Homework #3. Due Saturday, February 10th, by 11:59pm on Canvas

All reading assignments and references to exercises, definitions etc. are from our main book 'Coding Theory: A First Course' by Ling and Xing

Reading and plan for the next week:

1. For this homework assignment read 4.2-4.6

2. Next week we will continue with the basic theory of linear codes (4.2-4.6). Next Thursday we will also binary Hamming codes (5.3.1, page 84). If time left, we will go back to Chapter 4 and start discussing encoding and decoding for linear codes (4.7-4.8).

Problems:

1. Let F be a finite field, and let Q be the set of all nonzero squares in F, that is, all nonzero elements of F representable as a^2 for some $a \in F$.

(a) Assume that F has odd characteristic. Prove that $|Q| = \frac{|F|-1}{2}$. **Hint:** Prove that for every nonzero $b \in F$ the equation $x^2 = b$ has either no solutions (for x) in F or exactly two solutions.

(b) Now assume that F has characteristic 2. Prove that $|Q| = |F| - 1$, that is, every nonzero element of F is a square. **Hint:** Since F is finite, it suffices to prove that the map $x \mapsto x^2$ from $F \setminus \{0\}$ to $F \setminus \{0\}$ is injective (one-to-one). The latter is not hard to prove directly (using the assumption $\operatorname{char} F = 2$).

For both parts you will likely need to use the fact that fields have no zero divisors (Lemma 3.1.3(ii) from the book).

2. Problem 4.2, page 66. Ignore the question about the number of bases, but make sure to prove your answer whether the given set is a subspace or not. If the set in question is a subspace, compute its dimension (also with proof).

3. Problem 4.3. **Hint:** First count the number of ordered k-tuples $(v_1, \ldots, v_k)$ such that the vectors $v_1, \ldots, v_k$ are linearly independent. This can be done by using the argument from the proof of Theorem 4.1.15(ii).

4. Problem 4.15.

5. Problem 4.20 (see 4.3 for the definition of weight)

6. Problem 4.22.

7. Problem 4.31. **Note:** The book describes two algorithms for finding a generator matrix for a code (Algorithms 4.1 and 4.2 in Section 4.4) and one algorithm for finding a parity-check matrix (Algorithm 4.3 in Section 4.4), but does not provide justifications. For each algorithm we will either discuss in class next week why it works, or I will post an addendum to this assignment with an explanation. If you are using one of these algorithms in your solution to Problem 7, please clearly state which one you are using.

Hint for 2. If a code C in this problem is linear, you just need to find a linearly independent subset S such that $Span(S) = C$.