Assignment III

1. Solve problems 4,5,6,7 from Assignment II.

2. As discussed earlier in class, a Tanner graph corresponding to a parity check matrix H is a bipartite graph $G = (L, R, E)$ with one left vertex per variable, one right vertex per parity check and an edge connecting each variable to the parity checks in which the variable is involved. $\emptyset \neq S \subseteq L$ is called a *stopping set* in G if there is no parity check that is connected to exactly one variable in the set S. The *stopping distance* of a Tanner graph is the size of the smallest stopping set. Show that the stopping distance of a Tanner graph is at most the minimum distance of the code.

3. Show that Stopping distance is not an intrinsic property of the code. i.e., Two Tanner graphs for the same code may have different stopping distances.

4. Suppose $G = (L, R, E)$ is the Tanner graph corresponding to the parity check matrix H for a code $\mathcal{C}$. Suppose the code is used for transmission across $BEC(\epsilon)$ and the number of erasures in a received codeword is non-zero, but less than the stopping distance of G, then, there is at least one parity check which has exactly one unknown. Hence, we can solve this unknown and repeat the process. This decoding strategy is called *iterative decoding*. Argue that iterative decoding can correct erasures up to the stopping distance of G.

5. Consider an Tanner graph $G = (L, R, E)$, where $|L| = n > |R| = m$ with ever vertex on the left having degree c and every vertex on the right having degree d. Show that the code has rate at least $1 - \frac{c}{d}$. Suppose, we use a (d, r, δ) code for each parity check, show that the rate is at least $(1 - c(1 - r))$.

6. Suppose instead of binary alphabet, we construct code over the alphabet $\Sigma = \{0, 1, 2, 3\}$ (as in QPSK signaling), show that a code (even a non-linear one) $\mathcal{C}$ of length n with M codewords and minimum distance at least d must satisfy $M \leq 4^{n-d+1}$.

7. In this question, we will prove an asymptotic version of Gilbert Varshamov bound for linear codes. Suppose we pick a random $k \times n$ generator matrix G over F_2. We will denote by $B_{\delta n}$ the number of points in a Hamming ball of radius δn in $\{0,1\}^n$. Let S denote the set of all vectors of Hamming weight at most δn in $\{0,1\}^n$. Clearly S contain $B_{\delta n}$ vectors.

   1. Let $m_0 \in \{0,1\}^k$ $y_0 \in \{0,1\}^n$ be any two vectors. argue that $Pr(mG = y) = \frac{1}{2^n}$.
   2. Argue that $Pr(mG \in S) \leq \frac{B_{\delta n}}{2^n}$
   3. Argue that $Pr(\exists m \in \{0,1\}^k : mG \in S) \leq 2^k \frac{B_{\delta n}}{2^n}$.
   4. Argue that if $k = n(1-h(\delta)-\epsilon)$ for any $\epsilon > 0$, the probability above is strictly less than 1 for sufficiently large n.
   5. Hence prove that if $k < n(1 - h(\delta))$ for any $\epsilon > 0$, there exists a linear $(n, k, \delta n)$ code for sufficiently large n.

8. Consider the $(4, 2, 3)$ Reed Solomon code over $\mathbf{Z_5}$ obtained by evaluating the degree 2 polynomial $a_0 + a_1 x$ at the values $0, 1, 2, 3$ (where addition and multiplication are modulo 5). Suppose the codeword is transmitted across a binary symmetric channel and the vector $(1, 3, 3, 4)$ is received. Set up the equations for the Berlekamp Welch decoder and find out the polynomials $q(x)$ and $e(x)$ to recover the transmitted polynomial.