Name: _____ Score (Out of 11 points):

Let $\mathbb{F}_q$ be shorthand for the field $\mathbb{Z}/q\mathbb{Z}$ for some prime q.

1. [2 points] Which of the following codes are linear? Circle the number(s) of the linear code(s).

   i. $\Big\{(0,0,0),(1,0,0),(0,1,0),(0,0,1)\Big\} \subseteq (\mathbb{F}_2)^3$

   (ii.) $\Big\{(0,0,0,0),(1,1,1,1),(2,2,2,2),\ldots,\big(q-1,q-1,q-1,q-1\big)\Big\} \subseteq (\mathbb{F}_q)^4$

   (iii.) $\Big\{(a_1,a_2,a_3,a_4,a_5) \quad | \quad a_i \in \mathbb{F}_q, \quad a_1+a_2+a_3+a_4+a_5 \equiv 0 \pmod{q}\Big\} \subseteq (\mathbb{F}_q)^5$

   (iv.) $\Big\{(0,0,0),(1,2,1),(2,1,2)\Big\} \subseteq (\mathbb{F}_3)^3$

   Code (i) is not a linear code, since (for example) the sum of the two codewords

   $$(1,0,0)+(0,1,0)=(1,1,0)$$

   is not a codeword.

   All other codes are linear. In each case, we can check directly that all linear combinations of the codewords yield other codewords. Alternatively, we can note the following: Code (ii) is the $\mathbb{F}_q$–span of the vector $(1,1,1,1)$, which is necessarily a subspace of $(\mathbb{F}_q)^4$. Code (iv) is the $\mathbb{F}_3$–span of the vector $(1,2,1)$, which is necessarily a subspace of $(\mathbb{F}_3)^3$.

   Code (iii) is described as the set of solutions to a system of homogeneous linear equations (the equation $a_1+a_2+a_3+a_4+a_5 \equiv 0 \pmod{q}$) and must therefore be a vector subspace. Equivalently, with the vectors considered as column vectors, it is the nullspace of the matrix $[1,1,1,1,1]$, which is necessarily a vector subspace.

2. Let C be the $[n,k]$ linear binary code associated to the generator matrix

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

   (a) [1 point] What are n and k?

   Solution: $n=5$, $k=3$.

   Our code is by definition the subspace spanned by the rows of the matrix G. Since the rows have length 5, this a linear subspace of $(\mathbb{F}_2)^5$, and $n=5$. Since the matrix has rank 3, the subspace is 3–dimensional, and so $k=3$.

   (b) [1 point] List all codewords in C.

   Solution: A 3-dimensional binary vector space has $2^3=8$ elements, given by all linear combinations of the rows of G. These are:

   $$00000, \quad 10011, \quad 01010, \quad 00101, \quad 11001, \quad 10110, \quad 01111, \quad 11100$$

 The quiz continues on the back of the page.

These are: the zero vector, rows 1, 2, and 3, the sum of rows 1 and 2, the sum of rows 1 and 3, the sum of rows 2 and 3, and the sum of all three rows. Since we have eight distinct vectors, we can be sure we have found them all.

(c) [1 point] Given the vector $v = (1, 0, 1, 0, 1)$, write down all vectors in the coset $v + C$.

By definition, the coset $v + C$ is the set of all vectors of the form $v + c$ with $c \in C$. We can therefore list this set by adding v to each of the codewords computed in Part (b). Since $v = (1, 0, 1, 0, 1)$, in practice this means changing the first, third, and fifth entry of each codeword.

$$10101, \quad 00110, \quad 11111, \quad 10000, \quad 01100, \quad 00011, \quad 11010, \quad 01001$$

These are: the zero vector, rows 1, 2, and 3, the sum of rows 1 and 2, the sum of rows 1 and 3, the sum of rows 2 and 3, and the sum of all three rows. Since we have eight distinct vectors, we can be sure we have found them all.

(d) [2 points] Determine the minimum distance of C, and explain your reasoning.

The minimum distance of the code is the minimum of the weights of all the nonzero codewords, that is, the minimum number of nonzero entries to appear in any nonzero codeword. By inspection, this number is $d(C) = 2$.

(e) [1 point] Write down a parity check matrix for the code C.

Given a generating matrix $G = [I_k \;\; P]$, where I_k is the $k \times k$) identity matrix, and P is any matrix, we proved in class that a corresponding parity check matrix is $H = [-P^T \;\; I_{n-k}]$. In this case, we have

$$P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad -P^T = P^T \pmod 2 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

so our parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

(f) [1 point] Compute the syndrome of v. The syndrome of v is :

$$vH^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

That the syndrome is not the zero vector means that v is not a codeword (which we also could have verified by comparing v to our list of codewords in Part (a).

 The quiz continues on the back of the page.

(g) [1 point] Find a coset leader of the coset $v + C$.

A coset leader for $v + C$ is an element of the coset $v + C$ of minimum weight, that is, an element in $v + C$ with the fewest possible nonzero entries. By inspection, there is a unique such element, $v_0 = 10000$.

(h) [1 point] Find the nearest codeword (in Hamming distance) to v.

The nearest codeword to v is the difference between v and its coset leader. This is:

$$v - v_0 = (1, 0, 1, 0, 1) - (1, 0, 0, 0, 0) = (0, 0, 1, 0, 1).$$