Homework #10. Summary of common mistakes

2. Let F be a finite field, $q = |F|$ and $n = q - 1$. Recall that given $\beta \in F$, we let $\Sigma(\beta) = \sum_{j=0}^{n-1} \beta^j$. In most papers there was no full justification of the fact that $\Sigma(1) = -1$. Simply saying that $q-1 \equiv -1$ is not sufficient since, unless q is prime, we are working in the field $\mathbb{F}_q$, NOT in the ring of congruence classes $\mathbb{Z}_q$.

4. In many papers the overall structure of the proof of Lemma 21.2(2) was unclear. In that part you are asked to prove equivalence of 3 conditions (i), (ii), (iii), and you should clearly state how you are proving the equivalence (e.g. you can prove (i)$\Rightarrow$(ii), (ii)$\Rightarrow$(iii) and (iii)$\Rightarrow$(i) OR (i) $\Longleftrightarrow$ (ii) and (i) $\Longleftrightarrow$ (iii)). In this particular problem it is inconvenient to justify any of the two-sided arrows "simultaneously", so to prove, say, (i) $\Longleftrightarrow$ (ii), you probably have to give separate arguments for the implications in both directions.

5. As most people figured out, the key to proving Theorem 22.1 is understanding how the burst length of a single element of F^{mn} may change during interleaving. However, this by itself is not sufficient since for a linear code D, the possible burst lengths of elements of D only determine burst error DETECTION capability of D (this is the content of Lemma 21.1(1)). You need additional information to determine the maximal l such D is l-burst error CORRECTING.

Here is a hint on how to approach this problem. First we introduce some additional terminology. Given $m, n \in \mathbb{N}$ and a field F, define the interleaving map $IL_{m,n} : F^{mn} \to F^{mn}$ as follows: take any element $\vec{v} \in F^{mn}$, write its coordinates in the form of an $m \times n$ matrix where we first fill the first row, then the second row etc., and then again list all the coordinates as a single vector, but now going down the columns (starting from the first column and moving to the right). Declare the resulting vector to be $IL_{m,n}(\vec{v})$.

In other words, we can define $IL_{m,n} : F^{mn} \to F_{mn}$ by

$$IL_{m,n}((v_{11}, v_{12}, \ldots, v_{1n}, v_{21}, \ldots, v_{2n}, \ldots, v_{m1}, \ldots, v_{mn})) \\ = (v_{11}, v_{21}, \ldots, v_{m1}, v_{12}, \ldots, v_{m2}, \ldots, v_{1n}, \ldots, v_{mn}).$$

Now if $C \subseteq F^n$ is a code and $C^m = \{(\vec{c_1}, \ldots, \vec{c_m}) : \vec{c_i} \in C\}$, then $IL(C^m)$ as defined in class is the code $IL_{m,n}(C^m)$, the image of C^m under the map $IL_{m,n}$.

Now the actual hint for Problem 5:

(a) Take any $\vec{v} \in F^{mn}$ and write $\vec{v} = (\vec{v_1}, \ldots, \vec{v_m})$ where $\vec{v_i} \in F^n$ for each n. Let

$$b = \max_{1 \leq i \leq m} BL(\vec{v_i}).$$

Let $\vec{w} = IL_{m,n}(\vec{v})$, the image of $\vec{v}$ under the interleaving map. Prove inequality of the form $BL(\vec{w}) \geq f(b)$ where f is an explicit function of b.

(b) Now use (a), the fact that the map $IL_{m,n}$ is linear (more specifically the fact that $IL_{m,n}(\vec{v} + \vec{v'}) = IL_{m,n}(\vec{v}) + IL_{m,n}(\vec{v'})$) and Lemma 21.2 (more specifically, the equivalence (i) $\iff$ (iii)) to prove Theorem 22.1 from class (in order to do this, you will have to find the optimal function f in part (a)).