Review/Outline

Recall: Looking for good codes

High info rate vs. high min distance
Hamming bound for arbitrary codes
Gilbert-Varshamov bound for linear codes

Linear algebra, row reduction

to detect linear dependence
to determine linear dependence relations
Computing dimensions
... of row spaces of matrices

Specifying linear codes

(...as task apart from error correction)
Generating matrix
Check matrix

Cyclic codes

Naive idea for generating matrix
Reinterpret as polynomial algebra
Shifting as mult by x
Wrap-around as $\% \, (x^n - 1)$
Unique factorization ...

How to make check matrices?

Definition: One **standard form** for an m-by-n generating matrix G for a code C is a matrix presented in **blocks**, of the form

$$G = \begin{pmatrix} I_m & A \end{pmatrix}$$

where as usual I_m is the m-by-m **identity matrix** and A is an arbitrary m-by-$(n-m)$ matrix.

The code given by such a generating matrix has dimension m, because the generating matrix is row-reduced already, and its rows are linearly independent.

Then a check matrix is

$$H = \begin{pmatrix} -A^t & I_{n-m} \end{pmatrix} = (n-m)\text{-by-}n$$

Example: With generating matrix, over $\mathbf{F}_2$,

$$G = (\, I_4 \quad A\,) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

a check matrix is

$$H = (\, -A^t \quad I_{7-4}\,) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Cyclic codes

Cyclic codes still allow the conclusion of Shannon's theorem, so we're not searching for something that's not there when we look for good codes among the cyclic ones.

Definition: A (binary) **cyclic code** C is specified by a vector

$$v = (v_1, v_2, v_3, \ldots, v_n)$$

the **generator** (of some length n, which will be the block length). A generator matrix is obtained by taking rows to be v and all other length n vectors obtained by *cycling forward* the entries of v (with wrap-around):

$$G = \begin{pmatrix} v_1 & v_2 & v_3 & \ldots & v_n \\ v_n & v_1 & v_2 & \ldots & v_{n-1} \\ v_{n-1} & v_n & v_1 & \ldots & v_{n-2} \\ & \ldots & & & \\ v_2 & v_3 & \ldots & v_n & v_1 \end{pmatrix}$$

Example: With generator $v = 11100$, the associated cyclic code has generator matrix

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

Remark: Very often the cycled vectors are *not* linearly independent, the *dimension* of the code is not obvious.

Remark: How to make a check matrix for a cyclic code?

The underlying mechanism:

The shift-with-wraparound has a useful interpretation in terms of polynomial algebra.

Interpret a length n vector $v = (v_0, v_1, \ldots, v_{n-1})$ as a polynomial

$$p(x) = v_o + v_1 x + v_2 x^2 + \ldots + v_{n-2} x^{n-2} + v_{n-1} x^{n-1}$$

with coefficients in *ascending* order.

- Shifting to the right *without* wrap-around is *multiplication by* x.
- *Wrap-around* is $\% \, (x^n - 1)$

Remark: We believe that reduction modulo a polynomial interacts well with addition and multiplication.

A linear dependence relation among the shifts would be an equation

$$\big(c_o p(x)+c_1 x p(x)+\ldots+c_{n-1}x^{n-1}p(x)\big)\,\%(x^n-1)$$

$$=0$$

Make a polynomial $q(x)$ from the coefficients of the alleged relation,

$$q(x) = c_o + c_1 x + \ldots + c_{n-1}x^{n-1}$$

Then the alleged relation is

$$(q(x)\cdot p(x))\;\%\,(x^n-1) = 0$$

That is, $\boxed{(x^n-1) \text{ divides } q(x)\cdot p(x)}$

In terms of *unique factorization into irreducible polynomials*, any factors of $p(x)$ or of $q(x)$ that are not shared by x^n-1 cannot help x^n-1 divide the product $q\cdot p$.

Also, the whole code C is the set of polynomial multiples of $p(x)$ reduced modulo x^n-1

$$C = \{(r(x)\cdot p(x))\;\%\,(x^n-1) : r(x) \text{ arbitrary }\}$$

In terms of unique factorization, the cyclic code generated by vector v is determined by the shared factors of $x^n - 1$ and v:

Proposition: Let v be a length n vector. Let $v = a(x) \cdot b(x)$ where $a(x)$ has no common factor with $x^n - 1$. Then

$$\text{cyclic code } C \text{ gen'd by } v$$

$$= \text{cyclic code gen'd by } b$$

The **dimension** of the code is

$$\dim C = n - \deg \gcd(x^n - 1, v)$$

The **dual code** $C^\perp$ to C is also *cyclic*, generated by

$$h(x) = \frac{x^n - 1}{\gcd(x^n - 1, v)} \text{with coefficients reversed}$$

For example,

$$x^5 + 2x^3 + 5x + 3 \text{ with coefs reversed}$$

$$= 1 + 2x^2 + 5x^4 + 3x^5 = 3x^5 + 5x^4 + 2x^2 + 1$$

Further, a generator matrix with **linearly independent rows** is made from

$$g = \gcd(x^n - 1, v)$$

by padding g with 0's on the right until it has the same size as the block length, then right shifting (with wrap-around) **only** until the original g touches the right edge of the matrix.

Further, a check matrix with **linearly independent rows** is made from

$$h = (x^n - 1)/\gcd(x^n - 1, v)$$

by padding $h(x)$ with 0's on the right until it has the same size as the block length, then right shifting (with wrap-around) **only** until the original $h(x)$ touches the right edge of the matrix.

Remark: Depending on one's frame of mind, it may be more attractive to say, more simply,

$$h(x) = \frac{x^n - 1}{\gcd(x^n - 1, g)}$$

but then the check matrix is **not** made from $h(x)$ in the same way that the generator matrix was made from $g(x)$. That is, the coefficients of $g(x)$ are put into the matrix in *ascending* degree. If we don't reverse $h(x)$ when we *make* it in the first place, then we *must* reverse it when we put it into the check matrix, thus putting its coefficients in in *descending* order rather than *ascending*. Confusing...

Example: Let C be a cyclic binary code of length 7 with generator polynomial 100011. Find the dimension of C and find a check matrix for C.

Remark: True, we can write out a generator matrix G for C, specified by the very definition of *cyclic code*: its top row is 100011 padded by 0's on the right to make it length 7, namely 1000110. Then cycle until it repeats:

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

But this does not give much idea about dimension, nor of a check matrix.

First, compute

$$\gcd(x^{\text{length}} - 1, v) = \gcd(x^7 - 1, 1 + x^4 + x^5)$$

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

by Euclid. Arrange in ascending degree and padded by 0's on the right, this gives generator matrix

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

(stopping when the coefficients of the *gcd* bump into the right-hand edge), with *linearly independent rows*. So the dimension of this code is 4.

The generator for the dual code and/or check matrix is

$$h(x) = \frac{x^{\text{length}} - 1}{\gcd(x^{\text{length}} - 1, v)} \text{with coefs reversed}$$

$$\frac{x^{\text{length}} - 1}{\gcd(x^{\text{length}} - 1, v)} = \frac{x^7 - 1}{x^3 + x + 1}$$

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

So, reversing the coefficients, $h(x) = 1 + x^2 + x^3 + x^4$. Arranged in ascending degree, padded, and shifted until it touches the right edge, gives check matrix

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

(Just checking, in case you don't believe that this works,

$$G\,H^t = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

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

Ha!
