, \lambda) = 1 - \mathcal{J}_{\mathcal{L}}(\infty, \theta_0, q)$.

Otherwise, for $\lambda > 1$ and $0 < \theta \leq \chi_{\mathcal{L}}(q)$, $f(\theta, \infty) - 1 + \mathcal{J}_{\mathcal{L}}(\infty, \theta, q)$ is a $\cap$-concave quadratic polynomial in θ. Since $\frac{\lambda^2-1}{3\lambda} \leq \theta_0 \leq \chi_{\mathcal{L}}(q)$, it suffices to prove that for $\lambda > 1$, we have $f(\theta, \lambda) - 1 + \mathcal{J}_{\mathcal{L}}(\infty, \theta, q) > 0$ for $\theta = \frac{\lambda^2-1}{3\lambda}$ and $\theta = \chi_{\mathcal{L}}(q)$. This is indeed so.

Case 2 $\lambda < \lfloor q/2 \rfloor$: In this case, we have $\chi_{\mathcal{L}}(q) \geq \frac{\lambda+1}{2}$. Thus, it suffices to show that

$$f(\theta, \lambda) - 1 + 2\theta - \frac{\theta^2}{\left(\frac{\lambda+1}{2}\right)} \tag{3.5}$$

is positive for $\theta = \theta_0$. Equation (3.5) is $\theta^2/2$ for $\lambda = 1$ and $\cap$-concave for $\lambda > 1$, as a function of θ. Since $\frac{\lambda^2-1}{3\lambda} \leq \theta_0 < \frac{\lambda^2+2\lambda}{3(\lambda+1)}$, it suffices to show that for $\lambda > 1$, Equation (3.5) is positive for $\theta = \frac{\lambda^2-1}{3\lambda}$ and $\theta = \frac{\lambda^2+2\lambda}{3(\lambda+1)}$. This is indeed so.

■

Figure 3.1 plots $R(\theta, \ell)$ versus $1 - \mathcal{J}_{\mathcal{L}}(\infty, \theta, q)$ for specific q and ℓ.

Since $1 - \mathcal{J}_{\mathcal{L}}(\infty, \theta, q)$ is strictly decreasing for $0 < \theta \leq \chi_{\mathcal{L}}(q)$, we conclude from Proposition 3.5 that when $\ell \to \infty$, the decoding algorithm achieves a relative decoding radius which is generally better than the one promised by Proposition 1.4. Note that this holds regardless of the column multipliers $(v_i)_{i \in [n]}$. This is somewhat surprising; in the Hamming metric, the bound implied by a Johnson-type bound turns out to be exactly the relative decoding radius achieved by Koetter and Vardy [12]. Note that $q = 2$ and $q = 3$ are the two values for which the Hamming and Lee metrics are the same.

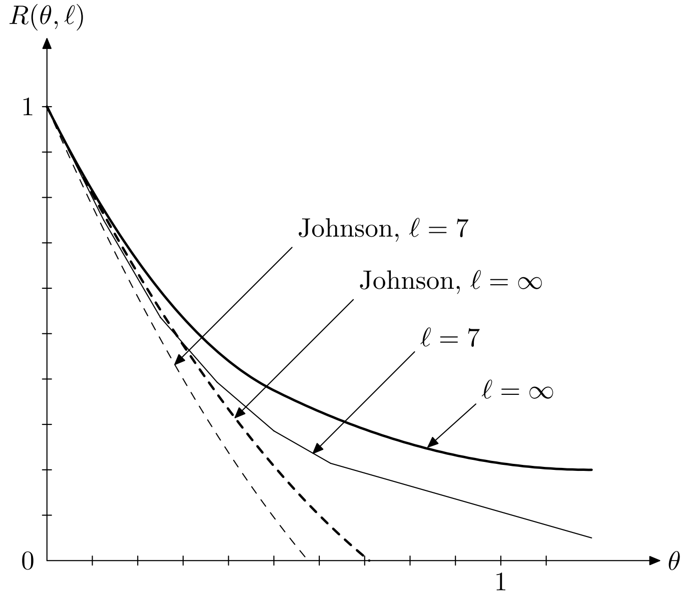

Figure 3.1: Curve $\theta \mapsto R(\theta, \ell)$ and the Johnson bound for $q = 5$ and $\ell = 7, \infty$.

Chapter 4

Justification for the Score Selection

At the start of Chapter 2, we introduced a mapping $\mathbf{y} \mapsto \mathcal{M}(\mathbf{y})$, defined in Equation (2.1). We will call this mapping and everything derived from it the *distance-linear score method*. The rest of the chapter was dedicated to the optimization of that mapping over r and Δ, in order to get the largest possible decoding radius τ. Chapter 3 was dedicated to further analysis of this mapping.

However, it is certainly possible that a mapping $\mathbf{y} \mapsto \mathcal{M}(\mathbf{y})$ not of the form of Equation (2.1) (along with a respective β) would yield a better decoding radius than what we could achieve from the distance-linear score method.

This chapter is dedicated to justifying Chapters 2 and 3 (partially). We will show that after some relaxation — essentially assuming a certain symmetry in the mapping $\mathbf{y} \mapsto \mathcal{M}(\mathbf{y})$ and moving from integers to rationals — the distance-linear score method is optimal. Thus, one would expect that the distance-linear score method is not too far from the optimum.

Consider a related setup. For ease of notation, denote

$$I = \{0, 1, \ldots, \lfloor q/2 \rfloor\} .$$

We are given two parameters. The first parameter is the vector $\boldsymbol{\mu} = (\mu_i)_{i \in I}$, termed the *multiplicity vector*, over the nonnegative rationals. We also require that, for two indexes i and j, if $i < j$ then $\mu_i \geq \mu_j$. The second parameter is the *critical score* β, which is also over the nonnegative rationals. We call a rational vector $\boldsymbol{\delta} = (\delta_i)_{i \in I}$ an *error distribution* if $\sum_{i \in I} \delta_i = 1$, and $\delta_i \geq 0$. For an error distribution $\boldsymbol{\delta}$ we define the *weight* of $\boldsymbol{\delta}$ as

$$\mathsf{w}(\boldsymbol{\delta}) = n \cdot \sum_{i \in I} i\delta_i \ .$$

The *score* of $\boldsymbol{\delta}$ with respect to $\boldsymbol{\mu}$ is defined as

$$S_{\boldsymbol{\mu}}(\boldsymbol{\delta}) = n \cdot \sum_{i \in I} \mu_i \delta_i \ .$$

We call $\boldsymbol{\delta}$ a *critical error distribution* with respect to a multiplicity vector $\boldsymbol{\mu}$ and critical score β, when the following three conditions are met:

1. $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}) = \beta$.
2. If $\boldsymbol{\delta}'$ is an error distribution such that $\mathsf{w}(\boldsymbol{\delta}') \leq \mathsf{w}(\boldsymbol{\delta})$, then $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}') \geq \beta$.
3. For all τ such that $\tau > \mathsf{w}(\boldsymbol{\delta})$, there exists an error distribution $\boldsymbol{\delta}'$ such that $\mathsf{w}(\boldsymbol{\delta}) < \mathsf{w}(\boldsymbol{\delta}') < \tau$ and $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}') < \beta$.

How are all these definitions connected to what we've been doing so far? Let $\mathbf{y} = (y_j)_{j \in [n]}$ be the received word. Suppose we were only interested in mappings $\mathbf{y} \mapsto \mathcal{M}(\mathbf{y}) = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$ of the form

$$\mathcal{M}_{\gamma,j} = \mu_{\mathsf{d}_{\mathcal{L}}(y_j,\gamma)} \ . \tag{4.1}$$

for some vector $\boldsymbol{\mu} = (\mu_i)_{i \in I}$, with nonincreasing entries. For a codeword $\mathbf{c}$ define $\boldsymbol{\delta}(\mathbf{c}, \mathbf{y}) = (\delta_i)_{i \in I}$ as

$$\delta_i = \frac{|\{j \in [n] : \mathsf{d}_{\mathcal{L}}(y_j, \gamma) = i\}|}{n} \ . \tag{4.2}$$

Then, under these definitions,

$$\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) = S_{\mu}(\boldsymbol{\delta}(\mathbf{c}, \mathbf{y}))$$

and

$$\mathsf{d}_{\mathcal{L}}(\mathbf{c}, \mathbf{y}) = \mathsf{w}(\boldsymbol{\delta}(\mathbf{c}, \mathbf{y})) \ .$$

Recall that $\mathcal{S}_{\mathcal{M}}(\mathbf{c})$ is defined in Equation (1.1).

For ease of analysis we will let $\boldsymbol{\mu}$ and β be defined over the nonnegative rationals (and not the nonnegative integers). Let $\boldsymbol{\delta}$ be a critical vector with respect to $\boldsymbol{\mu}$ and β. The value of $\mathsf{w}(\boldsymbol{\delta})$ is our best estimate for the decoding radius implied by $\boldsymbol{\mu}$ and β. That is, for all $\boldsymbol{\delta}'$ such that $\mathsf{w}(\boldsymbol{\delta}') \leq \mathsf{w}(\boldsymbol{\delta})$ we have $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}') \geq \beta$. Moreover, an error distribution $\boldsymbol{\delta}'$ such that $\mathsf{w}(\boldsymbol{\delta}') > \mathsf{w}(\boldsymbol{\delta})$ does not have this property. In addition, $\boldsymbol{\delta}$ realizes the critical score, $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}) = \beta$.

For the above model we have the following:

Proposition 4.1 *Let $\boldsymbol{\mu} = (\mu_i)_{i \in I}$ be a multiplicity vector and β be a critical score. Let $\boldsymbol{\delta}$ be a critical error distribution with respect to $\boldsymbol{\mu}$ and β. Then, there exists a multiplicity vector $\boldsymbol{\mu}' = (\mu'_i)_{i \in I}$ and rationals r and Δ such that*

$$\mu'_i = \max\{r - i\Delta, 0\} \le \mu_i \ ,$$

and $\boldsymbol{\delta}$ is a critical error distribution with respect to $\boldsymbol{\mu}'$ and β.

Proposition 4.1 states that under the model introduced in this chapter, we do not lose anything by assuming that μ_i is of the form $\max\{r - i\Delta, 0\}$. Also, note that $\mu'_i \le \mu_i$ is important in connection with Condition (C2), introduced on page 9. Namely, if we were dealing with integers, and not with rationals, and Condition (C2) held for the mapping induced by $\boldsymbol{\mu}$ and β (Equation (4.1)), then it would also hold for the mapping induced by $\boldsymbol{\mu}'$ and β.

Recall that our definition of a multiplicity vector $\boldsymbol{\mu} = (\mu)_{i \in I}$ required that if $j, k \in I$ are such that $j < k$, then $\mu_j \ge \mu_k$. This might be a good time to state that we do not lose any generality in this definition. Specifically, let $\boldsymbol{\mu} = (\mu)_{i \in I}$ be a vector for which there exists $j < k$ such that $\mu_j < \mu_k$. Let β be a critical score and let $\boldsymbol{\delta} = (\delta_i)_{i \in I}$ be a critical error distribution with respect to β and $\boldsymbol{\mu}$. Define the vector $\boldsymbol{\mu}' = (\mu'_i)_{i \in I}$ as

$$\mu'_i = \begin{cases} \mu_j & \text{if } i = k \\ \mu_i & \text{otherwise} \end{cases} .$$

Note that we can continue this process until we are left with a legitimate multiplicity vector. We claim that $\boldsymbol{\delta}$ is a critical error distribution with respect to $\boldsymbol{\mu}'$ and β. Assume this is not the case, namely, that $\mu_k \delta_k > (\mu'_k = \mu_j)\delta_k$. Define the error distribution $\boldsymbol{\delta}' = (\delta')_i \in I$ as

$$(\delta')_i = \begin{cases} \delta_j + \delta_k & \text{if } i = j \\ 0 & \text{if } i = k \\ \delta_i & \text{otherwise} \end{cases} .$$

We have $\mathsf{w}(\boldsymbol{\delta}') < \mathsf{w}(\boldsymbol{\delta})$, but $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}') = S_{\boldsymbol{\mu}'}(\boldsymbol{\delta}') < S_{\boldsymbol{\mu}}(\boldsymbol{\delta})$, contradicting the fact that $\boldsymbol{\delta}$ is a critical error distribution with respect to β and $\boldsymbol{\mu}$. Note that for all $i \in I$ we have that $\mu'_i \le \mu_i$, and as was the case in the previous paragraph, this is important in connection with Condition (C2).

The proof of Proposition 4.1 will be deferred to the end of this chapter. We will first prove some lemmas.

Lemma 4.2 *Let the multiplicity vector* $\boldsymbol{\mu} = (\mu_i)_{i \in I}$ *be of the form*

$$\mu_i = \max \{r - \Delta i, 0\} \ ,$$

and let $\boldsymbol{\delta}$ *be an error distribution such that* $\mathsf{w}(\boldsymbol{\delta}) = \tau$*. Then,*

$$S_{\boldsymbol{\mu}}(\boldsymbol{\delta}) \geq rn - \Delta\tau \ .$$

Proof Denote $\boldsymbol{\delta} = (\delta_i)_{i \in I}$. We have

$$\begin{aligned} S_{\boldsymbol{\mu}}(\boldsymbol{\delta}) &= n \sum_{i \in I} \mu_i \delta_i \\ &\geq n \sum_{i \in I} (r - \Delta i)\delta_i \\ &= nr - \Delta n \sum_{i \in I} i\delta_i \\ &= nr - \Delta \mathsf{w}(\boldsymbol{\delta}) \ , \end{aligned}$$

where the penultimate equality follows from $\sum_{i \in I} \delta_i = 1$. ■

Lemma 4.3 *Fix a multiplicity vector* $\boldsymbol{\mu}$ *and a critical score* β*. Let* $\boldsymbol{\delta}$ *be a critical error distribution with respect to* $\boldsymbol{\mu}$ *and* β*. Then, there exists* $\boldsymbol{\delta}'$ *that is also a critical error distribution with respect to* $\boldsymbol{\mu}$ *and* β *such that at most two entries of* $\boldsymbol{\delta}'$ *are nonzero.*

Proof Denote $\boldsymbol{\delta} = (\delta_i)_{i \in I}$. Let $a < b < c$ be indexes for which $\delta_a, \delta_b, \delta_c$ are all positive (if no such indexes exist then $\boldsymbol{\delta}' = \boldsymbol{\delta}$). For as yet an unspecified ϵ, consider the error distribution $\boldsymbol{\delta}' = (\delta_i')_{i \in I}$,

$$\delta_i' = \begin{cases} \delta_a - \epsilon \frac{c-b}{c-a} & \text{if } i = a \\ \delta_b + \epsilon & \text{if } i = b \\ \delta_c - \epsilon \frac{b-a}{c-a} & \text{if } i = c \\ \delta_i & \text{otherwise} \end{cases} \ . \tag{4.3}$$

Note that for a rational ϵ such that $-\delta_b \leq \epsilon \leq \min \left\{ \frac{c-a}{c-b} \cdot \delta_a, \frac{c-a}{b-a} \cdot \delta_c \right\}$, we have that $\boldsymbol{\delta}'$ is a valid error distribution. One can also prove that, $\mathsf{w}(\boldsymbol{\delta}') = \mathsf{w}(\boldsymbol{\delta})$, and

$$S_{\boldsymbol{\mu}}(\boldsymbol{\delta}') - S_{\boldsymbol{\mu}}(\boldsymbol{\delta}) = \frac{n\epsilon}{c-a} \left(-\mu_a(c-b) + \mu_b(c-a) - \mu_c(b-a) \right) \ . \tag{4.4}$$

Next we show that $-\mu_a(c-b)+\mu_b(c-a)-\mu_c(b-a)=0$. Otherwise, assume that it is negative (resp., positive). For a small enough $\epsilon>0$ (resp., $\epsilon<0$), we have that $\boldsymbol{\delta}'$ is a valid error distribution with $\mathsf{w}(\boldsymbol{\delta})=\mathsf{w}(\boldsymbol{\delta}')$ and $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}')<\beta$, contradicting the fact that $\boldsymbol{\delta}$ is a critical error distribution.

Therefore, if we take $\epsilon=-\delta_b$, the number of positive entries in $\boldsymbol{\delta}'$ would be one less than those in $\boldsymbol{\delta}$. We can continue this process until we are left with a vector with two positive entries. ■

Lemma 4.4 *Let $\boldsymbol{\mu}=(\mu_i)_{i\in I}$ be a multiplicity vector, and β be a critical score. Suppose $\boldsymbol{\delta}=(\delta_i)_{i\in I}$ is a critical error distribution such that $\delta_a+\delta_c=1$ for two indexes $a<c$, and both δ_a and δ_c are positive. Let $b\in I$ be an index different from a and c. Then,*

$$-\mu_a(c-b)+\mu_b(c-a)-\mu_c(b-a)\geq 0\ .$$

Proof Suppose $a<b<c$. Define $\boldsymbol{\delta}'$ as in Equation (4.3), with $\epsilon=\min\left\{\frac{c-a}{c-b}\cdot\delta_a,\frac{c-a}{b-a}\cdot\delta_c\right\}$. We have $\mathsf{w}(\boldsymbol{\delta})=\mathsf{w}(\boldsymbol{\delta}')$. Since $\boldsymbol{\delta}$ is a critical error distribution we have $S_{\boldsymbol{\mu}}(\boldsymbol{\delta}')\geq S_{\boldsymbol{\mu}}(\boldsymbol{\delta})$. Thus, by Equation (4.4), our result follows. The case $b<a<c$ is quite similar, we define $\boldsymbol{\delta}'$ as in Equation (4.3), up to the substitution $a\to b$, $b\to a$, and take $\epsilon=-\delta_a$. The case $a<c<b$ is similar as well. ■

Lemma 4.5 *Let $\boldsymbol{\mu}=(\mu_i)_{i\in I}$ be a multiplicity vector and β be a critical score. Suppose $\boldsymbol{\delta}=(\delta_i)_{i\in I}$ is a critical error distribution error such that $\delta_a+\delta_c=1$ for two indexes $a<c$, and both δ_a and δ_c are positive.*

Define $\boldsymbol{\mu}'=(\mu_i')_{i\in I}$ as

$$\begin{aligned}\mu_i' &= \max\left\{\frac{\mu_a(c-i)+\mu_c(i-a)}{c-a},0\right\}\\ &= \max\{r-i\Delta,0\}\ ,\end{aligned}$$

where $r=\frac{\mu_a c-\mu_c a}{c-a}$ and $\Delta=\frac{\mu_a-\mu_c}{c-a}$. Then, $\boldsymbol{\delta}$ is a critical error distribution with respect to $\boldsymbol{\mu}'$ and β.

Proof Let $\tau=\mathsf{w}(\boldsymbol{\delta})=n(a\delta_a+c\delta_c)$. Notice that $\mu_a'=\mu_a$ and $\mu_c'=\mu_c$. Thus, $rn-\tau\Delta=S_{\boldsymbol{\mu}'}(\boldsymbol{\delta})=S_{\boldsymbol{\mu}}(\boldsymbol{\delta})=\beta$. Therefore, from Lemma 4.2, for all $\boldsymbol{\delta}'$ such that $\mathsf{w}(\boldsymbol{\delta}')\leq\mathsf{w}(\boldsymbol{\delta})$, we have $S_{\boldsymbol{\mu}'}(\boldsymbol{\delta})\geq\beta$.

On the other hand, from Lemma 4.4 we have that $\mu_i'\leq\mu_i$, for all $i\in I$. Thus, for every error distribution $\boldsymbol{\delta}'$, we have $S_{\boldsymbol{\mu}'}(\boldsymbol{\delta}')\leq S_{\boldsymbol{\mu}}(\boldsymbol{\delta}')$. Specifically, this applies to any error distribution $\boldsymbol{\delta}'$ such that $\mathsf{w}(\boldsymbol{\delta}')>\mathsf{w}(\boldsymbol{\delta})$. ■

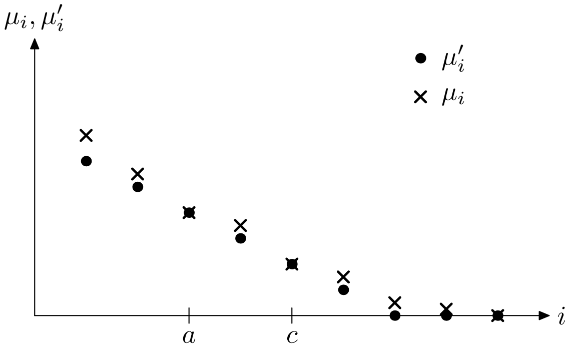

Figure 4.1: Graph of $\boldsymbol{\mu}$ versus $\boldsymbol{\mu}'$ in Lemma 4.5.

For a graphical representation of Lemma 4.5, see Figure 4.1.

Lemma 4.6 *Let $\boldsymbol{\mu} = (\mu_i)_{i \in I}$ be a multiplicity vector, and β be a critical score. Let $\boldsymbol{\delta} = (\delta_i)_{i \in I}$ be a critical error distribution with respect to $\boldsymbol{\mu}$ and β, such that $\delta_b = 1$ for an index $0 < b < \lfloor q/2 \rfloor$. Fix indexes a and c such that $a < b < c$. Then,*

$$-\mu_a(c-b) + \mu_b(c-a) - \mu_c(b-a) \leq 0 \ .$$

Proof Assume the contrary, and define $\boldsymbol{\delta}'$ as in Equation (4.3), for $\epsilon = -\delta_b$. We have $\mathsf{w}(\boldsymbol{\delta}) = \mathsf{w}(\boldsymbol{\delta}')$, and by Equation (4.4) we get that $S(\boldsymbol{\delta}') < S(\boldsymbol{\delta})$. This contradicts the fact that $\boldsymbol{\delta}$ is a critical error distribution. ■

Lemma 4.7 *Let $\boldsymbol{\mu} = (\mu_i)_{i \in I}$ be a multiplicity vector, and β be a critical score. Let $\boldsymbol{\delta} = (\delta_i)_{i \in I}$ be a critical error distribution with respect to $\boldsymbol{\mu}$ and β, such that $\delta_b = 1$ for an index $0 < b < \lfloor q/2 \rfloor$. Fix $a < b$ as an index such that for all $a' < b$*

$$\frac{\mu_{a'} - \mu_b}{b - a'} \geq \frac{\mu_a - \mu_b}{b - a} \ .$$

Define the multiplicity vector $\boldsymbol{\mu}' = (\mu_i)_{i \in I}$ as

$$\begin{aligned} \mu'_i &= \max\left\{\frac{\mu_a(b-i) + \mu_b(i-a)}{b-a}, 0\right\} \\ &= \max\{r - \Delta i, 0\} \ , \end{aligned}$$

where $r = \frac{\mu_a b - \mu_b a}{b-a}$ and $\Delta = \frac{\mu_a - \mu_b}{b-a}$. Then, $\mu'_i \leq \mu_i$ for $i \in I$, and $\boldsymbol{\delta}$ is a critical error distribution with respect to $\boldsymbol{\mu}'$ and β.

Proof We must first prove that for all indexes c,

$$-\mu_a(c-b)+\mu_b(c-a)-\mu_c(b-a)\leq 0 \ .$$

For $c=b$ this is obvious. For $c>b$ this follows from Lemma 4.6. For $c<b$ this follows from the definition of a. The rest of the proof is very similar to Lemma 4.5. ■

For a graphical representation of Lemma 4.7, see Figure 4.2.

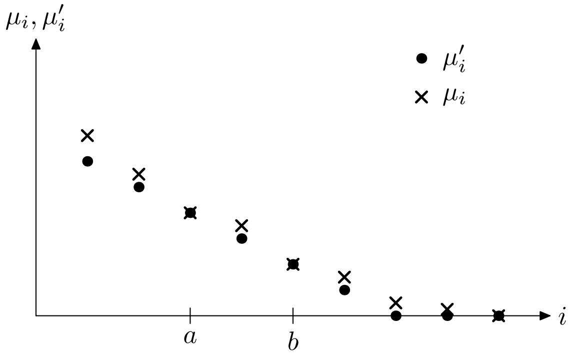

Figure 4.2: Graph of $\boldsymbol{\mu}$ versus $\boldsymbol{\mu}'$ in Lemma 4.7.

We are now able to prove Proposition 4.1.

Proof of Proposition 4.1 By Lemma 4.3, if $\boldsymbol{\delta}$ is a critical error distribution, then we can assume w.l.o.g. that $\boldsymbol{\delta}$ has either one or two nonzero entries. If $\boldsymbol{\delta}$ has two nonzero entries, the claim is proved by Lemma 4.5. Otherwise, $\boldsymbol{\delta}$ has one nonzero entry, and the claim is proved by Lemma 4.7. ■

Chapter 5

Notes

This chapter contains two sections. In the first section we discuss what code $\mathcal{C}$ and bijection $\langle\cdot\rangle : F \to \mathbb{Z}_p$ a designer might choose when working with our decoder. Specifically, we cite previous results about "good codes" for the Lee metric. In the second section we compare the decoding radius of our decoder to the decoding radii of other known decoders for the Lee metric.

5.1 Code and bijection selection

In [22], length-n normalized ($v_i = \alpha_i$ for all $i \in [n]$) alternant codes are analyzed for $F = \mathrm{GF}(p)$, where p is prime. If we take $\langle\cdot\rangle : F \to \mathbb{Z}_p$ as the identity function, the minimum Lee distance of these codes, d, satisfies

$$d \geq \begin{cases} 2(n-k), & \text{for } n-k \leq (p-1)/2 \\ p, & \text{for } (p+1)/2 \leq n-k < p \end{cases} , \tag{5.1}$$

where k is the dimension of the underlying (normalized) GRS code.

Normalized $[n, k]$ GRS codes are also analyzed in [22]. Let $\Phi = F = \mathrm{GF}(p)$, where p is prime, and let $\langle\cdot\rangle : F \to \mathbb{Z}_p$ be the identity function. Fix $\mathcal{C}$ as an $[n, k]$ GRS code, and denote $r = n - k$. The minimum Lee distance of $\mathcal{C}$, d, satisfies the following three bounds:

$$d \geq 2r , \tag{5.2}$$

$$d \geq \frac{r+1}{2} + \frac{(r+1)^2}{4(p-1-r)} , \tag{5.3}$$

$$d \geq \frac{1}{4}\left(p^2 - 1 - (p-r-2)\cdot p^{3/2}\right) , \tag{5.4}$$

where Equation (5.4) is due to Mazur [**?**].

Thus, it might be beneficial to choose a normalized alternant or GRS code, and to choose $\langle\cdot\rangle : F \to \mathbb{Z}_p$ as the identity function.

On the other hand, it is well-known that the minimum Hamming distance of a GRS code is $n - k + 1$. Let F, Φ, the bijection $\langle\cdot\rangle : F \to \mathbb{Z}_p$, and the code locators $(\alpha_i)_{i\in[n]}$ be given. Note that we could choose column multipliers $(v_i)_{i\in[n]}$ such that the minimum Lee distance of the resulting code satisfies $d = n - k + 1$. But we can do no worse than this.

In Section 1.2, we fixed a bijection $\langle\cdot\rangle : F \to \mathbb{Z}_q$. Different choices of $\langle\cdot\rangle$ generally lead to different minimum Lee distances of the codes. Moreover, we could just as well have n fixed bijections, one for each coordinate. Thus, when constructing a code, the mapping(s) $\langle\cdot\rangle$ are a design consideration. Note that our algorithm generalizes to the case where different mappings are chosen for different coordinates: When specifying column j of the score matrix (Equation (2.1)), use the mapping associated with coordinate j.

5.2 Other decoders

Suppose $F = \mathrm{GF}(p)$, where p is prime, and $\langle\cdot\rangle : F \to \mathbb{Z}_p$ is the identity function. When seeking a decoder for a normalized alternant or a normalized GRS code over F, the decoding radius promised by our decoder should be compared to that obtained in [22]. The latter is $\tau = n - k - 1$ (for $\ell = 1$), whenever the $2(n-k)$ lower bound on d applies (recall Equations (5.1) and (5.2)). One can also extend the decoding algorithm in [22] to $\tau = n - k - 1$ when $n - k \le p$ [**?**, Chapter 10]. This results in a list-2 decoder.

Let F and $\langle\cdot\rangle : F \to \mathbb{Z}_p$ be as in the previous paragraph. Suppose $F = \Phi$, and let $\mathcal{C}$ be an $[n, k]$ normalized GRS code. Thus, Equations (5.2)–(5.4) apply, with $r = n - k$. Denote by $d5.2$, d5.3, d5.4$theRHSofEquations$ (5.2), (5.3), and (5.4), respectively. These equations imply the existence of a classical (list-1) decoder, with decoding radius

$$\lfloor\lceil\max\{d$$

5.2,d5.3,d5.4 $-1\frac{}{2\,.(5.5)}$Although this result is non-algorithmic, we will compare ourselves to it.

Figure 5.1 plots decoding radii of three decoders: Our decoder, the Roth & Siegel decoder, and the non-algorithmic decoder (Equation (5.5)), for a normalized GRS code. Figure 5.2 plots the decoding radii of our decoder, and the Roth & Siegel decoder, for a normalized alternant code.

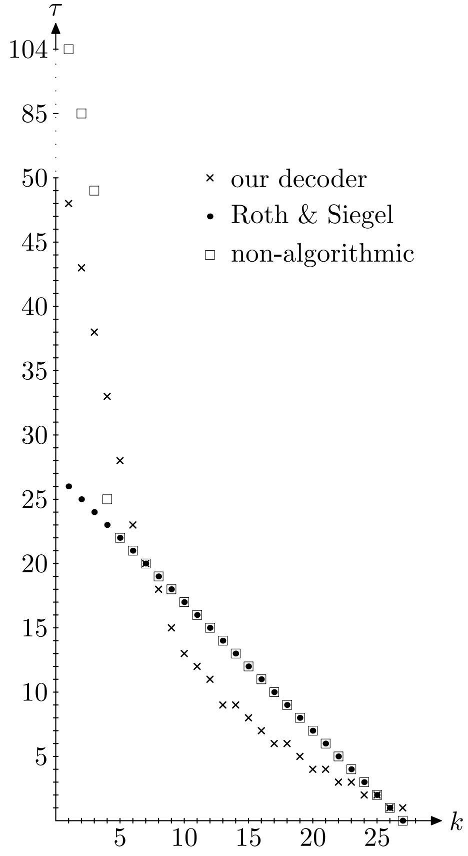

Figure 5.1: Let $F = \Phi = \mathrm{GF}(29)$, and let $\langle\cdot\rangle : F \to \mathbb{Z}_p$ be the identity function. Fix $\mathcal{C}$ as an $[n, k]$ normalized GRS code, with $n = 28$. For a specified k (x-axis), we compare the decoding radii, τ, of three decoders: Our decoder (with $\ell = 10$), the Roth & Siegel decoder, and the non-algorithmic decoder (Equation (5.5)).

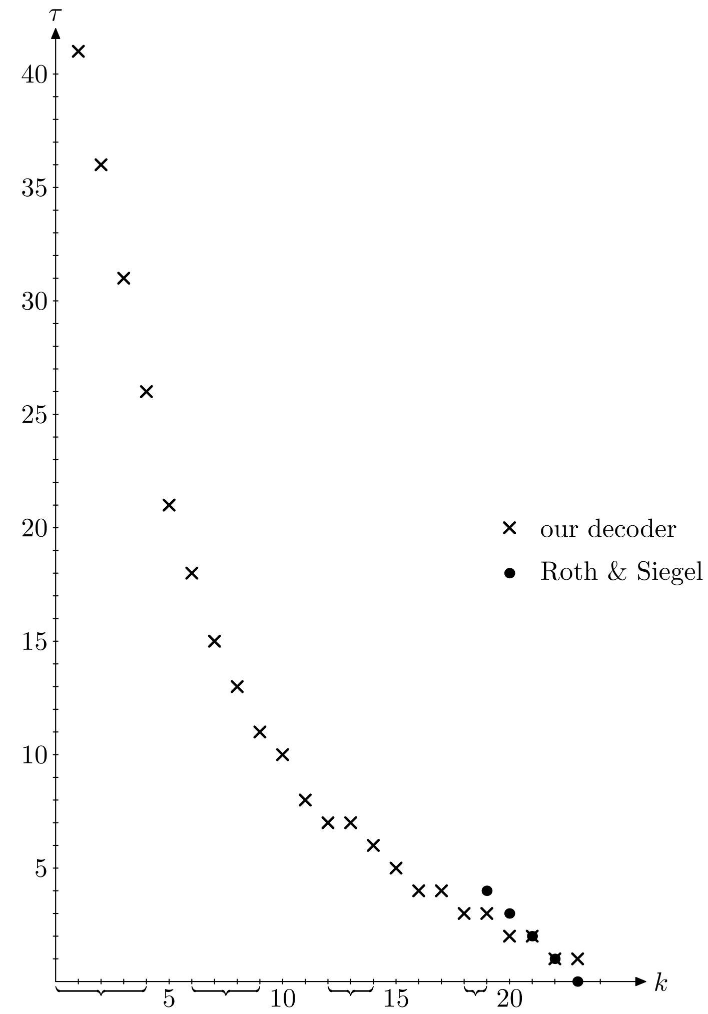

Figure 5.2: Let $F = \mathrm{GF}(5)$, $\Phi = \mathrm{GF}(25)$, and let $\langle\cdot\rangle : F \to \mathbb{Z}_p$ be the identity function. Fix $\mathcal{C}$ as an $[n, k]$ normalized alternant code, with $n = 24$. For a specified k (x-axis), we compare the decoding radius, τ, of our decoder (with $\ell = 10$) to that of the Roth & Siegel decoder. Note that two or more values of k may result in the same alternant code. Values of k which result in the same code are grouped by a brace. The left-most brace corresponds to the trivial code $\mathcal{C} = \{0^n\}$.

Appendix A

Proof of Proposition 2.16

A.1 The $\lambda_\Delta = \lambda_{\Delta+1}$ case

As stated in the beginning of Section 2.4, our goal is to prove that if $1 < \Delta < \ell$, then $\theta_{\Delta,\Delta+1}(\ell) \leq \theta_{\Delta-1,\Delta}(\ell)$. In this subsection, we will prove this for the case where $\lambda_\Delta = \lambda_{\Delta+1}$.

Claim A.1 *Let $\ell \geq 1$. Then,*

$$6(\ell+1)\theta_{\Delta,\Delta+1}(\ell, r, r', \lambda, \lambda')$$

is an integer for every integer r, r', λ, and λ'.

Proof Follows directly from the definition of R in Equation (2.2). ■

Lemma A.2 *Let $\ell \geq 1$, $1 < \Delta < \ell$, and $1 \leq \lambda \leq \lfloor q/2 \rfloor$. Then*

$$\theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\lambda), \lambda, \lambda) \geq \frac{-1}{12(\ell+1)} .$$

Proof A short calculation gives

$$\begin{aligned}
&\theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\lambda), \lambda, \lambda) \\
&\quad = \begin{cases} \frac{\lambda(\lambda^2-1)}{6(\ell+1)} & \text{if } \lambda = q/2 \\ \frac{-3-8\lambda-4\lambda^2+8\lambda^3+4\lambda^4}{12(\ell+1)(1+2\lambda)} & \text{otherwise} \end{cases} .
\end{aligned}$$

This expression is obviously positive for $\lambda > 1$. For $\lambda = 1$ and $q = 2$ it is 0. For $\lambda = 1$ and $q \neq 2$ it is $\frac{-1}{12(\ell+1)}$. ■

Lemma A.3 *Let $\ell \geq 1$ and $1 < \Delta < \ell$ be such that $\lambda_\Delta = \lambda_{\Delta+1}$. Then*

$$\theta_{\Delta,\Delta+1}(\ell) \leq \theta_{\Delta-1,\Delta}(\ell) .$$

Proof From Lemmas 2.20, 2.21, and A.2 we get

$$12(\ell+1)(\theta_{\Delta-1,\Delta}(\ell) - \theta_{\Delta,\Delta+1}(\ell)) \geq -1 ;$$

furthermore, from Claim A.1 we conclude that the LHS is even and, so, nonnegative. ■

A.2 The $\lambda_\Delta = \lambda_{\Delta+1} + 1$ case

In this section, we prove that $\theta_{\Delta,\Delta+1}(\ell) \leq \theta_{\Delta-1,\Delta}(\ell)$, for $1 < \Delta < \ell$ and $\lambda_\Delta = \lambda_{\Delta+1} + 1$.

Lemma A.4 *Let $\ell \geq 1$ and $1 \leq \Delta < \ell$ be such that $\lambda_\Delta > \lambda_{\Delta+1}$. Then*

$$\Delta = \left\lfloor \frac{\ell}{\lambda_\Delta^2} \right\rfloor .$$

Proof Fix $\lambda = \lambda_\Delta$. From Proposition 2.14 we conclude that Δ is the largest integer for which

$$\lambda \leq \left\lfloor \sqrt{\ell/\Delta} \right\rfloor .$$

This inequality is satisfied if and only if $\lambda \leq \sqrt{\ell/\Delta}$ or

$$\Delta \leq \frac{\ell}{\lambda^2} .$$

The largest value of Δ for which the latter inequality holds is obviously $\Delta = \lfloor \frac{\ell}{\lambda^2} \rfloor$. ■

Lemma A.5 *Let $\ell \geq 1$ and $1 \leq \Delta < \ell$ be such that $\lambda_\Delta = \lambda_{\Delta+1} + 1$. Denote $\lambda = \lambda_\Delta$. Then*

$$\theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\lambda-1), \lambda, \lambda-1) \geq 0 .$$

Proof

$$\theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\lambda-1), \lambda, \lambda-1) = \tag{A.1}$$

$$\begin{cases} \frac{-6\lambda^4\Delta^2+12\lambda^2(\ell+1-\lambda^2)\Delta-6((\ell+1)^2-2\ell\lambda^2)-3\lambda+22\lambda^2-8\lambda^3-10\lambda^4+8\lambda^5}{24(\ell+1)\lambda(2\lambda-1)} & \text{if } \lambda = q/2 \\ \\ \frac{-6\lambda^4\Delta^2+12\lambda^2(\ell+1-\lambda^2)\Delta-6((\ell+1)^2-2\ell\lambda^2)+\lambda+12\lambda^2-8\lambda^3+4\lambda^5}{6(\ell+1)(2\lambda-1)(2\lambda+1)} & \text{otherwise} \end{cases} .$$

By Lemma A.4, $\Delta = \left\lfloor \frac{\ell}{\lambda^2} \right\rfloor$. We could plug this value of Δ into the RHS of Equation (A.1) and prove that it is nonnegative. However, that would be messy.

Instead, fix λ and ℓ, and consider Equation (A.1) as a function of Δ. This function is a $\cap$-concave quadratic polynomial, whose maximum is attained at $\frac{\ell-(\lambda^2-1)}{\lambda^2}$. Since

$$\frac{\ell - (\lambda^2 - 1)}{\lambda^2} \le \left\lfloor \frac{\ell}{\lambda^2} \right\rfloor \le \frac{\ell}{\lambda^2} ,$$

it suffices to prove that if we substitute $\Delta = \frac{\ell}{\lambda^2}$, then the resulting equation is nonnegative. The latter substitution yields

$$\begin{cases} \frac{-6-3\lambda+22\lambda^2-8\lambda^3-10\lambda^4+8\lambda^5}{24(1+\ell)\lambda(2\lambda-1)} & \text{if } \lambda = q/2 \\ \frac{-6+\lambda+12\lambda^2-8\lambda^3+4\lambda^5}{6(\ell+1)(2\lambda-1)(2\lambda+1)} & \text{otherwise} \end{cases} ,$$

which is indeed nonnegative for $\lambda \ge 2$. ■

Lemma A.6 *Let $\ell \ge 1$ and $1 \le \Delta < \ell$ be such that $\lambda_\Delta = \lambda_{\Delta+1} + 1$. Then*

$$\theta_{\Delta,\Delta+1}(\ell) \le \theta_{\Delta-1,\Delta}(\ell) .$$

Proof Immediate from Lemmas 2.20, 2.21, and A.5. ■

A.3 The $\lambda_\Delta \ge \lambda_{\Delta+1} + 2$ case

In this subsection, we will prove that $\theta_{\Delta,\Delta+1}(\ell) \le \theta_{\Delta-1,\Delta}(\ell)$, for $1 < \Delta < \ell$ and $\lambda_\Delta \ge \lambda_{\Delta+1} + 2$.

Lemma A.7 *Let $\ell \ge 1$ and $1 \le \Delta < \ell$ be such that $\lambda_\Delta \ge \lambda_{\Delta+1} + 2$. Then*

$$\ell < \frac{1}{\frac{1}{(\lambda_{\Delta+1}+1)^2} - \frac{1}{\lambda_\Delta^2}}$$

Proof By Lemma A.4, $\Delta = \lfloor \ell/\lambda_\Delta^2 \rfloor$. Thus,

$$\Delta \leq \ell/\lambda_\Delta^2 \ . \tag{A.2}$$

Also, by Proposition 2.14, $\lambda_{\Delta+1} = \left\lfloor \sqrt{\ell/(\Delta+1)} \right\rfloor$. Thus,

$$(\lambda_{\Delta+1}+1)^2 > \ell/(\Delta+1) \ . \tag{A.3}$$

From Equations (A.2) and (A.3) we deduce

$$(\lambda_{\Delta+1}+1)^2 > \frac{\ell}{\frac{\ell}{\lambda_\Delta}+1} \Longrightarrow \ell < \frac{1}{\frac{1}{(\lambda_{\Delta+1}+1)^2} - \frac{1}{\lambda_\Delta^2}} \ .$$

■

Lemma A.8 *Let $\ell \geq 1$ and $1 \leq \Delta < \ell$ be such that $\lambda_\Delta \geq \lambda_{\Delta+1}+2$. Denote $\lambda = \lambda_\Delta$ and $\Lambda = \lambda_{\Delta+1}$. Then*

$$\theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\Lambda), \lambda, \Lambda) \geq 0 \ .$$

The proof of this lemma is quite long, and has thus been deferred to Appendix B. However, we will give here a proof sketch.

Proof Sketch Let Δ_0 and ℓ_0 be fixed constants such that $1 \leq \Delta_0 \leq \ell_0$, and the constants $\Lambda = \lambda_{\Delta_0+1}$ and $\lambda = \lambda_{\Delta_0}$ are such that $\lambda \geq \Lambda + 2$.

For real Δ and ℓ, denote

$$t(\Delta, \ell) = \theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\Lambda), \lambda, \Lambda) \ .$$

The mapping $\Delta \mapsto t(\Delta, \ell_0)$ is a $\cap$-concave quadratic polynomial. By Lemma A.4 we conclude that

$$\frac{\ell_0 - (\lambda^2-1)}{\lambda^2} \leq \Delta_0 = \left\lfloor \frac{\ell_0}{\lambda^2} \right\rfloor \leq \frac{\ell_0}{\lambda^2} \ .$$

Thus, it suffices to show that

$$t_1(\ell) = t(\frac{\ell - (\lambda^2-1)}{\lambda^2}, \ell) \ \text{ and } \ t_2(\ell) = t(\frac{\ell}{\lambda^2}, \ell)$$

are both nonnegative for $\ell = \ell_0$. The functions $t_1(\ell)$ and $t_2(\ell)$ are $\cap$-concave quadratic. By Lemma A.7 we have

$$0 < \ell_0 < \frac{1}{\frac{1}{(\Lambda+1)^2} - \frac{1}{\lambda^2}} \ .$$

Thus, if suffices to prove that

$$t_1(0),\ \ t_1(\frac{1}{\frac{1}{(\Lambda+1)^2}-\frac{1}{\lambda^2}}),\ \ t_2(0),\ \ t_2(\frac{1}{\frac{1}{(\Lambda+1)^2}-\frac{1}{\lambda^2}}),$$

are all nonnegative. This is indeed so. ■

Lemma A.9 *Let $\ell \geq 1$ and $1 \leq \Delta < \ell$ be such that $\lambda_\Delta \geq \lambda_{\Delta+1} + 2$. Then*

$$\theta_{\Delta,\Delta+1}(\ell) \leq \theta_{\Delta-1,\Delta}(\ell)\ .$$

Proof Immediate from Lemmas 2.20, 2.21, and A.8. ■

We can now prove Proposition 2.16.

Proof of Proposition 2.16 Immediate from Lemmas A.3, A.6, and A.9. ■

Appendix B

Proof of Lemma A.8

Proof of Lemma A.8 Let Δ_0 and ℓ_0 be fixed constants such that $1 \leq \Delta_0 \leq \ell_0$, and the constants $\Lambda = \lambda_{\Delta_0+1}$ and $\lambda = \lambda_{\Delta_0}$ are such that $\lambda \geq \Lambda + 2$. Let e and ϵ be integers such that $\Lambda = 1 + e$ and $\lambda = 1 + e + 2 + \epsilon$. Since $\Lambda \geq 1$ and $\lambda \geq 2 + \Lambda$, we conclude that $e \geq 0$ and $\epsilon \geq 0$. From this point to the end of the proof, let Λ be shorthand for $1 + e$, and let λ be shorthand for $1 + e + 2 + \epsilon$.

In the course of this proof we will derive expressions of the form

$$\sum_{i \geq 0, j \geq 0} a_{i,j} e^i \epsilon^j \ ,$$

where there are a finite number of $a_{i,j} \neq 0$. If the above expression satisfies $a_{i,j} \geq 0$ and $a_{0,0} > 0$, then we will call it a positive-term expression. Similarly, an expression for which $a_{i,j} \leq 0$ and $a_{0,0} < 0$ will be called negative-term. Obviously, if an expression is positive-term (negative-term), then it is positive (negative) when $e \geq 0$ and $\epsilon \geq 0$.

Denote

$$t(\Delta, \ell) = \theta_{\Delta-1,\Delta}(\ell, \rho_{\Delta-1}(\lambda), \zeta_\Delta(\lambda), \lambda, \lambda) - \theta_{\Delta,\Delta+1}(\ell, \zeta_\Delta(\lambda), \rho_{\Delta+1}(\Lambda), \lambda, \Lambda) \ .$$

We will prove that $t(\Delta_0, \ell_0) \geq 0$. However, we will not assume that Δ and ℓ are such that $1 \leq \Delta \leq \ell$. More so, we will let Δ and ℓ range over the reals. Note that this is OK, since all relevant equations ((2.2), (2.3), (2.17), (2.18), (2.19)) are defined for this general case.

Let

$$c_1 = \begin{cases} 24(3+2e)(3+e+\epsilon)(1+\ell) & \text{if } \lambda_0 = q/2 \\ 12(3+2e)(7+2e+2\epsilon)(1+\ell) & \text{otherwise} \end{cases} ,$$

$$c_2 = \lambda_0^4 , \quad c_3 = (1+\epsilon)(5+2e+\epsilon)^2 .$$

Note that c_1, c_2, and c_3 are positive. Denote

$$t'(\Delta, \ell) = t(\Delta, \ell) \cdot c_1 \quad .$$

The mapping $\Delta \mapsto t'(\Delta, \ell_0)$ is a quadratic polynomial. Since the coefficient of Δ^2 in $t'(\Delta, \ell_0)$ is negative-term, we conclude that it is a $\cap$-concave quadratic polynomial. From Lemma A.4 we conclude that

$$\frac{\ell_0 - (\lambda^2 - 1)}{\lambda^2} \leq \Delta_0 = \left\lfloor \frac{\ell_0}{\lambda^2} \right\rfloor \leq \frac{\ell_0}{\lambda^2} .$$

Thus, it suffices to show that

$$t_1(\ell) = t'(\frac{\ell - (\lambda^2 - 1)}{\lambda^2}, \ell) \cdot c_2 \text{ and } t_2(\ell) = t'(\frac{\ell}{\lambda^2}, \ell) \cdot c_2$$

are both nonnegative for $\ell = \ell_0$.

The mapping $\ell \mapsto t_1(\ell)$ is yet another quadratic polynomial. The coefficient of ℓ^2 is negative-term. The same goes for $\ell \mapsto t_2(\ell)$.

By Lemma A.7 we have

$$0 < \ell_0 < \frac{1}{\frac{1}{(\Lambda+1)^2} - \frac{1}{\lambda^2}} .$$

Thus, if suffices to prove that

$$t_1(0), \;\; t_1(\frac{1}{\frac{1}{(\Lambda+1)^2} - \frac{1}{\lambda^2}}) \cdot c_3, \;\; t_2(0), \;\; t_2(\frac{1}{\frac{1}{(\Lambda+1)^2} - \frac{1}{\lambda^2}}) \cdot c_3,$$

are all nonnegative. This is so because they are all positive-term. ■

B.1 'Mathematica' input for the $\lambda \neq q/2$ case

We have not stated the actual expressions referred to in the proof of Lemma A.8, since they are quite long. However, if the reader would like to validate the proof, he/she may find it useful to run the following on the ‘Mathematica’ software. The input is the series of calculations referred to in the proof of Lemma A.8, and should be self-explanatory. The output should validate the proof. The following is the input for the $\lambda \neq q/2$ case.

```
lambdaDelta = 1+e+2+epsilon
lambdaDeltaPlusOne = 1+e
ROdd = 1 / Binomial[l+1,2] ( (l+1)(r-theta delta)
       - Binomial[r+1,2](2lambda+1)
       + Binomial[lambda+1,2]
       delta(1+2r-(2lambda+1)/3 delta) )
rhoOdd = (l + delta(lambda^2+lambda) + 1/2 - lambda)
        / (2lambda+1)
zetaOdd = (l + delta(lambda^2+lambda) + 1) / (2lambda+1)
ROddRho = (ROdd /. r->rhoOdd)
ROddZeta = (ROdd /. r->zetaOdd)
RDeltaMinusOne = (ROddRho /. {delta->delta-1,
                 lambda->lambdaDelta})
RDelta = (ROddZeta /. lambda->lambdaDelta)
RDeltaPlusOne = (ROddRho /. {delta->delta+1,
                lambda->lambdaDeltaPlusOne})
Simplify[Solve[RDeltaMinusOne == RDelta, theta]]
thetaDeltaMinusOneDelta = %[[1]][[1]][[2]]
Simplify[Solve[RDeltaPlusOne == RDelta, theta]]
thetaDeltaDeltaPlusOne = %[[1]][[1]][[2]]
thetaDeltaMinusOneDelta - thetaDeltaDeltaPlusOne
t = Simplify[% * (12 (3 + 2 e)
            (7 + 2 e + 2 epsilon) (1 + l))]
Limit[%/delta^2, delta -> Infinity]
Expand[%]
t1 = Simplify[Expand[(t /. delta->l/lambdaDelta^2)
            * lambdaDelta^4]]
Limit[t1/l^2, l->Infinity]
Expand[%]
t1 /. l->0
Expand[%]
Simplify[( t1 /. l->1/(1/(1+lambdaDeltaPlusOne)^2
        - 1/lambdaDelta^2) )
        * ((1+epsilon)(5+2e + epsilon)^2)]
```

```
Expand[%]
t2 = Simplify[Expand[(t /. delta->(l - lambdaDelta^2 +1)
             / lambdaDelta^2)*lambdaDelta^4]]
Limit[t2/l^2, l->Infinity]
Expand[%]
t2 /. l->0
Expand[%]
Simplify[( t2 /. l->1/(1/(1+lambdaDeltaPlusOne)^2
        - 1/lambdaDelta^2) )
        * ((1+epsilon)(5+2e + epsilon)^2)]
Expand[%]
```

B.2 ‘Mathematica’ input for the $\lambda = q/2$ case

The following is the input for the $\lambda = q/2$ case.

```
lambdaDelta = 1+e+2+epsilon
lambdaDeltaPlusOne = 1+e
ROdd = 1 / Binomial[l+1,2] ( (l+1)(r-theta delta)
       - Binomial[r+1,2](2lambda+1)
       + Binomial[lambda+1,2]
       delta(1+2r-(2lambda+1)/3 delta) )
REven = 1 / Binomial[l+1,2] ( (l+1)(r-theta delta)
        - Binomial[r+1,2](2lambda+1)
        + Binomial[lambda+1,2]
        delta(1+2r-(2lambda+1)/3 delta)
        + Binomial[r - lambda delta + 1, 2])
rhoEven = (l + delta lambda^2 + 1 - lambda)/(2 lambda)
zetaEven = (l + delta lambda^2 + 1)/(2 lambda)
rhoOdd = (l + delta(lambda^2+lambda)
         + 1/2 - lambda) / (2lambda+1)
REvenRho = (REven /. r->rhoEven)
REvenZeta = (REven /. r->zetaEven)
ROddRho = (ROdd /. r->rhoOdd)
RDeltaMinusOne = (REvenRho /. {delta->delta-1,
                 lambda->lambdaDelta})
RDelta = (REvenZeta /. lambda->lambdaDelta)
RDeltaPlusOne = (ROddRho /. {delta->delta+1,
                lambda->lambdaDeltaPlusOne})
Simplify[Solve[RDeltaMinusOne == RDelta, theta]]
thetaDeltaMinusOneDelta = %[[1]][[1]][[2]]
Simplify[Solve[RDeltaPlusOne == RDelta, theta]]
thetaDeltaDeltaPlusOne = %[[1]][[1]][[2]]
thetaDeltaMinusOneDelta - thetaDeltaDeltaPlusOne
t = Simplify[Expand[% * 24(3 + 2e)
            (3 + e + epsilon)(1 + l)]]
Limit[%/delta^2, delta -> Infinity]
Expand[%]
t1 = Simplify[Expand[(t /. delta->l/lambdaDelta^2)
             * lambdaDelta^4]]
Limit[t1/l^2, l->Infinity]
Expand[%]
t1 /. l->0
Expand[%]
Simplify[( t1 /. l->1/(1/(1+lambdaDeltaPlusOne)^2
        - 1/lambdaDelta^2) )
        ((1+epsilon)(5+2e + epsilon)^2)]
Expand[%]
t2 = Simplify[Expand[(t /. delta->
             (l - lambdaDelta^2 +1)/lambdaDelta^2)
             lambdaDelta^4]]
Limit[t2/l^2, l->Infinity]
Expand[%]
t2 /. l->0
Expand[%]
Simplify[( t2 /. l->1/(1/(1+lambdaDeltaPlusOne)^2
        - 1/lambdaDelta^2) )
        ((1+epsilon)(5+2e + epsilon)^2)]
Expand[%]
```

Bibliography

[1] D. Augot and L. Pecquet. A Hensel lifting to replace factorization in list-decoding of algebraic-geometric and Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 46:2605–2614, 2000.

[2] E.R. Berlekamp. *Algebraic Coding Theory.* Aegean Park Press, Laguna Hills, California, revised edition, 1984.

[3] E.R. Berlekamp. Bounded distance +1 soft-decision Reed-Solomon decoding. *IEEE Trans. Inform. Theory*, 42:704–719, 1996.

[4] S.R. Blackburn. Fast rational interpoloation, Reed-Solomon decoding, and the linear complexity profile of sequences. *IEEE Trans. Inform. Theory*, 43:537–548, 1997.

[5] R.E. Blahut. *Theory and Practice of Error-Control Codes.* Addison-Wesley, Reading, Massachusetts, 1983.

[6] D. Dabiri and I.F. Blake. Fast parallel algorithms for decoding Reed-Solomon codes based on remainder polynomials. *IEEE Trans. Inform. Theory*, 41:873–885, 1995.

[7] P. Elias. Error-correcting codes for list decoding. *IEEE Trans. Inform. Theory*, 37:5–12, 1991.

[8] R.G. Gallager. *Information Theory and Reliable Communications.* John Wiley, New York, 1968.

[9] R.L. Graham, D.E. Knuth, and O. Patashnik. *Concrete Mathematics.* Addison-Wesley Publishing Company, second edition, 1994.

[10] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 45:1757–1767, 1999.

[11] S.M. Johnson. A new upper bound for error-correcting codes. *IEEE Trans. Inform. Theory*, 8:203–207, 1962.

[12] R. Koetter and A. Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. preprint, May 2000.

[13] R. Koetter and A. Vardy. Decoding of Reed-Solomon codes for additive cost functions. In *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2002)*, page 313, Lausanne, Switzerland, July 2002.

[14] C.Y. Lee. Some properties of nonbinary error-correcting codes. *IRE Trans. Inform. Theory*, 4:77–82, 1958.

[15] X. Ma and X.-M. Wang. On the minimal interpolation problem and decoding RS codes. *IEEE Trans. Inform. Theory*, 46:1573–1580, 2000.

[16] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[17] J.L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inform. Theory*, 15:122–127, 1969.

[18] L.E. Mazur. Codes correcting errors of large weight in Lee metric. *Problems. Inform. Transm.*, 9:277–281, 1973.

[19] R.R. Nielsen and T. Høholdt. Decoding Reed-Solomon codes beyond half the minimum distance. In J. Buchmann, T. Høholdt, H. Stichtenoth, and H. Tapia-Recillas, editors, *Coding Theory, Cryptography and Related Areas*, pages 221–236. Springer, Berlin, 2000.

[20] H. O'Keeffe and P. Fitzpatrick. Gröbner basis solution of constrained interpolation problems. *Lin. Alg. Appls.*, pages 533–551, 2002.

[21] V. Olshevsky and M.A. Shokrollahi. A displacement structure approach to efficient decoding of algebraic geometric codes. In *Proc. 31st ACM Symp. Theory of Computing (STOC'99)*, pages 235–244, Atlanta, Georgia, USA, 1999. ACM, New York, 1999.

[22] R.M. Roth. *Lecture Notes in Coding Theory.*

[23] R.M. Roth and G. Ruckenstein. Efficient decoding of Reed-Solomon codes beyond half the minimum distance. *IEEE Trans. Inform. Theory*, 46:246–257, 2000.

[24] R.M. Roth and P.H. Siegel. Lee-metric BCH codes and their application to constrained and partial-response channels. *IEEE Trans. Inform. Theory*, 40:1083–1096, 1994.

[25] S. Sakata, Y. Numakami, and M. Fujisawa. A fast interpolation method for list decoding of RS and algebraic-geometric codes. In *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2000)*, page 479, Sorrento, Italy, 2000.

[26] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *J. Compl.*, 13:180–193, 1997.

[27] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. A method for solving key equation for decoding Goppa codes. *Inform. Control*, 27:87–99, 1975.

[28] L.R. Welch and E.R. Berlekamp. Error correction of algebraic block codes. US Patenet 4,633,470, 1986.

פענות-רשימה עבור קודי מטריקת Lee

עדו טל

פענוח-רשימה עבור קודי מטריקת Lee

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת תואר
מגיסטר למדעים במדעי המחשב

עדו טל

הוגש לסנט הטכניון – מכון טכנולוגי לישראל
תמוז ה'תשס"ג חיפה יולי 2003

המחקר נעשה בהנחיית פרופ' רוני רוט בפקולטה למדעי המחשב.

ברצוני להודות מקרב לב לפרופ' רוני רוט על כך שמצא עבורי בעיה מעניינת לחקור, על הדיונים שהיו לעזר רב בהשגת תוצאות המחקר, על כל מה שלמדתי ממנו, ואחרון אך לא בחשיבותו – על סבלנותו והאופטימיות שלו לאורך הדרך.

תודה מיוחדת לאשתי סמדר על אהבתה ועידודה.

אני מודה לטכניון על התמיכה הכספית הנדיבה בהשתלמותי.

תוכן עניינים

תקציר 1

רשימת קיצורים וסמלים 2

1 מבוא 3

1.1 מפענח רשימה-ℓ 4

1.2 מטריקת Hamming ומטריקת Lee 6

1.3 קודי GRS וקודי alternant 7

1.4 פענוח-רשימה בעזרת פולינומים בעלי שני משתנים 7

1.5 חסם מסוג Johnson 10

1.5.1 חסם מסוג Johnson עבור מטריקת Lee 11

1.6 מבנה העבודה 12

2 מפענח רשימה עבור מטריקת **Lee** 13

2.1 מבוא 13

2.2 חסימת r^* ו- Δ^* 16

2.3 מקסימיזציה של R עבור Δ נתון 18

2.3.1 נוסחה עקיפה ל- r_Δ 19

2.3.2 מציאת λ_Δ 21

2.3.3 מסקנה לגבי Δ קבוע 22

2.4 מציאת המקטעים הלינאריים של $R(\theta, \ell)$ 22

2.4.1 טענות והגדרות קדם 24

2.5 הידוק נוסף של החסמים 27

2.5.1 חסמים שאינם הדוקים 28

2.5.2 חסם הדוק 28

3 אסימפטוטיקה 32

3.1 נוסחה עקיפה ל- w^* 33

3.2 מציאת $\Lambda(w^*)$ 35
3.3 מסקנה לגבי המקרה האסימפטוטי 35

4 הצדקה לבחירת ה- score 38

5 הערות 45
5.1 בחירת הקוד וההתאמה החח"ע 45
5.2 מפענחים נוספים 46

A הוכחת טענה 2.16 49
A.1 המקרה בו $\lambda_\Delta = \lambda_{\Delta+1}$ 49
A.2 המקרה בו $\lambda_\Delta = \lambda_{\Delta+1} + 1$ 50
A.3 המקרה בו $\lambda_\Delta = \lambda_{\Delta+1} + 2$ 51

B הוכחת למה A.8 54
B.1 קלט ‘Mathematica’ עבור המקרה בו $\lambda \neq q/2$ 55
B.2 קלט ‘Mathematica’ עבור המקרה בו $\lambda = q/2$ 57

תקציר בעברית ה

רשימת איורים

1.1 אלגוריתם פענוח גנרי עבור קוד $\mathcal{C}$ בעזרת פולינום בשני משתנים. 9

2.1 העקומה $\theta \mapsto R_\Delta(\theta, \ell)$ עבור $\ell = 5$, $q = 9$, ו- $\Delta = 1, 2, 3, 4, 5$. 23
2.2 $R(\theta, \ell, r, \Delta, \lambda)$ עבור ערכים שונים של r. 25
2.3 הוכחה גרפית של למה 2.20. 26
2.4 הוכחה גרפית של למה 2.21. 27
2.5 העקומה $\theta \mapsto R(\theta, \ell)$ עבור $q = 9$ ו- $\ell = 7, 8$. 29
2.6 $x \mapsto r - x\Delta$ בהשוואה ל- $x \mapsto r' - x\Delta'$. 30

3.1 העקומה $\theta \mapsto R(\theta, \ell)$ וחסם Johnson עבור $q = 5$ ו- $\ell = 7, \infty$. 37

4.1 גרף של μ לעומת μ' בלמה 4.5. 43
4.2 גרף של μ לעומת μ' בלמה 4.7. 44

5.1 השוואת רדיוסי פענוח עבור קודי GRS. 47
5.2 השוואת רדיוסי פענוח עבור קודי alternant. 48

תקציר

יהי F שדה סופי, ותהי $\mathcal{C}$ תת-קבוצה של F^n, הנקראת קוד. מילת קוד $\mathbf{c} \in \mathcal{C}$ משודרת דרך ערוץ רועש, ומשובשת ע"י וקטור שגיאה $\mathbf{e}$. אנו מקבלים את $\mathbf{y}$, שהיא המילה המשובשת ($\mathbf{y} = \mathbf{c} + \mathbf{e}$), ורוצים לגלות מהי $\mathbf{c}$.

יהי $\mathcal{D} : F^n \to 2^{\mathcal{C}}$ מפענח רשימה-ℓ בעל רדיוס פענוח τ ביחס למטריקה נתונה $\mathrm{d} : F^n \times F^n \to \mathbb{R}$. מפענח זה הוא הכללה של פענוח קלאסי; בהנתן מילה נקלטת $\mathbf{y}$, יהי $\mathcal{D}(\mathbf{y})$ הפלט של מפענח הרשימה-ℓ. הפלט $\mathcal{D}(\mathbf{y})$ הוא רשימה של ℓ מילות קוד לכל היותר, ומובטח שרשימה זו תכלול את כל מילות הקוד בכדור בעל רדיוס τ שמרכזו $\mathbf{y}$. תחת ההנחה שנפלו ב- $\mathbf{y}$ לכל היותר τ שגיאות, $\mathbf{c}$ שייכת בהכרח ל- $\mathcal{D}(\mathbf{y})$, מה שייחשב הצלחה בפענוח. בהנתן הרשימה $\mathcal{D}(\mathbf{y})$, עלינו לבחור מילה מסוימת מתוכה כניחוש שלנו למילת הקוד. בחירה זו יכולה להיות המילה הקרובה ביותר למילה הנקלטת. לחילופין, אם ידועה לנו אינפורמציה נוספת על התפלגות מילות הקוד, אנו יכולים להתחשב בה בעת בחירת מילה זו.

בעבודה זו נעסוק בקידוד למטריקת Lee, המופיעה ביישומים כמו אפנון PSK. נסמן ב-$[n]$ את הקבוצה $\{1, 2, \ldots, n\}$. בהנתן שדה F בגודל q, נסמן ב- $\mathbb{Z}_q$ את חוג השלמים מודולו q, ונסמן ב- 1 את היחידה הכפלית ב- $\mathbb{Z}_q$. אזי, משקל Lee של איבר $a \in \mathbb{Z}_q$, המסומן $|a|$, מוגדר כשלם האי-שלילי הקטן ביותר s כך ש- $s \cdot 1 \in \{a, -a\}$. עבור פונקציה חח"ע נתונה $\langle \cdot \rangle : F \to \mathbb{Z}_q$ נגדיר את מרחק Lee

$\mathsf{d}_{\mathcal{L}}$ בין שני איברים x, y ב- F כ-

$$\mathsf{d}_{\mathcal{L}}(x,y) \triangleq |\langle x \rangle - \langle y \rangle| \ .$$

מרחק Lee בין שתי מילים $\mathbf{x} = (x_i)_{i \in [n]}$ ו- $\mathbf{y} = (y_i)_{i \in [n]}$ (מעל F) מוגדר כ-

$$\mathsf{d}_{\mathcal{L}}(\mathbf{x},\mathbf{y}) \triangleq \sum_{i=1}^{n} \mathsf{d}_{\mathcal{L}}(x_i,y_i) \ .$$

מפענח רשימה בזמן פולינומי במטריקת Lee מוצג ומנותח עבור קודי alternant, שהם תת-קודים, השייכים לתת-שדה של קודי Reed-Solomon. יהי Φ שדה הר-חבה של F ותהי $\Phi_k[x]$ קבוצת כל הפולינומים מעל Φ ממעלה קטנה מ- k. קוד GRS בעל אורך n ומימד k מוגדר באמצעות מצייני עמודות $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Phi$ שונים וכופלי עמודות $v_1, v_2, \ldots, v_n \in \Phi$ שונים מאפס.

$$\mathcal{C}_{\mathrm{GRS}} = \{\mathbf{c} = (v_1 u(\alpha_1) \ \ v_2 u(\alpha_2) \ \ \ldots \ \ v_n u(\alpha_n)) \ : \ u(x) \in \Phi_k[x]\} \ .$$

קוד ה- alternant $\mathcal{C}_{\mathrm{alt}}$ מוגדר כחיתוך של קוד ה- GRS עם השדה F, דהיינו

$$. \ \mathcal{C}_{\mathrm{alt}} = \mathcal{C}_{\mathrm{GRS}} \cap F^n$$

בהנתן קוד alternant $\mathcal{C}$ ואורך רשימה ℓ, אנו מראים נוסחה לרדיוס הפענות τ. נוסחה זו היא פונקציה של אורך הרשימה ℓ, של פרמטרי קוד ה- GRS המתאים לקוד $\mathcal{C}$, ושל שני פרמטרים נוספים שיסומנו r ו- Δ. פרמטרים אלו נקבעים ע"י המתכנן. מכיוון שהפרמטרים r ו- Δ משפיעים על רדיוס הפענות, אנו נבחר את

הערכים האופטימליים עבורם.

חלק ניכר מהעבודה עוסק בניתוח הערכים האופטימליים של r ו- Δ. עבור ערך קבוע של Δ אנו מראים נוסחה לחישוב הערך האופטימלי של r. בנוסף, עבור Δ ו- ℓ נתונים, אנו יודעים לקבוע אם Δ הוא אופטימלי עבור הקוד $\mathcal{C}$. למעשה, אנו יודעים את תחום הפרמטרים של $\mathcal{C}$ עבורם Δ נתון הוא אופטימלי. כאשר $\ell \to \infty$ אנו מראים נוסחה סגורה לערכים האופטימליים של r ו- Δ. נוסחה סגורה לערכים האופטימליים של r ו- Δ רצויה, כמובן, גם עבור המקרה הלא אסימפטוטי, אך לא מצאנו כזאת.

מפענח הרשימה שלנו מתבסס על עבודות קודמות של Koetter&Vardy וכן של Guruswami&Sudan. בפרט, המפענח מבוסס על חישוב פולינום דו-משתני $Q(x,z)$ ומציאת שורשי z שלו, כלומר מציאת פולינומים $u(x)$ ב- $\Phi_k[x]$ עבורם $Q(x,u(x))=0$. קבוצת שורשים זו ממופה לקבוצת מילות הקוד ברשימה. המיפוי של פולינום $u(x)$ למילת קוד $\mathbf{c}$ הוא

$$\mathbf{c} = (v_1u(\alpha_1)\ \ v_2u(\alpha_2)\ \ \ldots\ \ v_nu(\alpha_n))\ .$$

הפולינום הדו-משתני נקבע ע"י מערכת משוואות לינאריות. בסכמה הכללית שהוצגה ע"י Koetter&Vardy (סכמה זו איננה מוגבלת למטריקה כלשהי), מתכנן המפענח קובע את מערכת המשוואות הלינאריות, ובכך קובע את ביצועי המפענח. אנו בחרנו להתמקד במשפחה מסוימת של משוואות לינאריות עבור מטריקת Lee. לכל ערך חוקי של r ו- Δ מתאימה מערכת משוואות לינאריות במשפחה זו. אנו מראים כי תחת הקלות מסוימות, משפחה זו מכילה את מערכת המשוואות הלינאריות, עבורה רדיוס הפענוח הוא אופטימלי.

חסם מסוג Johnson מאפשר לחסום מלמטה את רדיוס הפענוח האופטימלי שניתן להשיג עבור קוד נתון ואורך רשימה נתון. החסם איננו מוגבל למפ-

ענחי רשימה מסוג מסוים. רדיוס הפענוח שהושג ע"י Koetter&Vardy במטריקת Hamming מתלכד עם רדיוס הפענוח המובטח מחסם שכזה. אולם, שלא בדומה למקבילה במטריקת Hamming, רדיוס הפענוח של מפענח הרשימה שלנו הוא באופן כללי גדול ממש ממה שמובטח מגרסת מטריקת Lee של חסם Johnson.

בחירת הקוד וההעתקה החח"ע $\langle\cdot\rangle : F \to \mathbb{Z}_q$ הם באחריות המתכנן. חלקה האחרון של העבודה מוקדש לדיון בנושא זה. בפרט, מוזכרים קודים והעתקות בהן המרחק המינימלי של הקוד במטריקת Lee הוא טוב יותר מהמרחק המינימלי שלו במטריקת Hamming.