MSRI-UP 2009 Coding Theory Seminar, Week 2

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross

June 22 - 25, 2009

Outline

The definition

- Many codes that are used in practice have even more algebraic structure than the linear codes we have already seen.
- The *cyclic shift* $\pi : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ is the linear mapping defined by
$$\pi(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

- Definition
A linear code C is said to be a **cyclic code** *if $\pi(C) = C$ (that is, if the cyclic shift of every codeword is another codeword).*
  - Note: cyclic codes can be specified with less information.

Link to polynomials

- To study cyclic codes, we will introduce a *polynomial form* for the codewords:
- Given $u = (u_1, \ldots, u_n)$, we consider the polynomial $u(x) = u_1 + u_2 x + \cdots + u_n x^{n-1}$.
- Why do we do this?
- Mainly because the cyclic shift seems to be closely related to basic important operations on polynomials:
- The "ordinary" shift corresponds to $x \cdot u(x) = u_1 x + \cdots + u_{n-1} x^{n-1} + u_n x^n$.
- Then, to "cycle" the $u_n x^n$ back to the start, we could divide by $1 + x^n$ and take the remainder.

Algebra of polynomials

Definition

The set of all polynomials in the variable x with coefficients in a field $\mathbb{F}$ is denoted $\mathbb{F}[x]$.

- We can add and multiply polynomials in $\mathbb{F}[x]$ as usual.
- All the field axioms hold *except* that some nonzero polynomials have no multiplicative inverses.
- We say $\mathbb{F}[x]$ is a *commutative ring with (multiplicative) identity*.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Polynomial division

Another very important aspect of the algebra of polynomials is the existence of a *division algorithm* for polynomials.

Theorem (Division Algorithm)

Let $f(x)$ and $g(x) \neq 0$ be in $\mathbb{F}[x]$. There exist unique polynomials $q(x)$ ("quotient") and $r(x)$ ("remainder") such that $f(x) = q(x)g(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

If $r(x)$ is the remainder on division of $f(x)$ by $g(x)$, we will write $f(x) \equiv r(x) \bmod g(x)$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Division algorithm

The proof of the existence part of the theorem consists of the usual polynomial *long division* process from high school algebra. In "procedural notation:"

```
input: f,g
output: q,r
r:=f; q:=0;
while deg(g) <= deg(r) do
   q := q + in(r)/in(g);
   r := r - (in(r)/in(g))g;
end while
```

(where $\mathrm{in}(p)$ is the highest degree term in p)

Notes

Division example

Take $g(x) = x^2 + x + 1$ and $f(x) = x^7 + x^6 + x^4 + 1$ and divide g into f (taking coefficients in $\mathbb{F} = \mathbb{F}_2$ – it's amazing how simple the computations are in this case!)

[Work out on board]

The results are $q(x) = x^5 + x^3 + x + 1$ and $r = 0$. Note that this says g *divides* f in this case:

$$x^7 + x^6 + x^4 + 1 = (x^5 + x^3 + x + 1)(x^2 + x + 1).$$

We write $g|f$ for the assertion "g divides f" (or equivalently $f = qg$ for some $q \in \mathbb{F}[x]$.

Notes

A consequence of division

Theorem

Let $I \subset \mathbb{F}[x]$ be any subset with the properties that

- $f, g \in I \Rightarrow f + g \in I$, *and*
- $f \in I, q \in \mathbb{F}[x] \Rightarrow qf \in I$

Then $I = \langle g \rangle = \{qg \mid q \in \mathbb{F}[x]\}$ for some $g \in I$.

(Such sets are called *ideals* in the ring $\mathbb{F}[x]$ in abstract algebra; the theorem claims that any such set is generated by a single polynomial $g(x)$.)

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Proof of the theorem

Proof:

- If $I = \{0\}$, then we can take $g = 0$.
- If I contains nonzero polynomials, let g be any nonzero polynomial in I of *minimal degree*.
- If $f \in I$ is any other polynomial, divide g into f to yield $f = qg + r$ where either $r = 0$, or r is nonzero with $\deg(r) < \deg(g)$.
- We claim that the second case cannot happen.
- Rearranging gives $r = f - qg \in I$ since $f, g \in I$.
- If $r \neq 0$, then we get a contradiction to the choice of g. $\square$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Polynomial gcds

Definition

Let $f, g \in \mathbb{F}[x]$. We say $d = \gcd(f, g)$ if d is a polynomial with leading coefficient 1 such that

- *$d|f$, $d|g$, and*
- *if c is any other polynomial with $c|f$ and $c|g$, then $c|d$.*

(Equivalently, we could require d to be a nonzero divisor of *maximal degree*.)

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

More on polynomial gcds

- The polynomial $d = \gcd(f, g)$ is *unique* (because of the requirement on the leading coefficient).
- $d = \gcd(f, g)$ can be computed by *factoring* $f, g \in \mathbb{F}[x]$ and finding the highest common factor.
- There is also a more efficient method called the *Euclidean algorithm*, based on division, that we will discuss next.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Euclidean algorithm for the gcd

- (Assuming $\deg(f) \geq \deg(g)$), perform divisions as indicated, until $r_m | r_{m-1}$:

$$\begin{aligned} f &= q_0 g + r_1 \\ g &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \\ r_{m-2} &= q_{m-1} r_{m-1} + r_m \\ r_{m-1} &= q_m r_m + 0 \end{aligned}$$

- Note that the degrees of the r_i are strictly decreasing.
- The *last nonzero remainder* r_m is $\gcd(f, g)$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

First Euclidean algorithm example

Take $f(x) = x^4 + x^2 + x + 1$ and $g(x) = x^3 + x^2$. What is $\gcd(f, g)$? We form the remainder sequence as on the last slide:

$$\begin{aligned} x^4 + x^2 + x + 1 &= (x+1)(x^3 + x^2) + x + 1 \\ x^3 + x^2 &= x^2(x+1) + 0. \end{aligned}$$

Hence the final nonzero remainder in this case is the first one, $d = x + 1$. We can see here that $f = (x^3 + x^2 + 1)(x + 1)$ and $g = (x^2)(x + 1)$ so $x + 1$ is a common divisor. Moreover, the only divisors of $x + 1$ are $1, x + 1$, so $x + 1$ must be the gcd.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Another characterization of the gcd

The easiest way to explain why the Euclidean algorithm works is to use another characterization of the gcd.

Proposition

Let $f, g \in \mathbb{F}[x]$. Then $\gcd(f, g)$ *is the nonzero polynomial of least degree (and leading coefficient 1) in the set:*

$$\langle f, g \rangle = \{Af + Bg \mid A, B \in \mathbb{F}[x]\}.$$

(In particular, the polynomial $d = \gcd(f, g) = Af + Bg$ for some $A, B \in \mathbb{F}[x]$. We will see a way to find such polynomials A, B later.)

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Why does the Euclidean algorithm work?

Sketch of argument:

- The set $\langle f, g \rangle$ is an ideal in $\mathbb{F}[x]$ as in our previous theorem.
- From the remainder sequence, it is easy to see that

$$\langle f, g \rangle = \langle g, r_1 \rangle = \cdots = \langle r_m, 0 \rangle = \langle r_m \rangle.$$

- Hence $r_m = \gcd(f, g)$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Generator polynomial of a cyclic code

We now return to the case of a cyclic code and consider the set of all polynomials corresponding to the codewords.

Definition

Let C be a cyclic code. The **generator polynomial** *of C is the (unique) nonzero polynomial of smallest degree in C.*

(The uniqueness is a consequence of taking $\mathbb{F} = \mathbb{F}_2$; we get something similar in general if we require the leading coefficient to be 1.)

The proof that polynomial ideals are generated by a single polynomial shows that $qg \bmod x^n + 1$ represents a codeword for all $q \in \mathbb{F}_2[x]$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Consequences

Theorem

Let g be the generator polynomial for a cyclic code C, and assume that $\deg(g) = n - k$.

- *$g(x)$ divides $x^n + 1$.*
- *$u(x)$ is a codeword if and only if $u(x) = q(x)g(x)$ for some $q(x)$ of degree $< k$.*
- *The codewords corresponding to $\{g(x), xg(x), x^2g(x), \ldots, x^{k-1}g(x)\}$ form a basis for C, so* $\dim(C) = k$.

Proof: The second part follows by division; the third follows since these polynomials have distinct degrees, hence must be linearly independent.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Proof, continued

- We must show that if C is a cyclic code with generator polynomial $g(x)$, then $g(x)|x^n + 1$.
- The codewords all have the form $u(x) = q(x)g(x) \bmod x^n + 1$, so for each $u(x)$ we have an equation $u(x) = q(x)g(x) + s(x)(x^n + 1)$ for some $s(x)$.
- But we can write any $u(x)$ as a multiple of $g(x)$, and this implies $g(x)|(x^n + 1)$ as claimed. $\square$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Smallest cyclic code

Given $u \in \mathbb{F}_2^n$, we can ask: What is the smallest cyclic code containing u? The answer comes by looking for the generator polynomial of the code –

- It must be a polynomial that divides both $u(x)$ and $x^n + 1$,
- It must have maximum possible degree among polynomials satisfying the first condition (to get the *smallest* code)
- Hence, we get

$$g(x) = \gcd(u(x), x^n + 1).$$

- Hence we can find $g(x)$ by the Euclidean algorithm.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

An example

Find the generator polynomial for the smallest cyclic code containing the word 101100 ($n = 6$).

- We want $\gcd(1 + x^2 + x^3, 1 + x^6)$.
- Forming the remainder sequence,

$$\begin{aligned} x^6 + 1 &= (x^3 + x^2 + x)(x^3 + x^2 + 1) + (x^2 + x + 1) \\ x^3 + x^2 + 1 &= (x)(x^2 + x + 1) + x + 1 \\ x^2 + x + 1 &= (x)(x + 1) + 1. \end{aligned}$$

- Hence $\gcd(1 + x^2 + x^3, 1 + x^6) = 1$ (we say the polynomials are *relatively prime*).
- It follows that $g = 1$, so $C = \mathbb{F}_2^6$ is the "trivial" code consisting of all words of length 6.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Example, concluded

We can also see the last statement here as follows.

- If C is cyclic, then all the cyclic shifts of $u = 101100$ must also be in C.
- In particular, these words are all in C:

$$u = 101100, u + \pi(u) = 111010, u + \pi^2(u) = 100111,$$

  and

$$\pi^3(u + \pi^2(u)) = 111100.$$

- Hence $111010 + 111100 = 000110 \in C$
- Hence $\pi^5(000110) = 001100 \in C$
- So, finally, $u + 001100 = 100000 \in C$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Generator matrices for cyclic codes

Today we will continue our study of cyclic codes by considering

- generator matrices for these codes,
- parity-check matrices for these codes,
- how to construct all cyclic codes of a given block length n.

Notes

Generator matrices

From our theorem at the end of class yesterday, we know that if g is a generator polynomial for a cyclic code C, and $\deg(g) = n - k$ then

$$\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$$

is a basis for C. This gives a way to write down a generator matrix for C immediately – we simply take the vector of coefficients of g, make that the first row in G, then shift the first row to get the other rows.

Notes

Generator matrix example

Let C be the cyclic code with block length $n = 7$ and generator polynomial $g(x) = x^3 + x^2 + 1$ (check

$$x^7 + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)(x + 1),$$

so that $g(x)|(x^7 + 1)$. Then

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(Note $k = 4$ since $n = 7$ and $\deg(g) = 3$. Also, note how the first row determines the rest of the matrix – we don't actually need the whole matrix in this case!)

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Parity-check matrices

- H for a cyclic code can be constructed by the method we discussed last week (Algorithm 2.5.7).
- However, that method does not use the fact that the code is cyclic, so it does not show an important pattern.
- By results from yesterday, $w(x)$ represents a codeword of C with generator $g(x)$ if and only if $g(x)|w(x)$.
- Compute $r_i = x^i \bmod g(x)$ for $i = 0, \ldots, n-1$ and put the vectors of coefficients of r_i as rows in an $n \times n-k$ matrix H.
- Then $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ is a codeword if and only if $(a_0, \ldots, a_{n-1})H = 0$. It follows that H is a parity-check matrix for C.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Parity-check matrix example

Let C be the cyclic code from before with $g(x) = 1 + x^2 + x^3$ and $n = 7$.

- We compute

$$\begin{aligned}
1 \bmod g(x) &= 1, \\
x \bmod g(x) &= x, \\
x^2 \bmod g(x) &= x^2, \\
x^3 \bmod g(x) &= x^2 + 1, \\
x^4 \bmod g(x) &= x^2 + x + 1, \\
x^5 \bmod g(x) &= x + 1, \\
x^6 \bmod g(x) &= x^2 + x.
\end{aligned}$$

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

- Hence as on the last slide:

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

- Does this matrix look familiar (perhaps after permuting the rows)??

Comments on this example

- Note that the 7 rows of the matrix H are all the nonzero vectors of length $n - k = 3$.
- Hence, this cyclic code is a *Hamming* $[7, 4, 3]$ code.
- The codeword entries are ordered differently than we saw before, though.
- In general, two codes C and C' are said to be *equivalent* if there is some fixed permutation $\sigma \in S_n$ that gives a 1-1 correspondence between words in C and words in C'.
- Equivalent codes have the same n, k, d, so they are in effect equivalent for most coding-theoretic purposes.

Notes

Finding all cyclic codes of length n

Now we turn to the problem of determining all cyclic codes of a given length. Equivalently, we need to understand the factorization of $x^n + 1$ in $\mathbb{F}_2[x]$, since a generator polynomial must be a divisor of $x^n + 1$.

With $g(x) = 1$, we obtain the code containing all words in $\mathbb{F}_2^n$. On the other hand, if $g(x) = 0$, then we obtain the code containing only the zero word. Both of these are cyclic codes, but rather *uninteresting ones*(!) We will say a cyclic code is *proper* if it is *not* one of these.

Notes

Finding cyclic codes by factorization

- Over $\mathbb{F}_2$, since $2 = 0$, we have the "first year student's dream" factorization $a^2 + b^2 = (a + b)^2$.
- Hence if $n = 2^r s$, where s is odd, then

$$1 + x^{2^r s} = 1^{2^r} + (x^s)^{2^r} = (1 + x^s)^{2^r},$$

  and all the *interesting stuff* is going to come from the factorization of $1 + x^s$ in $\mathbb{F}_2[x]$.

- Proposition

  If $n = 2^r s$ with s odd, and $1 + x^s$ has z irreducible factors, then there are $(2^r + 1)^z$ cyclic codes of length n.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Example: $n = 10$

- We have $10 = 2 \cdot 5$, so in our general formula, $r = 1$ and $s = 5$.
- The polynomial $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$ and we can see the second factor is *irreducible* – it has no roots in $\mathbb{F}_2$, so no linear factors, and $(x^2+ax+1)(x^2+bx+1) = x^4+(a+b)x^3+abx^2+(a+b)x+1$ so $a = b = 1$ from coefficient of x^2 – but this does not work.
- Hence there are $3^2 = 9$ factors:
- Write $p = x + 1$, $q = x^4 + x^3 + x^2 + x + 1$. Then the factors are $1, p, p^2, q, pq, p^2q, q^2, pq^2, p^2q^2$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Another method – idempotents

- We will conclude today's lecture by discussing another method for finding all cyclic codes of length n. For simplicity now we restrict to the case n *odd*.
- Main reason for this is a connection with our next topic (general finite fields), but this method is also somewhat simpler than factorization of $x^n + 1$.

- Theorem
  Every cyclic code contains a unique **idempotent** *polynomial* $I(x)$ *satisfying* $(I(x))^2 \equiv I(x) \bmod x^n + 1$. $I(x)$ *generates the code.*

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Proof of the theorem

Proof:

- Let $g(x)$ be the generator polynomial and let $g(x)h(x) = x^n + 1$. Then $\gcd(g(x), h(x)) = 1$ (this is where the hypothesis n odd is used).
- By the facts about polynomial ideals and the Euclidean algorithm, there exist $A(x), B(x)$ such that $A(x)g(x) + B(x)h(x) = 1$.
- Multiply by $A(x)g(x)$: $(A(x)g(x))^2 + A(x)B(x)(x^n + 1) = A(x)g(x)$.
- This implies $(A(x)g(x))^2 \equiv A(x)g(x) \bmod x^n + 1$. So we take $I(x) = A(x)g(x)$.
- $I(x)$ generates C since $\gcd(I(x), x^n + 1) = g(x)$. $\square$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Properties of idempotents

- If I, J are idempotents, then so are $I + J$ (by the "first-year student's dream") and IJ.
- Let $C_j = \{2^i j \bmod n \mid i \in \mathbb{Z}\}$ (called the *cyclotomic coset* of j mod n),
- Then C_j is finite (e.g. C_3 for $n = 7$ is $C_3 = \{3, 6, 5\}$).
- The polynomial $I_j = \sum_{k \in C_j} x^k$ is idempotent. (Example: $(x^3 + x^6 + x^5)^2 = x^6 + x^{12} + x^{10} \equiv x^6 + x^5 + x^3 \bmod x^7 + 1$.)
- Hence we can construct an idempotent for each cyclotomic coset mod n, then take linear combinations. Fact: These are all the idempotents, hence all the cyclic codes of length n.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

An example

Question: What are all the cyclic codes of length $n = 21$?

- The distinct cyclotomic cosets mod 21 are

$$
\begin{aligned}
C_0 &= \{0\} \\
C_1 &= \{1, 2, 4, 8, 16, 11\} (= C_2 = \cdots = C_{11}) \\
C_3 &= \{3, 6, 12\} \\
C_5 &= \{5, 10, 20, 19, 17, 13\} \\
C_7 &= \{7, 14\} \\
C_9 &= \{9, 18, 15\}
\end{aligned}
$$

- Corresponding idempotents: $I_0 = 1$, $I_1 = x + x^2 + x^4 + x^8 + x^{16} + x^{11}$, etc.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Example, concluded

- Then, any linear combination

$$I = a_0 I_0 + a_1 I_1 + a_3 I_3 + a_5 I_5 + a_7 I_7 + a_9 I_9$$

  with $a_i \in \mathbb{F}_2$ is also an idempotent.
- The generator polynomials for the corresponding cyclic codes can be found by computing $\gcd(I(x), x^{21} + 1)$.
- For instance, the code with $I(x) = I_1(x) + I_9(x)$ has

$$g(x) = x^{17} + x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^3 + x + 1.$$

  (The actual computations are somewhat tedious, though, so we will stop here!)

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Introduction

So far, we have only considered the finite field $\mathbb{F}_2$ and studied codes over $\mathbb{F}_2$. The next steps we will take involve:

- Using the algebra larger finite fields $\mathbb{F}_{2^r}$ to construct "designer" cyclic codes with minimum distance as large as we like.
- Using the larger finite fields themselves as alphabets for codes. The main examples we will study here are the *Reed-Solomon codes*, a very important family with interesting properties and many practical applications.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Irreducible polynomials

- Irreducible polynomials are analogous to primes in $\mathbb{Z}$.

- Definition
  A nonconstant polynomial $h(x) \in \mathbb{F}_2[x]$ is said to be **irreducible** *in $\mathbb{F}_2[x]$ if the only divisors of $h(x)$ in $\mathbb{F}_2[x]$ are 1 and $h(x)$ itself.*
  - The definition above needs to be modified slightly if the coefficient field of the polynomials includes nonzero scalars other than 1 – in that case, the nonzero constants are also allowed as divisors (as are the nonzero constants times $h(x)$).
  - Fact: $\mathbb{F}_2[x]$ contains irreducible polynomials of all degrees $r \geq 1$ (see this week's Discussions).

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Examples of irreducibles

- degree 1: $x + 1$
- degree 2: $x^2 + x + 1$
- degree 3: $x^3 + x + 1$, $x^3 + x^2 + 1$
- degree 4: $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$
- degree 5: six of them
- There are rather extensive tables of these in the literature.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Residues modulo a polynomial

- The remainders modulo a polynomial $h(x)$ have natural sum and product operations coming from the sum and product on polynomials
- Sum: $(a(x) \bmod h(x)) + (b(x) \bmod h(x)) = (a(x) + b(x)) \bmod h(x)$.
- Product: $(a(x) \bmod h(x))(b(x) \bmod h(x)) = (a(x)b(x)) \bmod h(x)$.
- For *all* $h(x)$, the corresponding remainders ("residue classes") form a commutative ring with identity, called $\mathbb{F}_2[x]/\langle h(x)\rangle$.
- If $h(x)$ is *not irreducible*, though, this ring will not be a field, because it has *zero divisors*. If $h(x) = a(x)b(x)$ with neither constant, then $(a(x)b(x)) \bmod h(x) = 0$ but $a(x) \not\equiv 0 \bmod h(x)$ and $b(x) \not\equiv 0 \bmod h(x)$.

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Fields from irreducible polynomials

Theorem

Let $h(x) \in \mathbb{F}_2[x]$ be irreducible. Then the residue class ring $\mathbb{F}_2[x]/\langle h(x)\rangle$ is a field. If $\deg(h(x)) = r$, then

$$|\mathbb{F}_2[x]/\langle h(x)\rangle| = 2^r.$$

This will be clear in the examples we use, so we omit the complete proof. The claim about the order of the field follows by counting the possible remainders on division by $h(x)$:

$$a_0 + a_1 x + \cdots + a_{r-1}x^{r-1}.$$

There are 2^r such since $a_i \in \mathbb{F}_2$ all i.

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

An example – a field with 8 elements

Let $h(x) = x^3 + x + 1$, which is one of the irreducibles of degree 3 in $\mathbb{F}_2[x]$. By the theorem, $\mathbb{F} = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$ is a field with 8 elements. Let us describe its structure by giving addition and multiplication tables. The 8 elements of $\mathbb{F}$ are

$$\mathbb{F} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

The sum operation is easy (just add coefficients mod 2). For instance:

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

The full table is given on the next slide.

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

The addition table

For typographical reasons, we write $a = x^2 + x$, $b = x^2 + x + 1$ to save space!

$+$	0	1	x	$x+1$	x^2	x^2+1	a	b
0	0	1	x	$x+1$	x^2	x^2+1	a	b
1	1	0	$x+1$	x	x^2+1	x^2	b	a
x	x	$x+1$	0	1	a	b	x^2	x^2+1
$x+1$	$x+1$	x	1	0	b	a	x^2+1	x^2
x^2	x^2	x^2+1	a	b	0	1	x	$x+1$
x^2+1	x^2+1	x^2	b	a	1	0	$x+1$	x
a	a	b	x^2	x^2+1	x	$x+1$	0	1
b	b	a	x^2+1	x^2	$x+1$	x	1	0

Notes

An observation

Before we write the multiplication table, let us notice one important pattern about the multiplication operation. Let's take powers of x mod $x^3 + x + 1$ and see what happens:

$$\begin{aligned}
1 \bmod h(x) &= 1, \\
x \bmod h(x) &= x, \\
x^2 \bmod h(x) &= x^2, \\
x^3 \bmod h(x) &= x + 1, \\
x^4 \bmod h(x) &= x^2 + x, \\
x^5 \bmod h(x) &= x^2 + x + 1, \\
x^6 \bmod h(x) &= x^2 + 1, \\
x^7 \bmod h(x) &= 1.
\end{aligned}$$

Notes

Observation, continued

Note what happened here – the powers of x give all the nonzero elements of $\mathbb{F}$.

- This means that the multiplicative group of $\mathbb{F}$ is cyclic, generated by x.
- x is called a *primitive element* of $\mathbb{F}$.
- This says, among other things, that the multiplication table will be easy to write out if we represent each nonzero element as a power of x(!)

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

The multiplication table

Notes

Using the observation,

$\cdot$	0	1	x	x^2	x^3	x^4	x^5	x^6
0	0	0	0	0	0	0	0	0
1	0	1	x	x^2	x^3	x^4	x^5	x^6
x	0	x	x^2	x^3	x^4	x^5	x^6	1
x^2	0	x^2	x^3	x^4	x^5	x^6	1	x
x^3	0	x^3	x^4	x^5	x^6	1	x	x^2
x^4	0	x^4	x^5	x^6	1	x	x^2	x^3
x^5	0	x^5	x^6	1	x	x^2	x^3	x^4
x^6	0	x^6	1	x	x^2	x^3	x^4	x^5

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

The "big theorem" on finite fields

Notes

Theorem

- *There are fields of all orders 2^r, $r \geq 1$.*
- *Every finite field of order 2^r has primitive elements ($\phi(2^r - 1)$ of them, in fact – Euler ϕ-function).*
- *Every nonzero element of a field of order 2^r satisfies the polynomial equation $z^{2^r-1} + 1 = 0$.*
- *Any two fields of order 2^r are* **isomorphic***, so we will write $\mathbb{F}_{2^r}$ to denote the field of order 2^r.*
- *$\mathbb{F}_{2^r} \subset \mathbb{F}_{2^s}$ if and only if $r|s$.*

An example

The proof is not especially difficult, but it would take us too far afield, so we omit it. Instead, we illustrate what it is saying by considering fields of size $16 = 2^4$. Let us start by using the irreducible $h(x) = x^4 + x + 1$ to construct the field. The elements are the remainders on division by $h(x)$, so

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

for all choices of $a_i \in \mathbb{F}_2$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

x is primitive

Compute the powers of x mod $h(x)$:

$$\begin{aligned}
1 &\equiv 1 \bmod h(x) & x^8 &\equiv x^2 + 1 \bmod h(x) \\
x &\equiv x \bmod h(x) & x^9 &\equiv x^3 + x \bmod h(x) \\
x^2 &\equiv x^2 \bmod h(x) & x^{10} &\equiv x^2 + x + 1 \bmod h(x) \\
x^3 &\equiv x^3 \bmod h(x) & x^{11} &\equiv x^3 + x^2 + x \bmod h(x) \\
x^4 &\equiv x + 1 \bmod h(x) & x^{12} &\equiv x^3 + x^2 + x + 1 \bmod h(x) \\
x^5 &\equiv x^2 + x \bmod h(x) & x^{13} &\equiv x^3 + x^2 + 1 \bmod h(x) \\
x^6 &\equiv x^3 + x^2 \bmod h(x) & x^{14} &\equiv x^3 + 1 \bmod h(x) \\
x^7 &\equiv x^3 + x + 1 \bmod h(x) & x^{15} &\equiv 1 \bmod h(x).
\end{aligned}$$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

The polynomial $z^{15} + 1$

- The previous computation shows x is primitive and $x^{15} = 1$, so $x^{15} + 1 = 0$.
- Since every nonzero element of the field is a power of x, this means that every nonzero element of the field also satisfies the polynomial equation $z^{15} + 1 = 0$.
- If we *factor* $z^{15} + 1$ in $\mathbb{F}_2[z]$, we see something interesting:

$$z^{15}+1 = (z+1)(z^2+z+1)(z^4+z^3+z^2+z+1)(z^4+z+1)(z^4+z^3+1).$$

- That is, the factors are all the irreducibles of degree $1, 2, 4$ (the divisors of 4).
- This fact actually implies the last two parts of the theorem as well.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Example, continued

- $\mathbb{F}_{2^4}$ contains roots of $z^4 + z^3 + 1$ and $z^4 + z^3 + z^2 + z + 1$ as well. We would actually have obtained an isomorphic field starting from any one of the three irreducibles of degree 4.
- The factors $z + 1$ and $z^2 + z + 1$ have roots $1 \in \mathbb{F}_2$, and the elements of $\mathbb{F}_{2^2}$ not contained in $\mathbb{F}_2$, respectively. Hence we have "copies" of $\mathbb{F}_2, \mathbb{F}_{2^2}$ sitting as subfields of $\mathbb{F}_{2^4}$.
- **Caution:** It is *not always the case* that a root of an irreducible $h(x)$ of degree r is *primitive* for the field $\mathbb{F}_{2^r}$. The roots of the degree 4 polynomial $z^4 + z^3 + z^2 + z + 1$ are 5th roots of unity (so not *primitive* 15th roots of 1).

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Minimal polynomial of an element

- We will need the following notion.

- Definition
  Let $\alpha \in \mathbb{F}_{2^r}$. The **minimal polynomial** *of α over $\mathbb{F}_2$ is the nonzero polynomial of smallest degree in $\mathbb{F}_2[z]$ having α as a root.*

- Proposition
  The minimal polynomial of an element α is an irreducible polynomial in $\mathbb{F}_2[x]$.
  - **Proof:** If $m(z) = f(z)g(z)$ and $m(\alpha) = 0$, then either $f(\alpha) = 0$ or $g(\alpha) = 0$. $\square$

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Example

In $\mathbb{F}_{2^4}$ constructed with $h(x) = x^4 + x + 1$ as above:

- The element 1 has minimal polynomial $z + 1$
- The elements x^5, x^{10} have minimal polynomial $z^2 + z + 1$
- The elements x, x^2, x^4, x^8 have minimal polynomial $z^4 + z + 1$
- The elements $x^7, x^{14}, x^{13}, x^{11}$ have minimal polynomial $z^4 + z^3 + 1$
- The elements x^3, x^6, x^{12}, x^9 have minimal polynomial $z^4 + z^3 + z^2 + z + 1$

Notes

Example, concluded

For instance, if $z = x^7 = x^3 + x + 1$ (from before), then

$$z^4 + z^3 + 1 = x^{13} + x^6 + 1 = (x^3 + x^2 + 1) + (x^3 + x^2) + 1 = 0.$$

The other roots of this irreducible $z^4 + z^3 + 1$ come from a *cyclotomic coset* mod 15 as we discussed yesterday!
$C_7 = \{7, 14, 13, 11\}$. Can you see why?

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Introduction – BCH codes

It is possible to make cyclic codes with any d provided n is large enough. We will see one construction today, the so-called BCH codes. The name comes from the names of the original developers of these codes – Bose, Chaudhuri, and Hocquenghem.

To "warm up" for the BCH codes, we return to the cyclic Hamming code we saw a couple of days ago.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Hamming codes

Theorem

Let $h(x)$ be a primitive irreducible polynomial of degree r (that is, the roots of $h(x)$ are primitive elements of the field $\mathbb{F}_{2^r} = \mathbb{F}_2[x]/\langle h(x)\rangle$). Then the cyclic code C of length $n = 2^r - 1$ with **generator polynomial** *$h(x)$ is a $[2^r - 1, 2^r - r - 1, 3]$ Hamming code.*

Proof: Write $\alpha = x$ in the field $\mathbb{F}_{2^r}$. The powers of α give all the nonzero elements of the field.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Proof, continued

$u(x)$ is a codeword if and only if $h(x)|u(x)$, which is true if and only if $u(\alpha) = 0$. So if we write $u = u_0 + u_1 x + \cdots + u_{2^r-2}x^{2^r-2}$, then

$$(u_0 \ u_1 \ \ldots \ u_{2^r-2}) \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{2^r-2} \end{pmatrix} = 0.$$

Rewrite the entries in the column using the expansions of α^i in terms of $1, x, \ldots, x^{r-1}$. The resulting $2^r - 1 \times r$ matrix is a parity check matrix for C, and its rows are all the nonzero vectors of length r in some order. $\square$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Generalizing to get larger d

- We will present a construction of BCH codes with minimum distance $d \geq 5$ (actually $= 5$ with a bit more work), length $n = 2^r - 1$ and $k = 2^r - 2r - 1$. You will see how to get $d \geq \delta$ for any $\delta = 2t + 1$ in the Discussion today.
- Let α be a primitive element of $\mathbb{F}_{2^r}$, let $m_1(x)$ be the minimal polynomial of α, and let $m_3(x)$ be the minimal polynomial of α^3.
- Let $g(x) = m_1(x)m_3(x)$ be the generator polynomial for a cyclic code of length $n = 2^r - 1$.
- We claim that C has $d \geq 5$.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Some first observations

- First, note that the roots of $m_1(x)$ contain $\alpha, \alpha^2, \alpha^4$ (powers contained in the cyclotomic coset C_1). Hence the roots of $g(x)$ contain $\alpha, \alpha^2, \alpha^3, \alpha^4$ (a consecutive string of 4 powers of α).
- Hence the polynomial form of every codeword of C has roots containing the consecutive string $\alpha, \alpha^2, \alpha^3, \alpha^4$.
- This means that each codeword $u = (u_0\ u_1\ \cdots\ u_{2^r-2})$ satisfies the equation $u\tilde{H} = 0$ where $\tilde{H}$ is the $(2^r - 1) \times 4$ matrix over $\mathbb{F}_{2^r}$ on the next page.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

The matrix $\tilde{H}$

$$\tilde{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^2 & (\alpha^2)^2 & (\alpha^3)^2 & (\alpha^4)^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{2^r-2} & (\alpha^2)^{2^r-2} & (\alpha^3)^{2^r-2} & (\alpha^4)^{2^r-2} \end{pmatrix}$$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

More on the matrix $\tilde{H}$

- $\tilde{H}$ is *not* a parity-check matrix according to our definitions (entries not in $\mathbb{F}_2$, and if we replace each α^i by a vector in $\mathbb{F}_2^r$, the columns will be linearly dependent).
- But, the characterization of d in terms of linearly independent sets of the rows extends to this case.

- Proposition

  If all sets of 4 rows of $\tilde{H}$ are linearly independent over $\mathbb{F}_{2^r}$, then $d \geq 5$.

  - **Proof:** If $d \leq 4$, then there is some codeword of weight 4, which gives a linear dependence on a set of 4 rows in $\tilde{H}$. $\square$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

A special determinant

Notes

So consider the determinant of the 4×4 submatrix of $\tilde{H}$ in rows $1 \leq i < j < \ell < m \leq 2^r - 1$:

$$\det \begin{pmatrix} \alpha^i & (\alpha^2)^i & (\alpha^3)^i & (\alpha^4)^i \\ \alpha^j & (\alpha^2)^j & (\alpha^3)^j & (\alpha^4)^j \\ \alpha^\ell & (\alpha^2)^\ell & (\alpha^3)^\ell & (\alpha^4)^\ell \\ \alpha^m & (\alpha^2)^m & (\alpha^3)^m & (\alpha^4)^m \end{pmatrix}$$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Special determinant, continued

Notes

Using standard properties of determinants, we can factor α^i out of row 1, α^j out of row 2, etc. leaving

$$= \alpha^{i+j+\ell+m} \det \begin{pmatrix} 1 & \alpha^i & (\alpha^i)^2 & (\alpha^i)^3 \\ 1 & \alpha^j & (\alpha^j)^2 & (\alpha^j)^3 \\ 1 & \alpha^\ell & (\alpha^\ell)^2 & (\alpha^\ell)^3 \\ 1 & \alpha^m & (\alpha^m)^2 & (\alpha^m)^3 \end{pmatrix}$$

Special determinant, continued

- We see that this is a 4×4 Vandermonde matrix (possibly transpose, depending on how you define Vandermondes).
- General form is

$$V(a,b,c,d) = \det \begin{pmatrix} 1 & a & a^2 & a^3 \\ 1 & b & b^2 & b^3 \\ 1 & c & c^2 & c^3 \\ 1 & d & d^2 & d^3 \end{pmatrix}$$

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

The Vandermonde determinant

- We claim $V(a,b,c,d) = (b-a)(c-a)(d-a)(c-b)(d-b)(d-c)$ (for a,b,c,d in any field $\mathbb{F}$)
- Note that if $a = b$, etc. then the matrix has two equal rows, so the determinant is divisible by the product of the pairwise differences.
- The total degree is 6, so our formula for $V(a,b,c,d)$ is correct up to a constant factor.
- The coefficient of d^3c^2b is $+1$ in $V(a,b,c,d)$ and in the claimed formula.
- Hence the claim is proved.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Consequences

- The determinant of our Vandermonde matrix is *nonzero* because $\alpha^i, \alpha^j, \alpha^\ell, \alpha^m$ are distinct elements of $\mathbb{F}_{2^r}$.
- It follows that our code has $d \geq 5$.
- What about k, the dimension?

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

The dimension of the BCH code

- Going back to the definition of $\tilde{H}$, recall that the second and fourth columns come because we know other roots of the polynomial $m_1(x)$.
- So in fact we really only need the columns for α and α^3.
- If those are converted to binary vectors, we get a $(2^r - 1) \times 2r$ matrix whose columns are linearly independent.
- Hence, $k = 2^r - 2r - 1$.
- Finally, we see that $r \geq 4$ is necessary to get a code of dimension > 1 here.

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Notes

Cyclic Codes – Polynomial Algebra More on cyclic codes Finite fields BCH codes – "designer cyclic codes"

Summary

Modulo some details, we have proved the following.

Theorem

Let $r \geq 4$. There is a 2 bit error correcting BCH code of length $n = 2^r - 1$ and $k = 2^r - 2r - 1$ with $d = 5$ and generator polynomial $g(x) = m_1(x)m_3(x)$.

For instance, with $r = 5$, we get a $[31, 21, 5]$ code over $\mathbb{F}_2$. (This is the best possible d for $n = 31$, $k = 21$ over $\mathbb{F}_2$.)
A simple algebraic decoding method for these codes is given in §5.5 in the text.

Notes