FAMILIES OF CYCLIC CODES OVER FINITE CHAIN RINGS

An Undergraduate Research Scholars Thesis

by

ANDREW SCHMIDT NEMEC

Submitted to the Undergraduate Research Scholars program
Texas A&M University
in partial fulfillment of the requirements for the designation as an

UNDERGRADUATE RESEARCH SCHOLAR

Approved by
Research Advisor: Dr. Andreas Klappenecker

May 2016

Major: Computer Engineering
Mathematics

TABLE OF CONTENTS

ABSTRACT

Families of Cyclic Codes over Finite Chain Rings

Andrew Schmidt Nemec
Department of Computer Science and Engineering
Department of Mathematics
Texas A&M University

Research Advisor: Dr. Andreas Klappenecker
Department of Computer Science and Engineering

A major difficulty in quantum computation and communication is preventing and correcting errors in the quantum bits. Most of the research in this area has focused on stabilizer codes derived from self-orthogonal cyclic error-correcting codes over finite fields. Our goal is to develop a similar theory for self-orthogonal cyclic codes over the class of finite chain rings which have been proven to also produce stabilizer codes. We also will discuss these restrictions on families of cyclic codes, including, but not limited to quadratic residue codes and Bose-Chaudhuri-Hocquenghem codes. Finally, we will extend the concepts of weight enumerators to the class of Frobenius rings and use them to derive bounds for our codes.

CHAPTER I

INTRODUCTION

Unlike in classical computing where there is only one type of error, the bit-flip, quantum computing must deal with an infinite number of possible errors while also being more susceptible to them. One approach to solving this problem is to use quantum error-correcting codes, of which the stabilizer codes are the most popular, as they can be derived from self-orthogonal classical cyclic codes. The stabilizer codes were generalized from the binary field case to finite fields in [13, 14], and then further generalized to Frobenius rings in [17]. Codes over Frobenius rings are especially interesting, as the arithmetic over them is often much simpler than over finite fields, which is extremely important when designing systems that must constantly perform these error-correcting calculations.

In this thesis, we investigate classical cyclic codes over finite chain rings, a subclass of the Frobenius rings, and the stabilizer codes that are derived from them. Additionally, we give some conditions for self-orthogonal quadratic residue codes and Bode-Chaudhuri-Hocquenghem (BCH) codes and develop some symplectic weight enumerators over Frobenius rings and the bounds derived from them.

Frobenius and finite chain rings

Let R be a finite ring of order n. A character of the additive group $(R,+)$ of R is a homomorphism $\chi : (R,+) \to \mathbb{C}^*$, and the values of χ are the n^{th} roots of unity [2]. Denote the set of irreducible character of $(R,+)$ by $\mathrm{Irr}(R)$. An irreducible character χ of $(R,+)$ is called generating if and only if $\mathrm{Irr}(R) = \{\chi_b | b \in R\}$, where $\chi_b(x) = \chi(bx)$. A ring that admits a left or right generating character is called a Frobenius ring. One special subclass of the Frobenius rings are the finite chain rings, which are local rings with the additional constraint that the lattice of its left ideals (equivalently, right ideals) form a chain under set inclusion [17].

For a ring R, the Jacobson radical $J(R)$ is the instersection of all maximal left ideals (equivalently, the intersection of all maximal right ideals). If R is a finite chain ring, this means that $J(R) = \mathfrak{M}$, where $\mathfrak{M}$ is the unique maximal ideal of R. The nilpotency index of $J(R)$ is the smallest positive integer ν such that $J^{\nu}(R) = \{0\}$. If the residue field $R/J(R)$ has q elements, then $|R| = q^{\nu}$ [17].

Error bases and stabilizer codes

Let R be a finite ring with q elements. Let $\{|x\rangle\,|x \in R\}$ be an orthonormal basis of $\mathbb{C}^q$. For $a, b \in R$ define a shift operator $X(a) : \mathbb{C}^q \to \mathbb{C}^q$ and a multiplication operator $Z(b)\mathbb{C}^q \to \mathbb{C}^q$ by $X(a)|x\rangle = |x+a\rangle, \quad Z(b)|x\rangle = \chi(bx)|x\rangle$, where χ is an irreducible character of the additive group $(R,+)$. Define the set of error operators $\mathscr{E} = \{X(a)Z(b)\,|a, b \in R^n\}$. If R is a Frobenius ring with generating character χ, then $\mathscr{E}$ is a nice error basis on $\mathbb{C}^{q^n}$, that is a) it contains the identity matrix, b) the product of two matrices in $\mathscr{E}$ is a new scalar multiple of another element in $\mathscr{E}$, and c) the trace $\mathrm{Tr}\left(A^{\dagger}B\right) = 0$ for distinct $A, B \in \mathscr{E}$. Define the error group G_n as $G_n = \{\omega^c X(a)Z(b)\,|a, b \in R^n, c \in \mathbb{Z}\}$, where ω is a primitive m^{th} root of unity, $\omega = \exp(2\pi i/m)$, and m is the exponent of the additive group of R (the characteristic of R).

Let S be a subgroup of G_n. There is a stabilizer code $\mathrm{Fix}(S)$ associated with the subgroup S, given by $\mathrm{Fix}(S) = \left\{v \in \mathbb{C}^{q^n} | Ev = v, \forall E \in S\right\}$.

Structure of cyclic codes

Cyclic codes over fields are defined as a principle ideal of the ring $F_q[x]/\langle x^n - 1\rangle$. Over the field, $x^n - 1$ factors into two important polynomials, the generator polynomial $g(x)$ and the check polynomial $h(x) = (x^n - 1)/g(x)$. The generator and check polynomials themselves are products of basic irreducible factors of $x^n - 1$ The code consists of a single generating element $g(x)$ and all shifts of $g(x)$, shown as $x^m g(x)$ for all $1 \leq m < n$ where n is the degree of the polynomial.

Let R be a commutative finite chain ring with residue field $\overline{R}$ and denote by $- : R[x] \to \overline{R}[x]$ the natural projection from $R[x]$ onto $\overline{R}[x]$.

Lemma 1. *(Hensel's Lemma, [7, Theorem 2.4]) Let f be a polynomial over R and assume $\overline{f} = g_1 g_2 \cdots g_r$ are pairwise coprime polynomials over $\overline{R}$. Then there exist pairwise coprime polyniomials $f_1, f_2, \ldots, f_r$ over R such that $f = f_1 f_2 \cdots f_r$ and $\overline{f_i} = g_i$ for $i = 1, 2, \ldots, r$.*

CHAPTER II

QUADRATIC RESIDUE CODES

Let R be a commutative finite chain ring with maximal ideal $J(R)$ and residue field $\mathbb{F}_q = R/J(R)$. Denote by $-$ the natural projection $R[x] \to \mathbb{F}_q[x]$. Let n be an odd prime coprime to q, and let α denote a primitive nth root of unity in some extension field of $\mathbb{F}_q$. Denote by

$$Q = \left\{ r^2 \pmod{n} \,|\, r \in \mathbb{Z}, 1 \leq r \leq (n-1)/2 \right\}$$

the set of quadratic residues modulo n and by

$$N = \{1, \ldots, n-1\} \setminus Q$$

the set of quadratic non-residues modulo n. Let

$$f_Q(x) = \prod_{r \in Q} (x - \alpha^r) \text{ and } f_N(x) = \prod_{r \in N} (x - \alpha^r).$$

Then $x^n - 1 = (x-1) f_Q(x) f_N(x) \in \mathbb{F}_q[x]$. By Hensel's lemma [7, Theorem 2.4], there exist monic polynomials $(x-a)$, $q_Q(x)$, $q_N(x) \in R[x]$ that are pairwise coprime and satisfying $(x - \overline{a}) = (x-1)$, $\overline{q_Q}(x) = f_Q(x)$, $\overline{q_N}(x) = f_N(x)$, and $x^n - 1 = (x-a) q_Q(x) q_N(x) \in R[x]$. Substituting 1 into the equation, we obtain $(1-a) q_Q(1) q_N(1) = 0$; since $\overline{q_Q}(1) = f_Q(1) \neq 0$ and $\overline{q_N}(1) = f_N(1) \neq 0$, $q_Q(1)$ and $q_N(1)$ are both invertible elements of R, therefore $a = 1$ and $x^n - 1 = (x-1) q_Q(x) q_N(x) \in R[x]$.

We say that a codeword $x = x_1 x_2 \cdots c_n \in R^n$is even-like if $\sum_{i=1}^n x_i = 0$ and is odd-like otherwise. We say that a code is even-like if it has only even-like codewords and that it is odd-like if it is not even-like.

The quadratic residue codes C_Q, C'_Q, C_N, C'_N are the cyclic codes generated by $q_Q(x)$, $(x-1) q_Q(x)$, $q_N(x)$, $(x-1) q_N(x)$ respectively. C_Q and C_N have parameters $[n, (n+1)/2, d]_R$, and C'_Q and C'_N, the even-like subcodes of C_Q and C_N respectively, have parameters $[n,(n-1)/2,d']_R$, with $d' \geq d$.

Square root bound

Denote by R_n the ring $R[x]/\langle x^n-1\rangle$. The cyclic complement C^C of a cyclic code C is a code satisfying $C^C+C=R_n$, $C^C\cap C=\{0\}$, and C^C is cyclic.

Theorem 2. *Let C be a cyclic code of length n over R with generator polynomial $g(x)$ and generating idempotent $e(x)$. Let C^C be the cyclic complement of C. Then C^C has generator polynomial $\widehat{g}(x)=(x^n-1)/g(x)$ and generating idempotent $1-e(x)$.*

Proof. Since $\widehat{g}(x)$ is a divisor of x^n-1, $\langle\widehat{g}(x)\rangle$ is cyclic. Since $g(x)$ and $\widehat{g}(x)$ are coprime, $\langle g(x)\rangle+\langle\widehat{g}(x)\rangle=R[x]$, therefore $\langle g(x)\rangle+\langle\widehat{g}(x)\rangle=R_n$. Additionally, since they are coprime we also have that $\langle g(x)\rangle\cap\langle\widehat{g}(x)\rangle=\{0\}$, therefore $\langle\widehat{g}(x)\rangle=C^C$.

Let $1=e_1(x)+e_2(x)$, where $e_1(x)\in\langle g(x)\rangle$ and $e_2(x)\in\langle\widehat{g}(x)\rangle$. Then there exist $a(x),b(x)\in R_n$ such that $e_1(x)=a(x)g(x)$ and $e_2(x)=b(x)\widehat{g}(x)$. Then $e_1(x)^2=e_1(x)(1-e_2(x))=e_1(x)-e_1(x)e_2(x)=e_1(x)-a(x)g(x)b(x)\widehat{g}(x)=e_1(x)$, so $e_1(x)$ is an idempotent of C, thus $e_1(x)=e(x)$. Similarly, $e_2(x)^2=(1-e(x))^2=1-e(x)$ is the idempotent of C^C. □

Lemma 3. *Let $h(x)=\frac{1}{n}\left(1+x+x^2+\cdots+x^{n-1}\right)$, $a(x)=\sum_{i=0}^{n-1}a_ix^i\in R_n$, and C a cyclic subcode of R_n with generating polynomial $g(x)$. Then*

1. *$h(x)$ is the generating idempotent of the repetition code of length n over R*
2. *$a(x)$ is even-like if and only if $a(1)=0$ if and only if $a(x)h(x)=0$*
3. *$a(x)$ is odd-like if and only if $a(1)\neq 0$ if and only if $a(x)h(x)=\alpha h(x)$, $\alpha\neq 0$*

Proof. Expanding $(h(x))^2$, we find that

$$\left(\frac{1}{n}\left(1+x+\cdots+x^{n-1}\right)\right)^2=\frac{1}{n}\left(1+x+\cdots+x^{n-1}\right),$$

so $h(x)$ is an idempotent of R_n. Additionally, the codewords of the repetition code are all of the form $f(x) = a\left(1+x+x^2+\cdots+x^{n-1}\right)$ for $a \in R$, so $f(x)h(x) = \frac{a}{n}\left(1+x+x^2+\cdots+x^{n-1}\right)^2 = a\left(1+x+x^2+\cdots+x^{n-1}\right) = f(x)$, so $h(x)$ is the generating idempotent for the repetition code of length n over R. If $a(x) = \sum_{i=0}^{n-1} a_i x^i$ is in R_n, then

$$a(x)h(x) = \left(\sum_{i=0}^{n-1} a_i\right)\frac{1}{n}\left(1+x+x^2+\cdots+x^{n-1}\right),$$

so if $a(x)$ is even-like, $\sum_{i=0}^{n-1} a_i = 0$, so $a(x)h(x) = 0$; additionally, $a(x)$ is even-like precisely when $\sum_{i=0}^{n-1} a_i = 0$. This is the same as saying that $a(1) = 0$. If $a(x)$ is odd-like, $\sum_{i=0}^{n-1} a_i \neq 0$, then $a(x)h(x) = \alpha h(x)$, for some $\alpha \in R$, $\alpha \neq 0$, which is also the same as saying $a(1) \neq 0$. □

Lemma 4. *Let $\mathscr{E}_n$ denote the collection of even-like codewords in R_n. Then:*

1. *$\mathscr{E}_n$ is an $[n, n-1]$ cyclic subcode of R_n*
2. *$\mathscr{E}_n^{\perp}$ is the repetition code with generating idempotent $h(x) = \frac{1}{n}\left(1+x+x^2+\cdots+x^{n-1}\right)$*
3. *$\mathscr{E}_n$ has generating idempotent $1 - h(x)$*

Proof. Let $x, y \in \mathscr{E}_n$ and $a, b \in R$. Since $a\sum_{i=1}^{n} x_i = 0$ and $b\sum_{i=1}^{n} y_i = 0$, we have $\sum_{i=1}^{n}(ax_i + by_i) = 0$, so $(ax+by) \in \mathscr{E}_n$, and therefore $\mathscr{E}_n$ is a subcode of R_n, and must therefore be cyclic. Since R_n can be partitioned into $|R|$ equally sized partitions based on the parity of the codewords, $\mathscr{E}_n$ is an $[n, n-1]$ subcode of R_n, giving (1). Since $\mathscr{E}_n$ is an $[n, n-1]$ cyclic code, $\mathscr{E}_n^{\perp}$ must be an $[n, 1]$ cyclic code, so $\mathscr{E}_n^{\perp}$ is the repetition code. By Lemma 3, the repetition code has generating idempotent $h(x) = \frac{1}{n}\left(1+x+x^2+\cdots+x^{n-1}\right)$. Finally by [22, Theorem 2], $\mathscr{E}_n$ has generating idempotent $1 - h(x)\mu_{-1} = 1 - h(x)$. □

Define the function $\mu_a : \mathbb{Z}_n \to \mathbb{Z}_n$, where a and n are coprime, by $\mu_a(i) = ia \pmod{n}$. This function is known as a multiplier. The multiplier can also act on polynomials by $\mu_a : R_n \to R_n,\ f(x) \mapsto f(x^a)$.

Theorem 5. *Let $f(x), g(x) \in R_n$, $e(x)$ be an idempotent of R_n, and a be an integer coprime to n. Then:*

1. *if $b \equiv a \pmod{n}$, then $\mu_b = \mu_a$*

2. *μ_a is an automorphism of R_n*

3. *$e(x)\mu_a$ is an idempotent of R_n.*

Proof. All of the results follow from straightforward calculations. □

Theorem 6. *Let C be a cyclic code of length n over R with generating idempotent $e(x)$, and let a be an integer coprime to n. Then $C\mu_a = \langle e(x)\mu_a\rangle$ and $e(x)\mu_a$ is the generating idempotent of the cyclic code $C\mu_a$.*

Proof. Using Theorem 5,

$$\begin{aligned} C\mu_a &= \{(e(x)f(x))\mu_a | f(x) \in R_n\} \\ &= \{e(x)\mu_a f(x)\mu_a | f(x) \in R_n\} \\ &= \{e(x)\mu_a h(x) | h(x) \in R_n\} \\ &= \langle e(x)\mu_a\rangle \end{aligned}$$

as μ_a is an automorphism of R_n by Theorem 5. Hence $C\mu_a$ is cyclic and has generating idempotent $e(x)\mu_a$ by Theorem 5. □

Let $e_1(x)$ and $e_2(x)$ be two even-like idempotents with $C_1 = \langle e_1(x)\rangle$ and $C_2 = \langle e_1(x)\rangle$. The codes C_1 and C_2 form a pair of even-like duadic codes if

1. the idempotents satisfy

$$e_1(x) + e_2(x) = 1 - h(x) \tag{II.1}$$

2. there is a multiplier μ_a such that

$$C_1\mu_a = C_2 \text{ and } C_2\mu_a = C_1. \tag{II.2}$$

By Theorem 6, we have that $e_1(x)\mu_a = e_2(x)$ and $e_2(x)\mu_a = e_1(x)$ if and only if $C_1\mu_a = C_2$ and $C_2\mu_a = C_1$, so we can replace equation (II.2) by

$$e_1(x)\mu_a = e_2(x) \text{ and } e_2(x)\mu_a = e_1(x). \tag{II.3}$$

Associated to the pair of even-like duadic codes is the pair of odd-like duadic codes

$$D_1 = \langle 1 - e_2(x) \rangle \text{ and } D_2 = \langle 1 - e_1(x) \rangle. \tag{II.4}$$

Lemma 7. *Let C be a cyclic code over R with generating idempotent $i(x)$ and let C_e be the subcode of all even-like codewords in C. If $C \neq C_e$, then $i(x) - h(x)$ is the generating idempotent of C_e.*

Proof. Since C_e is the even-like subcode of C, $C_e = C \cap \mathscr{E}_n$. By [22, Theorem 1], the generating idempotent of C_e is $i(x)(1 - h(x)) = i(x) - i(x)h(x)$. Since $i(x)$ is the generating idempotent of C, but not the generating idempotent of C_e it is necessarily odd-like, so by Lemma 3 $i(x) - i(x)h(x) = i(x) - \alpha h(x)$, where $\alpha = \sum_{k=0}^{n-1} i_k$ is a nonzero element of R. Let $b(x)$ be an odd-like codeword in C. Then $b(x)i(x) = b(x)$. Evaluating this equation at $x = 1$ gives $\sum_{k=0}^{n-1} b_k = \sum_{k=0}^{n-1} \left(b_k \sum_{j=0}^{n-1} i_j \right) = \alpha \sum_{k=0}^{n-1} b_k$. Since $b(x)$ is an odd-like codeword, $\sum_{k=0}^{n-1} b_k \neq 0$, so $\alpha = 1$, giving $i(x) - h(x)$ as the generating idempotent of C_e. □

Theorem 8. *Let $C_1 = \langle e_1(x) \rangle$ and $C_2 = \langle e_2(x) \rangle$ be a pair of even-like duadic codes of length n over R. Suppose that μ_a gives the splitting for C_1 and C_2. Let D_1 and D_2 be the associated odd-like duadic codes. Then:*

1. $e_1(x)e_2(x) = 0$
2. $C_1 \cap C_2 = \{0\}$ *and* $C_1 + C_2 = \mathscr{E}_n$
3. C_1 *and* C_2 *each have dimension* $(n-1)/2$
4. D_1 *is the cyclic complement of* C_2 *and* D_2 *is the cyclic complement of* C_1
5. D_1 *and* D_2 *each have dimension* $(n+1)/2$
6. C_i *is the even-like subcode of* D_i*, for* $i = 1, 2$
7. $D_1\mu_a = D_2$ *and* $D_2\mu_a = D_1$
8. $D_1 \cap D_2 = \langle h(x) \rangle$ *and* $D_1 + D_2 = R_n$
9. $D_i = C_i + \langle h(x) \rangle = \langle h(x) + e_i(x) \rangle$*, for* $i = 1, 2$

Proof. Multiplying equation (II.1) by $e_1(x)$ gives $e_1(x)e_2(x) = 0$ by Lemma 3 so 1) holds. By [22, Theorem 1], $C_1 \cap C_2$ and $C_1 + C_2$ have generating idempotents $e_1(x)e_2(x) = 0$ and $e_1(x) + e_2(x) - e_1(x)e_2(x) = e_1(x) + e_2(x) = 1 - h(x)$ respectively, so 2) holds by Lemma 4. By equation (II.2), C_1 and C_2 are equivalent and hence have the same dimension. By 2) and Lemma 4 this dimension is $(n-1)/2$, giving 3). The cyclic complement of C_i has generating idempotent $1 - e_i(x)$ by Theorem 2; thus 4) is immediate from the definition of D_i. Part 5) follows from the definition of cyclic complement and parts 3) and 4). As D_1 is odd-like with generating idempotent $1 - e_2(x)$ by Lemma 7, the generating idempotent of the even-like subcode of D_1 is $1 - e_2(x) - h(x) = e_1(x)$. Thus C_1 is the even-like subcode of D_1; analogously, C_2 is the even-like subcode of D_2 yielding 6). The generating idempotent of $D_1\mu_a$ is $(1 - e_2(x))\mu_a = 1 - e_2(x)\mu_a = 1 - e_1(x)$ by Theorem 6 and equation (II.3). Thus $D_1\mu_a = D_2$; analogously $D_2\mu_a = D_1$, producing 7). By [22, Theorem 1], $D_1 \cap D_2$ and $D_1 + D_2$ have generating idempotents $(1 - e_1(x))(1 - e_2(x)) = 1 - e_1(x) - e_2(x) = h(x)$ and $(1 - e_1(x)) + (1 - e_2(x)) - (1 - e_1(x))(1 - e_2(x)) = 1$ respectively, as $e_1(x)e_2(x) = 0$. Thus 8) holds as the generating idempotent of R_n is 1. Finally by 3), 5), and 6), C_i is a subspace of D_i of codimension 1, as $h(x) \in D_i \setminus C_i$, $D_i = C_i + \langle h(x) \rangle$. Also, $D_i = \langle h(x) + e_i(x) \rangle$ by equations (II.1) and (II.4), which proves 9). □

Theorem 9. *(Square Root Bound) Let D_1 and D_2 be a pair of odd-like duadic codes of length n over R. Let d_0 be their (common) minimum odd-like weight. Then the following holds:*

1. *$d_0^2 \geq n$,*
2. *if the splitting defining the duadic codes is given by μ_{-1}, then $d_0^2 - d_0 + 1 \geq n$.*

Proof. Suppose that the splitting defining the duadic codes is given by μ_a. Let $c(x) \in D_1$ be an odd-like codeword of weight d_0. Then $c'(x) = c(x)\mu_a \in D_2$ is also odd like and $c(x)c'(x) \in D_1 \cap D_2$ as D_1 and D_2 are ideals in R_n. But $D_1 \cap D_2 = \langle h(x) \rangle$ by Theorem 8. By Lemma 3, $c(x)c'(x)$ is odd-like and in particular nonzero. Therefore $c(x)c'(x)$ is a nonzero multiple of $h(x)$, and so $\mathrm{wt}(c(x)c'(x)) = n$. The number of terms in the product $c(x)c'(x)$ is at most d_0^2, so 1) follows. If $\mu_a = \mu_{-1}$, then the number of terms in $c(x)c'(x)$ is at most $d_0^2 - d_0 + 1$ because d_0 terms contribute to the coefficient of x^0 in $c(x)c'(x)$, so 2) follows. □

Gleason-Prange theorem

Let $\widehat{C}$ denote the extended code of C.

Lemma 10. *Let C be an $[n,k,d]_R$ code.*

1. *Suppose that $MAut(C)$ is transitive. Then the n codes obtained from C by puncturing C on a coordinate are monomially equivalent.*
2. *Suppose that $MAut\left(\widehat{C}\right)$ is transitive. Then the minimum weight d of C is its minimum odd-like weight d_0. Furthermore, every minimum weight codeword of C is odd-like.*

Proof. Since $\mathrm{MAut}(C)$ is transitive, 1) is obvious. For 2), assume that the automorphism group of $\widehat{C}$ is transitive. Applying 1) to $\widehat{C}$, we conclude that puncturing $\widehat{C}$ on any coordinate gives a code monomially equivalent to C. Let c be a minimum weight codeword of C, and assume that c is even-like. Then $\mathrm{wt}(\widehat{c}) = d$ where $\widehat{c} \in \widehat{C}$ is the extended codeword. Puncturing $\widehat{C}$ on a coordinate where c is nonzero gives a codeword of weight $d-1$ is a code monomially equivalent to C, a contradiction. □

Definition 11. *Let v be a codeword of blocklength n over the ring R. Let ω be an element of order n in either R or some extension ring of R. The Fourier transform of v is another codeword V of blocklength n over R whose components are given by*

$$V_j = \sum_{i=0}^{n-1} \omega^{ij} v_i, j = 0, \ldots, n-1.$$

The codeword V is known as the spectrum of v. The inverse Fourier transform is given by

$$v_i = \frac{1}{n} \sum_{j=0}^{n-1} \omega^{-ij} V_j, i = 0, \ldots, n-1.$$

We will use $\chi(i)$ denote the Legendre symbol defined by

$$\chi(i) = \begin{cases} 0, \text{ if } i \text{ is a multiple of } p \\ 1, \text{ if } i \text{ is a nonzero square (mod } p) \\ -1, \text{ if } i \text{ is a nonzero nonsquare (mod } p) \end{cases}.$$

Additionally, the Gaussian sum is defined as

$$\theta = \sum_{i=0}^{p-1} \chi(i)\, \omega^i.$$

Lemma 12. *In the finite chain ring R with characteristic q, the element* $\sum_{i=1}^{p} 1_R$ *is a unit for p coprime to q.*

Proof. Since p and q are coprime, there exists $a, b \in \mathbb{Z}$ such that $ap + bq = 1$ which implies that $ap \equiv 1 \pmod{q}$. But this means that $ap \cdot 1_R = (\sum_{i=1}^{a} 1_R)\left(\sum_{i=1}^{p} 1_R\right) = 1_R$, so $\sum_{i=1}^{p} 1_R$ is a unit in R. □

Lemma 13. *[5, Theorem 1.11.2] The Gaussian sum satisfies* $\theta^2 = p\chi(-1)$.

Note that as a consequence of the previous lemma, θ is also a unit.

Definition 14. *Let* $v = \left(v_0, v_1, \ldots, v_{p-1}, v_\infty\right)$ *be a codeword of blocklength* $p+1$*, where p is prime, over a finite chain ring R of characteristic q, where p and q are coprime. The Gleason-Prange permutation of v is the codeword* $u = \left(u_0, u_1, \ldots, u_{p-1}, u_\infty\right)$ *defined by*

$$u_i = \chi\left(-i^{-1}\right) v_{-i^{-1}}, i = 1, \ldots, p-1$$
$$u_0 = \chi(-1)\, v_\infty$$
$$u_\infty = v_0$$

Theorem 15. *(Gleason-Prange Theorem) Let p be a prime. Suppose that over R, a finite chain ring of characteristic q coprime to p, the codeword* $v = \left(v_0, v_1, \ldots, v_{p-1}, v_\infty\right)$ *satisfies*

1. *if* $j \in \{0, 1, \ldots, p-1\}$ *is a nonzero square, then* $V_j = 0$
2. $v_\infty = \frac{-\theta}{p} \sum_{i=0}^{p-1} v_i$.

Then the Gleason-Prange permutation of v satisfies these same two conditions.

Proof. Suppose that $V_j = 0$ whenever j is a nonzero square modulo p. The inverse Fourier transform of v can be written as

$$\begin{aligned} v_i &= \frac{1}{p}\left(V_0 + \sum_{k=1}^{p-1} \omega^{-ik} V_k\right) \\ &= \frac{1}{p}\left(\frac{-p}{\theta} v_\infty + \sum_{k=1}^{p-1} \omega^{-ik} V_k\right). \end{aligned}$$

The Gleason-Prange permutation gives that

$$\begin{aligned} u_i &= \chi\left(-i^{-1}\right) v_{-i^{-1}} \\ &= \frac{1}{p}\chi\left(-i^{-1}\right)\left(\frac{-p}{\theta} v_\infty + \sum_{k=1}^{p-1} \omega^{i^{-1}k} V_k\right) \end{aligned}$$

for $i \neq 0$ and that $u_0 = \chi(-1)\, v_\infty$. Further,

$$\begin{aligned} U_j &= u_0 + \sum_{i=1}^{p-1} \omega^{ij} u_i \\ &= \chi(-1)\, v_\infty + \sum_{i=1}^{p-1} \frac{\omega^{ij}\chi\left(-i^{-1}\right)}{p}\left(\frac{-p}{\theta} v_\infty + \sum_{k=1}^{p-1} \omega^{i^{-1}k} V_k\right) \\ &= v_\infty\left(\chi(-1) - \frac{1}{\theta}\sum_{i=1}^{p-1} \chi\left(-i^{-1}\right)\omega^{ij}\right) + \\ &\frac{1}{p}\sum_{i=1}^{p-1} \omega^{ij}\chi\left(-i^{-1}\right)\sum_{k=1}^{p-1} \omega^{i^{-1}k} V_k. \end{aligned}$$

Denote the two summands as A_j and B_j respectively so that $U_j = A_j + B_j$.

Consider A_j:

$$\begin{aligned} A_j &= v_\infty\left(\chi(-1) - \frac{1}{\theta}\sum_{i=1}^{p-1} \chi\left(-i^{-1}\right)\omega^{ij}\right) \\ &= \chi(-1)\, v_\infty\left(1 - \frac{\chi(j)}{\theta}\sum_{i=1}^{p-1} \chi(ij)\,\omega^{ij}\right) \\ &= \chi(-1)\, v_\infty\left(1 - \frac{\chi(j)\,\theta}{\theta}\right). \end{aligned}$$

Therefore $A_j = 0$ whenever j is a nonzero square modulo p.

Now consider B_j:

$$\begin{aligned}
B_j &= \frac{1}{p}\sum_{i=1}^{p-1}\omega^{ij}\chi\left(-i^{-1}\right)\sum_{k=1}^{p-1}\omega^{i^{-1}k}V_k \\
&= \frac{1}{p}\chi(-1)\sum_{i=1}^{p-1}\omega^{ij}\sum_{k=1}^{p-1}\omega^{i^{-1}k}\chi\left(i^{-1}k\right)\chi(k)V_k \\
&= \frac{-1}{p}\chi(-1)\sum_{i=1}^{p-1}\omega^{ij}\sum_{k=1}^{p-1}\omega^{i^{-1}k}\chi\left(i^{-1}k\right)V_k.
\end{aligned}$$

The last equality hold since $V_k = 0$ whenever $\chi(k) \neq -1$. Redefine the indices using the Rader permutation $i = \pi^r, j = \pi^t, k = \pi^{-s}$, where π is a primitive element in $\mathbb{F}_p$. The sums remain unaffected as the permutations simply reorder the elements in the sums. Therefore we have

$$B_{\pi^{-s}} = \frac{-1}{p}\chi(-1)\sum_{r=0}^{p-2}\omega^{\pi^{r-s}}\sum_{t=0}^{p-2}\omega^{\pi^{-r+t}}\chi\left(\pi^{-r+t}\right)V_{\pi^t}.$$

This is a double cyclic convolution which we can rewrite as

$$B'_{-s} = \sum_{r=0}^{p-2} g_{r-s}\sum_{t=0}^{p-2} g'_{t-r}V'_t,$$

where $V'_t = V_{\pi^t}$, $B'_s = \frac{-p}{\chi(-1)}B_{\pi^s}$, $g_r = \omega^{\pi^{-r}}$, and $g'_r = \chi(\pi^r)\,\omega^{\pi^{-r}} = (-1)^r\,\omega^{\pi^{-r}}$. If t is even then $V'_t = 0$ since if j is a nonzero square $V_j = 0$. We can write this double convolution in polynomial form as

$$B'\left(x^{-1}\right) = g(x)\,g'(x)\,V'(x) \pmod{x^{p-1}-1}$$

where $g(x)\sum_{r=0}^{p-2}\omega^{\pi^{-r}}x^r$ and $g'(x) = \sum_{r=0}^{p-2}(-1)^r\,\omega^{\pi^{-r}}x^r$. Since they only differ in the sign of the odd-indexed terms, the product $g(x)\,g'(x)$ has only even-indexed coefficients nonzero. The polynomial $V'(x)$ has only odd-indexed coefficients nonzero, so the product $g(x)\,g'(x)\,V'(x)$ has all even-indexed coefficients equal to zero. Therefore $B'_s = 0$ when s is even and so $U_j = 0$ whenever j is a nonzero square.

Now we will show that $u_\infty = \frac{-\theta}{p}\sum_{i=0}^{p-1} u_i$.

$$\sum_{i=0}^{p-1} u_i = \chi(-1)\, v_\infty + \sum_{i=1}^{p-1} \chi\left(-i^{-1}\right) v_{-i^{-1}}$$
$$= \chi(-1)\, v_\infty + \sum_{i=1}^{p-1} \chi(i)\, v_i.$$

We can expand this sum out to

$$\sum_{i=1}^{p-1} \chi(i)\, v_i = \frac{1}{p}\sum_{i=1}^{p-1} \chi(i) \left(\sum_{k=1}^{p-1} \omega^{-ik} V_k + V_0\right)$$
$$= \frac{\chi(-1)}{p}\sum_{i=1}^{p-1}\sum_{k=1}^{p-1} \chi(-i)\, \omega^{-ik} V_k$$
$$= \frac{\chi(-1)}{p}\sum_{k=1}^{p-1} V_k \chi(k)\, \theta.$$

In the same way as in the previous part of the proof, we can replace $\chi(k)$ with -1 since $V_k = 0$ whenever $\chi(k) \neq -1$.

$$\sum_{i=1}^{p-1} \chi(i)\, v_i = \frac{-\chi(-1)\,\theta}{p}\sum_{k=1}^{p-1} V_k$$
$$= \frac{-\chi(-1)\,\theta}{p}\left(pv_0 - V_0\right).$$

Since $c_\infty = \frac{-\theta}{p} V_0$, we have

$$\sum_{i=0}^{p-1} u_i = -\chi(-1)\,\theta c_0 = -\chi(-1)\,\theta d_\infty.$$

Because $\theta^2 = p\chi(-1)$ and $\chi^2(x) = 1$, we have that $\chi(-1)\,\theta = p/\theta$, and thus

$$\sum_{i=0}^{p-1} u_i = \frac{-p}{\theta} u_\infty.$$

Therefore u satisfies the same two conditions as v. □

Using compositions of the shift permutation and the Gleason-Prange permutation, it is possible to send any coordinate to any other coordinate in $\widehat{C}$, so by Lemma 10, the minimum weight d of the code C is its minimum odd-like weight d_0.

Stabilizer codes

Theorem 16. *[17, Theorem 9] Let C_1 and C_2 denote two classical linear codes with parameters $[n,k_1,d_1]_R$ and $[n,k_2,d_2]_R$ such that $C_2^{\perp} \leq C_1$. Then there exists a $[[n,k_1+k_2-n,d]]_R$ stabilizer code with minimum distance $d = min\left\{wt(c)\,|c \in \left(C_1 \setminus C_2^{\perp}\right) \cup \left(C_2 \setminus C_1^{\perp}\right)\right\}$ that is pure to $min\{d_1,d_2\}$.*

Theorem 17. *[3, Proposition 4.3] Let $D_i, i \in \{1,2\}$ be the odd-like duadic codes over R, where $D_i = \langle g_i(x)\rangle$ and $(x-1)\,g_1(x)\,g_2(x) = x^n - 1$, and let C_i be the even-like duadic codes over R, where $C_i = \langle (x-1)\,g_i(x)\rangle$. Then*

1. *if the splitting is given by μ_{-1}, then $D_1^{\perp} = C_1$ and $D_2^{\perp} = C_2$*
2. *if the splitting is not given by μ_{-1}, then $D_1^{\perp} = C_2$ and $D_2^{\perp} = C_1$*

Theorem 18. *Let n be a prime of the form $n \equiv 3 \pmod 4$, and let $(q,n) = 1$. If q is a quadratic residue modulo n, then there exists a pure $[[n,1,d]]_R$ stabilizer code with distance d satisfying $d^2 - d + 1 \geq n$.*

Proof. The code C_Q has parameters $[n,(n+1)/2,d]_R$ and since $n \equiv 3 \pmod 4$, by [13, Lemma 6.2.4] we know that -1 is not a square modulo n, so μ_{-1} gives the splitting for C_Q and C_N. Therefore by Theorem 17 we know that $C_Q^{\perp} = C_Q'$, so C_Q is self-orthogonal. By Theorem 9 we know that the minimum distance d is bounded by $d^2 - d + 1 \geq n$. Furthermore, $\text{wt}\left(C_Q \setminus C_Q^{\perp}\right) = \text{wt}(C_Q) = d$, since the minimum weight of C_Q is its minimum odd-like weight. We can therefore construct a $[[n,(n+1)-n,d]]_R$ stabilizer code by Theorem 16. □

Theorem 19. *Let n be a prime of the form $n \equiv 1 \pmod 4$, and let $(q,n) = 1$. If q is a quadratic residue modulo n, then there exists a pure $[[n,1,d]]_R$ stabilizer code with distance d satisfying $d \geq \sqrt{n}$.*

Proof. The code C_Q has parameters $[n,(n+1)/2,d]_R$ and since $n \equiv 1 \pmod 4$, by [13, Lemma 6.2.4] we know that -1 is a square modulo n, so μ_{-1} does not give a splitting for C_Q and C_N. Therefore by Theorem 17 $C_Q^{\perp} = C_N'$, that is $C_Q^{\perp} \leq C_N$. By Theorem 9 we know that the minimum distance d is bounded by $d \geq \sqrt{n}$. Moreover, $\mathrm{wt}\left(C_Q \setminus C_N^{\perp}\right) = \mathrm{wt}\left(C_N \setminus C_Q^{\perp}\right) = \mathrm{wt}\left(C_Q\right) = \mathrm{wt}\left(C_N\right) = d$ since the minimum weight of C_Q and C_N is their (common) minimum odd-like weight. Therefore we obtain a pure $[[n,(n+1)/2+(n+1)/2-n,d]]_R$ stabilizer code by Theorem 16. □

CHAPTER III

BCH CODES

Preliminaries

Let A be a local finite commutative ring with maximal ideal $\mathfrak{M}$ and residue field $\mathbb{K} = A/\mathfrak{M} = \mathbb{F}_{p^m}$ for some prime p and $m \in \mathbb{N}$. Let f be a monic polynomial of degree h such that $\overline{f}$ is irreducible over $\mathbb{K}$ and therefore also irreducible over A. Let R denote the ring of residue classes $A[x]/\langle f(x)\rangle$ with maximal ideal $\mathfrak{m} = \langle \mathfrak{M} f(x)\rangle / \langle f(x)\rangle$ and residue field $\overline{\mathbb{K}} = R/\mathfrak{m}$. Following are several theorems given without proof from [1]:

Theorem 20. *[1, Theorem 2.1] There is only one maximal cyclic subgroup of R^* having order relatively prime to p. This cyclic subgroup is denoted by G_s and has order $s = p^{mh} - 1$.*

Theorem 21. *[1, Theorem 2.2] Suppose that α generates a subgroup of order s (a divisor of $p^{mh} - 1$) in R^*. Then $x^s - 1$ can be factored as $x^s - 1 = (x-\alpha)\left(x-\alpha^2\right)\cdots(x-\alpha^s)$ if and only if $\overline{\alpha}$ has order s in $\overline{\mathbb{K}}^*$.*

Definition 22. *[1, Definition 2.3] Let α be a primitive element of G_n. Then a cyclic BCH code defined over the ring A is a cyclic code of length n generated by a minimal degree polynomial $g(x)$ (over A) whose roots are $\alpha^{b+1}, \alpha^{b+2}, \ldots, \alpha^{b+2t}$, for some $b \geq 0$ and $t \geq 1$.*

In this case, the parity-check matrix H is given by

$$H = \begin{bmatrix} 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ 1 & \alpha^{b+2} & \alpha^{2(b+2)} & \cdots & \alpha^{(n-1)(b+2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+2t} & \alpha^{2(b+2t)} & \cdots & \alpha^{(n-1)(b+2t)} \end{bmatrix}.$$

Stabilizer codes

Lemma 23. *Let H be the parity-check matrix of a code C. Then $C^{\perp} \subseteq C$ if and only if $HH^T = 0$.*

Proof. Suppose $C^{\perp} \subseteq C$. By definition of the parity-check matrix, $xH^T = 0$ for all $x \in C$. Therefore we have $xH^T = 0$ for all $x \in C^{\perp}$. Since H generates $C^{\perp}$, the rows of H are elements of

$C^\perp$ and therefore $HH^T = 0$. Now suppose that $HH^T = 0$. Since H generates $C^\perp$, every $x \in C^\perp$ is a linear combination of the rows of H, so $xH^T = 0$, meaning that $x \in C$, so $C^\perp \subseteq C$. □

Theorem 24. *Let C be a cyclic BCH code of length ℓn over the ring R for $\ell \in \mathbb{N}$ and $n = p^{mh} - 1$ for an odd prime p. If $2t = \ell n$, then $C^\perp \subseteq C$.*

Proof. The parity-check matrix of C is given by $(H)_{i,j} = \alpha^{(i-1)(b+j)}$. Then

$$\begin{aligned}
\left(HH^T\right)_{i,j} &= \sum_{k=1}^{2t} \alpha^{(i-1)(b+k)} \alpha^{(j-1)(b+k)} \\
&= \sum_{k=1}^{\ell n} \alpha^{(b+k)(i+j-2)} \\
&= \alpha^{b(i+j-2)} \sum_{k=1}^{\ell n} \alpha^{k(i+j-2)} \\
&= \alpha^{b(i+j-2)} \sum_{x=0}^{\ell-1} \sum_{y=1}^{n} \alpha^{(xn+y)(i+j-2)} \\
&= \alpha^{b(i+j-2)} \sum_{x=0}^{\ell-1} \alpha^{xn(i+j-2)} \sum_{y=1}^{n} \alpha^{y(i+j-2)}.
\end{aligned}$$

Focusing on the inner sum, we see that

$$\begin{aligned}
\sum_{y=1}^{n} \alpha^{y(i+j-2)} &= \sum_{y=1}^{n/2} \alpha^{y(i+j-2)} + \sum_{y=(n/2)+1}^{n} \alpha^{y(i+j-2)} \\
&= \sum_{y=1}^{n/2} \alpha^{y(i+j-2)} + \alpha^{n/2} \sum_{y=1}^{n/2} \alpha^{y(i+j-2)} \\
&= \sum_{y=1}^{n/2} \left(\alpha^{y(i+j-2)} - \alpha^{y(i+j-2)} \right) = 0.
\end{aligned}$$

By substituting the inner sum back into the original expression, we have that $\left(HH^T\right)_{i,j} = 0$ for all values of i, j, so by Lemma 23 we have that $C^\perp \subseteq C$. □

Theorem 25. *Let R be a finite chain ring with residue field $\mathbb{F}_{p^m}$ for an odd prime p. Then there exists an $\left[\left[p^{mh} - 1, 0, 2t\right]\right]_R$ stabilizer code.*

Proof. Follows directly from Theorems 16 and 24. □

CHAPTER IV

CONCLUSION

One of the largest issues in quantum computing is the inherent instability of the quantum systems used in the qubits. While there has been previous work done on the existence of stabilizer codes over the more general class of Frobenius rings in [17], there has been little to no work done on constucting these codes. In this paper we focused on stabilizer codes based on classical codes over finite chain rings and gave a method for explicitly constructing stabilizer codes from quadratic reside and BCH codes over finite chain rings using a CSS construction. We also extended the Gleason-Prange theorem to the class of finite chain rings which allowed us to exactly characterize the minimum distance of the quadratic residue quantum stabilizer codes as the minimum odd-like weight of the classical quadratic residue code.

The codes that we have constructed over the finite chain rings are important because although they have been shown to never have minimum distances that beat their counterparts over finite fields, they may make up for this with simpler arithmetics, which reduces the amount of time that needed to perform calculations. This could be important especially with reguards to error correcting on a quantum computer, which must be done constantly to keep the qubits stable. One future direction of study would be to determine which of these stabilizer codes over finite chain ring perform better than their finte field analogues, as these codes might be of interest to researchers actively developing quantum systems.

Another future direction of study would be to find better bounds for the stabilizer codes we have constructed. One way to do this would be to use the symplectic weight enumerators of the codes and then to constuct a linear programming bound similar to the one in [14] for codes over finte fields.

REFERENCES

[1] A. Andrade and Jr. R. Palazzo. Construction and decoding of BCH codes over finite commutative rings. *Linear Algebra Applic.*, 286, 1999.

[2] L. Babai. The Fourier Transform and Equations over Finite Abelian Groups. Lecture Notes in Computer Science, University of Chicago, December 1989.

[3] A. Batoul, K. Guenda, and T. Gulliver. On Isodual Cyclic Codes over Finite Fields and Finite Chain Rings: Monomial Equivalence. 2013.

[4] R. Blahut. The Gleason-Prange Theorem. *IEEE Trans. Inform. Theory*, 37(5), 1991.

[5] R. Blahut. *Algebraic Codes on Lines, Planes, and Curves*. Cambridge University Press, 2008.

[6] M. Chiu, S. Yau, and Y. Yu. $\mathbb{Z}_8$-Cyclic Codes and Quadratic Residue Codes. *Adv. in Appl. Math.*, 25(1), 2000.

[7] H. Dinh and S. López-Permouth. Cyclic and Negacyclic Codes Over Finite Chain Rings. *IEEE Trans. Inform. Theory*, 50(8), 2004.

[8] J. Gao, L. Shen, and F. Fu. Quasi-Cyclic Codes Over Finite Chain Rings. 2013.

[9] D. Gottesman. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computing. *Proceedings of Symposia in Applied Mathematics*, 2009.

[10] J. Hall. Notes on Coding Theory. Lecture Notes in Mathematics, Michigan State University, September 2010.

[11] T. Honold and I. Landjev. Linear Codes over Finite Chain Rings. *The Electronic Journal of Combinatorics*, 7, 2000.

[12] W. Huffman. Codes and groups. In V. Pless and W. Huffman, editors, *Handbook of Coding Theory*. Elsevier Science, 1998.

[13] W. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[14] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11), 2006.

[15] H. Lee and Y. Lee. Construction of self-dual codes over finite rings $\mathbb{Z}_{p^m}$. *J. Combin. Theory Ser. A*, 115(3), 2008.

[16] S. Lee and A. Klappenecker. Subsystem Codes over Nice Nearrings. In *2013 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 912–916, July 2013.

[17] S. Nadella and A. Klappenecker. Stabilizer Codes over Frobenius Rings. In *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 165–169, July 2012.

[18] V. Pless, W. Huffman, and R. Brualdi. An instroduction to algebraic codes. In V. Pless and W. Huffman, editors, *Handbook of Coding Theory*. Elsevier Science, 1998.

[19] V. Pless and Z. Qian. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, 42(5), 1996.

[20] A. Sarma and A. Klappenecker. Quantum Codes over Rings and Quadratic Algebras. In *52nd Annual Allerton Conference on Communication, Control, and Computing*, October 2014.

[21] P. Shankar. On BCH Codes over Arbitrary Integer Rings. *IEEE Trans. Inform. Theory*, 25(4), 1979.

[22] B. Taeri. Quadratic Residue Codes Over $\mathbb{Z}_9$. *J. Korean Math. Soc.*, 46(1), 2009.

[23] M. Vo. *New Classes of Finite Commutative Rings*. PhD thesis, University of Hawaii, May 2003.

[24] Z. X. Wan. *Quaternary Codes*. World Scientific Publishing, 1997.