Suggested reading: Trappe-Washington 18.3–4.

1. (a) Define the bound $A_q(n, d)$ on the set of (n, M, d) codes.
   (b) Show that $A_q(n, 1) = q^n$ and $A_q(n, n) = q$.
   (c) State the Gilbert–Varshamov bound (18.3.2).

2. This question concerns vector spaces $\mathbb{F}^n$ over a field $\mathbb{F}$. Be sure that you're fluent with the definition and basic properties of the following. Almost all the results that hold when $\mathbb{F}$ is $\mathbb{R}$ also hold over other fields. Vector subspaces, linear (in)dependence, basis and dimension, matrices and linear transformations, matrix multiplication, column and row spaces, rank of a matrix, kernel of a matrix, transposes.
   (a) Let $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. Find a 2-dimensional subspace of $\mathbb{F}^4$ and explain why it is a subspace. Find a basis for the subspace and explain why it is a basis.
   (b) Let $\mathbb{F}^n$ be a subspace over a field $\mathbb{F}$ of q elements. Compute the number of vectors in $\mathbb{F}^n$, and the number of vectors in a subspace of $\mathbb{F}^n$ of dimension k.

3. (a) Define an $[n, k]$ linear code. What is the relationship between k and M?
   (b) Define the *Hamming weight* of vector $v \in \mathbb{F}^n$.
   (c) Let $u, v, w \in \mathbb{F}^n$, and let d be the Hamming metric. Explain why $d(u, v) = d(u - v, 0)$, and why $d(u, v) = d(u + w, v + w)$.
   (d) Define the *generating matrix* $G = [I_k \ P]$ of an $[n, k]$ linear code. What is the rank of G, and what does this imply about the dimension of the subspace $C = \{vG \mid v \in \mathbb{F}^k\} \subseteq \mathbb{F}^n$?
   (e) What are the *information symbols* and the *check symbols* in a code vector vG?
   (f) Define a *parity check matrix* for a code C.
   (g) Explain (in your own words) a proof of the following result from class: $[-P^T \ I_{n-k}]$ is a parity check matrix for a code C with generating matrix $G = [I_k \ P]$.
   (h) Define the *cosets* of a code C. What is a *coset leader*?
   (i) If $r \in \mathbb{F}^n$, define the *syndrome* of r. Show that two vectors have the same syndrome if and only if they are in the same coset.
   (j) Given $r \in \mathbb{F}^n$, we can compute the (possibly non-unique) closest codeword to r by finding the coset leader r_0 with the same syndrome as r and computing $c = r - r_0$. Explain why this method works. Why is c a codeword, and why is it minimal distance from r?

4. Trappe-Washington Chapter 18 Problem 3.

5. Trappe-Washington Chapter 18 Problem 4.

6. Trappe-Washington Chapter 18 Problem 5.

7. Trappe-Washington Chapter 18 Problem 15(a).

8. Read Chapter 18.5 on Hamming Codes
   (a) Define a *binary Hamming code*.
   (b) Let $v \in \mathbb{F}^n$, and let H be the parity check matrix for a binary Hamming code. Explain why $vH^T = 0$ when v is a codeword, and why, if v contains one error, then vH^T will be the row of H corresponding to the position of the error.

9. **Bonus.** A group of $2^k - 1$ math students are held prisoner by a malevolent mathematician. A green or purple hat is to be placed on the head of each prisoner at random. Each prisoner can see every other prisoners' hat colour, but not his or her own. Each prisoner is then simultaneously asked: "What colour is your hat?" and (before knowing anyone else's answer) can respond with one of three answers: "green", "purple", or no response. If at least one person guesses their hat colour correctly and none guesses the wrong colour, the prisoners are set free. Otherwise they will be assigned additional homework questions.

   The prisoners may meet beforehand to decide on their strategy, but they cannot communicate once the hats are placed. What is their best strategy? *Hint:* Hamming codes.