Review/Outline

Recall:
If all bunches of $d-1$ columns of a check matrix are linearly independent, then the minimum distance of the corresponding code is d.

Following this through as a counting argument gives the Gilbert-Varshamov bound.

Vandermonde determinants

Reed-Solomon (RS) codes

Making finite fields

Irreducible polynomials
Computational models of finite fields
Basic operations $\mathbf{F}_q$
Primitive elements/roots in $\mathbf{F}_q$

Vandermonde...

One type of **Vandermonde matrix** is

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & x_4 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 & \dots & x_n^2 \\ x_1^3 & x_2^3 & x_3^3 & x_4^3 & \dots & x_n^3 \\ x_1^4 & x_2^4 & x_3^4 & x_4^4 & \dots & x_n^4 \\ & & & \dots & & \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & x_4^{n-1} & \dots & x_n^{n-1} \end{pmatrix}$$

Amazing Theorem:

$$\det M = (-1)^{n(n-1)/2} \prod_{i<j} (x_i - x_j)$$

Corollary: If the x_i's lie somewhere such that a *product* of non-zero things is non-zero, and if $x_i \neq x_j$ for all $i < j$, then the Vandermonde determinant is non-zero.

Remark: Unfortunately, if we want to stay in the littlest finite field $\mathbf{F}_2$, we only have two distinct elements $0, 1$, so cannot make a big Vandermonde matrix with non-zero determinant.

Remark: In general the product of a bunch of non-zero things can be 0. For example, in $\mathbf{Z}/6$, neither $\overline{2}$ nor $\overline{3}$ is $\overline{0}$, but their product is $\overline{0}$.

Remark: In a **field**, by definition, every non-zero element has a multiplicative inverse. This prevents $ab = 0$ unless either a or b is 0. Indeed, if $ab = 0$ for non-zero a and b, then multiply both wides by a^{-1} to obtain

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$$

contradiction.

Variant check matrices

Keep in mind the theorem about Vandermonde determinants, and the aim of making every batch of $d-1$ columns of a check matrix linearly independent. Let $g(x)$ be a polynomial generating a cyclic code of length n with alphabet $\mathbf{F}_q$. (Assume for simplicity that $g(x)$ has no repeated factors.) Factor $g(x)$ into irreducible polynomials

$$g(x) = f_1(x) f_2(x) \dots f_\ell(x)$$

where each f_i has coefficients in $\mathbf{F}_q$. Let (!?) β_i be a root of the i^{th} irreducible factor f_i in a larger finite field $\mathbf{F}_{q^m}$.

Proposition:

$$H = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \beta_1^3 & \dots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \beta_2^3 & \dots & \beta_2^{n-1} \\ 1 & \beta_3 & \beta_3^2 & \beta_3^3 & \dots & \beta_3^{n-1} \\ & & \dots & & & \\ 1 & \beta_\ell & \beta_\ell^2 & \beta_\ell^3 & \dots & \beta_\ell^{n-1} \end{pmatrix}$$

is a check matrix for G.

Remark: This variant check matrix H has the property that pieces of it look like Vandermonde matrices. Good.

Remark: ... but without knowing anything further about the β_i's we cannot be sure that the powers $\beta_i^1, \beta_i^2, \ldots, \beta_i^{n-1}$ are distinct.

Remark: A downside to this construction is that the entries in the check matrix are in a possibly much larger finite field. But this is actually useful, as will be seen even more clearly with BCH codes.

Remark: The simplest family of codes constructed using these variant check matrices are the Reed-Solomon codes.

Description of RS codes

These form a family of *cyclic* codes which use larger and larger alphabets.

Let $\mathbf{F}_q$ be a finite field. If q is simply a prime number, then take $\mathbf{F}_q = \mathbf{Z}/p$. (Otherwise $\mathbf{Z}/q$ is not a field at all.)

The block length will be $n = q - 1$.

Let g be a *primitive root* in $\mathbf{F}_q$, so

$$1, \beta, \beta^2, \beta^3, \beta^4, \ldots, \beta^{q-3}, \beta^{q-2}$$

are distinct Choose **design distance** t. Take **generating polynomial**

$$g(x) = (x - \beta)(x - \beta^2) \ldots (x - \beta^{t-2})(x - \beta^{t-1})$$

for a cyclic code, a **Reed-Solomon code**.

Theorem: This code has minimum distance at least t. Length is $n = q - 1$, dimension is $q - t$, and a generator for the check matrix is

$$h(x) = \text{ coefficients-reversed version of}$$

$$(x - \beta^t)(x - \beta^{t+1}) \ldots (x - \beta^{q-3})(x - \beta^{q-2})$$

$$= (1 - \beta^t x)(1 - \beta^{t+1} x) \ldots (1 - \beta^{q-3} x)(1 - \beta^{q-2} x)$$

Remark: The minimum distance is (at least) t, and the dimension is $q - t$, which illustrates the conflict between trying to have high minimum distance and also high dimension (to have high information rate).

Remark: Since β is a primitive root,

$$x^{q-1} - 1 = (x - \beta)(x - \beta^2) \dots (x - \beta^{q-1})$$

This is what allows explicit factorization of $h(x)$.

Remark: We delay looking at the minimum-distance analysis of RS codes via variant check matrices.

Example: Make an RS code that will correct 1 error: Take *design distance* $t = 3$. We need $t \leq q - 1$, so take $q = 5$. Let β be a primitive root mod 5, for example $\beta = 2$. (Check!) Take generating polynomial (mod 5)

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

Thus, this will make a $[q-1, q-t] = [4, 2]$-code with generating matrix

$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}$$

Since $g(x)|x^4 - 1$, a check matrix in the usual form for cyclic codes will be made from $h(x)$, the coefficients-reversed version of

$$\frac{x^4 - 1}{g(x)} = (x - 2^3)(x - 2^4)$$

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

giving $h(x) = 1 + x + 3x^2$ and

$$H = \begin{pmatrix} 1 & 1 & 3 & 0 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Example: Let's make an RS code to correct 2 errors. Need *designed distance* $t = 5$. Since $t \leq q - 1$, take $q = 7$. Let β be a primitive root mod 7, for example $\beta = 3$. Take generating polynomial

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

This will make a $[6, 2]$-code with generating matrix

$$G = \begin{pmatrix} 4 & 2 & 3 & 6 & 1 & 0 \\ 0 & 4 & 2 & 3 & 6 & 1 \end{pmatrix}$$

A generator $h(x)$ for the check matrix is the coefficients-reversed version of

$$\frac{x^6 - 1}{g(x)} = (x-1)(x-5) = x^2 + x + 5$$

so $h(x) = 1 + x + 5x^2$, and

$$H = \begin{pmatrix} 1 & 1 & 5 & 0 & 0 & 0 \\ 0 & 1 & 1 & 5 & 0 & 0 \\ 0 & 0 & 1 & 1 & 5 & 0 \\ 0 & 0 & 0 & 1 & 1 & 5 \end{pmatrix}$$

Any 4 columns are linearly independent.

Remark: The **rate** of the RS code with parameters q, $n = q - 1$, and designed distance $t \leq q - 1$ is

$$\text{rate } = \frac{n - \deg g}{n} = \frac{q - t}{q - 1} = 1 - \frac{t - 1}{q - 1}$$

With $t = 2e + 1$ to correct e errors,

$$\text{info rate } = 1 - \frac{2e}{q - 1}$$

And the **relative error correction** is

$$\text{rel error corr } = \frac{2e}{\text{block length}} = \frac{2e}{q - 1}$$

We cannot both correct lots of errors per block length and maintain a high rate.

Remark: Though a suitable RS code can correct as many errors as we'd with, these are not *binary* codes. We might want a *binary* code, which is a possibility with the **BCH codes** below.

Proof: The proof that RS codes work as claimed wiill use a *variant* check matrix in which any t columns are a Vandermonde matrix, so are linearly independent,

$$\begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^n \\ 1 & \beta^2 & (\beta^2)^2 & \dots & (\beta^n)^2 \\ 1 & \beta^3 & (\beta^2)^3 & \dots & (\beta^n)^3 \\ 1 & \beta^4 & (\beta^2)^4 & \dots & (\beta^n)^4 \\ & & \dots & & \\ 1 & \beta^{t-1} & (\beta^2)^{t-1} & \dots & (\beta^n)^{t-1} \end{pmatrix}$$

where β is a *primitive root* in $\mathbf{F}_q$. The j^{th} column consists of powers of β^{j-1}. Since β is primitive, the entries of the top row are distinct. Thus, any $t-1$ columns together form a Vandermonde matrix with non-zero determinant! This proves linear independence, and by earlier discussions proves the minimum distance assertion. *What remains is to see that this really is a check matrix for C.*

Models of finite fields

The only possible sizes of finite fields are *prime powers* (meaning powers of prime numbers). (This is non-trivial.) That is, there are *no* finite fields with 6, 10, 12, 14, 15, 18, or other composite non-prime-power number of elements.

Fields with *prime* numbers p of elements have easy models:

$$\mathbf{F}_p = GF(p) \approx \mathbf{Z}/p$$

Fields with *prime power* (but not prime) numbers of elements are less elementary. They **cannot be modeled by Z mod something!**

Remark: For any value of q other than primes, $\mathbf{Z}/q$ **is not a field**. Such $\mathbf{Z}/q$ have non-zero elements whose products are 0, so it is not possible that every non-zero element is prime.

$$GF(4) = \mathbf{F}_4 \neq \mathbf{Z}/4$$

$$GF(8) = \mathbf{F}_8 \neq \mathbf{Z}/8$$

$$GF(16) = \mathbf{F}_{16} \neq \mathbf{Z}/16$$

$$GF(9) = \mathbf{F}_9 \neq \mathbf{Z}/9$$

Remark: Also, a widespread mistaken belief that it is easy to make finite fields with 2^k elements by taking all length-k binary vectors, having addition be vector addition (equivalently, XOR), and then making up some random/whimsical "multiplication". It is true that vector addition is a good addition, but it is **not easy** to make up a multiplication which is associative, commutative, distributive with respect to addition, and such that every non-zero element has a multiplicative inverse.

Definition: A polynomial $P(x)$ of positive degree with coefficients in $\mathbf{F}_p$ is **irreducible** if it cannot be factored into polynomials of strictly smaller degree.

Proposition: If P is not irreducible, then there exists a polynomial D with

$$\deg D \leq \frac{1}{2} \cdot \deg P$$

dividing P.

Proof: Use the fact that

$$\deg(A \cdot B) = \deg A + \deg B$$

for polynomials with coefficients in a field. If D divides P, then $E = P/D$ is a polynomial with

$$\deg E = \deg P - \deg D$$

If $\deg D > (\deg P)/2$, then $\deg E < (\deg P)/2$.

///

Thus, for small degree, we can test P for irreducibility by **trial division**: divide P by all polynomials of degree less-than-or-equal $\frac{\deg P}{2}$. If no such smaller polynomial divides P, then P is irreducible. Further, we need only attempt division by **monic** polynomials (highest coefficient 1).

Remark: If it is convenient, one may, further, only attempt division by *irreducible* smaller (monic) polynomials.

Example: Test $P = x^3 + x + 1$ for reducibility, in $\mathbf{F}_2[x]$. Since $(\deg P)/2 = 3/2$, we need only attempt division by polynomials D of degree $1 \leq d \leq 3/2$. Since degree must be an integer, we need only consider *linear* (monic) polynomials D. To enumerate these, we have only a choice of constant coefficient, 0 or 1. That is, try to divide by x and by $x + 1$.

$$x^3 + x + 1 \,\%\, x = 1 \neq 0$$

$$x^3 + x + 1 \,\%\, (x + 1) = 1 \neq 0$$

so $x^3 + x + 1$ is irreducible.

Example: Test $P = x^4 + x + 1$ for reducibility, in $\mathbf{F}_2[x]$. Since $(\deg P)/2 = 4/2$, we need only attempt division by polynomials D of degree $1 \leq d \leq 4/2$. Degree is an integer, so consider *linear* and *quadratic* (monic) polynomials D. Enumerate these by degree and by a lexicographic ordering on lower-degree coefficients. First, consider linear polynomials, where we have only a choice of constant coefficient, 0 or 1, giving x and $x + 1$. Try to divide by x and by $x + 1$

$$x^4 + x + 1 \,\%\, x = 1 \neq 0$$

$$x^4 + x + 1 \,\%\, (x + 1) = 1 \neq 0$$

To enumerate quadratic (monic) polynomials lexicographically, but excluding reducible ones, skipping polynomials divisible by x means to ignore polynomials with constant coefficient 0. And $(x + 1)^2 = x^2 + 1$, so the linear term must be 1 to avoid divisibility by $x+1$. Thus, we only attempt division by $x^2 + x + 1$:

$$x^4 + x + 1 \,\%\, (x^2 + x + 1) = 1 \neq 0$$

so $x^4 + x + 1$ is irreducible.

Let p be a prime. Then $\mathbf{F}_p = GF(p) = \mathbf{Z}/p$ is a field with p elements, since b not divisible by p has a multiplicative inverse mod p. This much is easy.

Remark: This is completely analogous to the notion of *prime number* in the integers.

Let P be an *irreducible* polynomial of degree k with coefficients in $\mathbf{F}_p$. The *abstract* model of $\mathbf{F}_{p^k}$ is

$$\mathbf{F}_{p^k} = \mathbf{F}_p[x] \bmod P(x) = \mathbf{F}_p[x]/P$$

Multiplication and addition are polynomial multiplication and addition of equivalence classes, which (one can prove) are *well defined.*

This is a viewpoint which allows us to prove theorems about fields, but is not optimal for computation.

Remark: Constructing larger fields containing a given field K as sets

$$K[x] \bmod P = K[x]/P$$

of equivalence classes mod P (for irreducible P) may be unsatisfying in some regards, but it is useful.

For example, with such a construction we do *not* need to postulate anything about the existence of desired entities *somewhere out there*.

For example, what about $\sqrt{-1}$ and the complex numbers $\mathbf{C}$ as a larger field containing the real numbers $\mathbf{R}$? On one hand, we may argue about whether $\sqrt{-1}$ exists or not, and in what sense. On the other hand,

$$\mathbf{C} = \mathbf{R}[x] \bmod x^2 + 1 = \mathbf{R}[x]/(x^2 + 1)$$

constructs C. Note that

$$x^2 = x^2 - (x^2 + 1) \bmod (x^2 + 1)$$

$$= -1 \bmod (x^2 + 1)$$

so x modulo $x^2 + 1$ *is* a square root of -1 in this construction.

For *computational* purposes we make tangible choices of elements from equivalence classes:

Definition: A polynomial f is **reduced mod** P if

$$\deg f < \deg P$$

For fixed choice of irreducible P of degree k with coefficients in $\mathbf{F}_p$, the corresponding computational model of $\mathbf{F}_{p^k}$ is

$$\mathbf{F}_{p^k} = \{\text{reduced polynomials mod } P(x)\}$$

addition given by polynomial addition (which does not increase degree), multiplication given by polynomial multiplication *followed by reduction modulo* $P(x)$.

This is reasonable because among the polynomials which are reduced mod P there is exactly one polynomial from each equivalence class:

Proposition: Two polynomials f, g which are reduced mod P are equal modulo P if and only if they are equal (in $\mathbf{F}_p[x]$).

Multiplicative inverses in $\mathbf{F}_{p^k}$, when modeling $\mathbf{F}_{p^k}$ as polynomials reduced modulo P, are simply inverses modulo P.

For $f \neq 0$ reduced mod P, P does not divide f, so

$$\deg \gcd(f, P) < \deg P$$

Since P is irreducible,

$$\deg \gcd(f, P) = 0$$

Adjusted by multiplying through by a non-zero constant

$$\gcd(f, P) = 1$$

By the *peculiar characterization of gcd's* for polynomials, there are polynomials a, b such that

$$af + bP = 1$$

Then

$$a \cdot f = 1 \bmod P$$

giving a multiplicative inverse of f mod P. ///

Remark: The Euclidean algorithm gives a good computational approach to compute these inverses.

The following peculiar result shows that this sort of construction creates 'numbers' satisfying any equation we like:

Theorem: Let P be irreducible of degree k with coefficients in $\mathbf{F}_p$. Let α be x-mod-P. Then

$$P(\alpha) = 0$$

Proof: This is as much an issue about well-definedness as anything. We want to show that, for any polynomial M,

$$P(x + M \cdot P) = 0 \bmod P$$

Indeed, by the Binomial Theorem,

$$(x + MP)^\ell = x^\ell + (\text{multiple of } P)$$

Applying this to all the terms of $P(x + MP)$ and adding gives

$$P(x + M \cdot P) = P(x) + (\text{mult of } P) = 0 \bmod P$$

as desired. ///

Primitive roots/elements in $\mathbf{F}_{p^k}$

Definition: An element β of $\mathbf{F}_{p^k}$ is a **primitive root** or **primitive element** if it has the *maximal possible order* $p^k - 1$, or, equivalently, if

$$\beta, \beta^2, \ldots, \beta^{p^k - 1}$$

are distinct.

Remark: It is a non-trivial theorem that any finite field has primitive elements.

For P irreducible degree k in $\mathbf{F}_p[x]$ model $\mathbf{F}_{p^k}$ as $\mathbf{F}_p[x]$ mod P. A reduced polynomial g mod P is a primitive element if and only if for every prime q dividing $p^k - 1$

$$g^{\frac{p^k - 1}{q}} \neq 1 \bmod P$$

Remark: Irreducibility of P assures that

$$g^{p^k} = g \bmod P$$

so this need not be checked.

Example: Find an element of order 15 in $\mathbf{F}_{2^4}$ modeled as $\mathbf{F}_2[x]/(x^4+x+1)$.

Remark: This question may be paraphrased as asking to find a primitive root in $\mathbf{F}_{2^4}$.

Remark: It deserves comment, but is implied by the question, that x^4+x+1 is irreducible. Still, it is nice that we happened to have verified this above as an example.

There is nothing more systematic to do than brute force, that is, to guess and check. First, guess that $x \bmod x^4+x+1$ is primitive. Applying the criterion above, we should verify that for every prime q dividing $2^{\text{degree}}-1 = 2^4-1$, namely $q = 3, 5$, that

$$x^{\frac{2^{\text{degree}}-1}{q}} \neq 1 \bmod (x^4+x+1)$$

Indeed, by dividing,

$$x^{\frac{2^4-1}{5}} = x^3 \neq 1 \bmod (x^4+x+1)$$

$$x^{\frac{2^4-1}{3}} = x^5 = x^2+x \neq 1 \bmod (x^4+x+1)$$

Thus, x is primitive modulo x^4+x+1.

Example: Find an element of order 15 in $\mathbf{F}_{2^4}$ modeled as $\mathbf{F}_2[x]/(x^4+x^3+x^2+x+1)$.

Remark: It is implied by the question that $x^4+x^3+x^2+x+1$ is irreducible. Still, one might check this.

Brute force. First, guess that x mod $x^4+x^3+x^2+x+1$ is primitive. Applying the criterion above, we should verify that for every prime q dividing $2^{\text{degree}}-1 = 2^4-1$, namely $q = 3, 5$, that

$$x^{\frac{2^{\text{degree}}-1}{q}} \neq 1 \bmod (x^4+x^3+x^2+x+1)$$

By dividing,

$$x^{\frac{2^4-1}{5}} = x^3 \neq 1 \bmod (x^4+x^3+x^2+x+1)$$

but

$$x^{\frac{2^4-1}{3}} = x^5 = 1 \bmod (x^4+x^3+x^2+x+1)$$

so x is *not* primitive.

Enumerating candidates by degree and some sort of lexicographic order, we would try $x+1$ next.

$$(x+1)^{\frac{2^4-1}{5}} = (x+1)^3 = x^3 + x^2 + x + 1$$

$$\neq 1 \bmod x^4 + x^3 + x^2 + x + 1$$

$$(x+1)^{\frac{2^4-1}{3}} = (x+1)^5 = x^5 + x^4 + x + 1$$

$$= x^3 + x + 1 \neq 1 \bmod (x^4 + x^3 + x^2 + x + 1)$$

by dividing.

Thus, $x+1$ is primitive mod $x^4+x^3+x^2+x+1$.

Remark: If $x + 1$ had also failed, we would proceed to try quadratic polynomials as candidates, then cubic, etc.
