Winter 2017, Math 148: Week 9 Problem Set
Due: Wednesday, March 15th, 2017
Error Correcting Codes

Discussion problems. The problems below should be completed in class.

(D1) *Working with linear codes and check matrices.* Consider the following matrices.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

(a) Row reduce each matrix above into the form $[I\ M]$, where I is the identity matrix.

(b) Find a basis for the kernel of each matrix.

(c) Find the parameters (n, d, δ) for the linear code defined by each matrix above.

(d) Have each member of your group pick a vector in V^5 with at least two nonzero entries. Find a basis for the subspace $C \subset V^5$ spanned by your chosen vectors.

(e) What is the value of δ for the code $C \subset V^n$ consisting only of the all 0's codeword and the all 1's codeword? Is this code linear?

(f) Which linear code in V^7 can correct the largest number of errors?

(g) Describe how to obtain a linear code $C \subset V^{11}$ with 256 codewords. Is it possible to do this in such a way that $\delta \geq 3$, so that at least one error can be corrected?

(D2) *Correcting errors with linear codes.* The goal of this problem is to prove the following.

Theorem. *If a check matrix H has no column of all 0's and no repeated columns, then the linear code C it defines can correct at least one error.*

(a) Verify the theorem for the matrices in Problem (D1).

(b) Suppose $w(c) = 1$ for some $c \in C$. What does this tell you about the matrix H?

(c) Suppose $w(c) = 2$ for some $c \in C$. What does this tell you about the matrix H?

(d) Why can we now conclude the above theorem holds?

(D3) *An error correcting code from a 2-design.* The goal of this problem is to construct a perfect error correcting code using the 2-design with parameters $(7, 3, 1)$.

(a) Write the blocks in the 2-design $(7, 3, 1)$. You may label elements however you wish.

(b) The *incidence matrix* of a 2-design is a matrix with v rows (one for each element), b columns (one for each block), a 1 in the (a, B)-entry if $a \in B$, and 0's elsewhere. Find the incidence matrix A for the 2-design $(7, 3, 1)$.

(c) Consider the code C comprised of the following codewords:

  (i) the rows of A;

  (ii) the complements of the rows of A (obtained by switching 0's and 1's); and

  (iii) the codewords 0000000 and 1111111.

Prove that any two distinct codewords in C are at least Hamming distance 3 apart. Hint: this can be done without manually checking all 120 pairs of codewords!

(d) Is the code constructed in part (c) linear?

(e) Prove that the code constructed in part (c) is *perfect*, i.e. every element of V^7 is within Hamming distance 1 of exactly one codeword of C. Hint: count the number of elements of V^7 within Hamming distance 1 of some codeword in C.

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) For each of the following codes, find (i) the minimum distance δ between any two codewords and (ii) the number of error that can be corrected.

(a) $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\} \subset V^4$

(b) $\{10000, 01010, 00001\} \subset V^5$

(c) $\{000000, 101010, 010101\} \subset V^6$

To which of the above codes can codewords be added without changing the value of δ?

(R2) Write down all of the codewords in the linear code associated with the parity check matrix

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

and determine the parameters (n, k, δ) for the resulting linear code.

(R3) What is the maximum dimension of a linear code $C \subset V^8$ that can correct 2 errors? Demonstrate that your bound is "tight" by finding such a code.

(R4) Write up your solution to Problem (D3).

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) Suppose $C \subset V^d$ is a linear code. Prove that the set C' of codewords in C with even weight is also a linear code. Find all possible values of $|C'|$ in terms of $|C|$.

(S2) Fix a codeword $x \in V^d$, and let $B_k(x) \subset V^d$ (called the *k-ball around x*) denote the set of binary sequences with Hamming distance at most k from x. Find a formula for $|B_k(x)|$.