MIDTERM

Davis
M350

Name:
Pledge:

3pts. **I.** Definitions and short answers: the following are worth 1 point apiece. Justify your answers, but be brief about it!

a. Define the minimum distance d of a code, and explain how it determines the error correcting capabilities of the code.

The minimum distance of a code is the smallest number of positions which differ between any pair of codewords. The error correcting capability of the code is $\lfloor \frac{d-1}{2} \rfloor$.

b. Define $A_2(n, d)$, and describe in one short sentence how it is computed.

$A_2(n, d)$ is the maximum number of codewords in a binary code of length n with minimum distance d. To compute this number, we need to find an upper bound (often with the Sphere Packing Bound) as well as a lower bound (through a construction).

c. Define $C^\perp$, and state the relationship between the dimension of C and the dimension of $C^\perp$.

$C^\perp = \{x | x \cdot c = 0 \text{ for every } c \in C\}$. The dimension of C plus the dimension of $C^\perp$ equals n.

6pts. **II.** Calculations : do 3 of the following (they are worth 2 points apiece).

a. Show that $4 \leq A_2(8, 5) \leq 6$.

The lower bound is demonstrated with the linear code generated by 11111000 and 00011111. The upper bound can be found by using the sphere packing bound: $M \leq \frac{2^8}{1+8+28} \cong 6.9$.

b. Show that $A_{11}(3, 2) = 121$. Suppose we have a code over Z_{11} of length 3 and minimum distance 2: if we delete the last position, we get a code of length 2 and minimum distance 1. The biggest this shortened code can be is to take all of the distinct ordered pairs, and that is 121, so that is an upper bound on the length 3 code as well. To actually construct the code, take all distinct ordered pairs over Z_{11} and tack on a digit at the end so that the sum of the three digits is 0 mod 11. If we take any pair of codewords from this list, if the pair is different by one position in the ordered pair, then the final digit will be different (otherwise the sum would not be 0), so they are at least 2 apart. If they are different in both positions of the ordered pair, then they are already at least 2 apart.

c. Write out a Slepian array for the binary code whose generator matrix is shown below. Write out the parity check matrix, and show how you would do syndrome decoding for the received words 11111, 10101, and 11100.

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

A Slepian array is

$$\begin{pmatrix} 00000 & 10010 & 01111 & 11101 \\ 00001 & 10011 & 01110 & 11100 \\ 00010 & 10000 & 01101 & 11111 \\ 00100 & 10110 & 01011 & 11001 \\ 01000 & 11010 & 00111 & 10101 \\ 00011 & 10001 & 01100 & 11110 \\ 00110 & 10100 & 01001 & 11011 \\ 11000 & 01010 & 10111 & 00101 \end{pmatrix}$$

A parity check matrix is

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

The syndromes for the coset leaders are 000; 001; 010; 100; 111; 011; 110; 101. The first received word is 11111; it has a syndrome of 010, so it decodes as 11101. The second received word is 10101; it has a syndrome of 111, so it decodes as 11101. The third received word is 11100; it has a syndrome of 001, so it decodes as 11101.

d. The binary Golay code is a linear code of length 23, dimension 12, and minimum distance 7. The ternary (the alphabet has 3 symbols) Golay code is a linear code of length 11, dimension 6, and minimum distance 5. Verify that both of these codes are perfect.

For the binary case, the number of codewords in a sphere of radius 3 around a codeword is $1 + 23 + 23(11) + 23(11)(7) = 2048 = 2^{11}$. When this is multiplied by 2^{12}, we get 2^{23} as required. In the ternary case, the number of codewords in a shpere of radius 2 around a codeword is $1 + 11(2) + 11(5)2^2 = 3^5$. When multiplied by 3^6, we get 3^{11} as required.

e. Construct the parity check matrix $H(2, 7)$ for the Hamming code over the alphabet with 7 symbols. What is the minimum distance for the code associated to this parity check matrix? Use your parity check matrix to decode the received word 01234562.

A parity check matrix is

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

The minimum distance is 3 because no two columns are scalar multiples (any pair of columns are linearly independent). If we compute the syndrome of 01234562, we get $(25) = 2(16)$. This indicates that an error of magnitude 2 has been made in the column associated to 16, so we subtract 2 to get 01234560.

6pts. **III.** Do two of the following (they are worth 3 points apiece).

a. State the Sphere packing bound, and argue why it is true.

The sphere packing bound states that for a code of length n over an alphabet with q symbols and a minimum distance of $d = 2t + 1$, the number of codewords M is bounded by $M \leq \frac{q^n}{1+\binom{n}{1}(q-1)^1+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t}$. The reason this is true is that the number of codewords times the size of the sphere of radius t around that codeword cannot exceed the total number of codewords of length n. In the denominator above, the 1 indicates the codeword, and each of the terms $\binom{n}{i}(q-1)^i$ counts the number of words that are distance exactly i from the codeword (the $\binom{n}{i}$ illustrates the number of ways to choose i positions to differ with the codeword, and the $(q-1)^i$ indicates the number of ways that those positions can differ from the codeword).

b. You are told that a design exists with $v = b = 4N^2, k = r = (2N^2 - N)$, and $\lambda = N^2 - N$ for some N. Form the incidence matrix, and define a binary code to consist of the rows of the incidence matrix, the all 0 codeword, the all 1 codeword, and the complements of the codewords. Determine n, M, and d for this code. Is this code linear?

For this code, $n = 4N^2; M = 8N^2 + 2$; and $d = 2N^2 - N$. The n is obvious; the M comes from the $4N^2$ rows of the incidence matrix, the $4N^2$ complements, and the all 0 and all 1 words. The minimum distance comes from comparing rows to rows (these have a distance of $2N^2 - N + 2N^2 - N - 2(N^2 - N) = 2N^2$); rows to complements (these have a distance of $2N^2 - N + 2N^2 + N - 2(N^2) = 2N^2$); and complements to complements (these have a distance of $2N^2+N+2N^2+N-2(N^2+N) = 2N^2$). The distances between the all 0 and all 1 codewords and all the other choices are at least as big as $2N^2 - N$, so that is the minimum distance. This code is not linear. There are two ways to see this. First, the number of codewords $M = 8N^2 + 2 = 2(4N^2 + 1)$ is not a power of 2, so it cannot be linear. Second, if we add two rows of the incidence matrix, we get a word of weight $2N^2$, and there are no words with that weight in the code (the rows have weight $2N^2 - N$ and the complements have weight $2N^2 + N$), so the set is not closed under addition. (NOTE: for the minimum distance, it is not enough to argue that the minimum weight of the code is the same as the minimum distance because this code is not linear).

c. Suppose that H is a parity check matrix with the property that no $d-1$ columns are linearly dependent. Argue that the code associated to this matrix has minimum distance at least d. Include in your discussion a justification for using the minimum weight to measure the minimum distance.

For a vector v to be in the code, we need $Hv = 0$. When we think of the matrix multiplication in the column way, Hv is adding up scalar multiples of the columns of H. If no $d-1$ columns of H are linearly dependent, then it will take at least d columns to get a nontrivial sum of columns to be 0. Therefore, the minimum weight of any codeword in the code is at least d as required. This code is linear, and the minimum weight of a linear code is the same as the minimum distance because if x and y are two codewords that are separated by the minimum distance, then $d(x, y) = w(x + y)$. Since the code is linear, $x + y$ is in the code, and its weight is the minimum distance.