Mathematics 392 – Seminar in Coding Theory
Selected Solutions – Problem Set 2

B) The main point to address here is why the minimum weight of a nonzero word in a linear code is the same as the minimum distance. Here is one argument: Let's write $w = \min_{x \neq 0} wt(x)$ for the minimum weight of a nonzero codeword in C. Let $x_0, y_0 \in C$ with $d = d(x_0, y_0)$. Then we have

$$d = d(x_0, y_0) = wt(x_0 + y_0) \geq w$$

because $x_0 + y_0 \neq 0$ is a word in C. Hence $d \geq w$. On the other hand, if $wt(z_0) = w$, then

$$w = wt(z_0) = d(z_0, 0) \geq d.$$

Since $d \geq w$ and $w \geq d$, we must have $d = w$.

F) We must analyze the number of ways to choose the vectors in a basis $\{v_1, v_2, \ldots, v_k\}$ in C. Choosing the vectors v_i in turn, v_1 can be any nonzero vector, so there are $2^k - 1 = 2^k - 2^0$ choices for v_1. Once v_1 is chosen, then to get a linearly independent set, v_2 can be any vector other than $0, v_1$. Similarly, once the first $i-1$ vectors are chosen, to get a linearly independent set, v_i can be any vector *not in the span of* $v_1, \ldots, v_{i-1}$. There are 2^{i-1} such vectors, so $2^k - 2^{i-1}$ choices for v_i, given $v_1, \ldots, v_{i-1}$. We multiply these to get the total number of ways to choose the vectors in a basis:

$$(2^k - 2^0)(2^k - 2^1) \cdots (2^k - 2^{k-1}) = \prod_{i=0}^{k-1} (2^k - 2^i)$$

But now each basis is a set (unordered). In choosing our vectors, we will have selected a given set of k basis vectors in every possible ordering, so we will have found each basis a total of $k!$ different times. The total number of distinct bases is

$$\frac{1}{k!} \prod_{i=0}^{k-1} (2^k - 2^i)$$

which is what we had to show.