Homework #3. Summary of common mistakes

1. There were several papers with the correct answer but incorrect or at least very unclear explanation. To avoid confusion, clearly state WHAT you are counting at each step.

5(b). It seems that many people were intimidated by this problem and possibly by the hint as well. So let me expand the hint and also rephrase it in a more friendly way. First, it is more convenient to prove a (formally) stronger statement by induction: If C is $[n, n-1, d]$-linear code with $d \geq 2$, then $C = PCC_n$ (of course the latter implies that $d = 2$, so there are no $[n, n-1, d]$ codes for $d \geq 3$ – this is also not hard to show directly).

So let us start with a binary $[n, n-1, d]$-linear code C with $d \geq 2$. Then we form the code C' as follows: take all the words in C that end with 0 and remove the last 0 from each of them. The set of obtained words is C' (thus, C' is a code of length $n-1$ and $|C'|$ is the number of codewords in C that end with 0). The next goal is to show that C' is an $[n-1, n-2, d']$-linear code with $d' \geq 2$ – once you showed this, you can use the induction hypothesis to deduce that $C' = PCC_{n-1}$. This already gives you a lot of information about C, namely you know exactly which words in $\mathbb{F}_2^n$ that end with 0 lie in C. Now use the fact that $d(C) \geq 2$ again and the fact that $\dim(C) = n-1$ (equivalently $|C| = 2^{n-1}$) to show that C must coincide with PCC_n.

6(b) There were many vague arguments for this part. You have to clearly explain how you use the assumption $p = 3$ in your proof.

7. The most common issue on 7 was the lack of justification for the distance of C. Note that in each part you can rigorously justify your answer for the distance without doing long boring computations (but you have to use different characterizations of $d(C)$ for different parts).