Review/Outline

Review:

Check matrix criterion for min dist
Vandermonde matrices
Reed-Solomon codes
(correct multiple errors, growing alphabet)
Basic computations in finite fields
Hamming codes
(correct single errors, fixed alphabet)

Bose-Chaudhuri-Hocquengham (BCH) codes
(correct multiple errors, fixed alphabet)

All these codes grow worse with size

Example: irreducible cubics over $\mathbf{F}_p$

Frobenius automorphisms

Other roots of equations
Equation satisfied by field element

BCH codes

BCH codes use variant check matrices and ideas from Hamming and Reed-Solomon codes. BCH codes keep a *fixed* alphabet, and correct *many* errors.

Unfortunately, BCH codes have the same shortcoming as Hamming and RS codes: as block size increases, they become worse and worse: relative error correction goes to 0 and/or information rate goes to 0.

Start with a finite field $\mathbf{F}_q$, often $q = 2$. Choose block size relatively prime to q.

Make check matrices over *larger* fields but keep the code alphabet itself *fixed*, to make multiple-error-correcting codes.

This trick is an example of taking a **subfield subcode**.

Variant check matrix (again):

Let α be a primitive element in $\mathbf{F}_{q^m}$. For simplicity, take

$$\text{block length } = n = q^m - 1$$

For **design distance** an integer t with $t < n = q^m - 1$ the matrix $H =$

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^{n-1})^2 \\ 1 & \alpha^3 & (\alpha^2)^3 & \dots & (\alpha^{n-1})^3 \\ & & & \dots & \\ 1 & \alpha^{t-2} & (\alpha^2)^{t-2} & \dots & (\alpha^{n-1})^{t-2} \\ 1 & \alpha^{t-1} & (\alpha^2)^{t-1} & \dots & (\alpha^{n-1})^{t-1} \end{pmatrix}$$

has the property that the $(t-1)$-by-$(t-1)$ matrix formed from any $t-1$ columns has non-zero (Vandermonde) determinant.

Remark: We will first do some examples in an *impractical* but obvious manner. We will refine the method a little later.

Example: We want a binary code (alphabet $\mathbf{F}_2$) with block size $n = 2^3 - 1 = 7$. (So $m = 3$ in notation above). What design distance t will give something worthwhile?

We must have $t < n = 7$. To make a binary code that corrects any 2 errors, we have to take $t = 5$. To specify a primitive element α in $\mathbf{F}_{2^3}$ we describe $\mathbf{F}_{2^3}$ as

$$\mathbf{F}_{2^3} = \mathbf{F}_2[x]/P$$

for irreducible cubic polynomial

$$P(x) = x^3 + x + 1$$

and verify that a primitive root is

$$\alpha = x\text{-mod-}P(x)$$

The check matrix is

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^6 \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^2)^6 \\ 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^6 \\ 1 & \alpha^4 & (\alpha^4)^2 & \dots & (\alpha^4)^6 \end{pmatrix}$$

The polynomial $x^n - 1 = x^7 - 1$ factors as

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

(by trial-and-error). By testing, all three irreducible factors are primitive. (We used one of them to define $\mathbf{F}_{2^3}$.) The α, α^2, and $\alpha^4 = (\alpha^2)^2$ are obtained by applying the Frobenius automorphism to α, so these are all the roots of $x^3 + x + 1 = 0$. The α^3 cannot be obtained in this manner, yet is not simply 1 (α is primitive), so must be a zero of the other factor $x^3 + x^2 + 1$ of $x^7 - 1$. Thus, the generating polynomial for this code is the product

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

A generating matrix is

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

Remark: Too bad: a majority-logic repetition code: send each bit 7 times. So actually the minimum distance is 7, larger than the design distance $t = 5$. But repetition codes are not good: *we were asking too much to demand that a length 7 code correct 2 errors.*

Example: We want a binary code (alphabet $\mathbf{F}_2$) with block size $n = 2^3 - 1 = 7$. (So $m = 3$ in notation above). Try (smaller) design distance $t = 3$, to correct single errors.

To specify primitive α in $\mathbf{F}_{2^3}$ describe $\mathbf{F}_{2^3}$ as

$$\mathbf{F}_{2^3} = \mathbf{F}_2[x]/P$$

for irreducible cubic

$$P(x) = x^3 + x + 1$$

and verify that

$$\alpha = x\text{-mod-}P(x)$$

is primitive. The check matrix is

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^6 \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^2)^6 \end{pmatrix}$$

The polynomial $x^n - 1 = x^7 - 1$ factors into irreducibles

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

(trial-and-error). By testing, all three factors are primitive. The $\alpha, \alpha^2, \alpha^4 = (\alpha^2)^2, \ldots$ are obtained by applying the Frobenius automorphism to α, so this list contains all the roots of $x^3 + x + 1 = 0$. Since this has just 3 roots, they must be $\alpha, \alpha^2, \alpha^4$. Thus, the generating polynomial for this code is the polynomial

$$g(x) = x^3 + x + 1$$

since the cubic equation $g(x) = 0$ has the elements of the second column, α and α^2, as roots. Then the a generating matrix is (coefficients in ascending order)

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

Remark: Better! A binary $[7, 4]$ code. We suspect that it is a recast form of the Hamming $[7, 4]$ code.

Example: Try again to correct 2 errors. Enlarge block size to $n = 2^4 - 1 = 15$. Take designed distance $t = 5$. To specify a primitive element α in $\mathbf{F}_{2^4}$ describe $\mathbf{F}_{2^4}$ as

$$\mathbf{F}_{2^4} = \mathbf{F}_2[x]/P$$

with primitive (check!) quartic

$$P(x) = x^4 + x + 1$$

and put

$$\alpha = x\text{-mod-}P(x)$$

The check matrix is $H =$

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{14} \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^2)^{14} \\ 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{14} \\ 1 & \alpha^4 & (\alpha^4)^2 & \dots & (\alpha^4)^{14} \end{pmatrix}$$

The polynomial $x^n - 1 = x^{15} - 1$ factors as

$$x^{15} - 1 = (x-1)(x^2 + x + 1)\times$$

$$\times(x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)$$

(trial and error). By testing, only the last two polynomials are primitive.

So identify which among

$$(x-1),\ (x^2+x+1),\ (x^4+x^3+x^2+x+1),$$

$$(x^4+x+1),\ (x^4+x^3+1)$$

are needed to have equations with $\alpha, \alpha^2, \alpha^3, \alpha^4$ as roots. Since $q = 2$, the image α^2 of α under the Frobenius map is the next power of α in the sequence, and $\alpha^4 = (\alpha^2)^2$. To have α^3 be a root we need another polynomial.

Try to be lucky: Since $\alpha^{15} = 1$, $(\alpha^3)^5 = 1$, so α^3 is a root of $x^5 = 1$, but this is not irreducible. From

$$x^5 - 1 = (x^4+x^3+x^2+x+1)(x+1)$$

and $\alpha^3 \neq 1$ (since α is primitive)

$$\alpha^4+\alpha^3+\alpha^2+\alpha+1 = 0$$

Thus, the generating polynomial is the product of x^4+x+1 and $x^4+x^3+x^2+x+1$, namely

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

$$= x^8 + x^4 + x^2 + x + 1$$

giving generating matrix (in ascending degree)

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

This is a *binary* $[15, 7]$-code and has minimum distance at least 5, by construction, so can correct any 2 errors.

Remark: It was not easy to predict that the code would be $[15, 7]$. As the check matrix had only 4 rows and had block size 15, we might have thought the code would have dimension $15 - 4 = 11$. The difference is accounted for (indirectly) by the fact that we restrict to a *binary* code, not with alphabet $\mathbf{F}_{16}$.

Algorithm to determine the dimension and estimate the minimum distance of BCH codes. *First version*

Apply the Frobenius automorphism $x \to x^p$ repeatedly to the rows of the initial check matrix H for the BCH code, making a larger check matrix, the *Frobenius-stable* check matrix (after all the different possibilities are included, but without repetition). The row rank of this Frobenius-stable check matrix is the 'true' row rank:

$$\text{dimension of BCH code}$$

$$= \text{length} - \text{ row rk Frob-stable chk mx}$$

A better estimate of minimum distance can be obtained from the Frobenius stable check matrix: *let t' be largest such that adjacent exponents $1, 2, 3, \ldots, t'-2, t'-1$ appear as exponents (of the primitive root) in the second column of the Frobenius-stable check matrix.*

Then the minimum distance is *at least t'*.

More efficiently, given the set of exponents (of the primitive root) in the second column of the usual check matrix for a length n BCH code using $GF(p^m)$ over $GF(p)$, to determine the set of such exponents in the Frobenius-stable version repeatedly multiply these exponents by p (reducing modulo $p^m - 1$).

Let r be the number of exponents in the Frobenius-stabilized set: then the actual dimension k of the code is $k = n - r$.

Remark: There is no need to write the whole rows of any check matrix, but only the list of exponents occurring in the second column.

Example: To determine dimension and estimate minimum distance of the BCH code of length 31 ($= 2^5 - 1$) constructed with designed distance $t = 7$ using the field extension $GF(2^5)$ of the finite field $GF(2)$, proceed as follows.

The initial set of exponents in the second column of the check matrix is $1, 2, 3, \ldots, 6$ (going up to $t - 1$). Repeatedly multiplying by 2 (applying the Frobenius) and reducing modulo $2^5 - 1 = 31$,

$$1, 2, 4, 8, 16, 32 = 1$$

$$3, 6, 12, 24, 48 = 17, 34 = 3$$

$$5, 10, 20, (40 =)9, 18, (36 =)5$$

Removing duplicates and reordering gives Frobenius-stable set

$$1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 17, 18, 20, 24$$

which has 14 elements. Thus, the row rank of the Frobenius-stable check matrix is 14, and the dimension of the BCH code is (with length 31)

$$\text{length - rk } H = 31 - 14 = 17$$

The largest t' so that adjacent exponents $1, 2, \ldots, t' - 1$ appear is 11. Thus, all we can say about actual minimum distance is that it is ≥ 7.

Example: To determine dimension and estimate minimum distance of the BCH code of length 26 constructed with designed distance $t = 9$ using the field extension $GF(3^3)$ of the finite field $GF(3)$, proceed as follows.

The initial set of exponents in the second column of the check matrix is $1, 2, 3, \ldots, 8$ (going up to $t - 1$). Repeatedly multiplying by 3 (applying the Frobenius) and reducing modulo $3^3 - 1$: all mod $3^3 - 1$

$$1, 3, 9, (27 =)1$$

$$2, 6, 18, (54 =)2$$

$$4, 12, (36 =)10, (30 =)4$$

$$5, 15, (45 =)19, (57 =)5$$

$$7, 21, (63 =)11, (33 =)7$$

$$8, 24, (72 =)20, (60 =)8$$

Removing duplicates and ordering gives Frobenius-stable set

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 18, 19, 20, 21, 24$$

which has 18 elements. Thus, the row rank of the Frobenius-stable check matrix is 18, and the dimension of the BCH code is (with length 26)

$$\text{length - rk } H = 26 - 18 = 8$$

The largest t' so that adjacent exponents $1, 2, \ldots, t' - 1$ appear is 13. Thus, the actual minimum distance is ≥ 13, not just 9.

Remark: No, we did *not* find a simple description of a generator polynomial for these cyclic codes. That is, the *complexity of description* has gone up.

Irreducible cubics over $\mathbf{F}_p$

In general it requires either patience or cleverness or both to factor polynomials in $\mathbf{F}_q[x]$ into irreducible polynomials.

However, the cases of *quadratic* and *cubic* polynomials $g(x)$ are more accessible, since trial division requires only that we look for *monic*, *linear* factors $x - \alpha$. And recall

Proposition: $x - \alpha$ divides a polynomial $g(x)$ if and only if α is a root of $g(x) = 0$.

Proof: By division

$$g(x) = q(x) \cdot (x - \alpha) + r$$

where the degree of the remainder r is less than the degree of the divisor $x - \alpha$, namely 1. Evaluate both sides at α to see

$$g(\alpha) = q(x) \cdot (\alpha - \alpha) + r = r$$

as desired. ///

If we take fields $\mathbf{F}_p$ with *prime* numbers of elements, which we can model as $\mathbf{Z}/p$, then these computations are elementary. Thus, we have

Theorem: Let p be prime. Let $g(x) \in \mathbf{F}_p[x]$ be quadratic or cubic. Then $g(x)$ is *irreducible* if and only if

$$g(t) \neq 0 \bmod p$$

for $t = 0, 1, 2, \ldots, p-2, p-1$.

Example: Test $g(x) = x^2 + x + 1$ for irreducibility in $\mathbf{F}_5[x]$. Evaluate

$$g(0) = 0^2 + 0 + 1 = 1 \neq 0 \bmod 5$$

$$g(1) = 1^2 + 1 + 1 = 3 \neq 0 \bmod 5$$

$$g(2) = 2^2 + 2 + 1 = 2 \neq 0 \bmod 5$$

$$g(3) = 3^2 + 3 + 1 = 3 \neq 0 \bmod 5$$

$$g(4) = 4^2 + 4 + 1 = 1 \neq 0 \bmod 5$$

Thus, by the criteria above, $x^2 + x + 1$ is irreducible in $\mathbf{F}_5[x]$.

Example: Test $g(x) = x^3 + x + 1$ for irreducibility in $\mathbf{F}_5[x]$. Evaluate

$$g(0) = 0^3 + 0 + 1 = 1 \neq 0 \bmod 5$$
$$g(1) = 1^3 + 1 + 1 = 3 \neq 0 \bmod 5$$
$$g(2) = 2^3 + 2 + 1 = 1 \neq 0 \bmod 5$$
$$g(3) = 3^3 + 3 + 1 = 1 \neq 0 \bmod 5$$
$$g(4) = 4^3 + 4 + 1 = 4 \neq 0 \bmod 5$$

Thus, by the criteria above, $x^3 + x + 1$ is irreducible in $\mathbf{F}_5[x]$.

Example: Test $g(x) = x^3 + x + 1$ for irreducibility in $\mathbf{F}_7[x]$. Evaluate

$$g(0) = 0^3 + 0 + 1 = 1 \neq 0 \bmod 7$$
$$g(1) = 1^3 + 1 + 1 = 3 \neq 0 \bmod 7$$
$$g(2) = 2^3 + 2 + 1 = 4 \neq 0 \bmod 7$$
$$g(3) = 3^3 + 3 + 1 = 3 \neq 0 \bmod 7$$
$$g(4) = 4^3 + 4 + 1 = 6 \neq 0 \bmod 7$$
$$g(5) = 5^3 + 5 + 1 = 5 \neq 0 \bmod 7$$
$$g(6) = 6^3 + 6 + 1 = 6 \neq 0 \bmod 7$$

Thus, by the criteria above, $x^3 + x + 1$ is irreducible in $\mathbf{F}_7[x]$.

Example: Test $g(x) = x^3 + x + 1$ for irreducibility in $\mathbf{F}_{11}[x]$. Evaluate

$$g(0) = 0^3 + 0 + 1 = 1 \neq 0 \bmod 11$$

$$g(1) = 1^3 + 1 + 1 = 3 \neq 0 \bmod 11$$

$$g(2) = 2^3 + 2 + 1 = 0 \bmod 11$$

Stop!

In $\mathbf{F}_{11}[x]$, the polynomial $x^3 + x + 1$ has a linear factor $x - 2$.

Indeed, divide through to obtain

$$x^3 + x + 1 = (x - 2) \cdot (x^2 + 2x + 5)$$

Finding other roots of equations

Part of the complexity of the BCH codes, or of using the *subfield subcode* stunt, is in understanding the other roots of a polynomial equation

$$g(x) = 0$$

with g an irreducible polynomial in $\mathbf{F}_p[x]$, given one root $\alpha \in \mathbf{F}_{p^m}$. The **Frobenius automorphism** gives an amazingly simple method for this, unlike the analogous question(s) for rational numbers:

Theorem: For an irreducible polynomial $g(x)$ in $\mathbf{F}_p[x]$ of degree d, given *one* root of $g(x) = 0$, the complete list of roots is

$$\alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{p^{d-1}}$$

Remark: For computational purposes, we might want α to be described as an element of $\mathbf{F}_p[x]/P(x)$ for some irreducible $P(x) \in \mathbf{F}_p[x]$. *One* choice is $P = g$, which makes things simple. But sometimes we are given a situation where $P \neq g$. This is ok.

Example: Model $\mathbf{F}_{2^3}$ as $\mathbf{F}_2[x]/(x^3+x+1)$, noting (trial division!) that $P(x) = x^3+x+1$ is irreducible in $\mathbf{F}_2[x]$. Let α be *one* root of $x^3+x+1=0$. Describe the other two roots *in terms of* α.

First, note that $\alpha = x$-mod-(x^3+x+1) really is a root of the equation

$$x^3+x+1=0$$

since for any polynomial multiple M of $P = x^3+x+1$

$$(x+MP)^3+(x+MP)+1$$

$$= x^3+3x^2MP+3x(MP)^2+(MP)^3+x+MP+1$$

$$= (x^3+x+1)+3x^2MP+3x(MP)^2+(MP)^3+MP$$

$$= (1+3x^2M+3xM^2P+M^3P^2+M)\cdot P$$

$$= 0 \bmod P$$

since the whole mess is a multiple of P, as ugly as that multiple may be. Yes, this α is a root of $x^3+x+1=0$.

So we *model* $\mathbf{F}_{2^3} = \mathbf{F}_8$ as polynomials reduced modulo $x^3 + x + 1$, and α is 'x' (thought of as modulo $x^3 + x + 1$).

So every element of $\mathbf{F}_{2^3} = \mathbf{F}_8$ is a polynomial in α of degree < 3.

Given *one* root α of $x^3 + x + 1 = 0$, since the coefficients are in the finite field $\mathbf{F}_q$ with $q = 2$, the other roots of a degree d equation (with irreducible polynomial) are

$$\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$$

which here with $q = 2$ and $d = 3$ gives additional roots

$$\alpha^2, \alpha^{2^2}$$

The first one of these is already reduced, so we do nothing to it. But we must reduce $\alpha^4 \sim x^4$ modulo $x^3 + x + 1$, obtaining $x^2 + x$, or $\alpha^2 + \alpha$. That is, the complete list of roots of

$$x^3 + x + 1 = 0$$

is

$$\alpha, \alpha^2, \alpha^2 + \alpha$$

Example: Model $\mathbf{F}_{5^3}$ as $\mathbf{F}_5[x]/(x^3+x+1)$, noting (trial division!) that $P(x) = x^3+x+1$ is irreducible in $\mathbf{F}_5[x]$. Let α be *one* root of $x^3+x+1=0$. Describe the other two roots *in terms of* α.

So $\mathbf{F}_{5^3} = \mathbf{F}_{125}$ is construed as polynomials reduced modulo x^3+x+1, and α is 'x' (thought of as modulo x^3+x+1). Every element of $\mathbf{F}_{5^3} = \mathbf{F}_{125}$ is a polynomial in α of degree < 3.

Given *one* root α of $x^3+x+1=0$, since the coefficients are in the finite field $\mathbf{F}_q$ with $q=5$, the other roots of a degree d equation (with irreducible polynomial) are

$$\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$$

which here with $q = 5$ and $d = 3$ gives additional roots

$$\alpha^5, \alpha^{5^2}$$

Reduce $\alpha^5 \sim x^5$ modulo x^3+x+1, obtaining

$$x^5 = (x^2+4)\cdot(x^3+x+1) + 4x^2 + x + 1$$

so the second root is

$$\alpha^5 = 4\alpha^2 + \alpha + 1$$

Before continuing: it is important to remember that by Fermat's Little Theorem for prime p and for any b

$$b^p = b \bmod p$$

Thus, to take the p^{th} power of a polynomial with coefficients in $\mathbf{F}_p$ just multiply all the exponents by p: with $a_i \in \mathbf{F}_p$

$$(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0)^p$$

$$= a_n x^{pn} + a_{n-1} x^{p(n-1)} + \ldots + a_2 x^{2p} + a_1 x^p + a_0$$

since, once again, all the middle binomial coefficients $\binom{p}{n}$ (meaning with $0 < n < p$ are divisible by p.

Then the third and last root of $x^3 + x + 1 = 0$ over $\mathbf{F}_5$ is

$$(\alpha^5)^5 = (4\alpha^2 + \alpha + 1)^5$$

$$= 4\alpha^{10} + \alpha^5 + 1$$

Reduce $4x^{10} + x^5 + 1$ modulo $x^3 + x + 1$: after a little work doing long division (mod 5)

$$(4x^{10} + x^5 + 1) \,\%\, (x^3 + x + 1) = x^2 + 3x + 4$$

So the complete list of roots of

$$x^3 + x + 1 = 0$$

is

$$\alpha,\ 4\alpha^2 + \alpha + 1,\ \alpha^2 + 3\alpha + 4$$

Remark: One might consider using fast modular exponentiation for some of this.