

ECE 7670
Lecture 8 – Other cyclic codes

Objective: To examine some other common families of cyclic codes

Reading:

- Chapter 6.

In this chapter we will introduce some other cyclic codes which are of both historical and practical significance. To get started, we will need some more matrix and number theory background.

1 Hadamard matrices

Consider the following:

$$H_1 = [1] \quad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

These are examples of **Hadamard** matrices, which have the property that they are ± 1 matrices such that

$$H_n H_n^T = nI.$$

Hadamard matrices exist of orders 1, 2, 4, or a multiple of 4. Hadamard matrices are of interest because we can define codes based on the rows of the Hadamard matrix.

There are two known ways of making Hadamard matrices. One way is as follows:

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

This is the **Sylvester** construction. The second construction, the **Paley** construction, is somewhat more subtle. We begin with a discussion of quadratic residues.

Suppose we wanted (for some strange reason) to know for which values of x the following quadratic equation has a solution:

$$y^2 \equiv x \pmod{p}$$

where p is prime. For example, let $p = 5$. Then we have

$$\begin{aligned} 1^2 &\equiv 1 \\ 2^2 &\equiv 4 \\ 3^2 &\equiv 4 \\ 4^2 &\equiv 1 \end{aligned}$$

In this example, only $x = 1$ and $x = 4$ have a solution to the quadratic equation. Those values mod p that are perfect squares are called the **quadratic residues** modulo p .

Example 1 When $p = 7$ we have

$$\begin{aligned} 1^2 &= \text{equiv}1 \\ 2^2 &= \text{equiv}4 \\ 3^2 &= \text{equiv}2 \\ 4^2 &= \text{equiv}2 \\ 5^2 &= \text{equiv}4 \\ 6^2 &= \text{equiv}1 \end{aligned}$$

So the quadratic residues (perfect squares) mod 7 are 1, 2, 4. \square

We observe:

1. We only need to check the first half, since $(p - x)^2 \equiv x^2 \pmod{p}$.
2. There are $(p - 1)/2$ quadratic residues mod p .
3. $R \cdot R = R$ and $R \cdot N = N$.

Definition 1 We define the Legendre symbol $\chi(x)$ (in the context of a given prime p) to be

$$\chi(x) = \begin{cases} 0 & \text{if } x \text{ is a multiple of } p \\ 1 & \text{if } x \text{ is a quadratic residue of } p \\ -1 & \text{if } x \text{ is not a quadratic residue of } p \end{cases}$$

\square

Now define a $p \times p$ matrix Q with elements (indexed starting from zero) of

$$q_{ij} = \chi(j - i).$$

For example, let $p = 5$. Then the quadratic residues are 1, 4, so we would have Q of the form

$$Q = \begin{bmatrix} 0 & 1 & - & - & 1 \\ 1 & 0 & 1 & - & - \\ - & 1 & 0 & 1 & - \\ - & - & 1 & - & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Such a matrix is called a **Jacobsthal matrix**. Now we form (without proof) the matrix

$$H_n = \begin{bmatrix} 1 & & & \mathbf{1} \\ \mathbf{1}^T & Q_{n-1} & - & I_{n-1} \end{bmatrix}.$$

For certain orders n this is a Hadamard matrix.

A Hadamard matrix is *normalized* if the left column is all equal to one.

1.1 Codes over Hadamard matrices

Take a Hadamard matrix H_n , and convert: $1 \rightarrow 0$ and $-1 \rightarrow 1$. Call the resulting matrix A_n . We can make codes three different ways:

1. The rows of H_n are orthogonal, so that the rows of A_n differ in $n/2$ places. These give us n code words of length n . We may delete the left column without affecting the distance to obtain a length $n - 1$ code with minimum distance $n/2$. This code is known as the \mathcal{A}_n code; it is also called a simplex code.
2. Take \mathcal{A}_n and complement each word. The resulting code is called \mathcal{B} and has $2n$ codewords of length $n - 1$ and minimum distance $n/2 - 1$.

If n is not a power of two, then the code is *nonlinear* (our first example this quarter). Every code resulting from a Paley-constructed matrix of order $n > 8$ gives rise to a nonlinear code.

If we take a nonlinear code, and adjoin all linear combinations of codewords we obtain a linear code. This is the *quadratic residue* code we will talk about later. (Overhead)

2 Quadratic residue codes

We begin with a review: Recall that cyclotomic cosets modulo n represent the exponents of conjugate elements in a field, such as

$$\beta, \beta^q, \beta^{q^2}, \dots,$$

where β is some element in $GF(q)$ with order n . Also recall that the set of roots of a polynomial with coefficients in $GF(q)$ must consist of the union of one or more sets of conjugacy classes with respect to $GF(q)$.

Now let us consider the quadratic residues of p in light of conjugacy classes. Let Q be the set of quadratic residues and let N be the set of quadratic nonresidues, mod p . The set of integers modulo p forms the field $GF(p)$, so this division into N and Q divides $GF(p)$ into two sets. $GF(p)$ has a generator γ , so that successive powers of γ generates the $p - 1$ distinct elements of $GF(p)$:

$$\gamma, \gamma^2, \dots, \gamma^{p-1} = 1.$$

- The generator γ must lie in N . Otherwise, there is some element $\delta \in P$ such that $\delta^2 = \gamma$ so that we could have

$$\delta, \delta^2 = \gamma, \delta^3, \delta^4 = \gamma^2, \dots, \delta^{2p-2}, \delta^{2p-2} = 1$$

which would have $2(p - 1)$ distinct elements in it, which cannot happen.

- Observe that $\gamma^e \in Q$ for an even number e and $\gamma^o \in N$ for an odd number o .
- We can write the elements of Q as the first $(p - 1)/2$ consecutive powers of γ^2 . Q is generated by γ^2 , and hence forms a cyclic group under multiplication mod p .

Let $p|s^m - 1$. Then $GF(s^m)$ has a primitive p th root of unity. Let us add another restriction: s is a quadratic residue mod p . Now, among the powers of β ,

$$\beta, \beta^2, \beta^3, \dots, \beta^p = 1,$$

are the exponents $1, 2, \dots, p$. Of these integers, some are in Q and some are in N . But by our restriction, $s \in Q$. Now consider the conjugates of β with respect to $GF(s)$:

$$\beta, \beta^s, \beta^{s^2}, \dots,$$

Since $s \in Q$ and Q forms a group we must also have

$$s^2 \in Q, \quad s^3 \in Q, \dots$$

Hence, the exponents of β that form its conjugates are all in Q . We conclude that **Q is the union of one or more cyclotomic cosets modulo p with respect to $GF(s)$.**

The bottom line is that a polynomial

$$q(x) = \prod_{i \in Q} (x - \alpha^i)$$

must have its coefficients in $GF(s)$. Similarly we must have

$$n(x) = \prod_{i \in N} (x - \alpha^i)$$

is in $GF(s)[x]$, and we can also write

$$x^p - 1 = (x - 1)q(x)n(x).$$

The **quadratic residue codes** \mathcal{Q} , $\overline{\mathcal{Q}}$, \mathcal{N} , and $\overline{\mathcal{N}}$, are generated by (respectively)

$$q(x), (x - 1)q(x), n(x), (x - 1)n(x).$$

QR codes have pretty good rates and pretty good distance properties: $d^2 \geq p$.

3 Golay codes

Let us take $p = 23$ and form the QR code. The binary Golay \mathcal{G}_{23} is the (23,12,7) code thus formed. Properties:

1. Every codeword with even weight has weight divisible by 4.
2. The min. distance is 7 (triple-error correcting)
3. Perfect code:

$$V_2(23, 3) = \binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}.$$

(It is said that this code was found by playing around with Pascal's triangle.)

We can add an overall parity check bit to obtain the (24, 12, 8) code.

Good decoding algorithms exist for the binary Golay codes; we will not go into them.