Assignment I

Submit only answers to questions marked [S]

Q 1.a) Let G be a $k \times n$ generator matrix for an (n, k) linear code $\mathcal{C}$. Show that by elementary row transformations on the matrix G we can get an equivalent matrix of the form $G' = [I_k A]$ (the row reduced canonical form or Echelon form) where I_k is the $k \times k$ identity matrix and A a $k \times (n-k)$ matrix. (The matrix G' is obtained by writing the matrices I_k and A together through row wise concatenation into a single $k \times n$ matrix).
Q 1.b) Consider the $(n-k) \times n$ matrix $H' = [A^T I_{n-k}]$. (Note that A^T is an $(n-k) \times k$ matrix and this concatenated with the identify matrix I_{n-k} yields an $(n-k) \times n$ matrix.) What can you say about the matrix product GH^T. From this exercise, how can you provide a procedure for producing a parity check matrix for a code, given its generator matrix?
Q 1.c)[S] Construct G' corresponding to the matrix G below and find the corresponding parity check matrix H'. $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1. & .1 & 1 \end{bmatrix}$
Q 1.d) This exercise takes up an "exceptional" case that can happen when we reduce a matrix to the Echelon form. It might happen that one of the first k columns in the Echelon form G' is an all zero column. In that case show that by column permutation, we can get an "equivalent" code (which has bits of the codewords in the original code permuted) for which the exception condition can be avoided. Hence, we may assume that the "exceptional" case can be ignored in general.
Q 1.e) From G', deduce that the minimum distance $d(\mathcal{C}) \leq n - k + 1$. This bound is called the *Singleton bound*. In the example above, does the code satisfy the Singleton bound with equality? (A code which satisfies equality condition of the Singleton bound is called a *maximum distance separable* code or MDS code).

Q 2.a) Consider the output space $\{0, 1, \alpha\}^n$ of an n bit erasure channel $BEC_n(\epsilon)$. Note that this space is not a vector space as no useful vector addition can be defined on this space. Nevertheless, we can define the distance between vectors $d(x, y)$ in the space $\{0, 1, \alpha\}^n$ as the number of positions in which x and y differ. Show that d satisfies all the axioms of a metric.

Q 2.b) Suppose $\mathcal{C}$ be any (n, k) (not necessary linear) code. Upon transmission of a codeword x from $\mathcal{C}$ using a $BEC_n(\epsilon)$, a vector $r \in \{0, 1, \alpha\}^n$ is received. What is the probability of receiving r conditioned on the event that x was transmitted? (Express your answer in terms of $d(x, r)$, n and ϵ).
Q 2.c) Using the above exercise, argue that Maximum Likelihood decoding on $BEC_n(\epsilon)$ is equivalent to minimum distance decoding.
Q 2.d) Show that if the minimum distance $d(\mathcal{C}) = d$, $x \in \mathcal{C}$ is transmitted across a $BEC_n(\epsilon)$ and at most $e < d$ bits are erased by the channel, then minimum distance decoding will correctly recover the transmitted codeword. Thus, if $d(\mathcal{C}) = d$, then $\mathcal{C}$ can correct upto $d - 1$ erasures.
Q 2.e) Suppose there are $e < d$ erasures. Suppose we treat the erasures as unknowns on the received vector, then using the parity check matrix, show that reduce computation of the erased bits into a problem solving e unknowns from a set of $n - k$ equations (note that by Singleton bound, $n - k \geq d - 1$ and hence the number of equations are sufficient to solve the number of unknowns).
Q 2.f)[S] For the code in Q 1.c), suppose $[0, \alpha, 0, 1, 0]^T$ is received upon transmission across a $BEC_n(\epsilon)\}$, solve the parity check equations to solve the erased bit. What happens if the received vector is $[0, \alpha, 0, \alpha, 0]^T$?
Q 2.g) In the last case of the example above, there are two unknowns and three equations, yet the solution is not unique. Why is this not a contradiction?
Q 2.h) What is the difficulty in trying to solve the decoding problem on the $BSC_n(\epsilon)$ channel using the same method of linear system of equations that worked in the case of the $BSC_n(\epsilon)$ channel?

Q 3.a)[S] Suppose $x \in \mathcal{C}$ e errors and f erasures to yield a vector $r \in \{0, 1, \alpha\}^n$. Prove that if $2e + f < d$, then for any $x' \in \mathcal{C}$ with $x' \neq x$, $d(r, x) < d(r, x')$. This shows that $\mathcal{C}$ is capable of recovering e transmission errors and f erasures provided $2e + f < d$.

Q 4) Consider an (n, k, d) linear code $\mathcal{C}$ with parity check matrix H. Let $H = [h_1, h_2, ..., h_n]$ where the h_i denotes column i of H. Suppose $x \in \mathcal{C}$ in transmitted across a $BSC_n(\epsilon)$ and $r = x + e$ is received where $e \in \{0, 1\}^n$ is the error introduced by the channel. The **syndrome** $s(r)$ is defined by the

equation $s(r) = Hr$.
Q 4.a) Show that $s(x+e) = H(y+e) = s(e)$ for every $x, y \in \mathcal{C}$. That is, the syndrome depends only on the error pattern added and not on the transmitted codeword. In particular show that $s(x) = 0$ if any only if x is a codeword, ie., $x \in \mathcal{C}$.
Q 4.b) Suppose $e = [e_1, e_2, ..., e_n]$ where $e_i \in \{0, 1\}$ is bit i of the error pattern, show that $s(x+e) = s(e) = h_1e_1 + h_2e_2 + ... + h_ne_n$.
Q 4.c) Show that the Hamming weight of the minimum weight codeword corresponds to the size of the smallest set of columns of H that adds up to 0. Hence conclude that $d(\mathcal{C})$ is the minimum number of columns of H that adds to zero. (This gives a method for finding the minimum distance from the parity check matrix, but not an efficient one).
Q 4.d) If $e, e' \in \{0, 1\}^n$ are error patterns with Hamming weight less than $\frac{d}{2}$, then show that $s(e) \neq s(e')$. This means that the syndrome uniquely identifies any error less than $\frac{d}{2}$ bits. This allows us to have a lookup table for each error pattern of weight less than $\frac{d}{2}$ and the corresponding syndrome. Note that $Hr = He$ is easy to compute and a table lookup will give the error for any error e of weight less than $\frac{d}{2}$. This procedure is called **syndrome decoding** for linear codes.
Q 4.e) Show that the size of the lookup table can be as large as 2^{n-k}. (look at $rank(H)$.). Hence, this method is not an efficient procedure.

Q 5.a)[S] Consider the following parity check matrix $H_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$
(Note that the columns of this matrix are all non-zero patterns in $\{0, 1\}^3$ hence the notation H_3.) Find the generator matrix for the above parity check matrix. (Use Q.1)
Q 5.b)[S] Find the rate k and the minimum distance d (Use Q.4) of the code.
Q 5.c)[S] Construct the syndrome lookup table (Q.4) for this code. Show that syndrome decoding corrects any one bit error in transmission. Write down the syndromes corresponding to each one bit error pattern.
Q 5.d)[S] Suppose a one bit error resulted in receiving $[1, 1, 0, 1, 0, 0, 1]^T$, Find the syndrome and the transmitted pattern. Can you give another error pattern (of multiple bits) that give the same syndrome?
Q 5.e)[S] Suppose you receive $[0, \alpha, 0, \alpha, 0, 0, 0]^T$ on a erasure channel, what

was the transmitted codeword (use Q.2)?
Q 5.f)[S] Define H_k as the parity check matrix whose columns comprises of all non-zero binary strings of length k. (the above case had $k = 3$). The resultant code family (one code for each k) is called the family of **Hamming Codes** $\mathcal{H}_k$. Find the rate and minimum distance of $\mathcal{H}_k$. How large will be the syndrome decoding lookup table for these codes?

Q 6.a)[S] This question develops the theory of **Extended Hamming Codes**, $\overline{\mathcal{H}}_k$. The parity check matrix $\overline{H}_k$ is the $(k+1) \times n$ matrix obtained by adding a row of all 1^s to to H. For instance, $\overline{H}_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$
Show that the minimum distance of $\overline{\mathcal{H}}_k = 4$. What is the rate?
Q 6.b)[S] Show that any two bit error pattern will give non-zero syndrome for these codes. Hence show that these codes can detect (but not correct-why?) two bit errors and correct one bit errors.
Q 6.c)[S] How will you modify the syndrome decoding procedure of Hamming codes to suit the extended Hamming codes so that we can detect two bit errors and correct one bit errors?