COMPLETE WEIGHT ENUMERATORS AND PROBABILITY OF UNDETECTED ERROR FOR SOME REED-SOLOMON CODES

by

KAIMING HO

B.A.Sc. (Electrical Engineering), University of Waterloo, Canada, 1993

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

in

THE FACULTY OF GRADUATE STUDIES

DEPARTMENT OF ELECTRICAL ENGINEERING

We accept this thesis as conforming

to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

August 1995

In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Electrical Engineering

The University of British Columbia
Vancouver, Canada

Date Aug. 14/95

Abstract

The Hamming weight enumerators for Reed-Solomon codes are known, but do not often adequately describe the structure of the codes. Complete weight enumerators, on the other hand, describe the code in more detail, but are more difficult to determine. A procedure described by Blake and Kith [1] is used to derive the complete weight enumerators for Reed-Solomon and extended Reed-Solomon codes of dimensions one, two and three.

Binary codes may be obtained from Reed-Solomon codes over a field with $q = 2^m$ elements. Many different bases may be used to obtain these binary codes. We analyse conditions under which two bases will yield binary codes with the same weight distribution.

We also consider the probability of undetected error of these binary codes. It has been shown by Kasami and Lin that (n,k) Reed-Solomon codes used over a q-ary symmetric channel are proper. In this thesis, it is shown that the binary expansions of these codes and their extensions, when used on the binary symmetric channel, are not necessarily proper. In particular, the codes of rate less than $[1 - \log_2 m + \frac{m-1}{m} \log_2(m-1)]$ are not proper.

Contents

List of Tables

List of Figures

Acknowledgment

The author would like to gratefully acknowledge the support of Dr. Cyril Leung, whose guidance and advice were invaluable. This work was also partially supported by NSERC Grant OGP0001731. Finally, many thanks to my brother, with whom I had many discussions about this thesis.

1 Introduction

1.1 Communications and coding theory

Error control coding theory is the study of redundant codes, used to make communication more reliable [2, 3, 4]. Data is transformed into a suitable format and transmitted to its destination through some media (a wire, or free space, for example), which we model mathematically as a channel. The most common type of channel model is the binary symmetric channel (BSC). One bit (0 or 1) is transmitted through the BSC at a time, with a certain probability ϵ of making an error (0 becomes a 1, and vice versa). The term symmetric refers to the fact that this probability is independent of whether a 0 or a 1 was transmitted. We often assume that the channel is memoryless. That is to say, the present and future performance of the channel is independent of its past behaviour. Other channel models exist [5, 6], but in this thesis, we only consider symmetric, memoryless channels.

In block error control coding, redundancy bits are added to a block of k information bits, resulting in a new block (called a codeword) of $n > k$ bits. The way in which this redundancy is added defines the encoding operation of the code. Since there are 2^k different k-tuples of information bits, not all 2^n binary n-tuples are valid codewords. The channel may introduce errors to the codeword by changing some of the co-ordinates in the n-tuple. The receiver takes the n-tuple, which may contain errors, and tries to determine the original k bits of information. If the received n-tuple is not a valid codeword, then errors must have occured. Some codes add enough redundancy such that some of these errors may be corrected. Others will simply detect the presence of errors, and ask for a re-transmission. Another possibility may arise. The errors may change the transmitted

n-tuple onto a different n-tuple which is also a valid codeword. In that case, the receiver has no way of knowing that an error occured. This is called an undetected error, and naturally, we want to minimize its probability.

Since the birth of coding theory, much research has been devoted to finding the weight enumerator of codes [4, 7, 8]. This enumerator gives a description of how the weights of the individual codewords are distributed, and gives insight into how best to design a decoder. The probability of undetected error can be completely determined if the weight distribution is known. In general, determination of the weight enumerator is a difficult problem. Exhaustive enumeration of the codewords to find the weights is not feasible, if k and $n - k$ are very large.

1.2 Finite fields and coding theory

Abstract algebra plays an important role in the design and analysis of codes. We may generalize the binary digits (0 and 1) in the above discussion with a finite field of q elements [9, 10]. Codewords may be viewed as vectors over a finite field, and the code as a vector space over a finite field. Note that the set $\{0,1\}$ is also a field. The counterpart to the binary symmetric channel is then the q-ary symmetric channel. Codes may then be defined over this field, with Reed-Solomon codes being the best known class of non-binary codes. Surprisingly, the Hamming weight enumerator for all Reed-Solomon codes is known [11, 12]. In this thesis, we derive the complete weight enumerator (which describes non-binary codes better) for some Reed-Solomon codes.

1.3 Definition of terms and conventions

In this thesis the following conventions and symbols will be used, unless otherwise noted. Denote the field of q elements by $\mathbb{F}_q$, with $q = 2^m$. Let n be the block length of a code $\mathcal{C}$. Only Reed-

Solomon codes are considered, so $n = 2^m - 1$ is used throughout. The symbol α is used to denote a primitive element of $\mathbb{F}_q$. A useful way of describing the elements of $\mathbb{F}_q$ is $\{\alpha^j, j \in B\}$, where the set $B = \{\star, 0, 1, \ldots, n-1\}$, and $\alpha^\star = 0$ by convention. The multiplicative group of the non-zero elements of $\mathbb{F}_q$ is denoted $\mathbb{F}_q^\star = \{\alpha^j, j \in B^\star\}$, with $B^\star = \{0, 1, \ldots, n-1\} = B \setminus \star$.

The Reed-Solomon code over $\mathbb{F}_q$ of length n, dimension k, and generator polynomial

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+n-k-1}) \tag{1.1}$$

is $\mathrm{RS}_b(n,k)$ and $\mathrm{ERS}_b(q,k)$ is its extension [2]. When $b = 1$, the code is referred to as *narrow-sense.* Note that the dual [2, 4] of $\mathrm{RS}_b(n,k)$ is $\mathrm{RS}_{n-k+b}(n, n-k)$.

1.4 Organization of thesis

Non-binary codes over $\mathbb{F}_q$ are discussed in chapter 2. Complete weight enumerators (cwe's), which give a more accurate description of the code than Hamming weight enumerators, are described. The cwe's of the various Reed-Solomon codes to be analysed in subsequent sections are derived.

In chapter 3, the mapping of a non-binary code over $\mathbb{F}_q$ to a binary code over $\mathbb{F}_2$ is described. This mapping depends on the choice of a particular basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. It it shown that the weight distribution of the resulting binary code (called the *binary expansion* of the non-binary code) may vary depending on the choice of this basis. Furthermore, an equivalence relation is defined which partitions the bases, and reduces the number of distinct binary expansions.

The binary expansions of various Reed-Solomon codes are examined in chapter 4. Although Reed-Solomon codes are proper over $\mathbb{F}_q$ [13], it is shown that their binary expansions are not necessarily proper. The rate, r^*, below which all binary expansions of narrow-sense RS codes are improper is derived.

2 Non-binary channel error control codes

Codes over non-binary fields such as $\mathbb{F}_q$ are a simple extension of the more common binary codes. The concepts remain the same, but the mathematical operations are carried out in $\mathbb{F}_q$, rather than $\mathbb{F}_2$. Reed-Solomon codes are perhaps the most well known class of non-binary codes.

2.1 Complete weight enumerators

Often, a weight enumerator is used to describe the characteristics of a code. Although weight enumerators do not completely describe a particular code (i.e., given a weight enumerator, the individual codewords in the code cannot, in general, be deduced) they are sufficiently useful in analysis to warrant study. The most commonly used weight enumerator of a code, C, is the *Hamming weight enumerator*, a polynomial in an indeterminant, z, of degree of at most n. The coefficient of the z^i term, A_i, is the number of codewords in C of Hamming weight i. While Hamming weight enumerators describe binary codes well, they do a poor job in describing non-binary codes, since in $\mathbb{F}_q$, there are multiple non-zero elements which Hamming weight enumerators do not differentiate between. Complete weight enumerators, account for this, and are described below.

Let c be a codeword in C, an (n,k) code over $\mathbb{F}_q$. Its cwe describes the number of times each field element appears in c. The complete weight enumerator of the code C is the sum of the cwe of its individual codewords.

In general, the cwe of c may be described as

$$z_\star^{s_\star} z_0^{s_0} z_1^{s_1} \cdots z_{n-1}^{s_{n-1}} = \prod_{j \in B} z_j^{s_j} \tag{2.1}$$

where s_j is number of times α^j occurs in c. Note that $\sum_B s_j = n$, and hence, the cwe is a homogeneous form of order n in q variables. The cwe of $\mathcal{C}$ is a sum of these types of products. There are q^k terms in this sum.

Example: Consider the Reed-Solomon code over $\mathbb{F}_8$ with $k = 1$, and generator polynomial $g(x) = \prod_{i=1}^{6}(x - \alpha^i)$. The set B associated with $\mathbb{F}_8$ is $\{\star, 0, 1, 2, 3, 4, 5, 6\}$. This is the $\mathrm{RS}_1(7,1)$ code, and has the following codewords:

codeword	cwe
$(0\ 0\ 0\ 0\ 0\ 0\ 0)$	$z_\star^7$
$(1\ 1\ 1\ 1\ 1\ 1\ 1)$	z_0^7
$(\alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha\ \alpha)$	z_1^7
$(\alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2\ \alpha^2)$	z_2^7
$(\alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3\ \alpha^3)$	z_3^7
$(\alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4\ \alpha^4)$	z_4^7
$(\alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5\ \alpha^5)$	z_5^7
$(\alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6\ \alpha^6)$	z_6^7

The cwe of the code is therefore

$$z_\star^7 + z_0^7 + z_1^7 + z_2^7 + z_3^7 + z_4^7 + z_5^7 + z_6^7 = \sum_{j \in B} z_j^7.$$

2.2 Deriving the cwe of some RS codes

The problem of finding the cwe of a code is difficult in general[1], and cannot be solved without explicitly enumerating the individual codewords, except in some simple cases. In this section, we describe the method used by Blake [1]. The cwe of some other codes, which are analysed in chapter 4, are derived, using the same methodology.

Let $f(x)$ be a polynomial over $\mathbb{F}_q$ and define $\mathrm{v}(f)$ to be the n-tuple

$$\mathrm{v}(f) = (f(1), f(\alpha), \ldots, f(\alpha^{n-1})) \in \mathbb{F}_q^n. \tag{2.2}$$

[1] See research problem 11.2 in [4].

For a subset $I \subseteq B^\star$, let $P(I)$ be

$$P(I) = \left\{ \sum_{i \in B^\star} a_i x^i \;\middle|\; \begin{array}{l} a_i \in \mathbb{F}_q \text{ if } i \in I \\ a_i = 0 \text{ otherwise} \end{array} \right\}.$$

In words, $P(I)$ is the set of all polynomials with coefficients ($\in \mathbb{F}_q$) corresponding to terms with degrees in I. If there are k elements in I, $P(I)$ will contain q^k polynomials, including the zero polynomial.

It can be shown that [14, 1]

$$\mathrm{RS}_b(n,k) = \{\mathbf{v}(f) \mid f \in P(\bar{Z})\} \tag{2.3}$$

where Z is the set of zeros of the code (i.e., roots of the generator polynomial), and $\bar{Z} = B^\star \setminus Z$. Note then, that $\bar{Z}$ is the set of zeros of the parity check polynomial. Also see [2].

For $\mathrm{RS}_b(n,k)$, $Z = \{b, b+1, \ldots, b+n-k-1\}$, and hence $\bar{Z} = \{b-k, b-k+1, \ldots, b-1\}$. Let

$$\theta_i = \begin{bmatrix} 1 & \alpha^i & \alpha^{2i} & \cdots & \alpha^{(n-1)i} \end{bmatrix}.$$

From [2], the parity check matrix of $\mathrm{RS}_b(n,k)$ is then,

$$H = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{b+n-k-1} & \alpha^{2(b+n-k-1)} & \cdots & \alpha^{(n-1)(b+n-k-1)} \end{bmatrix} = \begin{bmatrix} \longleftarrow & \theta_b & \longrightarrow \\ \longleftarrow & \theta_{b+1} & \longrightarrow \\ & \vdots & \\ \longleftarrow & \theta_{b+n-k-1} & \longrightarrow \end{bmatrix}$$

The corresponding generator matrix G can be worked out, since $GH^T = 0$.

$$G = \begin{bmatrix} \longleftarrow & \theta_{b-k} & \longrightarrow \\ \longleftarrow & \theta_{b-k+1} & \longrightarrow \\ & \vdots & \\ \longleftarrow & \theta_{b-1} & \longrightarrow \end{bmatrix}.$$

Note that θ_i is orthogonal to θ_j if $i+j \neq 0 \bmod n$, which follows from

$$\begin{aligned}\theta_i \cdot \theta_j &= \sum_{l=0}^{n-1} \alpha^{il}\alpha^{jl} = \sum_{l=0}^{n-1} \alpha^{l(i+j)} \\ &= \begin{cases} 0 & \text{if } i+j \neq 0 \bmod n. \text{ see eqn. (A.3)} \\ 1 & \text{otherwise} \end{cases}\end{aligned}$$

Let $f(x)$ from eqn. (2.3) be

$$c_1 x^{b-k} + c_2 x^{b-k+1} + \cdots + c_k x^{b-1} = \begin{bmatrix} c_1 & \cdots & c_k \end{bmatrix} \begin{bmatrix} x^{b-k} \\ x^{b-k+1} \\ \vdots \\ x^{b-1} \end{bmatrix}$$

A codeword c would then be of the form

$$\begin{aligned} c &= \begin{bmatrix} f(1) & f(\alpha) & \cdots & f(\alpha^{n-1}) \end{bmatrix} \\ &= \begin{bmatrix} c_1 & \cdots & c_k \end{bmatrix} \begin{bmatrix} 1 & \alpha^{b-k} & (\alpha^2)^{b-k} & \cdots & (\alpha^{n-1})^{b-k} \\ 1 & \alpha^{b-k+1} & (\alpha^2)^{b-k+1} & \cdots & (\alpha^{n-1})^{b-k+1} \\ 1 & \alpha^{b-k+2} & (\alpha^2)^{b-k+2} & \cdots & (\alpha^{n-1})^{b-k+2} \\ \vdots & & & & \vdots \\ 1 & \alpha^{b-1} & (\alpha^2)^{b-1} & \cdots & (\alpha^{n-1})^{b-1} \end{bmatrix} \\ &= \begin{bmatrix} c_1 & \cdots & c_k \end{bmatrix} G \end{aligned}$$

Each value of f corresponds to a codeword in the code. The cwe for the code is then determined by considering $\mathbf{v}(f)$ for all possible values of a_i. In the simple case for $\mathrm{RS}_1(n,1)$, $P(\bar{Z})$ consists of the set of constants a_0. Therefore, $f(x) = a_0$, for any value of x, and $\mathbf{v}(f) = (a_0, a_0, \ldots, a_0)$. The q codewords in the code are obtained by letting a_0 vary over $\mathbb{F}_q$, and it is clear that each codeword is then an n-tuple with identical elements. So,

$$\text{cwe of } \mathrm{RS}_1(n,1) = \sum_{j \in B} z_j^n. \tag{2.4}$$

In general, things are more complicated, since $f(x)$ is not necessarily a constant. We would like to examine the co-ordinates of $\mathbf{v}(f)$ in eqn. (2.2). To facilitate this, take a value of $j \in B$, and the equation

$$f(x) = \alpha^j . \tag{2.5}$$

The number of co-ordinates in the codeword corresponding to $f(x)$ is the number of different x (as x is varied over the non-zero elements of $\mathbb{F}_q$) for which eqn. (2.5) is true. So, the s_j in eqn. (2.1) are given by

$$s_j = \#\text{distinct solns of } x \text{ to eqn. (2.5)} \quad \text{over } \mathbb{F}_q^* . \tag{2.6}$$

Applying this, we can derive the cwe of some simple codes.

Lemma 2.1. *The cwe for $RS_1(n,2)^2$ and $RS_2(n,2)$ are the same, and is equal to*

$$\sum_{j \in B} z_j^n + n\gamma \sum_{i \in B} \frac{1}{z_i} \tag{2.7}$$

with $\gamma = \prod_{j \in B} z_j$.

Proof. For $\mathrm{RS}_1(n,2)$, $f(x) = a_0 + a_1 x^{n-1}$, while for $\mathrm{RS}_2(n,2)$, $f(x) = a_0 + a_1 x$. Therefore, s_j is equal to the number of solutions to the equation

$$a_0 + a_1 x^c = \alpha^j \tag{2.8}$$

whilst a_0 and a_1 are varied over $\mathbb{F}_q$, and c is either $n-1$ ($= -1 \bmod n$) or 1. There are two cases to consider.

Case I : $a_1 \neq 0$

[2] This case is given in [1].

If $a_1 \neq 0$, then

$$x^{\pm 1} = \frac{\alpha^j - a_0}{a_1} = \text{some constant in } \mathbb{F}_q. \tag{2.9}$$

Fixing a_1, eqn. (2.9) will have one solution for $x \in \mathbb{F}_q^\star$, provided $a_0 \neq \alpha^j$. If $a_0 = \alpha^j$, there will be no solutions for x, since x cannot be zero. So,

$$s_j = \begin{cases} 1 & \text{if } a_0 \neq \alpha^j \\ 0 & \text{if } a_0 = \alpha^j \end{cases} . \tag{2.10}$$

Varying a_0, the contribution to the cwe becomes

$$\underbrace{z_0 z_1 \cdots z_{n-1}}_{a_0=0} + \underbrace{z_\star z_1 \cdots z_{n-1}}_{a_0=1} + \underbrace{z_\star z_1 z_3 \cdots z_{n-1}}_{a_0=\alpha} + \cdots + \underbrace{z_\star z_0 \cdots z_{n-3} z_{n-1}}_{a_0=\alpha^{n-2}} + \underbrace{z_\star z_0 \cdots z_{n-2}}_{a_0=\alpha^{n-1}} = \gamma \sum_{i \in B} \frac{1}{z_i}$$

Since there are n non-zero values for a_1, the total contribution for Case I becomes $n\gamma \sum_{i \in B} \frac{1}{z_i}$.

Case II : $a_1 = 0$

For this case, eqn. (2.5) becomes $a_0 = \alpha^j$, and is independent of x. Therefore, x can take on any value in $\mathbb{F}_q^\star$, and hence,

$$s_j = \begin{cases} n & \text{if } a_0 = \alpha^j \\ 0 & \text{if } a_0 \neq \alpha^j \end{cases} .$$

So, the contribution for Case II is $\sum_{j \in B} z_j^n$, when the sum is taken over all possible values of a_0.

Combining the two cases, the cwe becomes:

$$\sum_{j \in B} z_j^n + n\gamma \sum_{i \in B} \frac{1}{z_i}$$

□

We now generalize the cwe given in eqn. (2.4) to values of b other than 1.

Lemma 2.2. *The cwe for $RS_b(n,1)$ for $b = 1 \bmod n$ is $\sum_{j\in B} z_j^n$. Otherwise, it is equal to*

$$z_\star + \frac{n}{d}\sum_{i=0}^{d-1} \prod_{j\in\{J_d+i\}} z_j^d \tag{2.11}$$

where $d = \gcd(b-1,n)$, and J_d is the set of elements in B^* which are a multiple of d. The set $\{J_d + i\}$ is obtained by adding i (modulo n) to every element in J_d.

Note that if $b-1$ and n are relatively prime (i.e., $d=1$) eqn. (2.11) becomes $z_\star^n + n\frac{\gamma}{z_\star}$. There are n elements in $B^\star$, of which only one in d is a multiple of d. So J_d has n/d elements.

Proof. The $b=1$ case was given earlier in eqn. (2.4). Since $\alpha^n = 1$, values of b such that $b = 1 \bmod n$ will give the same generator polynomial in eqn. (1.1). So, eqn. (2.4) is actually valid for values of $b = 1 \bmod n$. For other values of b, consider the argument given below:

The $z_\star^n$ term corresponds to the all-zeros codeword, present in every linear code. For the other codewords, the equation to examine is

$$ax^{b-1} = \alpha^j \qquad a \in \mathbb{F}_q. \tag{2.12}$$

The various possible values of a correspond to the different codewords in $\mathrm{RS}_b(n,1)$. Since $a=0$ corresponds to the all-zeros codeword, restrict a to lie in $\mathbb{F}_q^\star$. Eqn (2.12) then becomes:

$$x^{b-1} = \frac{\alpha^j}{a} \qquad b \neq 1, a \neq 0. \tag{2.13}$$

This equation has no solutions if $j = \star$. Otherwise, there is a unique solution if $b-1$ and n are relatively prime. If $d = \gcd(b-1,n) \neq 1$, there are d solutions when j is a multiple of d [9]. Therefore, the contribution for each a is $\prod_{j\in J_d} z_j^d$.

Thus the cwe of $\mathrm{RS}_b(n,1)$ is

$$\text{cwe of } \mathrm{RS}_b(n,1) = \begin{cases} z_\star^n + \dfrac{n}{d}\displaystyle\sum_{i=0}^{d-1} \prod_{j\in\{J_d+i\}} z_j^d & \text{if } b \neq 1 \bmod n, \text{ and } d = \gcd(b-1,n) \\ \displaystyle\sum_{j\in B} z_j^n & \text{otherwise} \end{cases} \tag{2.14}$$

□

The derivation of other cwe's requires application of some results from the theory of algebraic equations over finite fields[15]. Consider the $\mathrm{RS}_3(n,2)$ code, which is the dual of $\mathrm{RS}_1(n,n-2)$ code.

Lemma 2.3. *The cwe for $RS_3(n,2)$ is*

$$z_\star^n + 2n\frac{\gamma}{z_\star} + n\sum_{k\in B^\star} \frac{\beta_k}{z_\star}. \tag{2.15}$$

where

$$\begin{aligned} B_0 &= \{i \,|\, Tr(\alpha^i) = 0\} \\ B_k &= \{k + B_0\} \qquad \textit{addition is modulo } n, \textit{ and } j + \star = \star \\ \beta_k &= \prod_{j\in B_k} z_j^2 \end{aligned}$$

and for $x \in \mathbb{F}_q$, $Tr(x)$ is the trace of x over $\mathbb{F}_2$ defined as $Tr(x) = x + x^2 + x^4 + \cdots + x^{2^{m-1}}$. Note that $Tr(x) \in \mathbb{F}_2$ [4, ch. 4. §8.].

Proof. A well known fact [15] which will be useful in this proof is that the equation $x^2 + ax + b = 0$ over $\mathbb{F}_q$ has solutions for $x \in \mathbb{F}_q$ iff $\mathrm{Tr}(b/a^2) = 0$. When solutions exist, there will be two in number. The equation to consider for this code is:

$$a_1x + a_2x^2 = \alpha^j \tag{2.16}$$

Now, consider the following cases:

Case I : $a_1 = 0$

With this restriction, the code reduces to the $\mathrm{RS}_3(n,1)$ code, and hence its cwe will be part of the cwe for $\mathrm{RS}_3(n,2)$.

Case II : $a_2 = 0,\ a_1 \neq 0$

Here, eqn. (2.16) becomes $a_1 x = \alpha^j$, which is similar to eqn. (2.13), and the corresponding cwe will be $n\gamma/z_\star$, when a_1 is varied over all possible non-zero values.

Case III : all others

When $\mathrm{Tr}(\alpha^j a_2/a_1^2) = 0$, eqn. (2.16) has solutions. If $\alpha^j = 0$ (or $j = \star$), it is evident that the only non-zero solution to x is $x = -a_1/a_2$. For all other α^j, there will be two solutions for $x \in \mathbb{F}_q^\star$. For example, fixing $a_1 = a_2 = 1$,

$$s_j = \begin{cases} 1 & \text{if } j = \star \\ 2 & \text{if } j \in B_0 \text{, but } j \neq \star \\ 0 & \text{otherwise} \end{cases} \tag{2.17}$$

Allowing a_2 to vary will shift the solution for s_j. For example, if $a_2 = \alpha$, the condition $j \in B_0$ becomes $j + 1 \in B_0$. Therefore, as a_2 varies over $\mathbb{F}_q^\star$, the cwe contribution becomes

$$\sum_{k=0}^{n-1} \frac{1}{z_\star} \prod_{i \in B_k} z_i^2 \tag{2.18}$$

Note that each product corresponds to a codeword (a particular value of a_2 and a_1,) and there are n terms in the sum, one for each non-zero value of a_2. Varying a_1 over the n non-zero values yields a similar action, with terms being folded over. Eqn. (2.18) then becomes

$$n \sum_{k=0}^{n-1} \frac{1}{z_\star} \prod_{i \in B_k} z_i^2 = n \sum_{k \in B^\star} \frac{\beta_k}{z_\star},$$

and the total cwe is

$$\begin{aligned}\text{cwe of } \mathrm{RS}_3(n,2) &= \text{cwe of } \mathrm{RS}_3(n,1) + n\frac{\gamma}{z_\star} + n\sum_{k\in B_\star}\frac{\beta_k}{z_\star} \\ &= z_\star^n + 2n\frac{\gamma}{z_\star} + n\sum_{k\in B^\star}\frac{\beta_k}{z_\star} \qquad (2.19)\end{aligned}$$

□

It may seem like an easy extension to use the same methodology to obtain the cwe for codes with higher b, or higher k, but in practice, this is not feasible. The main problem is the lack of knowledge (other than [15]) about the solution of equations of arbitrary degrees over finite fields. A mere condition on the existence of solutions (and number) would suffice, but [15] only gives these for equations of degree 2 and 3. As k is increased, the number of terms and degree of $f(x)$ in eqn. (2.5) increases. Even increasing b, while fixing k will increase the degree of $f(x)$, making analysis more difficult. For example, an increase of b to 5 in the previous example will result in considering

$$a_1x^3 + a_2x^4 = \alpha^j \qquad (2.20)$$

to get the cwe of $\mathrm{RS}_5(n,2)$. Because of the constant term on the RHS of (2.20) can be non-zero, analysis of the general equation is difficult.

Due to the fact that $\alpha^n = 1$, certain symmetries may be exploited. Fixing k, the cwe corresponding to different values of b come in pairs. For a given b, eqn. (2.5) is of the form

$$f(x) = a_{i_0}x^{i_0} + a_{i_1}x^{i_1} + \cdots + a_{i_k}x^{i_k} = \alpha^j \qquad (2.21)$$

there will exist another b with a corresponding equation of the form

$$f(x) = a_{i_0}x^{-i_0} + a_{i_1}x^{-i_1} + \cdots + a_{i_k}x^{-i_k} = \alpha^j \qquad (2.22)$$

If (2.21) has s_j solutions, then (2.22) will have the same number of solutions. An equation of the form in (2.21) can be obtained by making the substitution $y = 1/x$. Hence, if the cwe of $\mathrm{RS}_b(n,k)$ is known, there will exist a b' such that $\mathrm{RS}_{b'}(n,k)$ has the same cwe. The relationship between b' and b is given in the lemma below:

Lemma 2.4. *If*

$$b + b' = (k+1) \bmod n$$

then $RS_b(n,k)$ and $RS_{b'}(n,k)$ have the same cwe.

Proof. Let Z be the set of zeros of the $\mathrm{RS}_b(n,k)$, i.e., the roots of $g(x)$ in eqn. (1.1), and $\bar{Z} = B^\star \setminus Z$. For $\mathrm{RS}_b(n,k)$,

$$\bar{Z}_b = \{b-k, b-k+1, \ldots, b-1\}.$$

Substituting

$$b + b' = (k+1) \bmod n$$

for b, we obtain

$$\{1-b', 2-b', \ldots, k-b'\}. \tag{2.23}$$

Powers of x are negated in eqn. (2.22), so negating each element of the set in (2.23), we get

$$\{b'-1, b'-2, \ldots, b'-k+1, b'-k\} = \bar{Z}_{b'}.$$

□

Table 2.1 shows the cwe for various b for $\mathrm{RS}_b(7,2)$ codes.

Table 2.1: cwe for various Reed-Solomon codes with $m = 3$

code	$\bar{I}$	cwe
$\mathrm{RS}_1(7,1)$	$\{0\}$	$\sum z_j^7$
$\mathrm{RS}_b(7,1)$	$\{b\text{-}1\}$	$z_\star^7 + 7\frac{\gamma}{z_\star}$
$\mathrm{RS}_1(7,2)$	$\{6{,}0\}$	$\left.\right\}\sum z_j^7 + 7\gamma\sum\frac{1}{z_i}$
$\mathrm{RS}_2(7,2)$	$\{0{,}1\}$	
$\mathrm{RS}_3(7,2)$	$\{1{,}2\}$	$\left.\right\}z_\star^7 + 14\frac{\gamma}{z_\star} + 7\sum_{k\in B^\star}\frac{1}{z_\star}\prod_{j\in B_k} z_j^2$
$\mathrm{RS}_7(7,2)$	$\{5{,}6\}$	
$\mathrm{RS}_4(7,2)$	$\{2{,}3\}$	$\left.\right\}z_\star^7 + 14\frac{\gamma}{z_\star} + 7z_\star\sum_{k\in B^\star} z_k^2\prod_{j\in\bar{B}_k} z_j$
$\mathrm{RS}_6(7,2)$	$\{4{,}5\}$	
$\mathrm{RS}_5(7,2)$	$\{3{,}4\}$	$z_\star^7 + 14\frac{\gamma}{z_\star} + 7\sum_{k\in B^\star}\frac{1}{z_\star}\prod_{j\in A_k} z_j^2$

Note:

$$\begin{aligned} B_k &= \{\star, 1, 2, 4\} + k \\ A_k &= \{\star, 3, 5, 6\} + k \end{aligned}$$

2.3 cwe for extended codes

Deriving similar equations for the cwe of extended RS codes is very similar to the method used for non-extended RS codes. In fact, the expressions obtained are sometimes easier to work with.

Recall the definition of $\mathbf{v}(f)$ given in eqn. (2.2), i.e.,

$$\mathbf{v}(f) = (f(1), f(\alpha), \ldots, f(\alpha^{n-1}))\,.$$

Since $f(1) + f(\alpha) + \cdots + f(\alpha^{n-1}) = f(0)$[3], we can define a similar concept for extended codes. Let

[3] See Appendix A for proof

$\mathbf{v}_e(f)$ be defined as

$$\mathbf{v}_e(f) = (f(0), f(1), f(\alpha), \ldots, f(\alpha^{n-1})) \in \mathbb{F}_q^q. \tag{2.24}$$

An extended Reed-Solomon code over $\mathbb{F}_q$, with dimension k may then be obtained by changing $\mathbf{v}$ to $\mathbf{v}_e$ in eqn. (2.3). The only consequence of this change is that the equations are now solved for $x \in \mathbb{F}_q$. The equation for s_j in (2.6) becomes

$$s_j = \#\text{distinct solns of } x \text{ to eqn. (2.5)} \quad \text{over } \mathbb{F}_q, \tag{2.25}$$

and $\sum_B s_j = q$.

Making minor changes to the argument given for $\mathrm{RS}_1(n,1)$, the cwe of the extended code may be seen to be:

$$\text{cwe of } \mathrm{ERS}_1(n,1) = \sum_{j \in B} z_j^q. \tag{2.26}$$

As with the non-extended case, the cwe for $\mathrm{ERS}_1(n,2)$ and $\mathrm{ERS}_2(n,2)$ are the same. Since x may be zero, the s_j in eqn. (2.10) is simplified to

$$s_j = 1 \qquad \forall a_0.$$

The cwe is then

$$\text{cwe of } \mathrm{ERS}_1(n,2) = \text{cwe of } \mathrm{ERS}_2(n,2) = \sum_{j \in B} z_j^q + q(q-1)\gamma. \tag{2.27}$$

In a similar vain, we can show that

$$\text{cwe of } \mathrm{ERS}_3(n,2) = z_\star^q + 2(q-1)\gamma + (q-1) \sum_{k \in B^\star} \beta_k.$$

The equation for s_j in (2.17) must be changed slightly, since x may have zero as a solution. The new equation for s_j is

$$s_j = \begin{cases} 2 & \text{if } j \in B_0 \\ 0 & \text{otherwise} \end{cases} .$$

For the cwe of $\mathrm{ERS}_b(n, 1)$ with $b \neq 1$, the solution to eqn.(2.13) is

$$s_j = \begin{cases} 1 & \text{if } j = \star \\ d & \text{if } j \text{ is a multiple of } d \\ 0 & \text{otherwise} \end{cases} .$$

So, the cwe is then

$$z_\star^q + \frac{q-1}{d} z_\star \sum_{i=0}^{d-1} \prod_{j \in \{J_d+i\}} z_j^d$$

2.4 Summary of cwe

Table 2.2 below summarizes the cwe of various Reed-Solomon codes discussed in this section. Note that the $b = 1$, $k = 3$ cases were not derived here, but by Blake and Kith in [1]. It is included here to demonstrate how expressions for cwe get complicated quickly.

Table 2.2: Summary of cwe for various Reed-Solomon and extended Reed-Solomon codes

code		cwe	
b	k	non-extended	extended
1	1	$\sum_{j \in B} z_j^n$	$\sum_{j \in B} z_j^q$
1	2	$\sum_{j \in B} z_j^n + n\gamma \sum_{i \in B} \frac{1}{z_i}$	$\sum_{j \in B} z_j^q + q(q-1)\gamma$
1	3	$\sum_{j \in B} z_j^n + 2n\gamma \sum_{i \in B} \frac{1}{z_i} + n \sum_{k \in B^\star} \left\{ \sum_{i \in B_0} \frac{\beta_k}{z_{i+k}} + \sum_{i \in \bar{B}_0} \frac{\bar{\beta}_k}{z_{i+k}} \right\}$	$\sum_{j \in B} z_j^q + 2q(q-1)\gamma + \frac{q(q-1)}{2} \left\{ \sum_{k \in B^\star} (\beta_k + \bar{\beta}_k) \right\}$
†	1	$z_\star^n + \frac{n}{d} \sum_{i=0}^{d-1} \prod_{j \in \{J_d + i\}} z_j^d$	$z_\star^q + \frac{q-1}{d} z_\star \sum_{i=0}^{d-1} \prod_{j \in \{J_d + i\}} z_j^d$
2	2	same‡ as $\mathrm{RS}_1(n, 2)$	same as $\mathrm{ERS}_1(n, 2)$
3	2	$z_\star^n + 2n \frac{\gamma}{z_\star} + n \sum_{k \in B^\star} \frac{\beta_k}{z_\star}$	$z_\star^q + 2(q-1)\gamma + (q-1) \sum_{k \in B^\star} \beta_k$

Notations used:

$$\begin{array}{rcll}
B & = & \{\star, 0, 1, \ldots, n-1\} & |B| = q = 2^m \\
B^\star & = & \{, 0, 1, \ldots, n-1\} & |B^\star| = n = 2^m - 1 \\
\gamma & = & z_\star z_0 z_1 \cdots z_{n-1} & \\
B_0 & = & \{i \mid \mathrm{Tr}(\alpha^i) = 0\} & \\
\bar{B}_0 & = & B \setminus B_0 & \\
B_k & = & B_0 + k & \text{addition is modulo } n \text{, and } j + \star = \star \\
\bar{B}_k & = & B \setminus B_k & \\
\beta_k & = & \prod_{j \in B_k} z_j^2 & \\
\bar{\beta}_k & = & \prod_{j \in \bar{B}_k} z_j^2 &
\end{array}$$

† : $b \neq 1$. If $b-1$ and n relatively prime, then the cwe is $z_\star^n + n\gamma/z_\star$ for non-extended, and $z_\star^q + (q-1)\gamma$ for extended. All values of b are taken modulo n.

‡ : due to Lemma 2.4. Other codes with identical cwe are not shown.

3 Obtaining binary codes from non-binary codes

In many applications, while the alphabet of the information symbols is non-binary, the channel to be used may be binary in nature. Hence, the non-binary codeword symbols must be converted, by some means, to binary bits. The methods discussed below show how an extension field of characteristic 2 may be mapped to the binary field. A general reference for the material in the first few sections is [4, ch. 10. §5].

3.1 Bases of $\mathbb{F}_q$ over $\mathbb{F}_2$

$\mathbb{F}_q$ may be viewed as an m-dimensional vector space over $\mathbb{F}_2$, and hence any m linearly independent elements in $\mathbb{F}_q$ may be used as a basis of this vector space. Let a_0, a_1, ..., a_{m-1} be m such elements, and

$$\mathbf{a} = \{a_0, a_1, \ldots, a_{m-1}\}$$

denote a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. There are $\Omega = (2^m - 1)(2^m - 2)(2^m - 4)\ldots(2^m - 2^{m-1})$ such bases. If the channel being considered here is memoryless, the order of the a_i's is immaterial, so only the $\Omega' = \Omega/m!$ different order independent bases need to be considered. This shall always be the case in this thesis, and unless otherwise specified, the elements in a basis are order independent.

Further, divide these Ω' bases into equivalence classes, defined by the following equivalence relation. Two bases $\mathbf{a}$ and $\mathbf{b}$, where

$$\begin{aligned} \mathbf{a} &= \{a_0, a_1, \ldots, a_{m-1}\}, \quad a_i \in \mathbb{F}_q \\ \mathbf{b} &= \{b_0, b_1, \ldots, b_{m-1}\}, \quad b_i \in \mathbb{F}_q \end{aligned}$$

are said to be in the same equivalence class, written $\mathbf{a} \sim \mathbf{b}$, if $\exists c \neq 0 \in \mathbb{F}_q$ s.t. $b_i = ca_i$ for all $i = 0, 1, \ldots, m-1$. Note that if $\{a_0, a_1, \ldots, a_{m-1}\}$ forms a linearly independent set, so does

$\{ca_0, ca_1, \ldots, ca_{m-1}\}$ if $c \neq 0$.

The relation partitions the bases into Ω'/n equivalence classes, consisting of n elements each. It is shown later in Theorem 3.2 that bases in the same equivalence class yield the same binary weight distribution. While this reduces the number of bases to consider, there is still an exponential growth in m, as shown below

m	Ω'	Ω'/n classes
3	28	4
4	840	56
5	83328	2688
6	27.99×10^6	44416

3.2 Mapping elements of $\mathbb{F}_q$ to m-tuples

If $\mathbf{a}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$, then any element $\beta \in \mathbb{F}_q$ can be written as:

$$\beta = b_0a_0 + b_1a_1 + \cdots + b_{m-1}a_{m-1}, \qquad b_i \in \mathbb{F}_2$$

The basis $\mathbf{a}$ is said to map β into the binary m-tuple $(b_0, b_1, \ldots, b_{m-1})$.

Chapter 4 examines some properties of the binary codes obtained this way, so it is important to look at the weights of the m-tuples generated. Let α^i be mapped to an m-tuple of weight w_i $(i = 0, 1, \ldots, n-1)$. The number of i's s.t. $w_i = j$ is $\binom{m}{j}$, and

$$\sum_{i=0}^{n-1} w_i = \sum_{j=1}^{m} j\binom{m}{j} = m2^{m-1} \overset{def}{=} W_m.$$

Note that if the basis $\mathbf{a}$ is changed, w_i for a given i may change as well.

Example: Let $\mathbf{a}$ and $\mathbf{b}$ be two different bases of $\mathbb{F}_8$ over $\mathbb{F}_2$. The individual mapping of elements in $\mathbb{F}_8$ is shown below:

Table 3.1: Mapping of $\mathbb{F}_8$ (as defined by x^3+x+1) using different bases

	$\mathbf{a} = \{1,\ \alpha,\ \alpha^2\}$						$\mathbf{b} = \{1,\ \alpha,\ \alpha^5\}$				
i		w_i	i		w_i	i		w_i	i		w_i
$\star$	$0 \rightarrow (000)$	0	3	$\alpha^3 \rightarrow (110)$	2	$\star$	$0 \rightarrow (000)$	0	3	$\alpha^3 \rightarrow (110)$	2
0	$1 \rightarrow (100)$	1	4	$\alpha^4 \rightarrow (011)$	2	0	$1 \rightarrow (100)$	1	4	$\alpha^4 \rightarrow (101)$	2
1	$\alpha \rightarrow (010)$	1	5	$\alpha^5 \rightarrow (111)$	3	1	$\alpha \rightarrow (010)$	1	5	$\alpha^5 \rightarrow (001)$	1
2	$\alpha^2 \rightarrow (001)$	1	6	$\alpha^6 \rightarrow (101)$	2	2	$\alpha^2 \rightarrow (111)$	3	6	$\alpha^6 \rightarrow (011)$	2

Lemma 3.1. *If* $\mathbf{a}$ *and* $\mathbf{b}$ *are in the same equivalence class s.t.* $b_i = \alpha^l a_i$*, and* $\mathbf{a}$ *maps* α^i *to a binary* m*-tuple of weight* w_i*, then* $\mathbf{b}$ *will map* α^{i+l} *to a binary* m*-tuple of weight* w_i*.*

Proof. Any element $\alpha^i \in \mathbb{F}_q$ can be written as

$$\alpha^i = x_0 a_0 + x_1 a_1 + \cdots x_{m-1} a_{m-1}$$

where the number of non-zero x_is is w_i. Multiplying by α, and choosing the basis $\{\alpha a_0,\ \alpha a_1,\ \ldots,\ \alpha a_{m-1}\}$

$$\begin{aligned} \alpha^{i+1} &= \alpha x_0 a_0 + \alpha x_1 a_1 + \cdots + \alpha x_{m-1} a_{m-1} \\ &= x_0 b_0 + x_1 b_1 + \cdots + x_{m-1} b_{m-1} \end{aligned}$$

Hence, by repeated use of the above argument, α^{i+l} will have the same weight w_i, when mapped using basis $\mathbf{b}$. □

By mapping each co-ordinate in each codeword of an (n,k) code $\mathcal{C}$, a binary code, $\mathcal{C}_2$, may be formed. We will refer to $\mathcal{C}_2$ as the *binary expansion* of $\mathcal{C}$ and the weight distribution of $\mathcal{C}_2$ as the *binary weight distribution* of $\mathcal{C}$. It should be emphasized that a particular non-binary code $\mathcal{C}$ may give rise to many different binary weight distributions, depending on the basis chosen. Only in certain special cases will there be a unique binary weight distribution.

If the cwe of $\mathcal{C}$ is

$$\mathcal{W}_{\mathcal{C}}(z_\star,\ z_0,\ \ldots,\ z_{n-1})$$

and given a basis which maps α^i to a vector of weight w_i, for $i \in B^\star$, the weight enumerator of $\mathcal{C}_2$ is obtained by substituting

$$\begin{aligned} z_\star &= 1 \\ z_i &= x^{w_i} \end{aligned} \tag{3.1}$$

into $\mathcal{W}_{\mathcal{C}}$. Hence $f_H(x) = \mathcal{W}_{\mathcal{C}}(1,\ x^{w_0},\ \ldots,\ x^{w_{n-1}})$.

Example : The cwe of $\mathrm{RS}_4(7,2)$ is given in Table 2.1 as

$$\begin{aligned} \mathcal{W}_{\mathcal{C}} &= z_\star^7 + 14\frac{\gamma}{z_\star} \\ &\quad +7z_\star z_0^3 z_3 z_5 z_6 + 7z_\star z_1^3 z_4 z_6 z_0 + 7z_\star z_2^3 z_5 z_0 z_1 + 7z_\star z_3^3 z_6 z_1 z_2 \\ &\quad +7z_\star z_4^3 z_0 z_2 z_3 + 7z_\star z_5^3 z_1 z_3 z_4 + 7z_\star z_6^3 z_2 z_4 z_5. \end{aligned}$$

Using the bases **a** and **b** in the previous example, the binary weight distributions are:

$$\begin{aligned} f_H(x) &= \mathcal{W}_{\mathcal{C}}(z_\star = 1, z_0 = x, z_1 = x, z_2 = x, z_3 = x^2, z_4 = x^2, z_5 = x^3, z_6 = x^2) \\ &= 7x^{14} + 21x^{12} + 21x^{10} + 14x^8 + 1 \qquad \text{with basis } \mathbf{a} \end{aligned} \tag{3.2}$$

and

$$\begin{aligned} f_H(x) &= \mathcal{W}_{\mathcal{C}}(1, x, x, x^3, x^2, x^2, x, x^2) \\ &= 42x^{12} + 21x^8 + 1 \qquad \text{with basis } \mathbf{b} \end{aligned} \tag{3.3}$$

Note that these are the only two binary expansions of $\mathrm{RS}_4(7,2)$. Of the 28 bases of $\mathbb{F}_8$ over $\mathbb{F}_2$, twenty-one will give rise to the distribution given in (3.3), while seven will result in the distribution in (3.2). This was determined by exhaustive enumeration of all possible bases.

3.3 Invariance properties

A mathematical description of an (n,k) linear code, $\mathcal{C}$, over $\mathbb{F}_q$ would be as a k-dimensional subspace of the vector space $\mathbb{F}_q^n$. This terse definition is not too useful, since it does not describe potential structure evident in $\mathcal{C}$. Indeed, it is this structure which makes a code easy to analyse and implement. Certain properties in codes will translate to patterns (groups of terms) in its cwe. Some examples are given below:

Property 1 : closure under scalar multiplication.

$$\begin{aligned} \text{If} \quad c &= (c_0,\ c_1, \ldots,\ c_{n-1}) \in \mathcal{C}, \text{ then for } a \in \mathbb{F}_q \\ ac &= (ac_0,\ ac_1, \ldots,\ ac_{n-1}) \in \mathcal{C} \end{aligned}$$

Assume that the cwe of c is $\prod_{j \in A} z_j^{s_j}$ for some $A \subseteq B$, and $a = \alpha^k \neq 0$. A particular co-ordinate $c_i = \alpha^l \neq 0$ in c would become $ac_i = \alpha^{l+k}$. Co-ordinates in c which were zero remain zero. Hence $s_{(i+k)\bmod n}$ in ac is equal to s_i in c and $s_\star$ remains unchanged. Given the cwe of c, the cwe of ac is then

$$\prod_{j \in \{A+k\}} z_j^{s_j}$$

where the sum $\{A+k\}$ is done modulo n, with $\star + x = \star$.

Therefore, the cwe of all such codes will comprise of terms of the form

$$\sum_{k \in B^*} \prod_{j \in \{A+k\}} z_j^{s_j}. \tag{3.4}$$

Note that all linear codes and some non-linear codes satisfy this property.

Property 2 : cyclic codes.

$$\begin{aligned} \text{If} \quad c &= (c_0,\ c_1, \ldots,\ c_{n-1}) \in \mathcal{C}, \text{ then its right cyclic shift} \\ c' &= (c_{n-1},\ c_0, \ldots,\ c_{n-2}) \in \mathcal{C}. \end{aligned}$$

If the cwe of c is $\prod_{j \in A} z_j^{s_j}$, so is the cwe of c'. The cyclic shifts of c would contribute terms of the form

$$p \prod_{j \in A} z_j^{s_j} \tag{3.5}$$

to the cwe of $\mathcal{C}$, where p is the period of c. Note that p divides n [16]. Combining this with property 1 would result in a multiplicative factor p for (3.4).

Definition 3.1. Let $\mathfrak{B}$ be the set of all bases of $\mathbb{F}_q$ over $\mathbb{F}_2$, and $\mathfrak{I}$ be a subset of $\mathfrak{B}$. A code over $\mathbb{F}_q$ is said to be *invariant* with respect to the bases in $\mathfrak{I}$ if every basis in $\mathfrak{I}$ maps the code to a binary code with the same weight distribution. If $\mathfrak{I} = \mathfrak{B}$, the code is invariant w.r.t. to all bases, and we shall simply call this code invariant.

Theorem 3.2. *A code $\mathcal{C}$ is invariant w.r.t. bases in the same equivalence class, provided $\mathcal{C}$ satisfies property 1 (closure under scalar multiplication).*

Proof. Let $\mathbf{a}$ and $\mathbf{b}$ be in the same equivalence class such that $b_i = \alpha^l a_i$. Lemma 3.1 states that $\mathbf{a}$ and $\mathbf{b}$ induce the following mappings[4]:

$$\begin{array}{ll} f_0 : z_i \rightarrow x^{w_i} & \quad \text{for basis } \mathbf{a} \\ f_l : z_{i+l} \rightarrow x^{w_i} & \quad \text{for basis } \mathbf{b} \end{array}$$

[4] Integer addition is done modulo n

Consider the mapping of the typical term $\prod_{j\in A} z_j^{s_j}$ under f_0 and f_l:

$$f_0\Big(\prod_{j\in A} z_j^{s_j}\Big) = x^{\sum_{j\in A} s_j w_j} \tag{3.6}$$

$$f_l\Big(\prod_{j\in A} z_j^{s_j}\Big) = x^{\sum_{j\in\{A+l\}} s_j w_j} = f_0\Big(\prod_{j\in\{A+l\}} z_j^{s_j}\Big) \tag{3.7}$$

Basis **a** maps the shifted typical term $\prod_{j\in\{A+l\}} z_j^{s_j}$ and basis **b** maps the typical term $\prod_{j\in A} z_j^{s_j}$ in the same way. Since the cwe a code which satisfies property 1 contains only patterns with all possible shifted terms, **a** and **b** will map the code to the same binary weight distribution, regardless of l[5]. □

Definition 3.2. For every basis $\mathbf{a} = \{a_1, a_2, \ldots, a_m\}$, there exists another basis $\mathbf{b} = \{b_1, b_2, \ldots, b_m\}$, with

$$\mathrm{Tr}(a_i b_j) = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{otherwise} \end{cases}, \tag{3.8}$$

called the *complementary (dual) basis* of **a**. If A is a subset of $\mathfrak{B}$, and $A^{\perp}$ the set of complementary bases of A, $A^{\perp}$ is well-defined, and contains the same number of elements as A, since **b** is unique [4, ch. 4. §8].

The trace operator is used often, and is known to have the following properties [10]. Let p be a prime, and m a positive integer. For elements x and $y \in \mathbb{F}_p^m$, and $a \in \mathbb{F}_p$.

(T–i). $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$

(T–ii). $\mathrm{Tr}(ax) = a\mathrm{Tr}(x)$

(T–iii). Trace is a linear transformation from $\mathbb{F}_p^m$ onto $\mathbb{F}_p$

(T–iv). $\mathrm{Tr}(x)$ takes on each value in $\mathbb{F}_p$ equally often, i.e., p^{m-1} times.

[5] Note that the definition of the equivalence relation precludes $l = \star$, and $l = 0$ implies that $\mathbf{a} = \mathbf{b}$.

(T–v). $\mathrm{Tr}(x^p) = \mathrm{Tr}(x)$

Lemma 3.3. *If C is invariant w.r.t. all bases in $A \subseteq \mathfrak{B}$, then the dual code $C^\perp$ is invariant w.r.t. all bases in $A^\perp$, the set of complementary basis of A. Note that in some cases, $A = A^\perp$.*

Proof. Let **a** and **b** be complementary bases. If C_a is the binary expansion of C when basis **a** is used, and $C_b^\perp$ is the the binary expansion of $C^\perp$ when **b** is used, then C_a and $C_b^\perp$ are duals. The proof for this is given in Kasami and Lin [14], and is repeated here for completeness.

Let $(u_1,\ u_2, \ldots,\ u_n) \in C$ and $(v_1,\ v_2, \ldots,\ v_n) \in C^\perp$. Expanding using the respective basis obtains

$$u_i = \sum_{j=1}^{m} u_{ij} a_j \tag{3.9}$$

$$v_i = \sum_{j=1}^{m} v_{ij} b_j \tag{3.10}$$

Since u and v are in dual codes,

$$\sum_{i=1}^{n} u_i v_i = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m} u_{ij} a_j\Big)\Big(\sum_{k=1}^{m} v_{ik} b_k\Big) = 0 \tag{3.11}$$

Taking the trace of (3.11)

$$\mathrm{Tr}\Big(\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{m} u_{ij} v_{ik} a_j b_k\Big) = 0 \tag{3.12}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{m} u_{ij} v_{ik} \mathrm{Tr}\,(a_j b_k) = 0 \tag{3.13}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} u_{ij} v_{ij} = 0 \tag{3.14}$$

Eqn. (3.13) follows from trace property (T–i). The u_{ij} are the individual co-ordinates of a codeword in C_a, and v_{ij} are the co-ordinates of a codeword in $C_b^\perp$. Thus, C_a and $C_b^\perp$ are dual codes.

Let $\mathbf{a_1}$ and $\mathbf{a_2}$ be two bases from A, with complementary bases $\mathbf{a_1^\perp}$ and $\mathbf{a_2^\perp}$ respectively. The binary codes generated have the following relationship:

$$\mathcal{C}_{a_1} \overset{dual}{\longleftrightarrow} \mathcal{C}^{\perp}_{a_1^\perp}$$

$$\mathcal{C}_{a_2} \overset{dual}{\longleftrightarrow} \mathcal{C}^{\perp}_{a_2^\perp}$$

Since $\mathcal{C}_{a_1} = \mathcal{C}_{a_2}$, and because the dual of a code is unique, $\mathcal{C}^{\perp}_{a_1^\perp} = \mathcal{C}^{\perp}_{a_2^\perp}$. A similar argument may be used to cover all bases in A. □

Corollary 3.4. *If C is invariant w.r.t. all bases, then the dual code $C^\perp$ is also invariant.*

Definition 3.3. A basis is called *self-dual* if it is equal to its complementary basis. The order of the individual elements is considered irrelevant. More precisely, $\mathbf{a} = \{a_1, a_2, \ldots, a_n\}$ is self-dual if $\exists \sigma \in \mathrm{S}_m$, the symmetric group of permutations with m elements, such that

$$\mathrm{Tr}(a_i a_{\sigma(j)}) = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{otherwise} \end{cases} .$$

If the permutation σ is the identity permutation, then the basis is termed *strictly self-dual*[6]. If all bases of a class and their complementary bases are in the same class, that class is said to be self-dual.

Lemma 3.5. *Given an equivalence class A, the following statements are equivalent:*

1. *A is a self-dual class.*
2. *A has exactly one self-dual basis.*
3. *Both basis $\mathbf{a}$, and its complementary basis $\mathbf{b}$ are in A.*

[6] Standard references, such as [10, 4], simply refer to this as self-dual.

In addition, if A does not satisfy the above criteria, then A will have no self-dual bases.

Proof. Let A be an equivalence class of bases, and $\mathbf{a}$ a basis in A. The basis $\mathbf{b}$, complementary to $\mathbf{a}$, is either in A, or another class B. To show that the three statements are equivalent, we will show that statement 1 implies statement 3 (and vice versa). Then, we show that statement 1 implies statement 2 (and vice versa).

If $\mathbf{b} \notin A$, then showing that the duals of other bases in A are in B proves that A has no self-dual bases. The duality between $\mathbf{a} = \{a_1, a_2, \ldots, a_m\}$ and $\mathbf{b} = \{b_1, b_2, \ldots, b_m\}$ means that

$$\mathrm{Tr}(a_i b_j) = \delta_{ij}$$

Consider then, another basis in A, such as $\alpha\mathbf{a} = \{\alpha a_1, \alpha a_2, \ldots, \alpha a_m\}$. The dual of this is easily determined, since

$$\mathrm{Tr}(\alpha a_i \alpha^{-1} b_j) = \delta_{ij}$$

and hence, the dual of $\alpha\mathbf{a}$ is $\alpha^{-1}\mathbf{b} \in B$. In a similar way, we may conclude that the duals of the other members of A lie in B, and therefore, A has no self-dual basis.

If $\mathbf{b} \in A$, then we must show that the other two statements in Lemma 3.5 are also true. With both $\mathbf{a} \in A$ and $\mathbf{b} \in A$, there must exist a unique integer l, and a permutation σ such that $b_i = \alpha^l a_{\sigma(i)}$. So,

$$\mathrm{Tr}(a_i \alpha^l a_{\sigma(j)}) = \delta_{ij}.$$

The dual of $\alpha^k\mathbf{a}$ is then $\alpha^{-k}\mathbf{b}$, since

$$\mathrm{Tr}(\alpha^k a_i \alpha^{l-k} a_{\sigma(j)}) = \delta_{ij}.$$

Because $\mathbf{b} \in A$, then $\alpha^{-k}\mathbf{b} \in A$ too. Therefore, statement 3 implies statement 1. That the converse is true is obvious from the definition of a self-dual class.

Because the powers of α are unique, and n is odd, the only time $\alpha^k\mathbf{a}$ is self-dual is when the equation

$$k = l - k \bmod n$$

is satisfied. For a given l, there is a unique solution for k, given by:

$$k = \begin{cases} \frac{1}{2}l & \text{if } l \text{ is even} \\ \frac{1}{2}(l+n) & \text{if } l \text{ is odd. (remember } n \text{ is odd also)} \end{cases}$$

So, statement 3 implies statement 2.

We also need to show that if A has exactly one self-dual basis, then A is a self-dual class. To see this, let $\mathbf{a}$ be this one self-dual basis, and so, there exists a $\sigma \in \mathrm{S}_m$ such that

$$\mathrm{Tr}(a_i a_{\sigma(j)}) = \delta_{ij}.$$

The other members of A, like $\alpha^k\mathbf{a} = \{\alpha^k a_1 , \alpha^k a_2, \ldots, \alpha^k a_m\}$ will have duals in A, since

$$\mathrm{Tr}(\alpha^k a_i \alpha^{-k} a_{\sigma(j)}) = \delta_{ij},$$

and so, the dual of $\alpha^k\mathbf{a}$ is $\alpha^{-k}\mathbf{a} = \alpha^{n-k}\mathbf{a} \in A$. Hence, statement 2 implies statement 3, and all three statements are then equivalent. □

There are two types of fields then to consider — fields where all classes are self-dual, and fields where there are some classes which are not self-dual. In the latter case, it would be useful to pair these classes with their duals. A class A which is not self-dual will have the duals of all its bases contained in a single class (call it $A^{\perp}$.)

In situations where all classes are self-dual, then the following statement may be made. Let the code $\mathcal{C}$ satisfy property 1 (closure under scalar multiplication). $\mathfrak{I}$ is then the union of equivalence classes, and the dual code $\mathcal{C}^{\perp}$ will be invariant w.r.t. the same set $\mathfrak{I}$. The only known case of this is when $m = 3$, i.e., in $\mathbb{F}_8$.

3.4 The binary weight distribution of certain RS codes

The code $\mathcal{C}$ is invariant when $\mathcal{W}_{\mathcal{C}}$ is symmetric in its variables [17]. It is sufficient to examine groups of terms in $\mathcal{W}_{\mathcal{C}}$, as dictated by its structure, to determine if they are invariant. If all the individual terms in $\mathcal{W}_{\mathcal{C}}$ are invariant, then $\mathcal{C}$ will be invariant. Note that symmetry in variables is a strong restriction, and there exists a weaker necessary condition. Commonly occuring patterns (see Table 2.2) which are invariant are listed below in Table 3.4.

In interpreting the table, the structures may be taken over any extension field, as determined by $m > 1$. d is any positive, non-zero integer constant. All entries are invariant w.r.t. all bases, even though not all are symmetric. The discussion below shows how the CW weights were determined.

1. $\sum_{i \in B} z_i^d$

   This sum over i covers every possible value for elements in the field. Any given basis will map $\binom{m}{i}$ field elements to binary m-tuples of weight i. Repeating d times yields the given binary weight distribution.

2. $\gamma / z_\star$

   γ is the product of all field elements, and hence has weight

$$\binom{m}{1} + 2\binom{m}{2} + \cdots + (m-1)\binom{m}{m-1} + m\binom{m}{m} = m2^{m-1} = W_m$$

Table 3.2: Binary weights of commonly occuring patterns

			weights of CW		
		# CW	wt.	number	
$\sum_{j\in B} z_j^d$	symmetric	q	id	$\binom{m}{i}$	$i = 0,\, 1,\, \ldots,\, m$
$\gamma\sum_{j\in B}\frac{1}{z_j}$	symmetric	q	$W_m - i$	$\binom{m}{i}$	$i = 0,\, 1,\, \ldots,\, m$
$\frac{\gamma}{z_\star}$	not symmetric	1	W_m	1	
$\sum_{k\in B^\star} \beta_k$	not symmetric	n	$(m-1)2^{m-1}$ $m2^{m-1}$	m $n-m$	
$\sum_{k\in B^\star} \bar{\beta}_k$	not symmetric	n	$(m+1)2^{m-1}$ $m2^{m-1}$	m $n-m$	

Notes:

$$\begin{aligned}
W_m &= m2^{m-1} \\
B_0 &= \{i \mid \mathrm{Tr}(\alpha^i) = 0\} \\
B_k &= B_0 + k \qquad \text{addition is modulo } n\text{, and } j + \star = \star \\
\beta_k &= \prod_{j\in B_k} z_j^2 \\
\text{CW} &: \text{codeword}
\end{aligned}$$

$z_\star$ has weight zero, and does not affect the overall weight.

3. $\gamma\sum_{j\in B}\frac{1}{z_j}$

Combining case 1 and case 2, the weight of γ must be reduced by an amount corresponding to the z_j. There are $\binom{m}{i}$ of the z_j's with weight i, and hence $\binom{m}{i}$ codewords with weight $W_m - i$.

4. $\sum_{k\in B^\star}\beta_k = \sum_{k\in B^\star}\prod_{j\in\{B_0+k\}} z_j^2$, and

5. $\sum_{k\in B^\star} \bar{\beta}_k = \sum_{k\in B^\star} \prod_{j\in\{\bar{B}_0+k\}} z_j^2$

Cases 4 and 5 are by far the most difficult distributions to show; a few facts must be exploited for this proof.

Each codeword may be mapped using one co-ordinate (in a given basis) at a time. Let $c = (c_1,\ c_2, \ldots,\ c_n)$ with $c_i \in \mathbb{F}_q$ be a vector to be mapped, using the basis $\{a_1,\ a_2,\ \ldots,\ a_m\}$. Let $\{b_1,\ b_2,\ \ldots,\ b_m\}$ be the dual basis. Mapping c with the co-ordinate a_1 yields the binary n-tuple [14]

$$(\mathrm{Tr}(b_1c_1), \mathrm{Tr}(b_1c_2), \ldots,\ \mathrm{Tr}(b_1c_n))$$

Repeating the procedure with the other co-ordinates will yield m n-tuples, or a binary vector of length mn.

Example: Over $\mathbb{F}_8$, let the vector to be mapped be $c = (1\,\alpha^2\,\alpha^5\,0)$, and basis $\{1, \alpha, \alpha^5\}$. The dual basis is $\{\alpha^3, \alpha^4, \alpha\}$

$$\begin{aligned}
\alpha^3 c &= (\alpha^3\,\alpha^5\,\alpha\ \ 0), & \mathrm{Tr}(\alpha^3 c) &= (1100)\\
\alpha^4 c &= (\alpha^4\,\alpha^6\,\alpha^2\,0), & \mathrm{Tr}(\alpha^4 c) &= (0100)\\
\alpha c &= (\alpha\ \ \alpha^3\,\alpha^6\,0), & \mathrm{Tr}(\alpha c) &= (0110)
\end{aligned}$$

Reading the binary vectors vertically, we can verify the mapping. With the given basis (see also Table 3.1), α^2 maps to (111), and α^5 maps to (001).

Lemma 3.6. *Let $v = (v_1,\ v_2, \ldots,\ v_i)$ be a vector over $\mathbb{F}_q$ consisting of all elements with trace zero. i.e., $Tr(v_j) = 0, j = 1,\ 2,\ \ldots,\ i$. Mapping v with any basis (using the method above) will yield a binary weight of either $m2^{m-2}$ or $(m-1)2^{m-2}$. Similarly, if v consists of all elements with trace one, the corresponding binary weight is either $m2^{m-2}$ or $(m+1)2^{m-2}$.*

Proof. We will make use of the following fact. Given the set Z of all field elements with trace 0, i.e., $Z = \{\alpha^i | i \in B_0\}$, then multiplying every element in Z by a constant $s \in \mathbb{F}_q$, $s \neq 0$, $s \neq 1$, will result in a set with half the elements having trace 0 and the other half having trace 1. Note that there are 2^{m-1} elements in Z, so 2^{m-2} elements in the new set have trace 0, while the other 2^{m-2} have trace 0. A proof for this is given in the Appendix B.

Writing out the mapping for each possible value of (dual) basis co-ordinate, and taking the trace, we can see that the binary vectors will either have weight zero (if co-ordinate is 1), or 2^{m-2}. For a given basis, there are m co-ordinates. If none of these co-ordinates are 1, then the binary weight of vector v will be $m2^{m-2}$. Otherwise, it will be $(m-1)2^{m-2}$.

This is shown in an example for $\mathbb{F}_{16}$ (as generated by $\alpha^4+\alpha+1$), where $v = (0,1,\alpha,\alpha^2,\alpha^4,\alpha^8,\alpha^5,\alpha^{10})$

$$\begin{array}{rcl@{\quad}lcl}
v & = & (0\ 1\ \alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^5\ \alpha^{10}), & \mathrm{Tr}(v) & = & (00000000) \\
\alpha v & = & (0\ \alpha\ \alpha^2\ \alpha^3\ \alpha^5\ \alpha^9\ \alpha^6\ \alpha^{11}), & \mathrm{Tr}(\alpha v) & = & (00010111) \\
\alpha^2 v & = & (0\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^6\ \alpha^{10}\ \alpha^7\ \alpha^{12}), & \mathrm{Tr}(\alpha^2 v) & = & (00101011) \\
\alpha^3 v & = & (0\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^7\ \alpha^{11}\ \alpha^8\ \alpha^{13}), & \mathrm{Tr}(\alpha^3 v) & = & (01001101) \\
\alpha^4 v & = & (0\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^8\ \alpha^{12}\ \alpha^9\ \alpha^{14}), & \mathrm{Tr}(\alpha^4 v) & = & (00010111) \\
\alpha^5 v & = & (0\ \alpha^5\ \alpha^6\ \alpha^7\ \alpha^9\ \alpha^{13}\ \alpha^{10}\ 1), & \mathrm{Tr}(\alpha^5 v) & = & (00111100) \\
\alpha^6 v & = & (0\ \alpha^6\ \alpha^7\ \alpha^8\ \alpha^{10}\ \alpha^{14}\ \alpha^{11}\ \alpha), & \mathrm{Tr}(\alpha^6 v) & = & (01100110) \\
\alpha^7 v & = & (0\ \alpha^7\ \alpha^8\ \alpha^9\ \alpha^{11}\ 1\ \alpha^{12}\ \alpha^2), & \mathrm{Tr}(\alpha^7 v) & = & (01011010) \\
\alpha^8 v & = & (0\ \alpha^8\ \alpha^9\ \alpha^{10}\ \alpha^{12}\ \alpha\ \alpha^{13}\ \alpha^3), & \mathrm{Tr}(\alpha^8 v) & = & (00101011) \\
\alpha^9 v & = & (0\ \alpha^9\ \alpha^{10}\ \alpha^{11}\ \alpha^{13}\ \alpha^2\ \alpha^{14}\ \alpha^4), & \mathrm{Tr}(\alpha^9 v) & = & (01011010) \\
\alpha^{10} v & = & (0\ \alpha^{10}\ \alpha^{11}\ \alpha^{12}\ \alpha^{14}\ \alpha^3\ 1\ \alpha^5), & \mathrm{Tr}(\alpha^{10} v) & = & (00111100) \\
\alpha^{11} v & = & (0\ \alpha^{11}\ \alpha^{12}\ \alpha^{13}\ 1\ \alpha^4\ \alpha\ \alpha^6), & \mathrm{Tr}(\alpha^{11} v) & = & (01110001) \\
\alpha^{12} v & = & (0\ \alpha^{12}\ \alpha^{13}\ \alpha^{14}\ \alpha\ \alpha^5\ \alpha^2\ \alpha^7), & \mathrm{Tr}(\alpha^{12} v) & = & (01110001) \\
\alpha^{13} v & = & (0\ \alpha^{13}\ \alpha^{14}\ 1\ \alpha^2\ \alpha^6\ \alpha^3\ \alpha^8), & \mathrm{Tr}(\alpha^{13} v) & = & (01100110) \\
\alpha^{14} v & = & (0\ \alpha^{14}\ 1\ \alpha\ \alpha^3\ \alpha^7\ \alpha^4\ \alpha^9), & \mathrm{Tr}(\alpha^{14} v) & = & (01001101)
\end{array}$$

The $m = 4$ possible co-ordinates in the (dual) basis will select either three binary 8-tuples of weight 4, and the all zero 8-tuple, or four binary 8-tuples of weight 4. □

Thus, we have shown that $\prod_{j \in B_0} z_j$ has a binary weight of either $m2^{m-2}$ or $(m-1)2^{m-2}$. The terms $\beta_0 = \prod_{j \in B_0} z_j^2$ have binary weights two times as large. Due to Lemma 3.1, this fact may be extended to $\beta_k = \prod_{j \in \{B_0+k\}} z_j^2$, with $k \in B^\star$.

We now determine the breakdown between the two different weights (as k is varied.) Let x be the number of codewords with binary weight $m2^{m-1}$, and y the number with binary weight $(m-1)2^{m-1}$. Then,

$$x + y = n. \tag{3.15}$$

Next, fixing j and varying k, each of the non-zero field elements is cycled through. Adding in this way, we get a weight of W_m. There are $2^{m-1} - 1$ possible non-zero values for j, and hence

$$\begin{aligned} 2W_m \times (2^{m-1} - 1) &= m2^{m-1}x + (m-1)2^{m-1}y \\ m2^m(2^{m-1} - 1) &= m2^{m-1}x + (m-1)2^{m-1}y. \end{aligned} \tag{3.16}$$

Solving (3.15) and (3.16), we obtain

$$\begin{aligned} x &= 2^m - 1 - m = n - m \\ y &= m. \end{aligned}$$

Having shown the binary weight distribution of certain common occuring structures in cwe's, we may determine the binary weight distribution of the codes given in Table 2.2. The result is shown in Table 3.3, where A_i denotes the number of codewords of weight i.

Table 3.3: Binary weight distribution for various Reed-Solomon and extended Reed-Solomon codes

code		non-extended			extended		
b	k	i	A_i		i	A_i	
1	1	jn	$\binom{m}{j}$	$j=0,1,\ldots,m$	jq	$\binom{m}{j}$	$j=0,1,\ldots,m$
1	2	jn	$\binom{m}{j}$	$j=0,1,\ldots,m$	jq	$\binom{m}{j}$	$j=0,1,\ldots,m$
		$m2^{m-1}-j$	$n\binom{m}{j}$	$j=0,1,\ldots,m$	$m2^{m-1}$	$q(q-1)$	
1	3				jq	$\binom{m}{j}$	$j=0,1,\ldots,m$
					$(m-1)2^{m-1}$	$\frac{1}{2}q(q-1)m$	
					$m2^{m-1}$	$2q(q-1)$ $+\frac{1}{2}q(q-1)(q-1-m)$	
					$(m+1)2^{m-1}$	$\frac{1}{2}q(q-1)m$	
$\neq 1$	1	$m2^{m-1}$	n		$m2^{m-1}$	n	
3	3	$(m-1)2^{m-1}$	mn		$(m-1)2^{m-1}$	mn	
		$m2^{m-1}$	$n(n-m)+2n$		$m2^{m-1}$	$n(n-m)+2n$	

4 The probability of undetected error for certain binary RS codes

The probability of undetected error of a code is an important measure of code performance, especially in determining error detection capabilities. We shall be considering the binary expansions of RS codes when used over the binary symmetric channel (BSC).

In the following sections, a *family* of codes refers to all codes with the same dimension k, and b. We obtain different codes by changing the field $\mathbb{F}_q$ (i.e., changing m).

4.1 $P_{ud}(\epsilon)$ and properness

Given a BSC, let ϵ denote its cross-over probability (i.e., the probability of a bit error.) The probability of undetected error, $P_{ud}(\epsilon)$, for a code[7] is the probability that the error vector matches one of the codewords, and is normally calculated as a function of ϵ. If the $P_{ud}(\epsilon)$ of a code is monotonically increasing with ϵ, it is referred to as a *proper code* [18]. If there exists an $\epsilon \in [0, \frac{1}{2}]$ such that

$$P_{ud}(\epsilon) > 2^{-p}, \tag{4.1}$$

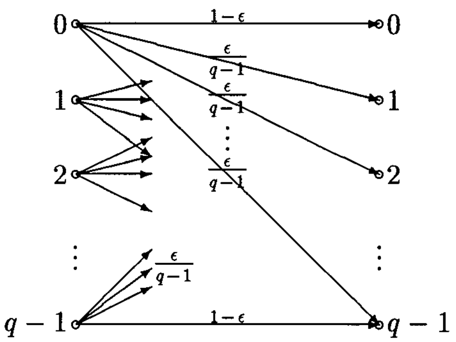
where p is the number of parity bits in the code, the code must be improper [2]. In the cases we consider here, $p = m(n-k)$ for non-extended codes, while $p = m(q-k)$ for the extended ones.

If the Hamming weight enumerator [2, 4] of a code is known, $P_{ud}(\epsilon)$ can be easily calculated. Given a binary code of block length n and dimension k, let A_i denote the number of codewords of Hamming weight i in the code. Its Hamming weight enumerator is:

$$A(z) = A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n = \sum_{i=0}^{n} A_i z^i.$$

[7] When used solely for error detection.

Figure 4.1: q-input, q-output symmetric, memoryless channel



The $P_{ud}(\epsilon)$ of the code, when used solely for error detection, may be expressed in terms of $A(z)$ since

$$\begin{aligned} P_{ud}(\epsilon) &= \sum_{i=1}^{n} A_i \epsilon^i (1-\epsilon)^{n-i} && (4.2) \\ &= (1-\epsilon)^n A\left(\frac{\epsilon}{1-\epsilon}\right) - (1-\epsilon)^n && (4.3) \end{aligned}$$

If $B(z)$ is the Hamming weight enumerator of the dual code, $P_{ud}(\epsilon)$ may also be expressed in terms of $B(z)$, using MacWilliams's identity [4]

$$P_{ud}(\epsilon) = \frac{1}{2^{n-k}} B(1-2\epsilon) - (1-\epsilon)^n. \qquad (4.4)$$

Kasami and Lin [13] showed that RS codes are proper when used over the q-ary symmetric channel, shown in Figure 4.1. We shall show in Theorem 4.1 the surprising result that the binary expansions of RS codes are not necessarily proper. In fact, most of the codes examined in this thesis are improper, and for a given m, a rate is found such that all binary RS codes with rate below this are improper. A comparison of the $P_{ud}(\epsilon)$ for $\text{RS}_1(7,1)$ over a q-ary channel, and the

$P_{ud}(\epsilon)$ of its binary expansion over the BSC is shown in Figure 4.2.

4.2 The properness of $k = 1$ RS codes

In the previous chapter it was shown that the binary weight distribution of $\mathrm{RS}_1(n, 1)$ is

$$\begin{aligned} A_0 &= 1 \\ A_{in} &= \binom{m}{i} \qquad i = 1, 2, \ldots, m \end{aligned}$$

while for $\mathrm{ERS}_1(q, 1)$, the distribution is

$$\begin{aligned} A_0 &= 1 \\ A_{iq} &= \binom{m}{i} \qquad i = 1, 2, \ldots, m \end{aligned}$$

By letting $N = n$ or q, the following discussion applies to the binary expansions of both non-extended and extended RS codes. Note that the block length of the binary expansion is then mN.

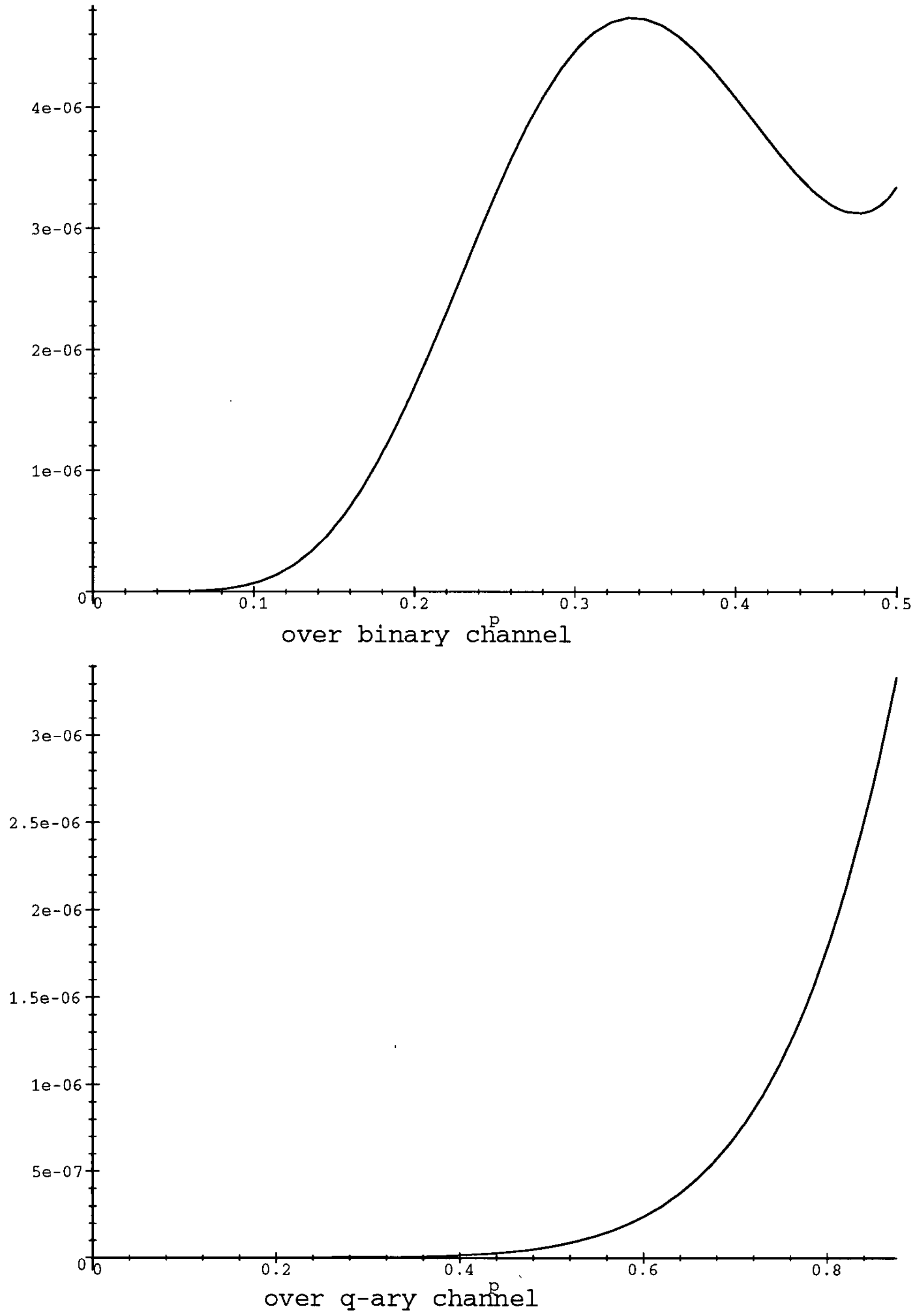
From eqn. (4.3) the $P_{ud}(\epsilon)$ of these codes, when used solely for error detection, is then

$$P_{ud}(\epsilon) = (1-\epsilon)^{mN} \sum_{j=0}^{m} \binom{m}{j} \left(\frac{\epsilon}{1-\epsilon}\right)^{jN} - (1-\epsilon)^{mN}. \tag{4.5}$$

At $\epsilon = 1/m$, we have

$$\begin{aligned} P_{ud}(1/m) &= \left(\frac{m-1}{m}\right)^{mN} \sum_{j=0}^{m} \binom{m}{j} \left(\frac{1}{m-1}\right)^{jN} - \left(\frac{m-1}{m}\right)^{mN} && (4.6) \\ &> \left(\frac{m-1}{m}\right)^{mN} \sum_{j=0}^{m} (m-1)^{-jN} - \left(\frac{m-1}{m}\right)^{mN} && (4.7) \\ &= \left(\frac{m-1}{m}\right)^{mN} r \left(\frac{r^m - 1}{r-1}\right), \qquad r = (m-1)^{-N} && (4.8) \\ &> \left(\frac{m-1}{m}\right)^{mN} r && (4.9) \end{aligned}$$

Figure 4.2: $P_{ud}(\epsilon)$ for $\mathrm{RS}_1(7,1)$ (over q-ary channel) and its binary expansion (over BSC)



over binary channel

over q-ary channel

Note that lower bounding (4.8) by (4.9) is quite tight, since $\frac{r^m-1}{r-1}$ approaches 1 as m increases. Taking log of both sides yields[8]:

$$\begin{aligned}\log P_{ud}(1/m) &> mN\log\frac{m-1}{m} - N\log(m-1) &(4.10)\\ &= N\left[(m-1)\log(m-1) - m\log m\right]. &(4.11)\end{aligned}$$

Because $\log 2^{-p} = m(1-N)$, the binary expansion code is not proper if:

$$N\left[(m-1)\log(m-1) - m\log m\right] > m(1-N),$$

or equivalently

$$\frac{N}{N-1} \times \left[\log m - \frac{m-1}{m}\log(m-1)\right] < 1, \qquad m \neq 0 \tag{4.12}$$

Since the first term $\frac{N}{N-1}$ in (4.12) monotonically decreases to 1 as $m \to \infty$, and the second tends to 0, the product tends to 0. Differentiating the second term with respect to m yields:

$$-\frac{\log(m-1)}{m} + \frac{(m-1)\log(m-1)}{m^2} = -\frac{\log(m-1)}{m^2} \tag{4.13}$$

which is negative for $m \geq 2$. Hence, the LHS of (4.12) is monotonically decreasing, and it follows that if m' satisfies the bound (4.12), all $m > m'$ will also satisfy (4.12). For this case, $m' = 4$.

The cases where $m < m'$ may be checked separately. When $m = 3$ (see Figure 4.2), the binary expansion is not proper, while for $m = 2$, it is. Thus, we have shown

Theorem 4.1. *The family of codes $RS_1(n,1)$ and $ERS_1(q,1)$ are not proper $\forall m \geq 3$.*

[8] All logs are to base 2.

4.3 Properness of higher dimensional codes and severity of improperness

For codes which are not proper, we wish to determine how improper. There exists an $\hat{\epsilon} \in [0, \frac{1}{2})$ such that $P_{ud}(\hat{\epsilon})$ is maximum. Define

$$\xi = \log_2 \frac{P_{ud}(\hat{\epsilon})}{2^{-m(n-k)}} < \log_2 \frac{P_{ud}(\hat{\epsilon})}{P_{ud}(\frac{1}{2})} \tag{4.14}$$

as the *severity of improperness* of the code. A code with a high severity of improperness may be exploited to show that codes over the same field of higher dimension have binary expansions which are also improper.

Table 4.1: Severity of improperness for various binary expansions of $k = 1$ codes

code	ξ	$\hat{\epsilon}$	code	ξ	$\hat{\epsilon}$
$\text{RS}_1(7,1)$	0.3123	0.3362	$\text{ERS}_1(8,1)$	0.5516	0.3347
$\text{RS}_1(15,1)$	9.323	0.2500	$\text{ERS}_1(16,1)$	10.07	0.2500
$\text{RS}_1(31,1)$	40.42	0.2000	$\text{ERS}_1(32,1)$	41.81	0.2000
$\text{RS}_1(63,1)$	128.9	0.1667	$\text{ERS}_1(64,1)$	131.0	0.1667
$\text{RS}_1(127,1)$	358.8	0.1429	$\text{ERS}_1(128,1)$	361.7	0.1429

Formalizing this concept, we have

Lemma 4.2. *Given ξ for a code of dimension k over $\mathbb{F}_2^m$, and k' such that*

$$\xi = mk' + r \qquad 0 < r < m.$$

Then, the codes of dimension $k+1$, $k+2$, ..., $k+k'$ are also improper.

Proof. All the codewords in the binary expansion of $\text{RS}_b(n, k_1)$ are contained in $\text{RS}_b(n, k_2)$, $k_2 > k_1$. This is because for $k_1 < k_2$, the generator polynomial for $\text{RS}_b(n, k_1)$ is a multiple of the generator polynomial for $\mathrm{RS}_b(n,k_2)$. As a consequence, the $P_{ud}(\epsilon)$ for $\mathrm{RS}_b(n,k_1)$ is always strictly less than the $P_{ud}(\epsilon)$ for $\mathrm{RS}_b(n,k_2)$, for all values of $\epsilon \in [0,\frac{1}{2}]$.

For the binary expansion of $\mathrm{RS}_b(n,k)$, the 2^{-p} bound is

$$2^{-m(n-k)},$$

while for $\mathrm{RS}_b(n,k+\Delta k)$, it is

$$2^{-m(n-k-\Delta k)} > 2^{-m(n-k)}.$$

The bound for the higher dimensional code is $2^{m\Delta k}$ times that of $\mathrm{RS}_b(n,k)$. Therefore, if the $P_{ud}(\epsilon)$ of $\mathrm{RS}_b(n,k)$ exceeds its 2^{-p} bound by at least $2^{m\Delta k}$, the $P_{ud}(\epsilon)$ of $\mathrm{RS}_b(n,k+\Delta k)$ must exceed its bound also. Hence, $\xi > m\Delta k$. Figure 4.3 illustrates this.

□

Note that there is no similar concept for proper codes. In general, the $\hat{\epsilon}$, and hence ξ are difficult to find. Using the ξ for the $k=1$, $b=1$ codes in Table 4.1, we shall show:

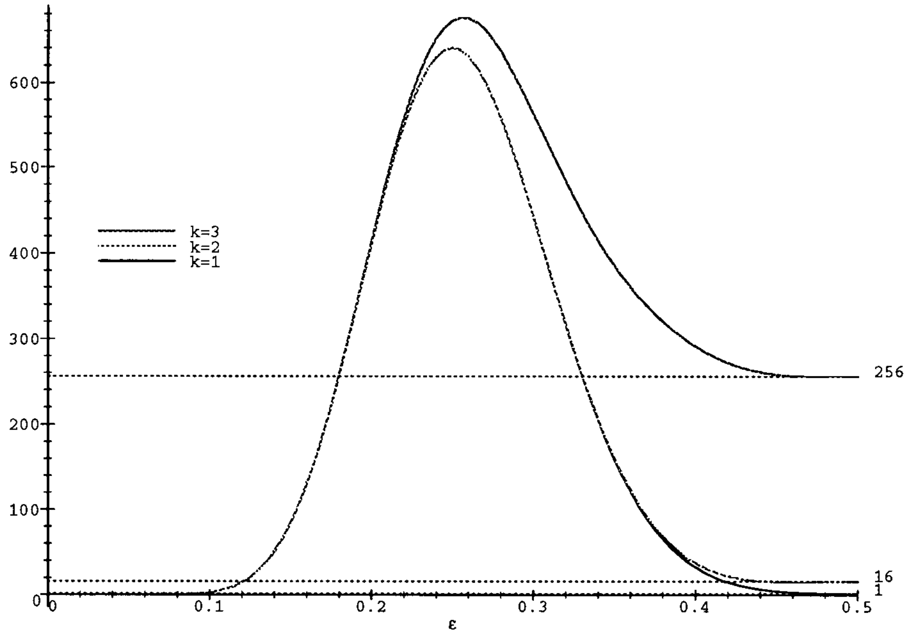
Theorem 4.3. *For a given m, the binary expansion of Reed-Solomon and extended Reed-Solomon codes with $b=1$ are not proper for rates*

$$r < 1 - \log m + \frac{m-1}{m}\log(m-1) = r^*. \tag{4.15}$$

Proof. [9] The bound in (4.12) may be generalized to higher values of k by changing the first term to $\frac{N}{N-k}$.

[9] Again, the proof applies to both non-extended and extended case. N is the block length of the (non-binary) code in question.

Figure 4.3: P_{ud} for binary expansions of RS codes, $m = 4$, $k = 1, 2, 3$.



The graph is normalized to 2^{-p} for $\mathrm{RS}_1(15,1)$, i.e., 2^{-56}. Note how P_{ud} for $\mathrm{RS}_1(15,1)$ exceeds the 2^{-p} bound for both $\mathrm{RS}_1(15,2)$ and $\mathrm{RS}_1(15,3)$.

Eqn. (4.12) then becomes:

$$\frac{N}{N-k} \times \left[\log m - \frac{m-1}{m}\log(m-1)\right] < 1.$$

Rearranging for k yields

$$k < N\left[1 - \log m + \frac{m-1}{m}\log(m-1)\right] = nr^*. \tag{4.16}$$

□

4.4 $P_{ud}(\epsilon)$ for some $b \neq 1$ RS codes

Staying with the one dimensional $k = 1$ case, we now examine the codes when $b - 1$ and n are relatively prime, whose binary weight distribution is (see Table 3.3)

$$\begin{aligned} A_0 &= 1 \\ A_{m2^{m-1}} &= n. \end{aligned} \tag{4.17}$$

It is known [18] that the maximum of $A_i\epsilon^i(1-\epsilon)^{n-i}$ occurs at $\epsilon = i/n$. So, for the weight distribution given in (4.17),

$$P_{ud}(\epsilon) = n\epsilon^{m2^{m-1}}(1-\epsilon)^{nm-m2^{m-1}}$$

which has a maximum at

$$\frac{m2^{m-1}}{m(2^m-1)} = \frac{2^{m-1}}{2^m-1} > 1/2. \tag{4.18}$$

For the extended case, the same binary weight distribution applies, but the block length is $mq = m2^m$. The ϵ for which $P_{ud}(\epsilon)$ is maximum is then

$$\frac{m2^{m-1}}{m2^m} = 1/2. \tag{4.19}$$

So, the families of codes $\mathrm{RS}_b(n,1)$ and $\mathrm{ERS}_b(n,1)$ with $b \neq 1$, $b-1$ and n relatively prime, have binary expansions which are proper for all values of m. The case where $b \neq 1$, but $b-1$ and n are not relatively prime have binary weight distributions which depend on the basis chosen, and hence are not analysed.

For the $k = 2$, $b = 3$ case, the binary weight distribution is

$$A_0 = 1$$

$$\begin{aligned} A_{(m-1)2^{m-1}} &= mn \\ A_{m2^{m-1}} &= n(n-m)+2n \end{aligned} \tag{4.20}$$

and in general is not proper for large values of m.

Using equations (4.20), the probability of undetected error is:

$$P_{ud}(\epsilon) = f_1(m)(1-\epsilon)^{nm-w_1(m)}\epsilon^{w_1(m)} + f_2(m)(1-\epsilon)^{nm-w_2(m)}\epsilon^{w_2(m)} \tag{4.21}$$

with

$$\begin{array}{llll} f_1(m) & = mn & f_2(m) & = 2n + n(n-m) \\ w_1(m) & = (m-1)2^{m-1} & w_2(m) & = m2^{m-1} \end{array}$$

We must show that there exists a value for $\epsilon \in [0, \frac{1}{2}]$ such that $P_{ud}(\epsilon)$ exceeds the $2^{-m(n-2)}$ bound. Because the first term in (4.21) dominates, we try

$$\epsilon = \frac{w_1(m)}{nm} = \frac{m-1}{m}\frac{2^{m-1}}{n} = a(m) \tag{4.22}$$

Taking the log of eqn. (4.21) and substituting (4.22),

$$\log f_1 + (nm - w_1)\log(1-a) + w_1 \log a \;>\; 2m - mn \tag{4.23}$$

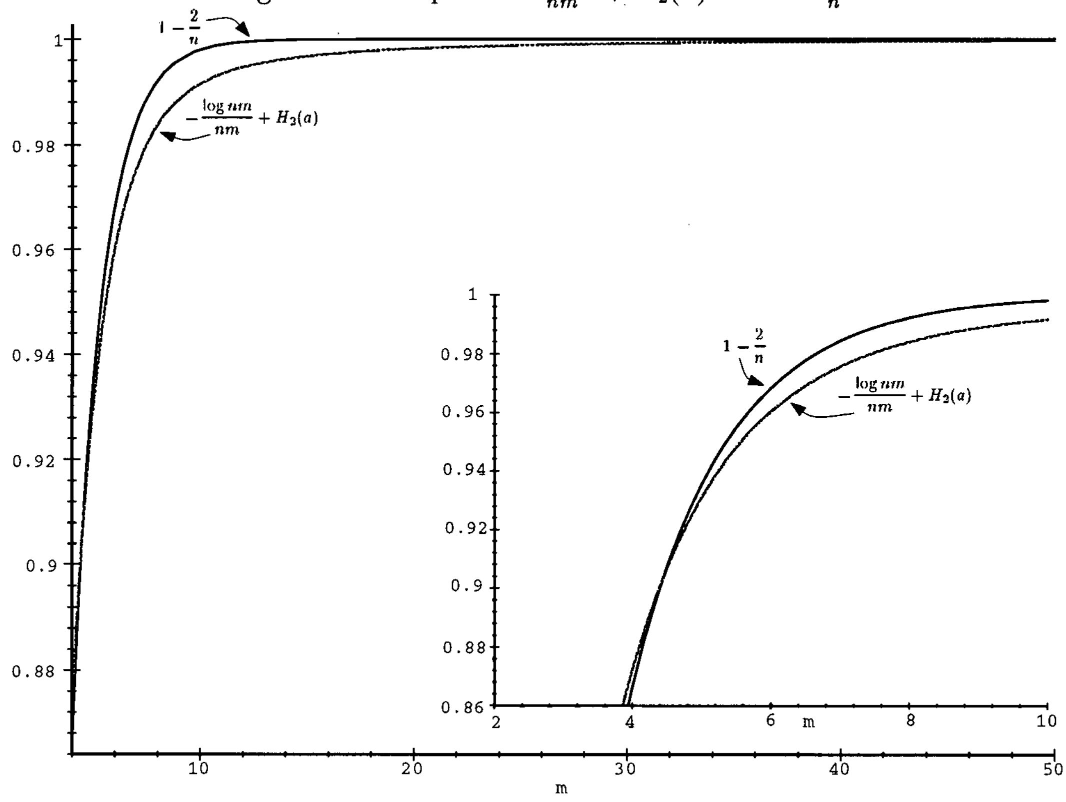
$$\frac{\log nm}{nm} + \left(1 - \frac{w_1}{nm}\right)\log(1-a) + \frac{w_1}{nm}\log a \;>\; \frac{2}{n} - 1 \tag{4.24}$$

$$\frac{\log nm}{nm} + (1-a)\log(1-a) + a\log a \;>\; \frac{2}{n} - 1 \tag{4.25}$$

$$-\frac{\log nm}{nm} + H_2(a) \;<\; 1 - \frac{2}{n} \tag{4.26}$$

where $H_2(a) = -a\log_2 a - (1-a)\log_2(1-a)$, is the entropy of a. Referring to Figure 4.4, we see that this inequality is true for $5 \geq m \geq 50$. The trend certainly shows that the inequality in (4.26) continues to be true for larger m. This, unfortunately, could not be rigourously proved. Instead, we make the following conjecture.

Figure 4.4: Graph of $-\frac{\log nm}{nm} + H_2(a)$ and $1 - \frac{2}{n}$



Conjecture 4.1. The binary expansion of $\mathrm{RS}_3(n, 2)$ over $\mathbb{F}_2^m$ is not proper for values of $m \geq 5$.

Below is a table of ξ for the $\mathrm{RS}_3(n, 2)$ family.

m	bin. wt. dist.		ξ
5	$A_{64} = 155$	$A_{80} = 868$	2.405
6	$A_{160} = 378$	$A_{192} = 3717$	3.007
7	$A_{384} = 889$	$A_{448} = 15494$	7.707
8	$A_{889} = 2040$	$A_{1024} = 63495$	16.79
9	$A_{2048} = 4599$	$A_{2304} = 257544$	33.92
10	$A_{4608} = 10230$	$A_{5120} = 1038345$	65.92

Applying Lemma 4.2 to this family would then show that $\mathrm{RS}_3(511, k)$ is improper for $k = 3$, 4, and 5, and $\mathrm{RS}_3(1023, k)$ improper for $k = 3 \ldots 8$.

A common trait for codes which are improper is its asymptotic behaviour in m. If one member of the family is improper, then it will remain improper as m is increased. We venture to make the following (unproven) conjecture:

Conjecture 4.2. Given a family of codes for which m' is the smallest value of m such that the binary expansion code is improper, then, the binary expansion codes for all $m > m'$ are also improper.

We see that this seems reasonable, since ξ increases rapidly with m. Note also that $\hat{\epsilon}$ decreases as m increases.

4.5 Properness of duals of some codes

The $P_{ud}(\epsilon)$ for some high rate codes are now examined, using eqn. (4.4). Codes of dimension $k = n - 1$ are dual to the $\mathrm{RS}_b(n, 1)$ codes. When $\gcd(b-1, n) = 1$, we can use the binary weight distribution

$$\begin{aligned} A_0 &= 1 \\ A_{m2^{m-1}} &= n = 2^m - 1. \end{aligned}$$

If $b = 2$ (note that 1 and n are always relatively we get prime), we get the dual to $\mathrm{RS}_1(n, n-1)^{10}$. In general, the dual code is $\mathrm{RS}_{n-1+b}(n, n-1) = \mathrm{RS}_{b-1}(n, n-1)$. Applying the restriction that $\gcd(b-1, n) = 1$, we conclude that

Lemma 4.4. *All $RS_b(n, n-1)$ codes, where* $\gcd(b, n) = 1$ *and $b \neq 0$ have binary expansions which are proper.*

[10] See the last sentence of section 1.3.

Proof. The probability of undetected error is given by

$$P_{ud}(\epsilon) = 2^{-m}\left[1+(2^m-1)(1-2\epsilon)^{m2^{m-1}}\right] - (1-\epsilon)^{m(2^m-1)} \tag{4.27}$$

This probability function is monotonically increasing for $\epsilon \in [0, \frac{1}{2}]$, so the code is proper. To see this, we take the derivative of (4.27)

$$\begin{aligned} P'_{ud}(\epsilon) &= m(2^m-1)(1-\epsilon)^{m2^m-m-1} - m(2^m-1)(1-2\epsilon)^{m2^{m-1}-1} && (4.28) \\ &= m(2^m-1)\left[(1-\epsilon)^x - (1-2\epsilon)^y\right] && (4.29) \end{aligned}$$

where

$$\begin{aligned} x &= m2^m - m - 1 \\ y &= m2^{m-1} - 1 \end{aligned}$$

Now, $(1-\epsilon)^{2x} = (1-2\epsilon+\epsilon^2)^x > (1-2\epsilon)^x$, so

$$(1-\epsilon)^x > (1-2\epsilon)^{\frac{x}{2}},$$

Also $y > x/2$, so that $(1-2\epsilon)^{\frac{x}{2}} > (1-2\epsilon)^y$. Therefore, eqn. (4.29) is always greater than 0. □

If $b = 1$, the binary weight distribution

$$\begin{aligned} A_0 &= 1 \\ A_{i2^{m-1}} &= \binom{m}{i} \qquad i = 1, 2, \ldots, m \end{aligned}$$

must be used instead. In this case,

$$\begin{aligned} P_{ud}(\epsilon) &= 2^{-m}\left[1+\sum_{j=1}^{m}\binom{m}{j}(1-2\epsilon)^{jn}\right] - (1-\epsilon)^{mn} && (4.30) \\ &= 2^{-m}\left[1+(1-2\epsilon)^n\right]^m - (1-\epsilon)^{mn}. && (4.31) \end{aligned}$$

Table 4.2: Severity of improperness for the binary expansions of $\mathrm{RS}_0(n, n-1)$ and $\mathrm{RS}_1(n, n-2)$

	$\mathrm{RS}_0(n, n-1)$		$\mathrm{RS}_1(n, n-2)$	
m	ξ	$\hat{\epsilon}$	ξ	$\hat{\epsilon}$
3	0.01996	0.1816	—	—
4	0.4642	0.04748	—	—
5	1.079	0.0167	0.02375	0.0425
6	1.774	0.00655	0.12829	0.0132
7	2.519	0.00275	0.33113	0.00495
8	3.302	0.00115	0.64708	0.00185

is the probability of undetected error for the binary expansion of $\mathrm{RS}_0(n, n-1)$. Table 4.5 shows the values of ξ for various m. The code is hence not proper for $3 \leq m \leq 8$, and most likely for all $m \geq 3$. Similarly, the binary expansion of $\mathrm{RS}_1(n, n-2)$ is obtained from the $\mathrm{RS}_3(n, 2)$ code (since it is the dual), and is not proper for all $m \geq 5$.

4.6 Codes which are not invariant w.r.t. basis

All the codes mentioned so far have binary expansions which are invariant w.r.t. all bases. The uniqueness of the binary weight distribution makes analysis easier. Kasami and Lin [14] show that codes (with $b = 1$) of dimension $k = 1$, 2, and 3 are invariant. Those with $k = 4$ are invariant only for odd m.

The properness/improperness of the invariant codes was discussed in previous sections. For the other codes, some mappings might result in proper binary weight distributions, whereas other may not. In fact, we are not aware of an easier way of determining the number of unique binary weight distributions, other than exhaustively trying all Ω'/n classes.

The smallest non-trivial code which is not invariant to all bases is the $\mathrm{RS}_1(15, 4)$ code, which yields 16 different binary weight distributions (from 56 equivalence classes.) Note that multiple classes may share the same distribution. Although these distributions are very similar, not all of them are proper. Table 4.3 shows the binary weight distributions for all possible bases.

All expansions which are proper have $A_{15} = 4$. While the higher weight codewords vary widely, the $P_{ud}(\epsilon)$ are fairly close, as shown in Figure 4.5. The three expansions with $A_{15} = 9$ are improper, but only slightly with $\xi \approx 0.02$. Expansion #8 has a lower minimum distance, with $A_{12} = 5$, and is much more improper with $\xi = 3.309$. These results are not surprising, since it is the low weight codewords which dominate the probability of undetected error. Again, note that there is no way of predicting the number or weight distribution of the binary expansion codes. The most important point to note is that selection of basis may, in some cases, affect the properness of the binary expansion.

There are cases, however, where codes are not invariant, but basis selection makes no difference to properness. All codes covered by Lemma 4.2 are improper, regardless of the basis chosen. The proof of the result does not depend in any way on the basis for the binary expansion. This fact, however, has not been verified by explicit enumeration of an example. The smallest codes for which this may be done are $\mathrm{RS}_1(31,5)$ or $\mathrm{RS}_1(63,4)$.

4.7 Summary

A number of codes have binary expansions which are improper. They are:

- $\mathrm{RS}_1(n,1)$ and $\mathrm{ERS}_1(q,1) \qquad \forall m \geq 3$
- the dual of the above, $\mathrm{RS}_0(n,n-1) \qquad \forall m \geq 3$
- $\mathrm{RS}_3(n,2) \qquad \forall m \geq 5$
- the dual of the above, $\mathrm{RS}_1(n,n-2) \qquad \forall m \geq 5$

Table 4.3: Binary weight distributions for the $\mathrm{RS}_1(15,4)$ code

#	bases	A_{12}	A_{15}	A_{16}	A_{17}	A_{18}	A_{19}	A_{20}	A_{21}	A_{22}
		A_{23}	A_{24}	A_{25}	A_{26}	A_{27}	A_{28}	A_{29}	A_{30}	
1	$\{1,\ \alpha,\ \alpha^2,\ \alpha^7\}$ $\{1,\ \alpha,\ \alpha^3,\ \alpha^5\}$ $\{1,\ \alpha,\ \alpha^8,\ \alpha^{11}\}$ $\{1,\ \alpha^2,\ \alpha^6,\ \alpha^{10}\}$	0	4	0	0	35	90	225	500	780
		1500	2375	2850	3285	4660	6585	6780	6136	
2	$\{1,\ \alpha,\ \alpha^6,\ \alpha^9\}$ $\{1,\ \alpha,\ \alpha^{10},\ \alpha^{13}\}$ $\{1,\ \alpha^2,\ \alpha^5,\ \alpha^{11}\}$ $\{1,\ \alpha^3,\ \alpha^6,\ \alpha^{11}\}$	0	9	15	45	20	45	135	395	840
		1545	2645	2955	3180	4715	6420	6675	6256	
3	$\{1,\ \alpha,\ \alpha^2,\ \alpha^{13}\}$ $\{1,\ \alpha,\ \alpha^2,\ \alpha^9\}$ $\{1,\ \alpha,\ \alpha^8,\ \alpha^{12}\}$ $\{1,\ \alpha^2,\ \alpha^4,\ \alpha^{11}\}$	0	4	0	0	50	60	270	470	780
		1590	2330	2940	3150	4600	6615	6720	6376	
4	$\{1,\ \alpha,\ \alpha^3,\ \alpha^6\}$ $\{1,\ \alpha,\ \alpha^7,\ \alpha^{10}\}$ $\{1,\ \alpha^2,\ \alpha^6,\ \alpha^{12}\}$ $\{1,\ \alpha^3,\ \alpha^6,\ \alpha^{10}\}$	0	4	0	0	70	60	90	560	1260
		1560	1110	2700	5850	4600	2895	6900	10216	
5	$\{1,\ \alpha,\ \alpha^3,\ \alpha^{12}\}$ $\{1,\ \alpha,\ \alpha^7,\ \alpha^{13}\}$ $\{1,\ \alpha,\ \alpha^9,\ \alpha^{12}\}$ $\{1,\ \alpha^2,\ \alpha^6,\ \alpha^9\}$	0	9	15	45	20	30	165	410	780
		1620	2555	2880	3420	4565	6480	6825	5896	
6	$\{1,\ \alpha,\ \alpha^5,\ \alpha^6\}$ $\{1,\ \alpha,\ \alpha^5,\ \alpha^{11}\}$ $\{1,\ \alpha^2,\ \alpha^5,\ \alpha^7\}$ $\{1,\ \alpha^2,\ \alpha^7,\ \alpha^{10}\}$	0	4	0	0	50	90	255	500	750
		1500	2465	2850	3270	4660	6525	6780	6196	
7	$\{1,\ \alpha,\ \alpha^3,\ \alpha^{13}\}$ $\{1,\ \alpha,\ \alpha^6,\ \alpha^7\}$ $\{1,\ \alpha^2,\ \alpha^6,\ \alpha^{11}\}$ $\{1,\ \alpha^3,\ \alpha^7,\ \alpha^{10}\}$	0	9	15	45	20	30	180	380	750
		1710	2510	2880	3540	4325	6510	7005	5716	
8	$\{1,\ \alpha,\ \alpha^9,\ \alpha^{13}\}$	5	64	15	0	0	0	60	320	1440
		960	1060	3840	5760	6400	2954	5800	10176	
9	$\{1,\ \alpha,\ \alpha^3,\ \alpha^8\}$ $\{1,\ \alpha,\ \alpha^7,\ \alpha^{11}\}$ $\{1,\ \alpha^2,\ \alpha^4,\ \alpha^{12}\}$ $\{1,\ \alpha,\ \alpha^2,\ \alpha^6\}$	0	4	0	0	35	105	225	485	840
		1425	2465	2945	3045	4810	6525	6630	6496	
10	$\{1,\ \alpha,\ \alpha^3,\ \alpha^{10}\}$ $\{1,\ \alpha,\ \alpha^7,\ \alpha^{12}\}$ $\{1,\ \alpha,\ \alpha^{10},\ \alpha^{12}\}$ $\{1,\ \alpha^2,\ \alpha^5,\ \alpha^9\}$	0	4	0	0	50	105	210	455	780
		1515	2510	2925	3150	4570	6495	6810	6376	
11	$\{1,\ \alpha,\ \alpha^2,\ \alpha^3\}$ $\{1,\ \alpha,\ \alpha^7,\ \alpha^8\})$ $\{1,\ \alpha^2,\ \alpha^4,\ \alpha^6\}$ $\{1,\ \alpha^3,\ \alpha^7,\ \alpha^{11}\}$	0	4	0	15	5	105	240	470	870
		1470	2420	2835	3195	4645	6555	6840	6196	
12	$\{1,\ \alpha,\ \alpha^3,\ \alpha^{11}\}$ $\{1,\ \alpha,\ \alpha^5,\ \alpha^7\}$ $\{1,\ \alpha,\ \alpha^5,\ \alpha^{13}\}$ $\{1,\ \alpha,\ \alpha^9,\ \alpha^{11}\}$	0	4	0	15	40	75	105	530	1290
		1530	1065	2685	6000	4585	2925	6960	9916	
13	$\{1,\ \alpha,\ \alpha^2,\ \alpha^{11}\}$ $\{1,\ \alpha,\ \alpha^5,\ \alpha^9\}$ $\{1,\ \alpha,\ \alpha^8,\ \alpha^{13}\}$ $\{1,\ \alpha^2,\ \alpha^4,\ \alpha^7\}$	0	4	0	15	20	105	210	470	840
		1470	2510	2835	3180	4645	6495	6840	6256	
14	$\{1,\ \alpha^3,\ \alpha^6,\ \alpha^9\}$	0	4	0	0	70	60	105	500	1350
		1500	1065	2940	5490	4840	2925	6540	10756	
15	$\{1,\ \alpha,\ \alpha^6,\ \alpha^{10}\}$ $\{1,\ \alpha^2,\ \alpha^5,\ \alpha^{12}\}$	0	4	0	0	55	90	75	590	1260
		1470	1155	2610	5985	4660	2865	6960	9976	
16	$\{1,\ \alpha,\ \alpha^2,\ \alpha^{12}\}$ $\{1,\ \alpha,\ \alpha^5,\ \alpha^{12}\}$ $\{1,\ \alpha,\ \alpha^6,\ \alpha^8\}$ $\{1,\ \alpha^2,\ \alpha^4,\ \alpha^9\}$	0	4	0	0	20	135	225	485	810
		1425	2465	2835	3300	4630	6525	6870	6076	

Distributions are symmetrical, so $A_i = A_{60-i}$.

Table 4.4: Improper binary expansions of $\mathrm{RS}_1(15,4)$

#	ξ	$\hat{\epsilon}$
7	0.0252	0.3008
5	0.0239	0.3009
2	0.0276	0.3005
8	3.309	0.2106

Using Lemma 4.2, we may also conclude that

- $\mathrm{RS}_1(n,k)$ and $\mathrm{ERS}_1(q,k)$ for all rates $< 1 - \log m + \frac{m-1}{m}\log(m-1)$
- $\mathrm{RS}_3(127,3)$ and $\mathrm{RS}_3(255,k)$ for $k = 3$ and 4
- $\mathrm{RS}_3(511,k)$ for $k = 3$, 4, and 5
- $\mathrm{RS}_3(1023,k)$ for $k = 3\ldots 8$

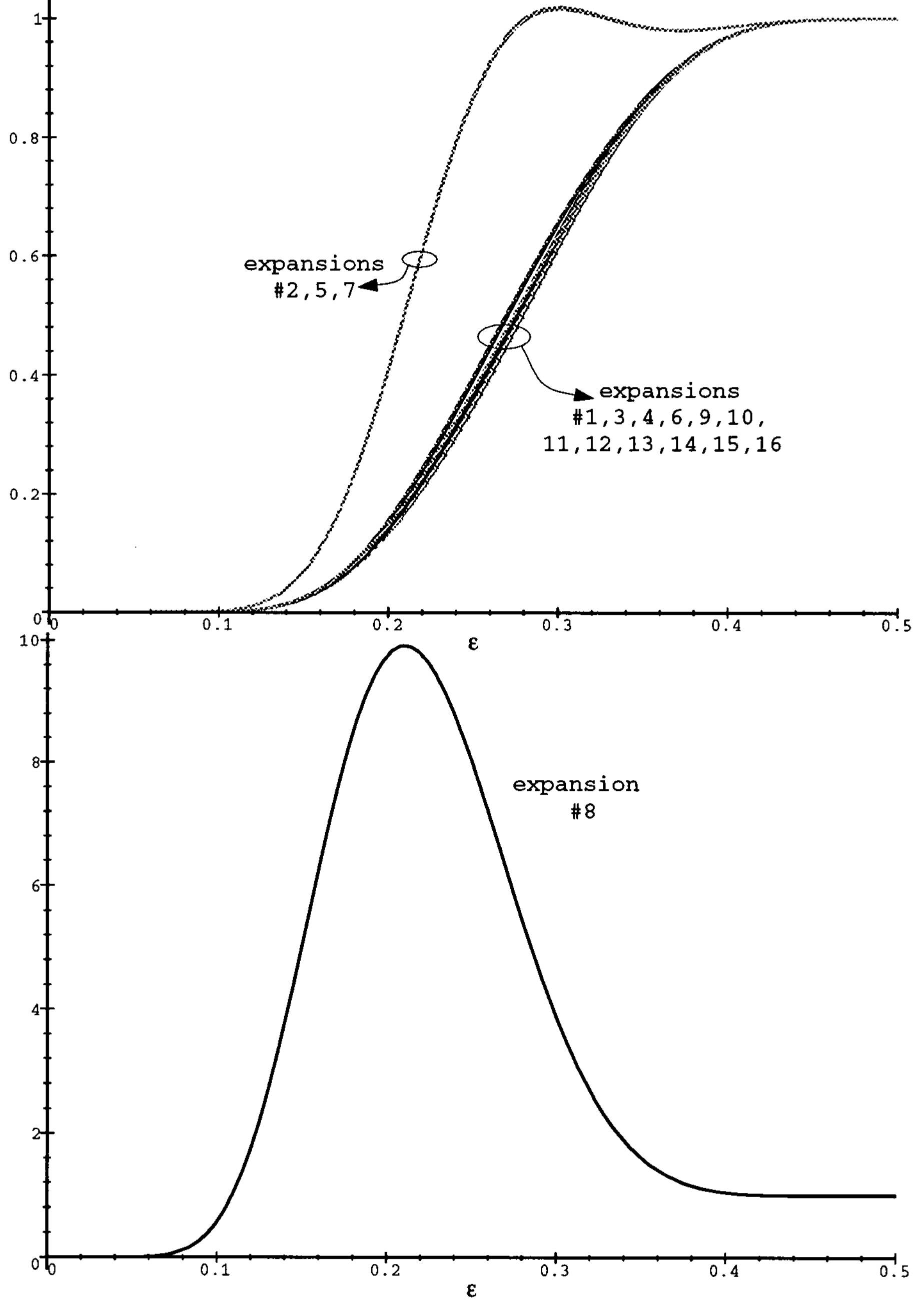
have improper binary expansions.

Although the number of codes with improper binary expansions is large, there are, nonetheless, some codes with binary expansions which are proper

- $\mathrm{RS}_b(n,1)$ with $\gcd(b-1,n) = 1$
- $\mathrm{RS}_b(n,n-1)$ with $\gcd(b,n) = 1$ (dual of the above)

One cannot help notice the relationship between dual codes. In general, the dual of a proper code is not necessarily proper [18]. However, there is no evidence of this here, suggesting perhaps that the structure of Reed-Solomon codes makes them an exception.

Figure 4.5: $P_{ud}(\epsilon)$ for the different binary expansions of $\mathrm{RS}_1(15,4)$



Vertical axis is normalized to $2^{-p} = 2^{-44}$ for the code.

5 Conclusions

In this thesis, we have considered Reed-Solomon and extended Reed-Solomon codes over $\mathbb{F}_q$. The complete weight enumerators for certain simple cases of these codes were derived. These expressions were obtained by considering the solutions to algebraic equations over $\mathbb{F}_q$, a method which is not scalable to codes with large values of k. The expressions, although complicated, contain a great deal of structure. Complete weight enumerators for extended RS codes were found to be simpler to deal with than their counterparts for RS codes.

In an effort to convert codes over $\mathbb{F}_q$ to binary codes, the bases of $\mathbb{F}_q$ over $\mathbb{F}_2$ were considered. An equivalence relation was defined, which partitions the bases into equivalence classes. For all linear codes over $\mathbb{F}_q$, bases in the same equivalence class map the code to binary expansions with identical weight enumerators. Given the set of bases a code is invariant to, the dual code is invariant to the dual set of bases. This dual set is in general not equal to the original set of bases (except for $m = 3$), but is not difficult to calculate. A certain basis and its dual do not necessarily yield the same binary code. For codes which are invariant with respect to all bases (i.e., have a unique binary expansion), we have calculated the weight distribution of this binary expansion.

The probability of undetected error for binary expansions was also considered. A majority of these were found to be improper, although specific examples of codes with proper binary expansions are given. For a given m, a rate r^* was found such that all codes with rates less than r^* are improper. This bound covers a great percentage of the codes, especially as m increases. Although the emphasis is on codes which are invariant with respect to all bases, an example of a code which is not invariant is given. It is important to remember that for such codes, the selection of basis may affect the properness of the resulting binary expansion. The r^* upper bound also affects codes which are not invariant with respect to all bases (i.e., for $k \geq 5$.)

6 Directions for future work

Many interesting questions and problems are left unanswered in this thesis.

First, the cwe's of Reed-Solomon and extended Reed-Solomon codes show considerable structure. The method used to derive them involves analysing algebraic equations of the form

$$f(x) = \alpha^j \tag{6.32}$$

over finite fields, where $f(x)$ is a polynomial in x. Thus, we are restricted to codes of dimension less than 3, since little is known if $f(x)$ has degree greater than 3. However, equations like (2.20) should be easier to solve, since x may be factored out. Thus, if the solution to eqn. (6.32) is known, perhaps equations of the form

$$x^k f(x) = \alpha^j, \qquad k \text{ a positive integer}$$

could be solved by breaking it into two separate equations:

$$\begin{aligned} x^k &= \alpha^{j-i} \\ f(x) &= \alpha^i \end{aligned}$$

These equations must be solved simultaneously for all integer i.

Also, the cwe's of extended Reed-Solomon codes are simpler than those for non-extended Reed-Solomon codes. The reason for this is unknown, but this additional structure may aid in determining their cwe's.

The bases of $\mathbb{F}_q$ over $\mathbb{F}_2$ are numerous in number, and are partitioned into equivalence classes to ease analysis. All bases in the same class were found to yield the same binary weight distribution, for all linear codes. Thus, the amount of work required to determine the invariance of a code is proportional to the number of classes. An alternative equivalence relation which partitions the bases into a smaller number of classes (more bases per class) would reduce this work.

Although symmetry of the variables of the cwe of a code implies invariance w.r.t. all bases, the $k = 3$ case is a simple example where this requirement is not necessary. We have tried to consider weaker conditions on a cwe to conclude a code is invariant w.r.t. all bases, with no concrete results. Classical invariant theory, developed by Hilbert in the late 1800s [17], may prove useful. Invariant theory has been used by Sloane [19][4, ch. 19] to determine codes which are self-dual. We had a similar analysis in mind.

The rate bound in Theorem 4.3 covers a large percentage of low rate codes. No similar bound was found for high rate codes, although there is evidence to suggest that many high rate codes are improper.

Conjecture 4.1 remains to be verified. However, in all practical terms, values of m outside the range for which this inequality has been shown to be true are rarely used. Conjecture 4.2 is more interesting. If it is true, inequalities such as eqn. (4.26) need not be solved. Induction on m seems the most likely proof. Consider a family of codes with l weights for which there are non-zero A_i. The weight enumerator of the binary expansion would then be of the form

$$\sum_{i=1}^{l} f_i(m) z^{w_i(m)}$$

with f_i and w_i monotonically increasing functions in m. Assuming that for some $m \geq m'$

$$P_{ud}(\epsilon) = \sum_{i=1}^{l} f_i \epsilon^{w_i} (1-\epsilon)^{nm-w_i} > 2^{-m(n-k)}$$

for some value of $\epsilon \in [0, \frac{1}{2}]$, we need to show that $\exists \epsilon \in [0, \frac{1}{2}]$ such that

$$\sum_{i=1}^{l} f_i(m+1)\epsilon^{w_i(m+1)}(1-\epsilon)^{n(m+1)-w_i(m+1)} > 2^{-(m+1)(n-k)}. \tag{6.33}$$

The restriction that f_i and w_i are monotonically increasing may be sufficient to show (6.33). If not, further restrictions on the differences $f_i(m+1) - f_i(m)$ and $w_i(m+1) - w_i(m)$, which are simple to test, may cause (6.33) to be true. Showing conjecture 4.2, or determining testable conditions under which conjecture 4.2 is true will allow us to avoid examining inequalities for $P_{ud}(\epsilon)$ for each code we wish to consider.

Glossary

$\mathbb{F}_q$ — the finite field with q elements.

$\mathbb{F}_q^\star$ — the non-zero elements of $\mathbb{F}_q$.

α — a primitive element of $\mathbb{F}_q$.

B — the set $\{\star, 0, 1, 2, \ldots, n-1\}$

$B^\star$ — the set $\{0, 1, 2, \ldots, n-1\}$

$\mathfrak{B}$ — the set of all bases of $\mathbb{F}_q$ over $\mathbb{F}_2$.

$\mathfrak{I}$ — a subset of $\mathfrak{B}$ such that all bases in $\mathfrak{I}$ yield a binary code with the same weight distribution.

$\mathcal{C}$ — a linear (n,k) code.

$\mathcal{C}^\perp$ — the dual code of $\mathcal{C}$.

n — the block length of a code, $n = 2^m - 1$.

q — number of elements in a field. $q = 2^m$, where $m \in \{2, 3, 4, \ldots\}$.

S_m — symmetric group of permutations with m elements.

RS — Reed-Solomon code.

ERS — Extended Reed-Solomon code.

cwe — complete weight enumerator.

$\mathrm{Tr}(x)$ — trace of a field element $x \in \mathbb{F}_q$.

$P_{ud}(\epsilon)$ — probability of undetected error.

References

[1] I. Blake and K. Kuth, "On the complete weight enumerator of Reed-Solomon codes," *SIAM journal on Discrete Mathematics*, vol. 4, no. 2, pp. 164–171, 1991.

[2] S. Lin and D.J. Costello, Jr., *Error Control Coding : Fundamentals and Applications.* Englewood Cliffs, N.J.: Prentice-Hall, 1983.

[3] W. Peterson and E.J. Weldon, Jr., *Error Control Codes.* Cambridge, M.A.: MIT Press, 1972.

[4] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting codes.* Amsterdam: North-Holland, 1977.

[5] E. Gilbert, "Capacity of a burst-noise channel," *Bell System Technical Journal*, vol. 39, pp. 1253–1266, 1960.

[6] B. Fritchman, "A binary channel characterization using partitioned markov chains," *IEEE Transactions on Information Theory*, vol. IT-13, pp. 221–227, 1967.

[7] F. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell System Technical Journal*, vol. 42, no. 1, pp. 79–94, 1963.

[8] V. Pless, "Power moment identities on weight distributions in error correcting codes," *Information and Control*, vol. 6, pp. 147–152, 1963.

[9] I. Herstein, *Topics in Algebra.* New York: Wiley, 1977.

[10] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications.* Cambridge: Cambridge University Press, 1986.

[11] E.F. Assmus, Jr., H.F. Mattson, Jr., and R. Turyn, "Cyclic codes," Tech. Rep. AFCRL-65-332, Air Force Cambridge Research Labs., 1965.

[12] T. Kasami, S. Lin, and W. Peterson, "Some results on weight distrbution of bch codes," *IEEE Transactions on Information Theory*, vol. 12, p. 274, 1966.

[13] T. Kasami and S. Lin, "On the probability of undetected error for maximum distance separable codes," *IEEE Transactions on Communications*, vol. COM-32, no. 9, pp. 998–1006, 1984.

[14] T. Kasami and S. Lin, "The binary weight distribution of the extended $(2^m, 2^m - 4)$ code of the Reed-Solomon code over GF(2^m)," *Linear Algebra and its Applications*, vol. 98, pp. 291–307, 1988.

[15] E. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Information and Control*, vol. 10, pp. 553–564, 1967.

[16] F. MacWilliams, "The structure and properties of binary cyclic alphabets," *Bell System Technical Journal*, vol. 44, no. 2, pp. 303–332, 1965.

[17] D. Hilbert, *Theory of Algebraic Invariants.* Cambridge: Cambridge University Press, 1993.

[18] S. Leung-Yan-Cheong, E. Barnes, and D. Friedman, "On some properties of the undetected error probability of linear codes," *IEEE Transactions on Information Theory*, vol. IT-25, pp. 110–112, Jan 1979.

[19] N. Sloane, "Error-correcting codes and invariant theory: new applications of a nineteenh-century technique," *American Math. Monthly*, vol. 84, pp. 82–109, 1977.

Appendix A

If $f(x)$ is a polynomial of degree $d < n$ with coefficients in the extension field $\mathbb{F}_2^m$, with $m > 1$, then

$$f(1) + f(\alpha) + f(\alpha^2) + \cdots + f(\alpha^{n-1}) = f(0).$$

Let α be a primitive element of the field, and $n = 2^m - 1$, which is odd.

Proof. Let $f(x) = a_0 + \sum_{i=1}^{d} a_i x^i$. Consider:

$$\begin{aligned}
f(1) &= a_0 + a_1 \quad + a_2 \quad + \ldots + a_d \\
f(\alpha) &= a_0 + a_1\alpha \ + a_2\alpha^2 + \ldots + a_d\alpha^d \\
f(\alpha^2) &= a_0 + a_1\alpha^2 + a_2\alpha^4 + \ldots + a_d\alpha^{2d} \\
&\vdots \\
f(\alpha^i) &= a_0 + a_1\alpha^i + a_2\alpha^{2i} + \ldots + a_d\alpha^{id} \\
&\vdots \\
f(\alpha^{n-1}) &= a_0 + a_1\alpha^{n-1} + a_2\alpha^{2(n-1)} + \ldots + a_d\alpha^{(n-1)d}
\end{aligned}$$

Summing the equations yields

$$\sum_{i=0}^{n-1} f(\alpha^i) = na_0 + a_1\sum_{i=0}^{n-1}\alpha^i + a_2\sum_{i=0}^{n-1}\alpha^{2i} + \cdots + a_d\sum_{i=0}^{n-1}\alpha^{di} \tag{A.1}$$

Further, it is well known that for $n > 2$

$$\sum_{i=0}^{n-1}\alpha^i = 1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1} = 0 \tag{A.2}$$

The sums in (A.1) may be written as

$$\sum_{i=0}^{n-1}(\alpha^d)^i = \sum_{i=0}^{n-1}\beta^i \tag{A.3}$$

where $\beta = \alpha^d$, another field element in $\mathbb{F}_2^m$. All elements have orders which divide n, so $\beta^n = 1$. Multiplying eqn. (A.3) by β yields

$$\beta\sum_{i=0}^{n-1} = \beta + \beta^2 + \cdots + \beta^{n-1} + \beta^n$$

and therefore

$$(1-\beta)\sum_{i=0}^{n-1} = 1-\beta^n = 0$$

Since $\beta \neq 1$, $\sum_{i=0}^{n-1}\beta^i = 0$, and the sum in (A.1) then simplifies to

$$\begin{aligned} na_0 + a_1\sum_{i=0}^{n-1}\alpha^i + a_2\sum_{i=0}^{n-1}\alpha^{2i} + \cdots + a_d\sum_{i=0}^{n-1}\alpha^{di} = na_0 & \\ = \; & a_0 \qquad \text{since } n \text{ is odd, and the field has characteristic 2} \\ = \; & f(0) \end{aligned}$$

□

Appendix B

Given the set of elements in $\mathbb{F}_q$ with trace 0, $\{\alpha^i | i \in B_0\}$, the new set $\{\alpha^k \alpha^i | i \in B_0, k \in B \setminus \{0, \star\}\}$, has elements evenly distributed between those with trace 0 and those with trace 1. There are 2^{m-1} elements in these sets.

Proof. By trace property (T–i), the set of all elements having trace 0 is closed. Multiplying each element of the set by α^k does not change this closure property. In this new set, there is at least one element with trace 1. The zero element guarantees that there is at least one element with trace 0 in the new set. We assert that of the $N = 2^{m-1}$ elements, there must be exactly $N/2$ elements with trace 1.

Elements have either trace 0, or trace 1 (property (T–iii)). Suppose there are Δ_1 elements with trace 1, and Δ_0 elements with trace 0. Taking an element with trace 1, and adding it to each element with trace 0 generates Δ_0 elements with trace 1. So, $\Delta_1 \geq \Delta_0$. Similarly, taking an element with trace 1, and adding it to all other elements with trace 1 generates Δ_1 elements of trace 0. This implies that $\Delta_0 \geq \Delta_1$, from which $\Delta_0 = \Delta_1 = 2^{m-2}$. □