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

Recall: some linear algebra

- Linear combinations
- Linear independence
- Vector subspaces
- Row reduction
  - to detect linear dependence
  - to determine linear dependence relations

Today:

- Computing dimensions
  - ... of row spaces of matrices
- Specifying linear codes
  - Generating matrix
  - Check matrix
- **Cyclic codes**
  - Generating matrix
  - Check matrix

Computing dimensions, generating matrices

The **dimension** of C is the dimension of that vector subspace, which means, by definition, the number of elements in a **basis**.

Theorem: The dimension of the rowspace of a matrix can be computed by row reducing it and counting the non-zero rows. ///

Corollary: The dimension of the vector subspace spanned by a set of vectors can be computed by creating a matrix with rows consisting of those vectors, row reducing, and counting the non-zero rows. ///

A **linear code** C of (block) length over an alphabet $\mathbf{F}_q$ is a vector subspace of $\mathbf{F}_q^n$, by definition.

Definition: A **generating matrix** G for a linear code C of block length n is an m-by-n matrix G (for *some* m) whose row space is C.

Example: To determine the dimension of the subspace spanned by 0111, 1010, 0011, 1110, stack these vectors as the rows of a matrix, and row reduce: $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ Interchange 1 and 0 rows, to get $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ Add row 0 to row 3, to obtain $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ Add row 1 to row 3, to obtain $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ Add row 2 to row 3, to obtain $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ Three non-zero rows means $\boxed{\text{dimension is 3}}$.

Example: Dimension of the subspace spanned by 0111001, 1010001, 0011111, 1110111? Stack these vectors as rows, reduce:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$ Interchange 1 and 0 rows, to get $$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$ Add row 0 to row 3, to obtain $$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Add row 1 to row 3, to obtain

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$ Add row 2 to row 3, to obtain $$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$ Three non-zero rows means $\boxed{\text{dimension is 3}}$.

Generating matrices

Again, a **generating matrix** G for a linear code C of block length n is an m-by-n matrix G (for *some* m) whose row space is C. The **row rank** of G is the **dimension** of the code.

Remark: There is no assurance that the rows are linearly independent. In fact, some procedures to make generating matrices produce matrices with linearly *dependent* rows.

Remark: If the generating matrix is of certain special forms it may be visibly *row-reduced*, in which case the non-zero rows are definitely linearly independent.

Example: Just looking at the 3 leftmost columns of

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

shows it is row-reduced, so has row-rank 3, since it has 3 non-zero rows.

Thinking in terms of row reduction as in the previous example:

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**

$$I_m = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

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.

Check matrices

$A^\top$ or A^t is **transpose** of a matrix A. By definition, the $(i,j)^{\text{th}}$ entry of A^t is the $(j,i)^{\text{th}}$ entry of A. A^t is A flipped across its diagonal.

Definition: A **check matrix** H for an $[n,k]$-code C given by an m-by-n generating matrix G is a matrix H of size something-by-n such that

$$v \in C \Leftrightarrow vH^t = 0$$

So a vector v is in C if and only if the vector-matrix product vH^t is the 0 vector.

Example: With code C given by generating matrix

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

with a little insight we see that a vector v is in C if and only if the sum of its entries is 0. Thus, a check matrix for C is

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

Remark: The **dot product** or **scalar product** $v \cdot w$ of two row vectors v, w of the same length can be expressed as the vector-matrix product

$$v \cdot w = vw^t$$

For example,

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

$$= 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1 = 0 \in \mathbf{F}_2$$

Remark: Even though having dot product 0 here does not have the same physical sense of perpendicularity, we would still say that two vectors are *orthogonal* if their dot product is 0.

Thus, a vector is in a code C if and only if it is orthogonal to all the rows of a check matrix.

Definition: The **dual code** $C^\perp$ to a linear code C of length n is the length n code of vectors perpendicular to all vectors in C.

Example: The dual code to the code with generating matrix

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

has generating matrix

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

Theorem: The dual code to the dual code is the original code. That is, for a linear code C,

$$C^{\perp\perp} = C$$

Remark: This plausible-sounding theorem is not trivial to prove!

Corollary: The check matrix for a code is a generating matrix for its dual code.

How to make check matrices?

The first case of interest is for a generating matrix of the special form (in blocks)

$$G = (\, I_m \quad A \,) = m\text{-by-}n$$

Then a check matrix is

$$H = (\, -A^t \quad I_{n-m} \,) = (n-m)\text{-by-}n$$

Example: With generating matrix

$$G = (\, I_3 \quad A \,) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

a check matrix is

$$H = (\, -A^t \quad I_{7-3} \,) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Cyclic codes

An even *simpler* to specify subclass of the linear codes are **cyclic codes**, which (luckily) still allow the argument 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 single (binary) 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 for the code 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 $v = 11000$, the associated cyclic code has generator matrix

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

Remark: But as in this example, very often the cycled vectors are *not* linearly independent, so we cannot immediately tell the *dimension* of the code from the size of G. This is annoying.

... and of course we'd want to know how to systematically make **check matrices** for cyclic codes.

The underlying mechanism:

The big trick in study of cyclic codes is to realize that the *cycling* forward 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 becomes *multiplying by* x.

• The *wrap-around* is *reduction modulo* $x^n - 1$.

Now we need to believe that reduction modulo a polynomial interacts well with polynomial addition and multiplication.

Then any linear dependence relation among the shifts is an equation

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

$$= 0$$

Make up a polynomial 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,

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

Thinking 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, this shows that the cyclic code generated by vector v with associated polynomial $p(x)$ is determined by the shared factors of $x^n - 1$ and $p(x)$.

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

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

Proof: On one hand, the collection of polynomial multiples of $b(x)$, reduced mod $x^n - 1$, certainly includes multiples of $p(x)$ reduced mod $x^n - 1$, since $p(x)$ is a multiple of $b(x)$. On the other hand, since $a(x)$ is relatively prime to $x^n - 1$, it has an inverse $i(x)$ modulo $x^n - 1$. For any polynomial $r(x)$, **with everything modulo** $x^n - 1$

$$r \cdot b = r \cdot i \cdot a \cdot b = r \cdot i \cdot p$$

so multiples of $b(x)$ are also multiples of $p(x)$, modulo $x^n - 1$. ///

Theorem: Let v be a length n vector with n **odd**. Let C be the cyclic code generated by v. Then the **dual code** $C^{\perp}$ to C is also *cyclic*, generated by polynomial

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

Remark: That is, $h(x)$ is obtained from $r(x) = (x^n - 1)/\gcd(x^n - 1, v)$ by reversing the order of coefficients of $r(x)$, meaning that the constant coefficient of $r(x)$ becomes the highest-degree coefficient of $h(x)$, and the highest-degree coefficient of $r(x)$ becomes the constant coefficient of $h(x)$, etc. For example,

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

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