The Dissertation Committee for Philippa Liana Charters
certifies that this is the approved version of the following dissertation:

Generalizing binary quadratic residue codes to higher power residues over larger fields

Committee:

Felipe Voloch, Supervisor

David Helm

Fernando Rodriguez-Villegas

Sriram Vishwanath

Jeffrey Vaaler

Generalizing binary quadratic residue codes to higher power residues over larger fields

by

Philippa Liana Charters, B.A.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2009

Dedicated to my mother.

Acknowledgments

I wish to thank the many people who helped me. To my advisor, who helped me figure out the tricky details. My parents, who always knew that I could do it. And to my friends, who made me love the time I spent here.

Generalizing binary quadratic residue codes to higher power residues over larger fields

Publication No. _____

Philippa Liana Charters, Ph.D.
The University of Texas at Austin, 2009

Supervisor: Felipe Voloch

In this paper, we provide a generalization of binary quadratic residue codes to the cases of higher power prime residues over the finite field of the same order, which we will call qth power residue codes. We find generating polynomials for such codes, define a new notion corresponding to the binary concept of an idempotent, and use this to find square root lower bound for the codeword weight of the duals of such codes, which leads to a lower bound on the weight of the codewords themselves. In addition, we construct a family of asymptotically bad qth power residue codes.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 A short introduction to coding theory

With the advent of the internet, an increasing proportion of our communication is taking place electronically, using computers or other machines. Because of this, we must be sure that these machines are able to transmit information both quickly and reliably. Such transmission is typically accomplished by converting the message into a sequence of zeros and ones dividing this sequence into blocks of some set length k, then transmitting the result across a communications network. Since technology is not perfect, however, there are often errors that occur during the transmission process; bits are flipped because we are sending information across what is known in coding theory as a *noisy channel*. If we attempted to send only the message across the channel, we would sometimes inadvertently add errors to our original message. Thus we first send our message through an encoder to add some redundancy so that the original message can be recovered, even if some errors occur during the transmission process. This need for error correction is originally why coding theory was born. Figure 1.1 illustrates this message encoding, transmission, and decoding process.

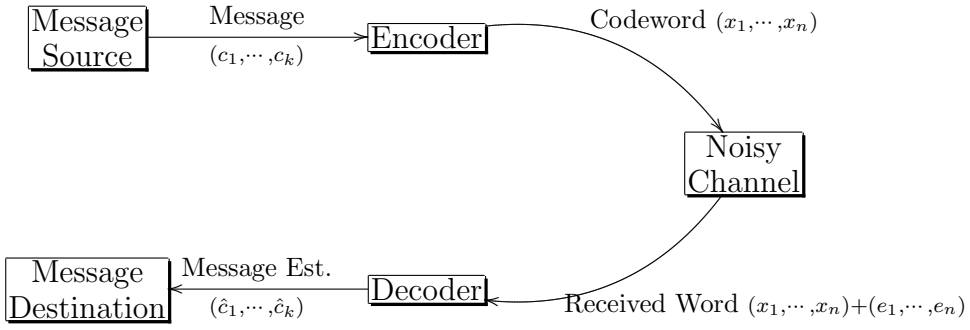

Figure 1.1: The message transmission process

A "good" code is one that allows for both the detection and correction of errors, while at the same time not taking up too much of the computer's memory. We want to reliably fix any errors that occur in the machinery while the message is being transmitted without adding a lot of extraneous information to the original message we are trying to encode. Such codes are said in coding theory to have both a good minimal distance and a good transmission rate, respectively. Families of codes meeting these criteria are called *asymptotically good*. This concept will be explained more thoroughly at the end of the chapter.

1.2 Definitions and background material

1.2.1 Algebraic Background

Most of the work in this thesis is related to concepts learned in abstract algebra and finite field theory. Many definitions in coding theory are specialized uses of ideas contained in these branches of mathematics.

The qth power residue codes that we will explore in this paper are an example of what is known as a *linear code*.

Definition 1.2.1. A *linear code* is a linear subspace $\mathcal{C}$ of the vector space $\mathbb{F}_q^n$. The dimension of this subspace, k, is called the *rank* or *dimension* of the code $\mathcal{C}$, and n is called the *length* of the code. The number $r = k/n$ is called the *(transmission) rate* of the code, and is the ratio of the original message length k to the length of the final codeword, n. In other words, it measures the quantity of information that the code can transmit in a given number of bits. We will say that $\mathcal{C}$ is a $[n, k]$ code, and the *codewords* in $\mathcal{C}$ will be denoted by vectors $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$.

In addition to being linear, the qth power residue codes have the property that they are *cyclic*:

Definition 1.2.2. A code $\mathcal{C}$ is *cyclic* if and only if it is linear and for each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathcal{C}$, the word $\mathbf{c}' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a codeword in $\mathcal{C}$. The codeword $\mathbf{c}'$ is called a *cyclic shift* of $\mathbf{c}$.

It turns out that it will be more useful for us to think about cyclic codes algebraically. In order to do this, associate the vector $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$. Using this association, we get the alternative definition:

Definition 1.2.3. A *cyclic code* $\mathcal{C}$ of length n is an ideal of the ring $R_{n,q} = \mathbb{F}_q[x]/(x^n - 1)$.

Note that multiplication by x in $R_{n,q}$ corresponds to a cyclic shift. Furthermore, $R_{n,q}$ is a principal ideal domain where every ideal is generated by one element, which we call the *generator polynomial* for $\mathcal{C}$. The following theorem from [11], p. 190, will be helpful to us later.

Theorem 1.2.1. *Let $\mathcal{C}$ be a nonzero ideal in $R_{n,q}$, i.e. a cyclic code of length n. Then*

1. *There is a unique monic polynomial $g(x) = \sum_{i=0}^{r} g_i x^i$ of minimal degree in $\mathcal{C}$.*

2. *$\mathcal{C} = \langle g(x) \rangle$, i.e. $g(x)$ is a generator polynomial of $\mathcal{C}$.*

3. *$g(x)$ is a factor of $x^n - 1$.*

4. *Any $c(x) \in \mathcal{C}$ can be written uniquely as $c(x) = f(x)g(x)$ in $\mathbb{F}_q[x]$, where $f(x) \in \mathbb{F}_q[x]$ has degree $< n - r$, $r = \deg g(x)$. The dimension of $\mathcal{C}$ is $n - r$ (i.e., $\mathcal{C}$ is an $[n, n-r]$ code). Thus the message $f(x)$ becomes the codeword $f(x)g(x)$.*

5. *If $g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_r x^r$, then $\mathcal{C}$ is generated (as a subspace of $\mathbb{F}_q^n$) by the rows of the generator matrix*

$$
\begin{aligned}
G &= \begin{bmatrix}
g_0 & g_1 & g_2 & \cdots & g_r & & 0 \\
 & g_0 & g_1 & \cdots & g_{r-1} & g_r & \\
 & & & \cdots & \cdots & & \\
0 & & g_0 & \cdots & \cdots & & g_r
\end{bmatrix} \\
&= \begin{bmatrix}
g(x) & & & & & & \\
 & xg(x) & & & & & \\
 & & & \cdots & & & \\
 & & & & x^{n-r-1}g(x) & &
\end{bmatrix}
\end{aligned}
$$

We do not include a proof of this theorem here, but the curious reader can find it in [11].

Besides the length and dimension of a code, we will also be concerned with what is known as its *minimum distance*. The *(Hamming) distance* $\mathrm{d}(\mathbf{c}, \mathbf{d})$ between two distinct codewords $\mathbf{c} = (c_1\ c_2\ \ldots\ c_n)$ and $\mathbf{d} = (d_1\ d_2\ \ldots\ d_n)$ in the code $\mathcal{C}$ is the number of places where they differ: $\mathrm{d}(\mathbf{c}, \mathbf{d}) = |\{0 \leq i \leq n \mid c_i \neq d_i\}|$. The *(Hamming) weight* of the codeword $\mathbf{c}$, denoted $\mathrm{wt}(\mathbf{c})$, is the distance $\mathrm{d}(\mathbf{c}, \mathbf{0})$ between $\mathbf{c}$ and the zero vector and measures the number of nonzero entries in the vector $\mathbf{c}$.

Definition 1.2.4. The *minimum distance* of a code $\mathcal{C}$, denoted $\mathrm{d}_{\min}(\mathcal{C})$, is

$$\mathrm{d}_{\min}(\mathcal{C}) = \min_{\substack{\mathbf{c},\mathbf{d}\in\mathcal{C} \\ \mathbf{c}\neq\mathbf{d}}} \mathrm{d}(\mathbf{c}, \mathbf{d}) = \min_{\substack{\mathbf{c}\in\mathcal{C} \\ \mathbf{c}\neq 0}} \mathrm{wt}(\mathbf{c})$$

Note that this definition implies that we may use the terms minimum weight and minimum distance interchangably. Both terms will be used frequently in this paper. An $[n, k]$ code in which we know this final parameter of minimum distance, d, is called an $[n, k, d]$ code.

In general we prefer codes with large minimum distance because of their ability to correct more errors.

Theorem 1.2.2. *A code $\mathcal{C}$ with odd minimum distance d can correct $\frac{1}{2}(d-1)$ errors. If d is even, then $\mathcal{C}$ can correct $\frac{1}{2}(d-2)$ errors and detect $\frac{d}{2}$ errors.*

Figure 1.2.1 shows an example of this theorem. In the figure, we see that codewords $\mathbf{a}, \mathbf{b}$ and $\mathbf{c}$ differ from each other in three places. Thus if only

one error occurs, choosing the codeword closest to the received message will correct the error.

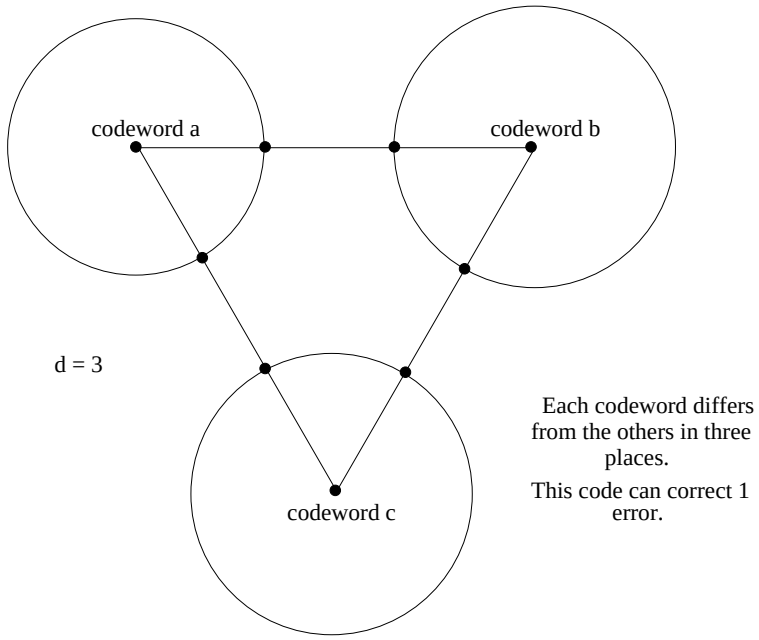

Figure 1.2: A code with minimal distance 3 can correct 1 error

A larger minimum distance implies more powerful error-correction capabilities. Computing the minimum distance of a code is usually quite difficult. In fact, this problem has been shown to be NP-hard [16]; there is no known way of doing the computation in less than exponential time. What we will do instead for our family of qth power residue codes is find a lower bound on this minimum distance. The minimum distance itself will only be found for a few select cases, using available technology. A table of some of these results can be found in Appendix 1.

For any $[n, k]$ code, we do have a best-case scenario for the minimum distance known as the *Singleton bound*.

Theorem 1.2.3. *(Singleton Bound) If $\mathcal{C}$ is an $[n, k, d]$ code, then we must have*

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

Ideally, we want an $[n, k]$ code to have minimum distance as close to this maximum as possible, but note that many perfectly good codes do not meet this bound, and it is unrealistic to expect them to. In fact, a family of codes can have good minimum distance without coming close to meeting this upper bound. It is only important that the codes be what we will call *asymptotically good*. We will discuss this notion in greater detail in Section 1.2.2.

In studying codes, it is often helpful to look instead at their *dual codes*. This technique will be used later in this thesis. To understand the notion of a dual code, note that by Theorem 1.2.1 every cyclic linear code $\mathcal{C}$ can be generated over $R_{n,q}$ by some polynomial $g(x)$ of minimal degree which divides the polynomial $x^n - 1$. Let $h(x) = \frac{x^n-1}{g(x)} = \sum_{i=0}^{k} h_i x^i$. We call $h(x)$ the *check polynomial* of $\mathcal{C}$. To see why this name fits, note that if $a(x) \in \mathcal{C}$, then $a(x) = b(x)g(x)$ for some polynomial $b(x)$. Thus in $R_{n,q}$, $a(x)h(x) = b(x)g(x)h(x) = b(x)(x^n-1) \equiv 0 \mod (x^n-1)$. In other words, the polynomial $h(x)$ checks whether the polynomial $a(x)$ is a codeword in $\mathcal{C}$.

Definition 1.2.5. The dual code $\mathcal{C}^{\perp}$ is the cyclic code generated over $R_{n,q}$ by the polynomial

$$g^{\perp}(x) = x^{\deg h(x)} h(x^{-1}).$$

where $h(x)$ is the check polynomial defined above. This code is generated as a subspace of $\mathbb{F}_q^n$ by the rows of the $r \times n$ generator matrix

$$\begin{aligned} H &= \begin{bmatrix} & & & h_l & \cdots & h_2 & h_1 & h_0 \\ & & h_l & \cdots & h_2 & h_1 & h_0 & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ h_l & \cdots & h_2 & h_1 & h_0 & & & \end{bmatrix} \\ &= \begin{bmatrix} & & & & & \overleftarrow{h(x)} \\ & & & & \overleftarrow{xh(x)} & \\ & & & \ddots & & \\ x^{n-l-1}\overleftarrow{h(x)} & & & & & \end{bmatrix} \end{aligned}$$

where $l = \deg h(x) = n - \deg g(x) = n - r = \dim(\mathcal{C})$.

Note that $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are duals as vector spaces: if $\mathbf{c} \in \mathcal{C}$ and $\mathbf{c}^* \in \mathcal{C}^{\perp}$ then $\mathbf{c} \cdot \mathbf{c}^* = \mathbf{0}$.

Example 1. Let us look at a simple example. Suppose $q = 2$ and $n = 4$. Our codes are ideals of the ring $R_{4,2} = \mathbb{F}_2[x]/(x^4 + 1)$. Let $g(x) = x + 1$ be the generating polynomial for a code $\mathcal{C}_g$ over $R_{4,2}$. From Theorem 1.2.1 $\mathcal{C}_g$ has generator matrix given by

$$G_g = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The check polynomial for $\mathcal{C}_g$ is given by $h(x) = \frac{x^4+1}{x+1} = x^3 + x^2 + x + 1$, hence we have check matrix $H_g = [\,1\ 1\ 1\ 1\,]$. It is clear that this code has length 4 and

dimension 3. The message

$$(1\ 0\ 1) \leftrightarrow 1 + x^2$$

is encoded by either computing $(1\ 0\ 1)G_g = (1\ 1\ 1\ 1)$ or $(1 + x^2)g(x) = 1 + x + x^2 + x^3$. We can calculate that the codewords in $\mathcal{C}_g$ are elements of the set (written two different ways):

$$\{(0000), (1100), (0110), (0011), (1010), (0101), (1111), (1001)\} \subseteq \mathbb{F}_2^4$$

or

$$\{0, 1 + x, x + x^2, x^2 + x^3, 1 + x^2, 1 + x + x^2 + x^3, 1 + x^3\} \subseteq \mathbb{F}_2/(x^4 - 1)$$

It follows that $d_{\min}(\mathcal{C}_g) = 2$, which means that this $[4, 3, 2]$ code can detect one error, but cannot correct any errors. Note that $\mathcal{C}_g$ meets the Singleton Bound and hence has optimal minimal distance for a code of its length and dimension.

1.2.2 Some notation and vocabulary

Recall that a good code is one that has both a good transmission rate (we add as few extra bits to the length of the original message as possible) and a good minimum distance (as close to the Singleton bound as possible). In Chapter 5 we construct a family of qth power residue codes that is *asymptotically bad*. Ideally, however, we are looking for families of codes that are *asymptotically good*. What that means for us is that for a fixed prime q we are looking at qth power residue codes with prime lengths p_i, with the prime

p_i approaching infinity as i approaches infinity. For each of these increasing prime values, let $\mathcal{C}_{p_i}$ denote the qth power residue code of length p_i, let r_{p_i} denote the dimension or rate of $\mathcal{C}_{p_i}$ and let d_{p_i} denote the minimum distance of $\mathcal{C}_{p_i}$. Ideally, we would like to find a family of qth power residue codes with the property that

$$\lim_{i\to\infty} \frac{r_{p_i}}{p_i} = \epsilon_r > 0 \text{ and } \lim_{i\to\infty} \frac{d_{p_i}}{p_i} = \epsilon_d > 0.$$

Such codes are said to be *asymptotically good*; both their rate and relative distance are asymptotically non-vanishing. An *asymptotically bad* family of codes is one in which at least one of these limits approaches zero.

In the construction of an asymptotically bad family of qth power residue codes, we will frequently use some notation which may not be familiar to all readers. Specifically, the symbol $\ll$ will be used to denote asymptotic behavior. $f \ll g$ stands for $f(x) = O(g(x))$ for $x \to \infty$. In other words, there exists some positive real number γ and a real number x_0 with the property that $|f(x)| \leq \gamma|g(x)|$ for all $x > x_0$.

Chapter 2

A brief discussion of binary quadratic residue codes

Now that we have the background material required, we are ready to begin working towards our main result. We will be primarily interested in further exploring codes that are similar to a well-studied class of codes known as quadratic residue codes. Specifically, we extend the notion of binary quadratic residue codes to qth power residue codes over $\mathbb{F}_q$ for q an arbitrary prime. In extending the methods of [7], we find a bound on the weight of these codes, as well as a bound on the weight of the dual codes. In addition, an asymptotically bad subfamily of these codes is constructed and explored, following the argument contained in [17] which finds such a family for binary quadratic residue codes.

2.1 Definitions

Set up a correspondence between $\mathbb{F}_p$ and the set $\{0, 1, \ldots, p-1\}$. Let $\alpha \in \mathbb{F}_p^*$. If there exists some $\beta \in \mathbb{F}_p^*$ such that $\beta^2 = \alpha$ we will say that α is a *quadratic residue* modulo p. The binary quadratic residue codes are defined as follows. Let p be an odd prime such that $p \equiv \pm 1 \mod 8$ (which we choose

so that 2 is a quadratic residue modulo p), and let α be a primitive pth root of unity in the smallest field extension of $\mathbb{F}_2$ containing such an element.

Definition 2.1.1. If Q is the set of quadratic residues modulo p, and N is the set of nonresidues, then the binary quadratic residue codes $\mathcal{Q}, \bar{\mathcal{Q}}, \mathcal{N}, \bar{\mathcal{N}}$ of length p are the ideals of $R_{p,2}$ generated by $q(x) = \prod_{i \in Q}(x - \alpha^i)$, $(x-1)q(x)$, $n(x) = \prod_{i \in N}(x - \alpha^i)$, and $(x-1)n(x)$ respectively.

$\mathcal{Q}$ and $\mathcal{N}$ are sometimes called *augmented* quadratic residue codes, while $\bar{\mathcal{Q}}$ and $\bar{\mathcal{N}}$ are called *expurgated* quadratic residue codes, so named because they are gotten by deleting or expurging those codewords of odd weight from $\mathcal{Q}$ and $\mathcal{N}$ respectively. Note that our choice of α in this construction was arbitrary - choosing a different α might switch the polynomials $q(x)$ and $n(x)$.

The quadratic residue codes are known to have minimum distance $d \geq \sqrt{p}$ (though minor improvements are known) and dimension $\frac{1}{2}(p+1)$ (augmented) or $\frac{1}{2}(p-1)$ (expurgated) [11]. In other words, their transmission rate is close to $\frac{1}{2}$ as p approaches infinity; they have a good transmission rate, even for large values of p. We also notice that because of the way these codes are defined, $x^p - 1 = (x-1)q(x)n(x)$; hence $\mathcal{Q}^\perp$ is equivalent to $\bar{\mathcal{Q}}$ and $\mathcal{N}^\perp$ is equivalent to $\bar{\mathcal{N}}$, with equality occuring when $p = 4k - 1$.

Example 2. To see how these codes work, let us look at the simplest case. Let $p = 7$. Then $Q = \{1, 2, 4\}$ and $N = \{3, 5, 6\}$. The smallest field with a primitive seventh root of unity is $GF(2^3) = \mathbb{F}_2[\alpha]/(\alpha^3+\alpha+1)$. The powers of α in this field are $\alpha,\ \alpha^2,\ \alpha^3 = \alpha+1,\ \alpha^4 = \alpha^2+\alpha,\ \alpha^5 = \alpha^2+\alpha+1,\ \alpha^6 = \alpha^2+1,$

and $\alpha^7 = 1$. It follows that α is a primitive seventh root of unity in this definition of $GF(2^3)$. Hence the generating polynomial for $\mathcal{Q}$ is

$$\begin{aligned} q(x) &= (x+\alpha)(x+\alpha^2)(x+\alpha^4) \\ &= x^3 + (\alpha+\alpha^2+\alpha^4)x^2 + (\alpha^3+\alpha^5+\alpha^6)x + 1 \\ &= x^3 + (\alpha+\alpha^2+(\alpha+\alpha^2))x^2 \\ &\quad +((\alpha+1)+(\alpha^2+\alpha+1)+(\alpha^2+1))x+1 \\ &= x^3+x+1 \end{aligned}$$

and similarly $\mathcal{N}$ is generated by the polynomial

$$n(x) = x^3 + x^2 + 1.$$

Both of these codes have minimal weight 3, and are thus $[7,4,3]$ codes. As mentioned above, $q(x)$ and $n(x)$ may be switched by choosing a different primitive root. In particular, choosing α^3, α^5 or α^6 as this primitive root will switch these polynomials.

2.2 Historical Importance

Because of the relatively good properties of quadratic residue codes there has historically been a great deal of interest in them. As previously mentioned, they have transmission rate close to $\frac{1}{2}$ for all values of p. Moreover, their minimum distance is consistently larger than the square root bound would indicate, which gives us hope that an even better bound can be achieved. Many of the properties of the quadratic residue codes have been explored in

detail in other books and papers, most comprehensively in Chapter 16 of [11]. The qth power residue codes that we introduce here have a better transmission rate than their quadratic counterparts. We will prove a square root bound for the minimum distance of the duals of the qth power residue codes, and from this deduce a lower bound for the minimum distance of the codes themselves. Specifically, if the generator polynomial a qth power residue code $\mathfrak{A}_0$ factors into m irreducible elements over $\mathbb{F}_p[x]$, then:

$$d_{min}(\mathfrak{A}_0) \geq p^{\frac{1}{2(qm-1)}}.$$

The proof of this theorem relies on the fact that the dual of the code $\mathfrak{A}_0$ is generated by the product of the generator polynomials for $q-1$ different codes, each of which is isometric to $\mathfrak{A}_0$.

Chapter 3

Defining qth power residue codes

3.1 Basic definitions

For the remainder of this paper, let q be some fixed odd prime number (letting $q = 2$ would give us the quadratic residue codes, which have already been thoroughly explored. For a more in-depth treatment, see [11]). Let $p \neq q$ be an odd prime such that q is a qth power residue modulo p. That is, there exists some $\beta \in \mathbb{F}_p$ such that $\beta^q \equiv q \mod p$. Moreover, let $q \mid (p-1)$. We can divide $\mathbb{F}_p^*$ into q cosets as follows.

Choose a primitive qth root of unity $\zeta \in \mathbb{F}_p$ and define a homomorphism $\psi_q : \mathbb{F}_p^* \to (\mathbb{F}_q, +)$ by

$$\psi_q(j) = i \quad \text{when } j^{\frac{p-1}{q}} \equiv \zeta^i \mod p$$

Note that $\psi_q(j) = 0$ if and only if j is a qth power residue modulo p, and moreover $\psi_q(j)^q \equiv \psi_q(j) \mod q$ by Fermat's Little Theorem. $\mathbb{F}_p^*$ can be divided into q cosets $A_0, A_1, \ldots, A_{q-1}$ given by $A_i = \{j \in \mathbb{F}_p^* \mid \psi_q(j) = i\}$. A_0 is the set of qth power residues modulo p.

Let α be a primitive pth root of unity in the smallest field extension of

$\mathbb{F}_q$ containing such an element. We define the polynomials

$$\mathfrak{a}_i(x) = \prod_{a \in A_i} (x - \alpha^a) \in \mathbb{F}_q[x].$$

Note that we may write $x^p - 1 = (x-1)\prod_{i=0}^{q-1} \mathfrak{a}_i(x)$.

Definition 3.1.1. The qth **power residue codes** $\mathfrak{A}_i$, $\bar{\mathfrak{A}}_i$ are cyclic codes (ideals) of the ring $R_{p,q} = \mathbb{F}_q[x]/(x^p - 1)$ with generator polynomials $\mathfrak{a}_i(x)$ and $(x-1)\mathfrak{a}_i(x)$ respectively, for $i = 0, \ldots, q-1$.

In keeping with the convention established for the quadratic residue codes we will call $\mathfrak{A}_i$ an *augmented* qth power residue code, while $\bar{\mathfrak{A}}_i$ will be known as an *expurgated* qth power residue code. This time, the codewords we are expurging correspond to those $\mathbf{c} = (c_0, \ldots, c_{p-1})$ where $\sum_{i=0}^{p-1} c_i \equiv 0 \mod q$.

We note here that this definition is not new, as qth power residue codes have been defined in a similar manner and briefly explained by Berlekamp in Section 15.2 of [1]. However, the techniques we use will differ substantially from this prior source, and the lower bound we establish will be more general than the one proved by Berlekamp in his book. It is also important to mention that the qth power residue codes being studied here are significantly different than those explored by Chapman in [2] and by vanLint and MacWilliams in [15], despite having a similar name.

By Theorem 1.2.1, $\mathfrak{A}_i$ has a generator matrix given by

$$G_{\mathfrak{A}_i} = \begin{bmatrix} \mathfrak{a}_i(x) & & & \\ & x\mathfrak{a}_i(x) & & \\ & & \cdots & \\ & & & x^{p-\frac{p-1}{q}-1}\mathfrak{a}_i(x) \end{bmatrix}.$$

It follows easily that these codes have dimension $p - \frac{p-1}{q} = \frac{p(q-1)+1}{q}$, and hence a rate of $\frac{p(q-1)+1}{q}/p = \frac{q-1}{q} + \frac{1}{pq}$, which approaches $\frac{q-1}{q}$ as p approaches infinity. That is, the transmission rate of these codes is asymptotically good, as defined in Chapter 1.

Much of the remainder of this thesis will be concerned with the second important property for determining the effectiveness of codes: estimating their minimum distance. This proves to be a much harder task. The *Singleton bound* tells us that

$$d_{\min}(\mathfrak{A}_0) \leq p - (p - \frac{p-1}{q}) + 1 = \frac{p-1}{q} + 1.$$

While approaching this bound is extremely unlikely for any family of codes, we do succeed in finding a lower bound on the minimum distance for the qth power residue codes. Unfortunately, it can (and will) be shown in Chapter 5 that for every prime q there exists an asymptotically *bad* family of qth power residue codes. It is currently unknown whether an asymptotically good family can be found. A variation of this question has been studied for years by those interested in quadratic residue codes, with no substantial progress being made towards finding a solution.

3.2 A new "idempotent": the q-idempotent

In order to obtain a lower bound on the minimum distance of the qth power residue codes, it will be helpful to first find a different, easier to work with, generator polynomial. This polynomial will be constructed to be what we call a q-idempotent of our code, with this name being taken from the classic binary concept of the idempotent of a code.

Definition 3.2.1. A polynomial $E_2(x)$ of $R_{n,2}$ is an *idempotent* if $E_2(x) = E_2(x)^2 = E_2(x^2)$.

This concept is important because of the following theorem.

Theorem 3.2.1. *Let $\mathcal{C} = \langle g(x) \rangle$ be a binary cyclic code. Then $\mathcal{C}$ contains a unique idempotent $E_2(x)$ such that*

1. *$\mathcal{C} = \langle E_2(x) \rangle$ (and hence $E_2(x) = p(x)g(x)$ for some polynomial $p(x)$).*
2. *$c(x) \in \mathcal{C}$ if and only if $c(x)E_2(x) = c(x)$.*

That is, every binary cyclic code can be generated by an idempotent, which because of its special properties can be helpful in finding out more about the code itself. When we define q-idempotents, we will not be quite so thorough. Rather, we will simply define what we mean by a q-idempotent, and show that one exists for our qth power residue codes (though not for codes over $\mathbb{F}_q$ in general). This result, though limited, will prove to be enough for our purposes.

Definition 3.2.2. Let $E_q(x)$ be a polynomial in $R_{n,q}$. Then we call $E_q(x)$ a *q-idempotent* if $E_q(x) = E_q(x^q) = E_q(x)^q$.

In what follows we will find a q-idempotent that generates the same code as the original generator polynomial for $\bar{\mathfrak{A}}_0$. To prove that this q-idempotent ends up generating the same code as $(x-1)\mathfrak{a}_0(x)$, we will need the following Lemma found on p. 199 of [11]:

Lemma 3.2.2. *Let $g(x) \mid x^n - 1 \in R_{p,q}$ be the generator polynomial for some code $\mathcal{C}$. If $a(x) \in R_{p,q}$ is any polynomial with $(a(x), x^n - 1) \mid g(x)$, then $g(x)$ and $a(x)g(x)$ generate the same code.*

That is, any two polynomials that share the same roots of $x^n - 1$ generate the same code in $R_{p,q}$.

Claim 1. *Define*

$$E_q(x) = \sum_{m=1}^{p-1} \psi_q(m) x^m,$$

where $\psi_q(m)$ is the homomorphism from $\mathbb{F}_p^*$ to $(\mathbb{F}_q, +)$ defined in Section 3.1. Then there exists some pth root of unity α in the smallest field extension of $\mathbb{F}_q$ containing such an element so that $E_q(x)$ is a q-idempotent which generates the code $\bar{\mathfrak{A}}_0$. That is, the polynomial $E_q(x)$ generates the same code as $(x-1)\mathfrak{a}_0(x)$.

Proof. Note that for any qth power residue ξ, we have $\psi_q(\xi n) = \psi_q(n) = \psi_q(n/\xi)$ since ψ_q is an additive homomorphism. That is, multiplication by qth power residues fixes cosets. In our case, this means we have $\psi_q(qn) = \psi_q(n)$,

as q is a qth power residue modulo p. Choose α any primitive pth root of unity in the corresponding field extension of $\mathbb{F}_q$. Then because of the previous assertion, properties of the field $\mathbb{F}_q$, and Fermat's Little Theorem we may write:

$$\begin{aligned} E_q(x)^q &\equiv \left(\sum_{m=1}^{p-1} \psi_q(m)x^m\right)^q \equiv \sum_{m=1}^{p-1} \psi_q(m)^q x^{qm} \\ &\equiv \sum_{m=1}^{p-1} \psi_q(m)x^{qm} \equiv \sum_{m=1}^{p-1} \psi_q(qm)x^{qm} \\ &\equiv E_q(x) \mod q \end{aligned}$$

and similarly we find that $E_q(x^q) = E_q(x)$. It follows that $E_q(\alpha) \in \mathbb{F}_q$, and moreover that $E_q(x)$ is a q-idempotent. Now choose α so that $E_q(\alpha) = 0$ (it will shortly become clear why such an α must exist). Then for all $a \in A_0$ we have

$$\begin{aligned} E_q(\alpha^a) &= \sum_{m=1}^{p-1} \psi_q(m)\alpha^{ma} = \sum_{n=1}^{p-1} \psi_q(\frac{n}{a})\alpha^n \\ &= \sum_{n=1}^{p-1} \psi_q(n)\alpha^n = E_q(\alpha) = 0. \end{aligned}$$

Moreover,

$$\begin{aligned} E_q(1) &= \sum_{m=1}^{p-1} \psi_q(m) = \frac{p-1}{q}(0+1+2+\cdots+(q-1)) \\ &= \frac{p-1}{q}\left[q \cdot \frac{(q-1)}{2}\right] = \frac{(p-1)(q-1)}{2} \equiv 0 \mod q \end{aligned}$$

where the last equivalence follows since we know that $2 \mid (q-1)$ and $q \mid (p-1)$. It follows that all of the factors of $(x-1)\mathfrak{a}_0(x)$ are also factors of $E_q(x)$, hence

$$\langle (x-1)\mathfrak{a}_0(x) \rangle \supseteq \langle E_q(x) \rangle$$

in $R_{p,q}$. To show the reverse inclusion, let $b \notin A_0$. Then

$$\begin{aligned} E_q(\alpha^b) &= \sum_{m=1}^{p-1} \psi_q(m)\alpha^{bm} = \sum_{n=1}^{p-1} \psi_q(\frac{n}{b})\alpha^n \\ &= \sum_{n=1}^{p-1} \psi_q(n)\alpha^n - \sum_{n=1}^{p-1} \psi_q(b)\alpha^n \\ &= E_q(\alpha) - \psi_q(b) \sum_{n=1}^{p-1} \alpha^n \\ &= -\psi_q(b) \cdot (-1) = \psi_q(b) \neq 0. \end{aligned}$$

That is, $E_q(x)$ has no additional factors of $x^n - 1$ in $R_{p,q}$.

To show that we have not done anything fishy in our choice of α, note that the previous series of equalities tells us that there must be some α satisfying our original assumption that $E_q(\alpha) = 0$. If $E_q(\beta) = n$, choose $e \in \mathbb{F}_q$ such that $\psi_q(e) \equiv -n \mod p$ and let $\alpha = \beta^e$. Then $E_q(\alpha) = E_q(\beta^e) = E_q(\beta) + \psi_q(e) = n + (-n) = 0$ as desired.

It follows from Lemma 3.2.2 that

$$\langle E_q(x) \rangle = \langle (x-1)\mathfrak{a}_0(x) \rangle = \bar{\mathfrak{A}}_0,$$

and we have found a new generator polynomial for $\bar{\mathfrak{A}}_0$. We may slightly alter $E_q(x)$ to find similar polynomials for each of the $\mathfrak{A}_i$'s and $\bar{\mathfrak{A}}_i$'s. Specifically, if $\xi_k \in A_k$, define $E_q^{(k)}(x) = \sum_{m=1}^{p-1} \psi_q(\frac{m}{\xi_k})x^m$ has roots 1 and α^a, $a \in A_k$, hence generates $\bar{\mathfrak{A}}_k$.

□

Chapter 4

Codeword weight and minimal distance

4.1 Codeword weight of qth power residue codes

Based on a lemma originally proved by Helleseth in [6] (although we will follow the simpler proof later used in [7]), we are able to find a bound on the codeword weight of the qth power residue codes using the q-idempotent found in Section 3.2.

Consider the polynomial $a(x) = \sum_{i=1}^{r} \gamma_{k_i} x^{k_i} \in \mathbb{F}_q[x]/(x^p - 1)$, where $\gamma_{k_i} \neq 0$ and the k_i are unique elements of $\mathbb{F}_p$ so that $a(x)$ has weight r. Let $K = \{k_1, \ldots, k_r\}$ be the set of exponents of $a(x)$. Create a corresponding polynomial $f_a(t) = \prod_{k \in K} (t-k)^{\gamma_k} \in \mathbb{F}_p[t]$. When there is no ambiguity as to the indentity of the polynomial a, we will use $f(t)$ to denote the polynomial $f_a(t)$. Let $E_q(x)$ be the q-idempotent of $\bar{\mathfrak{A}_0}$ defined previously. Then $a(x)E_q(x)$ is a codeword in $\bar{\mathfrak{A}_0}$, and we want to be able to determine its weight.

Write $c(x) = a(x)E_q(x) = \left(\sum_{k \in K} \gamma_k x^k\right) \left(\sum_{m=1}^{p-1} \psi_q(m) x^m\right) \equiv \sum_{i=0}^{p-1} c_i x^i$. We want to count those places where $c_s \neq 0$ in order to determine the weight $w(\mathbf{c})$ of this codeword. In order to do this, first note that

$$c_s = \sum_{k \in K} \psi_q(s-k)\gamma_k, \quad s \notin K \quad \text{or} \quad \sum_{k \in K, k \neq s} \psi_q(s-k)\gamma_k, \quad s \in K.$$

Define a homomorphism $\chi_q : \mathbb{F}_p \to \mathbb{C}$ by

$$\chi_q(x) \quad = \quad \begin{cases} 0 & x = 0 \\ e^{2\pi i k} & x \in A_k \end{cases}$$

χ_q is what is known as a multiplicative *character* of $\mathbb{F}_p^\times$.

Definition 4.1.1. A *character* χ of a group G with values in a field L is a homomorphism $\chi : G \to L^*$ from G to the multiplicative group of L.

Because $\chi_q(x)$ is a primitive qth root of unity for all nonzero $x \notin A_0$, it follows that for nonzero x we have the equality:

$$\frac{1 + \chi_q(x) + \chi_q(x)^2 + \ldots + \chi_q(x)^{q-1}}{q} = \begin{cases} 1 & x \in A_0 \\ 0 & \text{otherwise} \end{cases}$$

Also note that the correspondence between the maps ψ_q and χ_q given by the isomorphism between the additively and multiplicatively written fields $\mathbb{F}_q$ tells us that for $s \notin K$,

$$\begin{aligned} c_s = 0 = \sum_{k \in K} \psi_q(s-k)\gamma_k \quad &\iff \quad \prod_{k \in K} e^{2\pi i \psi_q(s-k)\gamma_k} = 1 \\ &\iff \quad \prod_{k \in K} \chi_q(s-k)^{\gamma_k} = 1 \\ &\iff \quad \chi_q(f(s)) = 1 \end{aligned}$$

It follows that

$$\frac{1 + \chi_q(f(s)) + \chi_q(f(s))^2 + \cdots + \chi_q(f(s))^{q-1}}{q} = \begin{cases} 1 & c_s = 0 \\ 0 & \text{otherwise} \end{cases}$$

On the other hand, if $s \in K$, suppose $\gamma_s = i \in \mathbb{F}_q^*$. Then look at the ith derivative of f evaluated at s, and find that $\frac{f^{(i)}(s)}{i!} = \prod_{k \in K,\ k \neq s}(s-k)^{\gamma_k}$. By the same logic as above, we find that $c_s = \sum_{k \in K, k \neq s} \psi_q(s-k)\gamma_k = 0 \iff \chi_q(\frac{f^{(i)}(s)}{i!}) = 1$, which allows us to arrive at the following lemma.

Lemma 4.1.1. *If* $a(x) = \sum_{i=1}^{r} \gamma_{k_i} x^{k_i} \in \mathbb{F}_q[x]/(x^p - 1)$ *be a polynomial of weight* r*. Then the weight* $w(\mathbf{c})$ *of the codeword* $c(x) = a(x)E_q(x)$ *is*

$$\begin{aligned} w(\mathbf{c}) &= \frac{(q-1)p}{q} - \frac{1}{q}\left[\sum_{t\in\mathbb{F}_p}(\chi_q(f(t)) + \cdots + \chi_q(f(t))^{q-1}) + \right. \\ &\quad \sum_{t\in K,\gamma_t=1}(\chi_q(f'(t)) + \cdots + \chi_q(f'(t))^{q-1}) + \cdots \\ &\quad \left. + \sum_{t\in K,\gamma_t=q-1}\left(\chi_q(\frac{f^{(q-1)}(t)}{(q-1)!}) + \cdots + \chi_q(\frac{f^{(q-1)}(t)}{(q-1)!})^{q-1}\right)\right]. \end{aligned}$$

where $f(t) = f_a(t) = \prod_{i=1}^{r}(t - k_i)^{\gamma_{k_i}} \in \mathbb{F}_p[t]$ *is the polynomial corresponding to* $a(x)$ *defined at the beginning of the chapter.*

Proof. The weight of our codeword $w(\mathbf{c})$ is

$$\begin{aligned} w(\mathbf{c}) &= p - \{\text{number of places where code is } 0\} \\ &= p - \left[\sum_{s\notin K}\frac{1 + \chi_q(f(s)) + \cdots + \chi_q(f(s))^{q-1}}{q} + \right. \\ &\quad \sum_{s\in K,\gamma_s=1}\frac{1 + \chi_q(f'(s)) + \cdots + \chi_q(f'(s))^{q-1}}{q} + \cdots \\ &\quad \left. + \sum_{s\in K,\gamma_s=q-1}\frac{1 + \chi_q(\frac{f^{(q-1)}(s)}{(q-1)!}) + \cdots + \chi_q(\frac{f^{(q-1)}(s)}{(q-1)!})^{q-1}}{q}\right] \\ &= \frac{(q-1)p}{q} - \frac{1}{q}\left[\sum_{s\in\mathbb{F}_p}(\chi_q(f(s)) + \cdots + \chi_q(f(s))^{q-1}) + \right. \\ &\quad \sum_{s\in K,\gamma_s=1}(\chi_q(f'(s)) + \cdots + \chi_q(f'(s))^{q-1}) + \cdots \\ &\quad \left. + \sum_{s\in K,\gamma_s=q-1}\left(\chi_q(\frac{f^{(q-1)}(s)}{(q-1)!}) + \cdots + \chi_q(\frac{f^{(q-1)}(s)}{(q-1)!})^{q-1}\right)\right] \end{aligned}$$

□

Corollary 4.1.2. *If* $a(x) = \sum_{i=1}^{r} \gamma_{k_i} x^{k_i} \in \mathbb{F}_q[x]/(x^p - 1)$ *is a polynomial of weight* r*, then the weight* $w(\mathbf{c})$ *of the codeword* $\mathbf{c}$ *corresponding to the polynomial* $c(x) = a(x)E_q(x)$ *satisfies:*

$$\frac{q-1}{q}\left[p - (r-1)\sqrt{p} - r\right] \leq w(\mathbf{c}) \leq \frac{q-1}{q}\left[p + (r-1)\sqrt{p} + \frac{r}{q-1}\right]$$

To prove this corollary, we will rely not only on Lemma 4.1.1 but also on the well-known Hasse-Weil bound for exponential sums.

Theorem 4.1.3 (Hasse-Weil Bound)**.** *[12] Let* p *be an odd prime, and let* χ *denote a non-principal multiplicative character modulo* p*. Furthermore, let* $F(x)$ *be a polynomial with integer coefficients of degree* $n \geq 1$*. Then*

$$\left|\sum_{1 \leq i \leq p} \chi(F(i))\right| \leq (n-1)\sqrt{p}$$

unless F *is a* k*th power of another polynomial modulo* p*, where* k *is the order of the character* χ*.*

The proof of this theorem will be omitted here, but we will use the Hasse-Weil bound in the proof of 4.1.2.

Proof of 4.1.2. Consider the polynomial $f(t) = f_a(t) = \prod_{i=1}^{r}(t - k_i)^{\gamma_i} \in \mathbb{F}_p[t]$. The multiplicative character χ_q as defined previously has the property that for any $x \in \mathbb{F}_p$,

$$\chi_q(x) + \cdots + \chi_q(x)^{q-1} = \begin{cases} 0 & x = 0 \\ q-1 & x \text{ is a } q\text{-th power residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

It follows that

$$\begin{aligned} -r &\leq \sum_{s\in K,\gamma_s=1} (\chi_q(f'(s)) + \cdots + \chi_q(f'(s))^{q-1}) + \cdots \\ &\quad + \sum_{s\in K,\gamma_s=q-1} \left(\chi_q(\frac{f^{(q-1)}(s)}{(q-1)!}) + \cdots + \chi_q(\frac{f^{(q-1)}(s)}{(q-1)!})^{q-1} \right) \\ &\leq (q-1)r \end{aligned}$$

Moreover, the Hasse-Weil bound tells us that:

$$\left| \sum_{s\in\mathbb{F}_p} \chi_q(f(s)) + \ldots + \chi_q(f(s))^{q-1} \right| \leq (q-1)(r-1)\sqrt{p}$$

as per Theorem 4.1.3. Using these two facts together with Lemma 4.1.1 gives us the lower bound

$$\frac{(q-1)p}{q} - \frac{1}{q}[(q-1)(r-1)\sqrt{p} + (q-1)r] \leq w(\mathbf{c})$$

and the upper bound

$$w(\mathbf{c}) \leq \frac{(q-1)p}{q} + \frac{1}{q}[(q-1)(r-1)\sqrt{p} + r]$$

or alternatively we may write

$$\frac{q-1}{q}\left[p - (r-1)\sqrt{p} - r\right] \leq w(\mathbf{c}) \leq \frac{q-1}{q}\left[p + (r-1)\sqrt{p} + \frac{r}{q-1}\right].$$

□

4.2 Bounding the weight of the dual code

We now use the lower bound on $w(\mathbf{c})$ found above to find a square root bound on $d_{\min}(\bar{\mathfrak{A}}_0^{\perp})$.

Corollary 4.2.1. *Let* $a(x) = \sum_{i=1}^{r} \gamma_{k_i} x^{k_i}$ *be a non-zero polynomial in* $\mathbb{F}_q[x]/(x^p - 1)$*, and again let* $E_q(x)$ *be the q-idempotent of* $\bar{\mathfrak{A}_0}$*. Then if* $a(x)$ *is in the dual code* $\bar{\mathfrak{A}_0}^{\perp}$ *(that is,* $a(x)E_q(x) = 0$*) then* $r \geq \sqrt{p}$*. In other words,* $d_{\min}(\bar{\mathfrak{A}_0}^{\perp}) \geq \sqrt{p}$*.*

Proof. We have just bounded the weight of the codeword $\mathbf{c}$ corresponding to the polynomial $c(x) = a(x)E_q(x)$ where $a(x)$ has r non-zero coefficients. This can help us find a lower bound for the weight of codewords in the dual code in the following manner.

For small enough r, we will have

$$\frac{q-1}{q}\left[p - (r-1)\sqrt{p} - r\right] > 0$$

which will in turn imply $w(\mathbf{c}) \neq 0$, or that $a(x)$ is NOT an element of the dual code. Which possible weights r for our polynomial $a(x)$ might actually correspond to a codeword in the dual code? To find out, we must figure out the values r for which the above inequality does not true. Solving the inequality $\frac{(q-1)p}{q} - \frac{1}{q}[(q-1)(r-1)\sqrt{p} + (q-1)r] \leq 0$ yields the following series of inequalities:

$$\begin{aligned}
\frac{(q-1)p}{q} &\leq \frac{1}{q}[(q-1)(r-1)\sqrt{p} + (q-1)r] \\
p &\leq (r-1)\sqrt{p} + r \\
p &\leq r(\sqrt{p}+1) - \sqrt{p} \\
\sqrt{p}(\sqrt{p}+1) &\leq r(\sqrt{p}+1) \\
\sqrt{p} &\leq r
\end{aligned}$$

Thus, in order for $a(x)$ to be in the dual code, we must have

$$r \geq \sqrt{p}.$$

It follows that $d_{\min}(\bar{\mathfrak{A}_0}^{\perp}) \geq \sqrt{p}$ and we have the desired lower bound. $\square$

Notice that since the $\bar{\mathfrak{A}_i}^{\perp}$ are isometric, this same bound holds for all i. It is interesting to note that this is the same bound that was found in the case of quadratic residue codes. Thus it seems likely that some improvements to this bound can be made, although it is currently not clear how to proceed with this.

4.3 Using the dual bound to get a lower bound on the minimum distance of the qth power residue code of length p

It turns out that we can use the lower bound found in Section 4.2 for the weight of the dual code to our advantage when trying to find a better lower bound on the minimum distance of the qth power residue codes. As Berlekamp has proved in Theorem 15.22 of [1], we have the lower bound $d_{\min}(\mathfrak{A}_0) \geq \sqrt[q]{p}$ for codewords that are in only the *augmented* qth power residue code of length p but not those codewords that are in both the augmented and expurgated codes; the bound holds for only those codewords in $\mathfrak{A}_0 \setminus \bar{\mathfrak{A}_0}$. The following theorem establishes a lower bound for *all* codewords $\mathbf{c} \in \mathfrak{A}_0$.

As a reminder, let p be a prime, and let q be a qth power residue modulo p. We will obtain the following bound.

Theorem 4.3.1. *Suppose $\mathfrak{a}_0(x)$ is the generator polynomial for $\mathfrak{A}_0$ over $R_{p,q} = \mathbb{F}_q[x]/(x^p - 1)$. Moreover, suppose that $\mathfrak{a}_0(x)$ factors as*

$$\mathfrak{a}_0(x) = c_1(x)c_2(x)\cdots c_m(x), \quad c_i(x) \text{ irreducible.}$$

Then

$$d_{\min}(\bar{\mathfrak{A}_0}) \geq p^{\frac{1}{2(mq-1)}}.$$

It is important to realize that in many cases m is small. In particular, m is non-trivial only when in addition to being a qth power residue, q is also an mth power residue modulo p. That is, m divides $\frac{p-1}{q}$ and there exists some element $y \in \mathbb{F}_p$ with $y^{mq} \equiv q \mod p$. Why this is so will become clear in the proof of the theorem.

The proof of Theorem 4.3.1 requires the following lemma.

Lemma 4.3.2. *Let p be any prime and let $\mathfrak{E} \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set of distinct elements containing zero of size at most $p-2$. Then for any fixed $t \notin \mathfrak{E}$, if we choose r such that $r \neq t$, $r \notin \mathfrak{E}$, then there exists some number $s \in \mathbb{Z}/p\mathbb{Z}$ such that*

$$r \in s + \mathfrak{E}, \quad t \notin s + \mathfrak{E}.$$

That is, we may shift $\mathfrak{E}$ by s modulo p so that the new set $s + \mathfrak{E}$ contains r but not t.

Example 3. Pictorally, we want to show that Figure 3 is always possible. In the figure, we choose $p = 11$, and see that one possible value for s is $s = 3$ for our choice of $\mathfrak{E}$, r, and t.

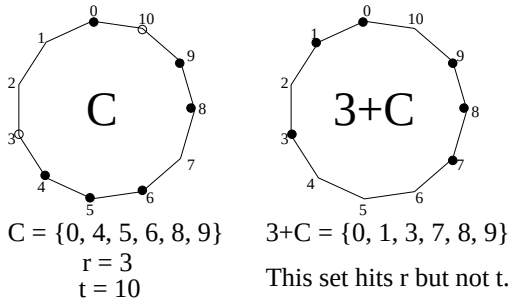

Figure 4.1: Lemma 4.3.2 in action

Proof of Lemma. Let $\mathfrak{E} \subseteq \mathbb{Z}/p\mathbb{Z}$ be as specified above. Fix some $t \notin \mathfrak{E}$. Now, suppose that the theorem above is not true. Then there exists some $r \neq t$ with $r \notin \mathfrak{E}$, such that no matter what s we choose, if $r \in s + \mathfrak{E}$ then $t \in s + \mathfrak{E}$ as well. Let $d = t - r$, the distance (possibly negative) between the two numbers t and r. Now let us look at all the ways we can choose s so that $r \in s + \mathfrak{E}$.

Start out with $s = r$ (We may choose this by the assumption that $0 \in \mathfrak{E}$). It follows that

$$\begin{aligned} t &\in s + \mathfrak{E} = r + \mathfrak{E} \\ &= (t - d) + \mathfrak{E} \end{aligned}$$

That is, $t = t - d + k_1$ for some $k_1 \in \mathfrak{E}$. Therefore, it must be the case that $d = k_1$, hence $d \in \mathfrak{E}$.

Now, let $s = r - d$, where we just determined that $d \in \mathfrak{E}$. Clearly

$r \in s + \mathfrak{E}$, hence by our assumption $t \in s + \mathfrak{E}$. Again we calculate t by:

$$\begin{aligned} t &= s + k_2 = (r - d) + k_2 = [(t - d) - d] + k_2 \\ &= t - 2d + k_2 \end{aligned}$$

Where $k_2 \in \mathfrak{E}$. It follows that $k_2 = 2d \in \mathfrak{E}$. Repeat this process with $s = r - k_2$ to discover that if we set $t = s + k_3$ for some $k_3 \in \mathfrak{E}$, then $k_3 = 3d \in \mathfrak{E}$, and similarly this pattern continues until we have each member of $\{0, d, 2d, 3d, \ldots (p-1)d\}$ in $\mathfrak{E}$.

But now $\{0, d, 2d, 3d, 4d, \ldots, (p-1)d\} = \{0, 1, 2, 3, \ldots, p-1\}$ since $d \neq 0$ and we are working over a field of prime order. That is, continuing this process would give us p *distinct* k_i (including 0) in $\mathfrak{E}$, or in other words

$$|\mathfrak{E}| = p.$$

This is a contradiction of the fact that $t \notin \mathfrak{E}$ and $r \notin \mathfrak{E}$. It follows that for each $r \notin \mathfrak{E}$, there exists some s with the desired properties.

□

Proof of Theorem. Let $B(x) \in \mathfrak{A}_0$ be a nonzero codeword. Then $B(x) = b(x)\mathfrak{a}_0(x)$ for some polynomial $b(x)$, and $\mathfrak{a}_0(x)$ the generator polynomial for the qth power residue code.

But now $\mathfrak{a}_0(x) = c_1(x)c_2(x)\cdots c_m(x)$ implies that $qm \mid (p-1)$, hence there exists some element $\xi \in \mathbb{F}_p$ such that ξ is a primitive mqth root of

unity modulo p; that is, $\xi^{mq} \equiv 1 \mod p$, but $\xi^i \not\equiv 1 \mod p$ for any other $0 < i < mq$. Define a map $\phi : \mathbb{F}_p^* \to \mathbb{Z}/mq\mathbb{Z}$ by

$$\phi(j) = i \quad \text{when} \quad j^{\frac{p-1}{mq}} \equiv \xi^i \mod p.$$

Note that $j^{(p-1)/q} \equiv 1 \mod p$ (those elements $j \in A_0$ that are qth power residues modulo p) if and only if $j^{(p-1)/mq} \equiv \xi^{kq} \mod p$, as then we would find that $j^{(p-1)/q} \equiv (\xi^{kq})^m \equiv 1 \mod p$. Now we choose some $n \in \mathbb{F}_p^*$ such that $\phi(n) = 1$. In other words, $n^{(p-1)/mq} \equiv \xi \mod p$. But then $(n^2)^{(p-1)/mq} \equiv \xi^2$, so $\phi(n^2) = 2$. Similarly, $\phi(n^i) = i$ for $0 \leq i \leq mq-1$. Thus the elements of $\mathbb{F}_p^*$ are divided into mq different sets $I_k = \{j \in \mathbb{F}_p^* \mid j^{(p-1)/mq} \equiv \xi^k \mod p\}$, where we can see that $n^k \in I_k$. We will say that $j \in I_k$ is in the same class as n^k. The elements of $\mathbb{F}_p^*$ that are qth power residues modulo p are exactly those in I_{kq} for all $0 \leq k \leq (m-1)$; $A_0 = \bigcup_{k=0}^{m-1} I_{kq}$. Furthermore, multiplication by n^q maps $I_{kq} \to I_{(k+1)q}$, as $j \in I_{kq}$ implies that $(n^q j)^{(p-1)/mq} \equiv (n^q)^{(p-1)/mq}(j)^{(p-1)/mq} \equiv \xi^q \xi^{kq} = \xi^{(k+1)q}$.

Now note that

$$\begin{aligned}
\mathfrak{a}_0(x) &= \prod_{j \in A_0} (x - \alpha^j) \\
&= \left(\prod_{j \in I_0} (x - \alpha^j)\right)\left(\prod_{j \in I_q} (x - \alpha^j)\right) \cdots \left(\prod_{j \in I_{(m-1)q}} (x - \alpha^j)\right) \\
&\equiv c_1(x) c_1(x^{n^{(m-1)q}}) \cdots c_1(x^{n^q})
\end{aligned}$$

where equivalency is in terms of the resulting code generated, and follows

because the polynomial

$$\prod_{j \in I_q} (x - \alpha^j)$$

has exactly the same roots as the polynomial given by:

$$\prod_{j \in I_0} (x^{n^{(m-1)q}} - \alpha^j), \qquad \left[j \in I_0 \implies \frac{j}{n^{(m-1)q}} \in I_q \right]$$

hence generates the same code by Theorem 3.2.2. Using a similar argument, it follows that

$\prod_{i=1}^{mq} c_1(x^{n^i})$ generates the same code as $\mathfrak{a}_0(x)\mathfrak{a}_0(x^n)\mathfrak{a}_0(x^{n^2}) \cdots \mathfrak{a}_0(x^{n^{q-1}})$.

Notice that this construction proves what we claimed earlier: that if $\mathfrak{a}_0(x)$ has m irreducible factors, then q is also an mth power residue modulo p. Since $\alpha \mapsto \alpha^q$ fixes each of the $\prod_{a \in I_k}(x - \alpha^a)$, it follows that if $n^k \in I_k$ then $qn^k \in I_k$ as well. That is, $k = \phi(n^k) = \phi(qn^k) = \phi(q) + \phi(n^k) = \phi(q) + k$ so that $\phi(q) = 0$.

Going back to our codeword $B(x) = b(x)\mathfrak{a}_0(x)$, suppose that

$$b(x) \in \langle c_1(x^{n^{i_1}}) \rangle \cap \langle c_1(x^{n^{i_2}}) \rangle \cap \cdots \cap \langle c_1(x^{n^{i_k}}) \rangle.$$

We will use $B(x)$ to construct an element in $\bar{\mathfrak{A}_i}^{\perp}$ for some i.

Let $\mathfrak{E} \subseteq \{0, 1, \ldots, mq-1\}$ be the set such that $B(x) \in \langle c_1(x^{n^i}) \rangle$ for all $i \in \mathfrak{E}$ and $B(x) \notin \langle c_1(x^{n^j}) \rangle$ for all $j \notin \mathfrak{E}$. Let $t \notin \mathfrak{E}$. That is, $c_1(x^{n^t}) \not| B(x)$. Then from Lemma 4.3.2 it follows that for each $r \neq t$, there exists some integer s permuting $\mathfrak{E}$ such that $r \in s + \mathfrak{E}$ but $t \notin s + \mathfrak{E}$, where each of these sums is taken modulo p.

Let $\{0, s_1, s_2, \ldots, s_l\}$ be the smallest possible set of integers such that $\{s_i + \mathfrak{E}\}$ hits every $r \neq t$. (Note that we must have $l < mq-1$ [or alternatively, $l \leq mq-2$], since $c_1(x^{n^{k+mq}}) = c_1(x^{n^k \cdot n^{mq}}) = c_1((x^{n^k})^{n^{mq}}) = c_1((x^{n^k})^1) = c_1(x^{n^k})$, so having both k and $k+mq$ in the set of s_i's would be redundant, and since there are only $mq-1$ possible i's, choosing all $mq-1$ of them would mean that we hit $c_1(x^{n^t})$, a contradiction.) We now consider the polynomial

$$B(x)B(x^{n^{s_1}}) \cdots B(x^{n^{s_l}}) \in \mathbb{F}_q[x]/(x^p - 1)$$

which we claim is a nonzero element of $\bar{\mathfrak{A}}_i^{\perp}$ for some i. To see that this is true, suppose that

$$B(x)B(x^{n^{s_1}}) \cdots B(x^{n^{s_l}}) \equiv 0 \mod x^p - 1.$$

Then it would follow that $c_1(x^{n^t}) \mid B(x^{n^{s_i}})$ for some i, hence $B(x) \in \langle c_1(x^{n^{t-s_i}}) \rangle \implies t - s_i \in \mathfrak{E} \implies t \in \mathfrak{E} + s_i$, a contradiction of how we chose the s_i's. Thus this element is nonzero as desired. To see that it is in the dual of some code $\bar{\mathfrak{A}}_i$, note that $c_1(x^{n^r}) \mid B(x)B(x^{n^{s_1}}) \cdots B(x^{n^{s_l}})$ for all $r \neq t$ by construction. Hence this polynomial is in all but one of the codes generated by the polynomials $\mathfrak{a}_0(x), \mathfrak{a}_0(x^n), \ldots, \mathfrak{a}_0(x^{n^{q-1}})$ respectively, so is in $\bar{\mathfrak{A}}_i{}^{\perp}$ for some i as desired.

The following inequality must then be true:

$$\sqrt{p} \leq d_{\min}(\bar{\mathfrak{A}}_i{}^{\perp}) \leq |B(x)B(x^{n^{s_1}}) \cdots B(x^{n^{s_l}})| \leq |B(x)|^{l+1} \leq |B(x)|^{mq-1}$$

and hence

$$|B(x)|^{mq-1} \geq \sqrt{p} \implies |B(x)| \geq p^{\frac{1}{2(mq-1)}}$$

It follows that $d_{\min}(\mathfrak{A}_0) \geq p^{\frac{1}{2(mq-1)}}$ as desired, and in fact because of isometry $d_{\min}(\mathfrak{A}_i) \geq p^{\frac{1}{2(mq-1)}}$ for all $i = 0, \ldots, q-1$.

□

It turns out that it is possible to improve this lower bound if $2 \mid m$. In this case, we have the following theorem.

Theorem 4.3.3. *Suppose $\mathfrak{a}_0(x)$ is the generator polynomial for $\mathfrak{A}_0$ over $R_{p,q} = \mathbb{F}_q[x]/(x^p - 1)$. Moreover, suppose that $\mathfrak{a}_0(x)$ factors as*

$$\mathfrak{a}_0(x) = c_1(x)c_2(x)\cdots c_m(x), \quad c_i(x) \text{ irreducible and } \quad 2 \mid m.$$

Then

$$d_{\min}(\bar{\mathfrak{A}_0}) \geq p^{1/mq}.$$

Proof. Let $B(x)$, n and $\mathfrak{E}$ be as in the proof of Theorem 4.3.1. Note that we still have $x^p - 1 = (x-1)\prod_{i=0}^{mq-1} c_1(x^{n^i})$, but because of the stipulation that $2 \mid m$, we can create two quadratic residue codes generated by $\mathfrak{q}(x) = \prod_{i \in I} c_1(x^{n^i})$ and $\mathfrak{n}(x) = \prod_{i \notin I} c_1(x^{n^i})$, where I is the set integers i modulo mq such that n^i is a quadratic residue modulo p, a set of size $\frac{mq}{2}$.

We now have two possibilities. In the first case, either $\mathfrak{n}(x) \mid B(x)$ or $\mathfrak{q}(x) \mid B(x)$ and it follows that $|B(x)| \geq \sqrt{p}$ by the square root bound that exists for the quadratic residue codes. Otherwise, we may assume that $B(x)$ is divisible by neither of these. Therefore we may choose some t such that $c_1(x^t) \not| B(x)$ and $c_1(x^t) \mid \mathfrak{n}(x)$. Let $\{0, s_1, \ldots, s_\ell\}$ be the smallest set of

integers such that $\{s_i + \mathfrak{E}\}$ hits every $i \in I$ but does not hit t. Then $\ell \leq \frac{mq}{2} - 1$, and it follows that

$$\begin{aligned} \sqrt{p} &\leq d_{\min}(\bar{\mathfrak{A}}_0^{\perp}) \leq \left| \prod_{s \in S} B(x) \right| \\ &= |B(x)|^{\ell+1} \leq |B(x)|^{\frac{mq}{2}}. \end{aligned}$$

It follows that $|B(x)| \geq p^{1/mq}$, and hence

$$d_{\min}(\mathfrak{A}_0) \geq p^{1/mq}$$

as desired. □

4.4 Why we must alter a previous proof technique

When dealing with the binary quadratic residue codes, there was a straightforward proof for the square root bound on the minimum distance as per Theorem 16.1 of [11]. The proof notes that any codeword $c(x)$ of minimum distance d in $\mathcal{Q}$ has a corresponding codeword $\bar{c}(x) = c(x^n), n \in N$ of minimum distance in $\mathcal{N}$. The codeword $c(x)\bar{c}(x)$ is then a codeword in $\mathcal{Q} \cap \mathcal{N}$, making it a multiple of $\mathfrak{a}_0(x)\mathfrak{a}_1(x) = \prod_{j=1}^{p-1}(x - \alpha^j) = \sum_{j=0}^{p-1} x^j$. It follows that $c(x)\bar{c}(x)$ has weight p. Thus

$$d^2 = |c(x)|^2 \geq |c(x)\bar{c}(x)| = p \implies d \geq \sqrt{p},$$

which is the desired bound. But this method only works because it has been shown that the minimum distance of these codes must be odd, hence $(x - 1)$ does not divide the minimum distance codeword. As previously mentioned,

Theorem 15.22 in [1] gives a qth root bound for codewords that are in only the augmented but not the expurgated qth power residue codes, (i.e. those codewords that $(x-1)$ does not divide) proved in much the same way. Ideally, we would like to see this qth root bound hold for all codewords, but the previous proof will not get us there, as qth power residue codes can be constructed in which the minimum distance codewords come from the expurgated code.

Recently, Semyonovykh uses this method in his paper [13] (Proposition 2(4), p. 574) to prove a qth root bound on the minimum distance of *binary* qth power residue codes, a variation of what we have done here, when $q = 3$ and $q = 4$. Unfortunately there appears to be a hole in this proof, which we conjecture would also occur in our qth power residue codes over $\mathbb{F}_q$, which arises because the minimum distance of these binary qth power residue codes is no longer always odd. A codeword of minimum distance may now be a member of the expurgated qth power residue code.

Consider the case where $q = 3$ and let $p = 43$. The set of cubic residues modulo 43 is then

$$A_0 = \{1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42\}$$

A 43rd root of unity α may be found in the field

$$GF(2^{14}) = \mathbb{F}_2[x]/(x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^2 + 1)$$

The polynomial $f(x) = x$ is a generator for this field, hence we may take:

$$\alpha = x^{(2^{14}-1)/43} = x^{12} + x^{10} + x^9 + x^8 + x^7 + x^3.$$

Using this α, we get the code

$$\begin{aligned}\mathfrak{A}_0 &= \langle \prod_{a\in A_0}(x-\alpha^a)\rangle \\ &= \langle x^{14}+x^{12}+x^{10}+x^7+x^4+x^2+1\rangle \subseteq \mathbb{F}_2[x]/(x^{43}-1).\end{aligned}$$

The proof suggests taking a codeword $a(x) \in \mathfrak{A}_0$ of the least weight d, then getting a correspondence to the dual code by $a(x) \leftrightarrow r(x) = a(x)a(x^q)a(x^{q^2})$, where $a(x)a(x^q)a(x^{q^2})$ is supposedly divisible by $\frac{x^p-1}{x-1}$, hence has weight p, which in turn gives a cube root bound on the minimum distance of such cubic residue codes. A problem arises, however: in this case using PARI/GP we can determine that $d_{\min}(\mathfrak{A}_0) = 6$, and find such a minimum weight codeword $a(x) = x^{38}+x^{37}+x^{35}+x^{34}+x^{28}+x \in \mathfrak{A}_0$. Using this polynomial with the suggested map gives us:

$$\begin{aligned}r(x) &= a(x)a(x^3)a(x^9) \\ &\equiv 0 \mod x^{43}-1 \text{ (also using PARI/GP)}\end{aligned}$$

which we can also discover for ourselves, as we know that

$$\prod_{a\in A_0}(x-\alpha^a)\prod_{a\in A_1}(x-\alpha^a)\prod_{a\in A_2}(x-\alpha^a) = \frac{x^{43}-1}{x-1} \mid r(x),$$

and moreover since $d = 6$ is even, $(x-1) \mid r(x)$ as well (the binary codeword $a(x)$ has even weight $\iff a(1) = 0$).

It follows that the conclusion of the proof as it stands gives us the trivial bound $d \geq 0$. Thus, though in this case direct calculation tells us that the bound $d = 6 \geq \sqrt[3]{43}$ still holds, the proof presented does not work in the

general case, although I have not found a counterexample to the cube root bound presented.

4.5 A cubic residue code example

It may now be helpful to the reader to see a simple example of the construction of a qth power residue code. We will use $q = 3$ (a cubic residue code) to keep the example relatively straightforward. It is much harder to come up with cubic residue code examples than quadratic residue codes, as we are now forced to deal with much larger primes. For example, the smallest p for which $3 \mid (p-1)$ that also has 3 as a cubic residue mod p turns out to be $p = 61$, which is the prime that we will be working with. That is, our code will have words of length 61.

Let $p = 61$. Then 2 is a primitive element modulo 61, and from this we can get the primitive cube root of unity $2^{20} \equiv 47 \mod 61$. Using this cube root of unity, we can find $\psi_q(j)$ for all $j \in \mathbb{F}_{61}^*$ and get cosets

$$A_0 = \{1, 3, 8, 9, 11, 20, 23, 24, 27, 28, 33, 34, 37, 38, 41, 50, 52, 53, 58, 60\}$$

$$A_1 = \{2, 5, 6, 7, 13, 15, 16, 18, 21, 22, 39, 40, 43, 45, 46, 48, 54, 55, 56, 59\}$$

and

$$A_2 = \{4, 10, 12, 14, 17, 19, 25, 26, 29, 30, 31, 32, 35, 36, 42, 44, 47, 49, 51, 57\}.$$

In order to find our generator polynomials, we must now find a primitive 61st root of unity in some field extension of $\mathbb{F}_3$. Using GP, we find that $\mathbb{F}_{3^{10}}$ is the

smallest such field extension. Write

$$\mathbb{F}_{3^{10}} = \mathbb{F}_3[x]/(x^{10} + 2x^8 + x^6 + x^5 + x^4 + x^3 + x + 2)$$

In this field, x is a primitive element, and from this we can calculate the primitive 61st root of unity

$$\alpha = x^{(3^{10}-1)/61} = x^9 + 2x^8 + x^7 + 2x^5 + x^4 + 2x^3 + x^2 + 1$$

in this field. Now look at how $x^{61} - 1$ factors over $\mathbb{F}_3$. We have:

$$x^{61} - 1 = (x-1)f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x)$$

(i.e. seven irreducible factors) where

$$\begin{aligned}
f_1(x) &= x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + 1 \\
f_2(x) &= x^{10} + x^8 - x^7 - x^5 - x^3 + x^2 + 1 \\
f_3(x) &= x^{10} - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + 1 \\
f_4(x) &= x^{10} + x^9 - x^8 + x^7 - x^6 - x^5 - x^4 + x^3 + x + 1 \\
f_5(x) &= x^{10} + x^9 - x^8 - x^7 - x^6 - x^4 - x^3 - x^2 + x + 1 \\
f_6(x) &= x^{10} - x^9 + x^8 - x^7 + x^5 - x^3 + x^2 - x + 1.
\end{aligned}$$

We can now calculate the generator polynomials, which turn out to

break apart as follows:

$$\begin{aligned}
\mathfrak{a}_0(t) &= f_4(t)f_5(t) \\
&= t^{20} + 2t^{19} + 2t^{18} + t^{17} + 2t^{16} + t^{14} + 2t^{13} \\
&\quad +2t^{12} + t^{11} + t^9 + 2t^8 + 2t^7 + t^6 + 2t^4 + t^3 + 2t^2 + 2t + 1 \\
\mathfrak{a}_1(t) &= f_1(t)f_2(t) \\
&= t^{20} + t^{18} + t^{16} + t^{15} + t^{14} + 2t^{11} + 2t^{10} \\
&\quad +2t^9 + t^6 + t^5 + t^4 + t^2 + 1 \\
\mathfrak{a}_2(t) &= f_3(t)f_6(t) \\
&= t^{20} + 2t^{19} + t^{17} + 2t^{15} + 2t^{14} + 2t^{13} + t^{12} \\
&\quad +2t^{11} + 2t^{10} + 2t^9 + t^8 + 2t^7 + 2t^6 + 2t^5 + t^3 + 2t + 1.
\end{aligned}$$

Notice that because $\frac{x^{61}-1}{x-1}$ factors into six irreducible factors rather than three, it follows that 3 is not only a cubic residue modulo 61, but 3 is also a quadratic residue modulo 61. That is, there exists a quadratic residue code of length 61 over $\mathbb{F}_3$. We used the existence of such a code to our advantage in Theorem 4.3.3 when proving a better bound on the minimum distance.

Let us now calculate the minimum distance of the cubic residue code generated by the polynomial:

$$\begin{aligned}
(t-1)\mathfrak{a}_0(t) &= t^{21} + t^{20} + 2t^{18} + t^{17} + t^{16} + t^{15} + t^{14} + 2t^{12} + 2t^{11} \\
&\quad +t^{10} + t^9 + 2t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + 2t + 2
\end{aligned}$$

In order to do this, we used the following Magma code:

```
P<x> := PolynomialRing(FiniteField(3));
F := Factorization(x^61 - 1);
H := CyclicCode(61, F[1][1]*F[5][1]*F[6][1]);
SetVerbose(‘‘Code’’,true);
MinimumWeight(H);
```

From this I determined that the minimum weight of the extended Cubic Residue Code of length 61 is $d = 10$. Note here that the lower bound predicted by Theorem 4.3.3 for this code is

$$d_{\min}(\mathfrak{A}_0) \geq p^{\frac{1}{2 \cdot 3}} = \sqrt[6]{p} \approx 1.984,$$

which is much smaller than the actual minimum distance. Thus it seems possible that a better bound exists, though a better one is not currently known.

Looking at a couple more examples, however, we can conclude a few things about the lower bound on these qth power residue codes in general. Specifically the square root bound that is commonly accepted for the quadratic residue codes no longer holds here, even for relatively small primes q. See Appendix A for a table of some of these examples.

For example, let $q = 5$ and $p = 31$. If the square root bound held here, we would have $d_{\min} \geq \sqrt{31}$, or rounding up to the nearest integer, $d_{\min} \geq 6$. Performing the computations in Magma, in a manner similar to the above, gives the minimum weight of this 5th power residue code as less than or equal to 4, certainly below this square root bound.

Chapter 5

A family of asymptotically bad q-residue codes

5.1 An overview of algebraic number theory

In what follows we will construct an asymptotically bad family of qth power residue codes, a construction which will rely heavily on ideas found in algebraic number theory. Thus a brief overview of the relevant topics will be given here.

Let F be a number field, and K/F a finite extension. Denote the *ring of algebraic integers of* F by $\mathcal{O}_F := \{y \in F \mid y \text{ is a solution to a monic polynomial } f \in \mathbb{Z}[x]\}$, and similarly for the extension K/F. Then if $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_F$, we may look at its unique factorization in $\mathcal{O}_K$ as

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_j^{e_j}.$$

The positive integer e_i is called the *ramification index* for $\mathfrak{P}_\mathrm{i}/\mathfrak{p}$, and $\mathfrak{p}$ is said to be *ramified* in K if one of the $e_i \neq 1$. We say that $\mathfrak{p}$ *splits completely* in K if $[K : F] = j$. This implies that $e_i = 1$ for all i (i.e. $\mathfrak{p}$ is unramified in K) and $\mathcal{O}_K/\mathfrak{P}_i = \mathcal{O}_F/\mathfrak{p}$.

Example 4. Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(i)$, a degree 2 extension of F. Then $\mathcal{O}_F = \mathbb{Z}$, and $\mathcal{O}_K = \mathbb{Z}[i]$, as i is the solution to the monic polynomial $f =$

$x^2 + 1$. Consider the prime ideal $\mathfrak{p} = \langle 13 \rangle$ of $\mathcal{O}_F$. Then over $\mathcal{O}_K$, $\mathfrak{p}$ factors as $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$, where $\mathfrak{P}_1 = \langle 2 + 3i \rangle$ and $\mathfrak{P}_2 = \langle 2 - 3i \rangle$ are both prime ideals in $\mathcal{O}_K$. We say that $\mathfrak{p}$ splits completely in K, and is unramified in K.

The interested reader may wish to refer to [8] for a more comprehensive overview of this topic.

5.2 The Chebotarev density theorem

In addition to class field theory, the construction of an asymptotically bad family of qth power residue codes relies on an applicaton of the Chebotarev density theorem. Specifically, we will use this theorem in bounding the smallest prime p that splits in some field K. For an overview of the theorem itself, see [5]. The bounds of [10] and [9] use Chebotarev's theorem to estimate this prime p in terms of the discriminant D of K; their results in this area will play an important role in the construction of our family.

5.3 What we are looking for

In the following, we will be constructing an asymptotically bad family of qth power residue codes. That is, we construct a sequence of qth power residue codes with lengths p_i, p_i tending towards infinity, with the property that $\lim_{i\to\infty} \frac{d_{p_i}}{p_i} = 0$, where d_{p_i} is the minimum distance of the code of length p_i. Note that when we first defined the qth power residue codes we saw that they had dimension given by $\frac{q-1}{q} + \frac{1}{pq}$. It follows that if r_{p_i} is the dimension

of the qth power residue code of length p_i, then $\lim_{i\to\infty} \frac{r_{p_i}}{p_i} = \frac{q-1}{q}$ for *any* sequence of p_i's which tends toward infinity. Thus the transmission rate of these codes is actually asymptotically *good*, even though the family of codes we construct is asymptotically *bad* because it violates the second criterion for an asymptotically good family.

5.4 Constructing the family

In the following construction we will follow the argument of [17] closely, in which Voloch constructs a similar asymptotically bad family of the binary quadratic residue codes.

Theorem 5.4.1. *For infinitely many primes p, the minimum distance d_p of the qth power residue code of length p over $\mathbb{F}_q$ is $O(p/\log\log p)$. If furthermore the generalised Riemann hypothesis is true, then the bound can be improved to $O(p/\log p)$.*

Proof. Let ℓ be an odd prime, ζ a primitive complex ℓth root of unity and K the extension of the rational number field obtained by adjoining ζ, $\sqrt[q]{q}$, $\sqrt[q]{1}$, and $\sqrt[q]{\zeta^m - 1}$ for all $m = 1, \ldots, \ell - 1$. This ensures that $\zeta^m - 1$ and q are qth powers in K, which we will need to construct our code.

Let p be a prime that splits completely in K. Then $\ell \mid (p-1)$ and $q \mid (p-1)$, hence we can form a qth power residue code of length p with some minimum weight d_p.

Claim 2. $d_p \leq \frac{(q-1)(p-1)}{q\ell}$.

Proof of Claim. To prove this claim, we will construct a codeword of the desired weight. Let $f(t) = t^{(p-1)/\ell} - 1 = \prod_{i=1}^{(p-1)/\ell}(t - m_i)^{\gamma_i} \in \mathbb{F}_p[t]$ for some set $M = \{m_1, \ldots, m_{(p-1)/\ell}\}$. Then $f(t)$ has all of its roots in $\mathbb{F}_p$, hence we may use it to construct a codeword $\mathbf{c}$ as in Lemma 4.1.1. By the way we constructed our field, $f(s)$ is a qth power for all $s \in \mathbb{F}_p$ since $s^{(p-1)/\ell}$ is an ℓth root of unity for $s \in \mathbb{F}_p^*$. Hence when $s \in \mathbb{F}_p$, we have

$$\chi_q(f(s)) = \begin{cases} 1 & s \text{ not a root of } f \\ 0 & s \text{ a root of } f \end{cases},$$

where $\chi_q(x)$ is the character introduced in Chapter 4. Moreover, note that the elements of M form a (cyclic) subgroup G of index ℓ in $\mathbb{F}_p$, and that for every $s \in G$ we have $f'(s) = \frac{(p-1)}{\ell}s^{(p-1)/l-1} = \frac{(p-1)}{\ell s}$, since $s^{(p-1)/\ell} = 1$ for all $s \in G$. We now go back to Lemma 4.1.1 to see that

$$\begin{aligned} w(\mathbf{c}) &= \frac{(q-1)p}{q} - \frac{1}{q}\left[\sum_{s\in\mathbb{F}_p}(\chi_q(f(s)) + \cdots + \chi_q(f(s))^{q-1}) \right. \\ &\quad + \sum_{s\in M,\gamma_s=1}(\chi_q(f'(s)) + \cdots + \chi_q(f'(s))^{q-1}) + \cdots \\ &\quad \left. + \sum_{s\in M,\gamma_s=q-1}\left(\chi_q(\frac{f^{(q-1)}(s)}{(q-1)!}) + \cdots + \chi_q(\frac{f^{(q-1)}(s)}{(q-1)!})^{q-1}\right)\right]. \\ &= \frac{(q-1)p}{q} - \frac{1}{q}\left[(q-1)\cdot(p - \frac{(p-1)}{\ell}) + 0 + \cdots + 0\right] \\ &= \frac{(q-1)(p-1)}{q\ell} \end{aligned}$$

where every sum after the first two is zero by virtue of the fact that the polynomial $f(t)$ has no repeated roots, and $\sum_{s\in M,\gamma_s=1}(\chi_q(f'(s)) + \cdots + \chi_q(f'(s))^{q-1}) =$

$\sum_{s\in G}(\chi_q(f'(s)) + \cdots + \chi_q(f'(s))^{q-1}) = 0$ since G is a group. $\square$

To complete the theorem we vary ℓ, choosing for each ℓ the smallest prime p that splits completely in the field K corresponding to ℓ. Let D be the discriminant of K. From the estimates of [10] and [9] we may bound p in terms of D. In particular, we conclude that $\log p \ll \log D$ and under the generalized Riemann hypothesis, $p \ll (\log D)^2$. To prove our theorem we want to estimate D in terms of ℓ. In order to do this, note that the only primes that ramify in K are q and ℓ. We now use Hensel's bound on the discriminant (see [14] remark 1 after Proposition III.13), which tells us that the contribution of a ramified prime to the discriminant has exponent at most $n(n+1)$, where n is the absolute degree of K. Hence $D \leq (ql)^{n(n+1)}$. Estimating n, it is clear from looking at how we defined the field K that $n \leq (\ell-1)\cdot q^{\ell+1}$. Plugging this back in for D, we may conclude that

$$\begin{aligned}
\log p &\ll \log D \\
&\leq \log(q\ell)^{(\ell-1)q^{\ell+1}[(\ell-1)q^{\ell+1}+1]} \\
&\ll [(\ell-1)q^{\ell+1}]^2 \log q\ell
\end{aligned}$$

It follows that

$$\begin{aligned}
\log\log p &\ll 2(\ell+1)\log q + 2\log(\ell+1) + \log\log q\ell \\
&\ll \ell \log q \ll \ell
\end{aligned}$$

since q remains constant for any given family of qth power residue codes.

Finally, note that we have

$$\begin{aligned} d_p &\leq w(\mathbf{c}) \leq \frac{(q-1)(p-1)}{q\ell} \\ &\ll \frac{(q-1)(p-1)}{q\log\log p} \ll \frac{p}{\log\log p}. \end{aligned}$$

which is what we desired. A similar argument also gives us the desired result when the generalised Riemann hypothesis is assumed to be true.

To see that we have found our asymptotically bad family of qth power residue codes for any given q, we note that $\lim_{\ell\to\infty} \frac{d_p}{p} \ll \lim_{\ell\to\infty} \frac{p}{\log\log p}/p = \lim_{\ell\to\infty} \frac{1}{\log\log p} = 0$, since p is the length of the code constructed using the prime ℓ, and tends to infinity as ℓ approaches infinity. Hence we have found an asymptotically bad family of qth power residue codes, as desired.

□

Chapter 6

Conclusion

In this thesis, we have defined a new family of codes, the qth power residue codes, found a lower bound on their minimal distance, and proved that there exists an asymptotically bad subfamily of these codes for every prime q. While the discovery of such a subfamily does not seem to bode well, I am optimistic that the lower bound found for these codes can be substantially improved. I would like to see the bound $d_{\min} \geq \sqrt[q]{p}$, which would correspond to the square root bound for the quadratic residue codes. I currently have no reason to believe that this bound does not hold, and am quite optimistic that it does.

Ideally, we would like to be able to find an asymptotically good family of these qth power residue codes. The construction of such a family seems very difficult, if not impossible; for many years coding theorists have struggled to find a better bound for the quadratic residue codes, but have only succeeded on slight improvements to the square root bound, a conclusion that would seem to imply that any family of quadratic residue codes of increasing lengths would have asymptotic minimum distance approaching zero. Finding an asymptotically good subfamily would therefore be tantamount to proving

this better bound.

Eventually, I would not only like to work on improving the current lower bound on the qth power residue codes, but also develop reliable method for decoding them. Finding the automorphism group that fixes these codes would also be a worthwhile goal, as it could help us find out even more about their properties and potential usefulness in the world of coding theory.

Appendix

Appendix 1

Table of minimum weights for qth power residue codes

$q = 3$				
p	Factors of $\mathfrak{a}_0(x)$	Calculated $d_{\min}$	Singleton Bound	Bound from Theorem 4.3.1
61	6	10	21	2
67	3	10	23	3
73	6	10	25	2
103	3	9-14	35	4
151	3	9-17	51	4
$q = 5$				
31	10	3-4	7	2
191	10	7-17	39	2
$q = 7$				
43	7	4	7	2
281	14	5-22	41	2
$q = 13$				
157	26	5-6	14	2
443	26	4-22	35	2

Table 1.1: Table of minimum distances for selected qth power residue codes

Bibliography

[1] E. Berlekamp. *Algebraic Coding Theory.* McGraw-Hill, 1968.

[2] R. Chapman. Higher power residue codes. *Finite Fields and Applications*, 3(4):353–369, 1997.

[3] P. Charters. Finding an asymptotically bad family of q-th power residue codes. *Advances in Mathematics of Communications*, 3(1):53–58, 2009.

[4] P. Charters. Generalizing binary quadratic residue codes to higher power residues over larger fields. *Finite Fields and Their Applications*, 15:404–413, 2009.

[5] Jr. H. W. Lenstra and P. Stevenhagen. Chebotarev and his density theorem. *The Mathematics Intelligencer*, 18(2):26–37, 1996.

[6] T. Helleseth. Legendre sums and codes related to qr codes. *Discrete Applied Mathematics*, 35:107–113, 1992.

[7] T. Helleseth and J.F. Voloch. Double circulant quadratic residue codes. *IEEE Trans. Inform. Theory*, 50(9):2154–2155, 2005.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, 1982.

[9] J.L. Montgomeray J.C. Lagarias and A.M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54:271–296, 1979.

[10] J.C. Lagarias and A.M. Odlyzko. Effective versions of the Chebotarev density theorem. *Algebraic Number Fields*, pages 409–464, 1997.

[11] J. MacWilliams and N. Sloane. *The theory of error-correcting codes*. North-Holland, 1977.

[12] P. Roquette. Exponential sums: the estimate of Hasse-Davenport-Weil. *An introductory course, following the 1934 papers of Hasse and Davenport. Notes from Escola de Algebra, Rio de Janiero*, 1996.

[13] D.N. Semyonovykh. A generalization of quadratic residue codes to the case of cubic and biquadratic residues. *Discrete Math Appl.*, 15(6):573–580, 2005.

[14] J.P. Serre. *Local Fields*. Springer, 1979.

[15] J.H. vanLint and F.J. MacWilliams. Generalized quadratic residue codes. *IEEE Trans. on Inform. Theory*, IT-24(6), 1978.

[16] A. Vardy. Algorithmic complexity in coding theory and the minimum distance problem. *Annual ACM Symposium on Theory of Computing, Proceeding of the twenty-ninth annual ACM Symposium on Theory*, pages 92–109, 1997.

[17] J.F. Voloch. Asymptotics of the minimal distance of quadratic residue codes. *Finite fields: theory and applications. Abstracts from the workshop held December 5-11, 2004. Organized by Joachim vo zur Gathen, Igor E. Shparlinski and Henning Stichtenoth. Oberwolfach Rep. 1*, (4):2946–2947, 2004.

Index

Vita

Philippa Liana Charters was born in Hazelwood, Missouri on 17 February 1981, the daughter of Dr. Duncan Charters and Patricia M. Charters. She received the Bachelor of Arts degree in Mathematics and Computer Science from Williams College in May of 2003, when she applied and was accepted into the mathemaics PhD program at the University of Texas at Austin. She started graduate studies in September of 2003.

Permanent address: 4408 Avenue A Apt. B
Austin, Texas 78751

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.