Math 259 - Spring 2019
Quiz 3 Information

As usual, no formulae will be provided for Quiz 3. However, you will be provided with any generating matrix you need. In other words you do need to be familiar with the Hamming $[7, 4]$ code and its decoding algorithm, but you do not need to remember its generating matrix by heart; that will be given to you if you need it.

For the quiz, you should:

- Know the definition of code, linear code, binary code, Hamming distance, Hamming weight, minimal distance, generating matrix, parity check matrix, syndrome. This includes being able to state these definitions if asked.
- Know what it means to detect and correct errors, and their relationship to the minimal distance of a code.
- Be able to generate codewords from a generating matrix.
- Be able to compute a parity check matrix from a generating matrix.
- Be able to detect errors using a parity check matrix.
- Be able to decode the Hamming code.
- Know the encryption and decryption algorithms for classic McEliece and be able to perform them on small examples, including one that uses the Hamming $[7, 4]$ code.

Also, any problem substantially similar to a homework problem is fair game for the quiz.