Information Theory [MA5103]
Homework 6

1. On Hamming distance: $GF(q)^n \times GF(q)^n \ni (x, x') \mapsto d(x - x') = |\{1 \leq i \leq n : x_i \neq x'_i\}|$.
   (a) Show that the Hamming distance satisfies the triangle inequality.
   (b) Let $q = 2$. Show that minimum distance decoding with the Hamming distance and maximum likelihood decoding are the same for a binary symmetric memoryless channel with error probability $< 1/2$. For an output y, the former method maximizes the conditional probability $p(y|c)$ and the later minimizes the Hamming distance $d(y - c)$ where $c \in C$.

2. Prove existence of a generator $(n \times k)$ matrix in "systematic form" $G = (I_k\, G')^T$ for any $[n, k]$ linear code $C \subseteq GF(q)^n$ if we allow permutations of row vectors.

3. Let H be a parity check matrix for a linear code, say, C. Prove that C has minimum distance at least $d + 1$ if and only if any d columns of H are linearly independent.

4. Consider the $[7, 4]$ Hamming code as in the lecture.
   (a) Prove that this code corrects any single error.
   (b) Prove that this code is perfect.

5. Another version of Gilbert-Varshamov bound for binary case.
   (a) Suppose $n, k \in \mathbb{N}$ satisfy
   $$2^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i}$$
   Prove that there exists an $[n, k, d]$ linear binary code.
   (b) Prove that for any $2 \leq d \leq n$ there exists an $[n, k, d]$ binary linear code, say, C which has the following bound:
   $$|C| \geq \frac{2^{n-1}}{\sum_{i=0}^{d-2} \binom{n-1}{i}}$$
   by choosing k cleverly.