Math 110 Homework 8 Solutions

March 5, 2015

1. (a) Define the bound $A_q(n,d)$ on the set of (n,M,d) codes.

   (b) Show that $A_q(n,1) = q^n$ and $A_q(n,n) = q$.

   (c) State the Gilbert–Varshamov bound (18.3.2).

   Solution: (a) The integer $A_q(n,d)$ is the largest M such that there exists a code with parameters (n,M,d).

   (b) If $d = 1$ then this is asking for the largest code with the requirement that all code words be at least 1 apart. Distance one is automatic, so we may take all q^n elements of $\mathcal{A}^n$ as code words. Thus $A_q(n,1) = q^n$. If $d = n$, then all code words must be at least n apart, so all letters of all code words must be different. But if there are $q+1$ code words, two must share a digit. Thus $A_q(n,n) \leq q$. This bound is achieved for example by the code whose words consist of a single repeated letter.

   (c) The Gilbert–Varshamov bound states that

$$A_q(n,d) \geq \frac{q^n}{\sum_{j=0}^{d-1} \binom{n}{j}(q-1)^j}.$$

2. This question concerns vector spaces $\mathbb{F}^n$ over a field $\mathbb{F}$. Be sure that you're fluent with the definition and basic properties of the following. Almost all the results that hold when $\mathbb{F}$ is $\mathbb{R}$ also hold over other fields. Vector subspaces, linear (in)dependence, basis and dimension, matrices and linear transformations, matrix multiplication, column and row spaces, rank of a matrix, kernel of a matrix, transposes.

   (a) Let $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. Find a 2-dimensional subspace of $\mathbb{F}^4$ and explain why it is a subspace. Find a basis for the subspace and explain why it is a basis.

   (b) Let $\mathbb{F}^n$ be a vector space over a field $\mathbb{F}$ of q elements. Compute the number of vectors in $\mathbb{F}^n$, and the number of vectors in a subspace of $\mathbb{F}^n$ of dimension k.

   Solution: (a) Let $V \subset \mathbb{F}^4$ consist of all vectors of the form $\{(c_1, c_2, 0, 0) : c_1, c_2 \in \mathbb{F}\}$. It is closed under addition and multiplication by scalars in $\mathbb{F}$ because $(c_1, c_2, 0, 0) + (d_1, d_2, 0, 0) = (c_1 + d_1, c_2 + d_2, 0, 0) \in V$ and likewise $\lambda(c_1, c_2, 0, 0) = (\lambda c_1, \lambda c_2, 0, 0) \in V$. V is the span of $w_1 = (1, 0, 0, 0)$ and $w_2 = (0, 1, 0, 0)$ by the definition of span. These vectors are linearly independent as $c_1 w_1 + c_2 w_2 = 0$ only if $c_1 = c_2 = 0$. Thus they form a basis.

   (b) $\mathbb{F}^n$ has q^n elements: there are q choices for each of the n components of a vector. Now let V be a k dimensional subspace. Picking a basis $\{w_i\}$, we can say that

$$V = \{c_1 w_1 + \dots c_k w_k : c_1, \dots c_k \in \mathbb{F}\}$$

   and furthermore that there is a unique way to express a vector of V as a linear combination of this form. There are q^k choices for the k elements of $\mathbb{F}$, so there are q^k elements of V.

3. (a) Define an $[n,k]$ linear code. What is the relationship between k and M?

   (b) Define the *Hamming weight* of vector $v \in \mathbb{F}^n$.

(c) Let $u, v, w \in \mathbb{F}^n$, and let d be the Hamming metric. Explain why $d(u, v) = d(u - v, 0)$, and why $d(u, v) = d(u + w, v + w)$.

(d) Define the *generating matrix* $G = [I_k \ P]$ of an $[n, k]$ linear code. What is the rank of G, and what does this imply about the dimension of the subspace $C = \{vG \mid v \in \mathbb{F}^k\} \subseteq \mathbb{F}^n$?

(e) What are the *information symbols* and the *check symbols* in a code vector vG?

(f) Define a *parity check matrix* for a code C.

(g) Explain (in your own words) a proof of the following result from class: $[-P^T \ I_{n-k}]$ is a parity check matrix for a code C with generating matrix $G = [I_k \ P]$.

(h) Define the *cosets* of a code C. What is a *coset leader*?

(i) If $r \in \mathbb{F}^n$, define the *syndrome* of r. Show that two vectors have the same syndrome if and only if they are in the same coset.

(j) Given $r \in \mathbb{F}^n$, we can compute the (possibly non-unique) closest codeword to r by finding the coset leader r_0 with the same syndrome as r and computing $c = r - r_0$. Explain why this method works. Why is c a codeword, and why is it minimal distance from r?

Solution:

(a) An $[n, k]$ linear code (over a finite field $\mathbb{F}$ with q elements) is a k-dimensional subspace of $\mathbb{F}^n$. By the previous problem, the number of code words is q^k.

(b) The Hamming weight of a vector is the number of non-zero entries it has.

(c) A place of u and v is the same if the corresponding place of $u - v$ is zero. Thus the number of different places in u and v, the definition of the Hamming distance, is the number of non-zero places of $u - v$. But the distance between $u - v$ and 0 is the number of non-zero places. A place in u and v is the same if and only if the place in $u + w$ and $v + w$ is the same. Thus $d(u, v) = d(u + w, v + w)$.

(d) The generating matrix for a linear code is a way to specify a basis for the subspace. To do so, pick a k by n matrix of rank k, and let the rows be the basis for the linear code. It is convenient to use a generating matrix of the form $[I_k \ P]$: the left k by k block is the identity matrix and the rest determines the code. This is automatically rank k (the rank is at most k, and the the first k columns are obviously linearly independent), and hence the span of the rows is also k dimensional. (Note that C is the span of the rows. Also, remember that the column rank and the row rank of a matrix are the same.)

(e) The first k symbols are the information symbols, because they tell you how many of each basis vector was used. The remaining symbols are check symbols because they help you detect errors.

(f) The parity check matrix for C is a matrix H such that $v \in C$ if and only if $vH^T = 0$. In other words, it gives a way to check whether v is a code word.

(g) This is the theorem on page 411. The explanation there is good.

(h) The cosets of a code C are the set of translates of C (picture them as hyperplanes that don't pass through the origin in $\mathbb{R}^n$). A coset leader is an element of a coset with minimal weight. (Picture it as the closest point on a hyperplane to the origin.)

(i) The syndrome of w is wH^T. It is an invariant of a coset: let $w = c + v$ with $c \in C$. Then $wH^T = cH^T + vH^T = vH^T$ because for $c \in C$, we have $cH^T = 0$. Conversely, if $wH^T = vH^T$, then $(w - v)H^T = 0$. This implies $w - v \in C$, so w and v are in the same coset.

(j) The vector $r - r_0$ is a code word because $(r - r_0)H^T = rH^T - r_0H^t = 0$. We will see it is the closest code word to r. The distance from any code word w to r is the distance from $w - r$ to $r - r = 0$. But $r - w$ is in the same coset as r_0 because $r - w - r_0 = (r - r_0) - w \in C$. By definition, r_0 is an element of the coset with minimal distance from zero. Thus $d(r - w, 0) \geq d(r_0, 0)$. But we know $d(r, w) = d(r - w, 0)$ and $d(r_0, 0) = d(r, r - r_0)$, hence $d(r, w) \geq d(r, r - r_0)$. So $r - r_0$ is a closest code word.

4. Trappe-Washington Chapter 18 Problem 3.

   Solution: Here $n-k=3$ and $n=5$, so $k=2$. The matrix P^T is the left two columns of the matrix, so the generator matrix is

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

   This is the two by two identity matrix together with P. The code words of C are the span of the rows: the zero vector, the first row, the second row, and $(1,1,0,1,1)$. The code rate is $\log_2(4)/5 = 2/5$.

5. Trappe-Washington Chapter 18 Problem 4.

   Solution: This can be viewed as a linear code with generator matrix

   $$(1\,1\,1)$$

   Then $k=1$ and the parity check matrix is

   $$[-P^T I_2] = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

   The cosets of this code are $\{(0,0,0),(1,0,0),(0,1,0),(0,0,1)\}$. Note that adding $(1,1,1)$ makes a word with m ones have $3-m$ ones, so these are distinct. These are also the coset leaders, because the other element of the cosets have more ones.

   The syndrome of each coset is vH^T, and are $(0,0)$, $(1,1)$, $(1,0)$, and $(0,1)$.

   The message $(1,1,0)$ has syndrome $(0,1)$, so is in the coset with coset leader $(0,0,1)$ (not that this is hard to spot). Then their difference $(1,1,1)$ is the decoding.

6. Trappe-Washington Chapter 18 Problem 5.

   Solution: This is not linear because the sum of the first and last code words is not a code word.

   By computing the distances between the 6 pairs of code words, I see the minimum distance is two.

   The singleton bound says $A_q(n,d) \leq q^{n-d+1}$. In this case $q=2$, $n=3$, and $d=2$. Therefore the bound is $2^2 = 4$. This code has four words.

7. Trappe-Washington Chapter 18 Problem 15(a).

   Solution: Recall that a perfect code is one where the Hamming bound is sharp. In other words, the bound on the number of possible code words obtained by counting the elements in balls around them and comparing to the total number of words is achieved. But in this example, any length n word has at least $\frac{n+1}{2}$ zeros or $\frac{n+1}{2}$ ones (and not both), so the balls of radius $\frac{n+1}{2}$ around the two code words cover all possible code words and do not overlap. Thus the bound is sharp.

8. Read Chapter 18.5 on Hamming Codes

   (a) Define a *binary Hamming code.*

   (b) Let $v \in \mathbb{F}^n$, and let H be the parity check matrix for a binary Hamming code. Explain why $vH^T = 0$ when v is a codeword, and why, if v contains one error, then vH^T will be the column of H corresponding to the position of the error.

   Solution: A binary Hamming code can be defined by specifying a parity check matrix. It is a generating matrix where the columns are all possible k element vectors with entries $0,1$. Order them so the right k by k block is the identity matrix.

If v is a code word, then $vH^T = 0$ for general reasons. If v contains one error, say in the ith spot, then letting e_i denote the vector with a 1 in the ith spot and 0s elsewhere, we have $v = c + e_i$ where c is the code word v should decode to. But then we have $vH^T = (c + e_i)H^T = e_iH^T$. Unraveling the matrix multiplication, this is the ith column of H.

9. **Bonus.** A group of $2^k - 1$ math students are held prisoner by a malevolent mathematician. A green or purple hat is to be placed on the head of each prisoner at random. Each prisoner can see every other prisoners' hat colour, but not his or her own. Each prisoner is then simultaneously asked: "What colour is your hat?" and (before knowing anyone else's answer) can respond with one of three answers: "green", "purple", or no response. If at least one person guesses their hat colour correctly and none guesses the wrong colour, the prisoners are set free. Otherwise they will be assigned additional homework questions.

   The prisoners may meet beforehand to decide on their strategy, but they cannot communicate once the hats are placed. What is their best strategy? *Hint:* Hamming codes.

   Solution: In the meeting beforehand, the prisoners choose a binary Hamming code of length $2^k - 1$. This code has minimum distance 3, and so every word is distance at most 1 from a codeword. The prisoners assign themselves an order, and they designate purple and green to be 0 and 1 (say, purple=0, green=1), so every possible combinations of hats corresponds to a binary length-$(2^k - 1)$ word.

   Once the game begins, each prisoner can see $(2^k - 2)$ components of a word. If the components they see correspond to a codeword, they guess that their hat is the colour that would make the word *not* a codeword. Otherwise, they pass.

   This means that if the hat configuration does not correspond to a codeword, then exactly one prisoner will guess, and guess correctly. If the hats do correspond to a codeword, then every prisoner will guess, and guess incorrectly.

   There are 2^{2^k-1} possible words, and 2^{2^k-k-1} possible codewords, so the probability that the prisoners succeed is

$$\text{Probability of success} = \frac{2^{2^k-1} - 2^{2^k-k-1}}{2^{2^k-1}} = \left(1 - \frac{1}{2^k}\right).$$