Homework Assignment 5, Solutions

Problem 1.

(a) Let $A = \{$ the set of 4×6 binary matrices with exactly 2 ones per column and 3 ones per row$\}$, $B=\{b \mid b\in A,$ all columns in b are distinct$\}$, $C=\{c \mid c\in A,$ there are two columns in c that are the same, but no three columns in c are the same$\}$, $D=\{d \mid d\in A,$ there are three columns in d that are the same$\}$. Then clearly $A = B\cup C\cup D,$ and $|A| = |B| + |C| + |D|$.

There are totally $\binom{4}{2} = 6$ different vectors of length 4 containing 2 ones. Considering each such vector as a column, we know $|B| = 6! = 720$.

Consider any matrix c in C. Let $\{\underline{c_1},\ \underline{c_2},\ \underline{c_3},\ \underline{c_4},\ \underline{c_5},\ \underline{c_6}\}$ be the 6 columns of c (we are not considering the order of them), without loss of generality say $\underline{c_1} = \underline{c_2}$. Since $\sum_{i=3}^{6}\underline{c_i} = \sum_{i=1}^{6}\underline{c_i} = (1\ \ 1\ \ 1\ \ 1)^T$, and no four distinct columns with 2 ones in each will have the sum $(1\ \ 1\ \ 1\ \ 1)^T$, there must be two columns among $\{\underline{c_3},\underline{c_4},\underline{c_5},\underline{c_6}\}$ that are the same—WLOG say $\underline{c_3} = \underline{c_4}$. Since $\sum_{i=5}^{6}\underline{c_i} = \sum_{i=1}^{6}\underline{c_i} = (1\ \ 1\ \ 1\ \ 1)^T$, $\underline{c_5} \neq \underline{c_6}$. By the definition of C we have $c_1 \neq c_3 \neq c_5 \neq c_6$. Since there are 3 ones in each row of c, $\underline{c_1} + \underline{c_3} = (1\ \ 1\ \ 1\ \ 1)^T$, and $\underline{c_5} + \underline{c_6} = (1\ \ 1\ \ 1\ \ 1)^T$. There are $\binom{3}{1}$ ways to select $\underline{c_1}$ and $\underline{c_3}$, and $\binom{6}{2}\binom{4}{2}$ ways to select the ordered positions of $\underline{c_1},\underline{c_2}$ and $\underline{c_3},\underline{c_4}$. Now fix $\underline{c_1},\underline{c_2},\underline{c_3},\underline{c_4}$ as well as their positions, there are 2 ways to select $\underline{c_5}$ and $\underline{c_6}$, and $2!$ ways to select their ordered positions. So there are totally $\binom{3}{1}\binom{6}{2}\binom{4}{2}\cdot 2\cdot 2! = 1080$ matrices in C.

Consider any matrix d in D. Let $\{\underline{d_1},\ \underline{d_2},\ \underline{d_3},\ \underline{d_4},\ \underline{d_5},\ \underline{d_6}\}$ be the 6 columns of d (we are not considering the order of them), without loss of generality say $\underline{d_1} = \underline{d_2} = \underline{d_3}$. Then it's easy to see that $\underline{d_4} = \underline{d_5} = \underline{d_6}$, and $\underline{d_1} + \underline{d_4} = (1\ \ 1\ \ 1\ \ 1)^T$. There are $\binom{3}{1}$ ways to select $\underline{d_1}$ and $\underline{d_4}$, and $\binom{6}{3}$ ways to select the ordered positions of the 6 columns. So $|D| = \binom{3}{1}\binom{6}{3} = 60$.

Therefore there are $|A| = 720 + 1080 + 60 = 1860$ 4×6 binary matrices with exactly 2 ones per column and 3 ones per row. It's simple to figure out that all matrices in B and C have rank 3, while all matrices in D have rank 2. So among those 1860 matrices there are $|B| + |C| = 720 + 1080 = 1800$ of them which can be parity check matrices for (6,3) codes.

(b) From part (a) we know there are $|B| = 720$ such matrices with distinct columns.

The significance of having distinct columns in a parity-check matrix is that a code's weight ≥ 3 (which means it can correct single-bit errors) if and only if all the columns in the parity-check matrix are distinct. If two columns in the parity-check matrix are the same, then the two single-bit error patterns whose error positions correspond to those two columns respectively will have the same syndrome.

(c) There are $\dfrac{\prod_{i=0}^{k-1}(2^n - 2^i)}{\prod_{i=0}^{k-1}(2^k - 2^i)} = \dfrac{\prod_{i=0}^{2}(2^6 - 2^i)}{\prod_{i=0}^{2}(2^3 - 2^i)} = 1395$ (6,3) binary linear codes.

(d) From part (a) we know the $|B| + |C| = 720 + 1080 = 1800$ matrices in set B and C can be parity-check matrices for (6,3) codes. For any matrix, say matrix x, in set B or C, if we permute the rows of x, we get a matrix different from x because all rows of x are distinct, but clearly that matrix is also in set B or C and is a parity-check matrix for the same code as x is. There are $4!$ ways to permute the rows of x. Now we want to ask if there is a matrix in set B or C which is a parity-check matrix for the same code as x is, but whose rows are not the permutation of x's rows. The answer is no. To show that let's suppose such a matrix exists, and call it y. Then there is a row in y which contains 3 ones and is not a row in x—however it must be the summation of some rows in x. Each row in x contains 3 ones, so the summation of any two rows in x will have an even number of ones in it. All the four rows in x sum up to be $(0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)$, so the summation of any three rows of x is just another row of x. Therefore there is a contradiction, and y doesn't exist! So two matrices in set B or C are parity-check matrices for the same code if and only if their rows are permutations of each other. So there are $\dfrac{1800}{4!} = 75$ codes in part (c) with parity-check matrices of the form in part (a).

For the second question of part (d) the above reasoning also holds. So there are $\dfrac{|B|}{4!} = \dfrac{720}{4!} = 30$ codes in part (c) with parity-check matrices of the form in part (b).

Problem 2.

The condition $p_i(0) \to 0$ is equivalent to the condition $p\lambda(\rho(x)) < x \quad \forall 0 < x \leq 1$. Since for (3,6) LDPC codes $\lambda(x) = x^{j-1} = x^{3-1} = x^2$, $\rho(x) = 1 - (1-x)^{k-1} = 1 - (1-x)^{6-1} = 1 - (1-x)^5$, the condition becomes:

$p[1-(1-x)^5]^2 < x \quad \forall 0 < x \leq 1$. By using matlab/mathematica/maple/… we find the threshold value for p $(0 \leq p \leq 1)$ is 0.429.