# Problem set 1

Date: Feb 03, 2021 | Error Correcting Codes-S21
Instructor: Mrinal Kumar | Due: March 10, 2021

---

## Instructions

- Please type the soutions neatly in LaTeXand submit the pdf. If you need to draw any pictures, feel free to do them by hand and attach the pictures. However, handwritten text will not be accepted.
- Discussion on the problems with other members of the class is permitted and to an extent, even encouraged. But, you *must* write the solutions on your own. You *must* also acknowledge any discussions you might have had with others separately for every problem.
- Please do not look up solutions on the internet or in other references. In case you use any sources outside the notes for this course, again properly acknowledge them.
- To get the most out of the problem sets, you are encouraged to think about the problems on your own before discussing them with others, consulting the references or looking at the hints (which some of the problems might have).
- For late submissions, you lose 20% of the points for every day after the deadline.
- The first three problems are from the book, Essential Coding Theory.

## Problems

1. **(10 points)**. A set of vector $S \subseteq \mathbb{F}_q^n$ is called $t$-wise independent if for every set of positions $I \subseteq [n]$ with $|I| = t$, the set $S$ projected to $I$ has each of the vectors in $\mathbb{F}_q^t$ appear the same number of times. In other words, for every $I \subseteq [n]$ with $|I| = t$ and $\mathbf{a} \in \mathbb{F}_q^t$,

$$|\{\mathbf{c} : \mathbf{c} \in C \text{ such that } \mathbf{c}_I = \mathbf{a}\}| = |C|/q^t\,,$$

   where $\mathbf{c}_I$ is the projection of the codeword $\mathbf{c}$ to the coordinates in $I$. Prove that any linear code $C$ whose dual $C^\perp$ has distance $d^\perp$ is $(d^\perp - 1)$-wise independent.

2. **(10 points)**. Let $C_1$ be an $[n_1, k_1, d_1]_2$ binary linear code, and $C_2$ an $[n_2, k_2, d_2]_2$ binary linear code. For vectors $u \in C_1$ and $v \in C_2$, let $u \otimes v$ be the $n_1 \times n_2$ matrix over $\mathbb{F}$ such that $(u \otimes v)_{i,j} = u_i \cdot v_j$. Let $C \subseteq \mathbb{F}_2^{n_1 \times n_2}$ be the subset of $n_1 \times n_2$ matrices whose columns belong to $C_1$ and whose rows belong to $C_2$. $C$ is called the tensor of $C_1$ and $C_2$ and is denoted by $C_1 \otimes C_2$. Prove that $C$ is an $[n_1 n_2, k_1 k_2, d_1 d_2]_2$ binary linear code.

3. In the class, we saw a greedy construction of a $q$-ary code with block length $n$ and message length $k$ on the GV bound in deterministic time $q^n$. In this problem, we will try to get a similar construction for linear codes on the GV bound. We already saw the existence of such codes in the class via a probabilistic argument.

   (a) **(5 points)**. Argue that the probabilistic argument from the class can be derandomized to give a deterministic construction of a linear code of dimension $k$ and block length $n$ over $\mathbb{F}_q$ on the GV bound in time $q^{O(kn)}$.

(b) **(5 points)**. A $k \times n$ matrix $A$ is a Toeplitz Matrix if it satisfies the property that for all $i \in \{2, 3, \ldots, k\}$ and $j \in \{2, 3, \ldots, n\}$, $A_{i,j} = A_{i-1,j-1}$. In particular, a random Toeplitz matrix can be picked by just picking the entries in the first row and column uniformly and independently at random, and then using the relation $A_{i,j} = A_{i-1,j-1}$ to deduce the other entries.

Prove that for any non-zero $\mathbf{x} \in \mathbb{F}_q^k$, the vector $A^T \cdot \mathbf{x}$ is distributed uniformly over $\mathbb{F}_q^n$, where $A$ is a random Toeplitz matrix picked as described above.

(c) **(5 points)**. Argue that the above question implies that a random linear code picked by picking a random Toeplitz matrix as its generator matrix lies on the GV code with non-zero probability (in fact, with high probability).

(d) **(5 points)**. Conclude from the above discussion that there is a deterministic construction of a random linear code with block length $n$ and dimension $k$ over $\mathbb{F}_q$ in time $q^{O(k+n)}$.

4. This question builds up on the lecture on tensor rank. Let $p$ be a prime and $q = p^k$ for $k \in \mathbb{N}$. We did not explictly discuss this in the class, but a useful fact is that the field $\mathbb{F}_q$ is a vector space of dimension $k$ over the field $\mathbb{F}_p$. However, we did discuss that we can view the finite field $\mathbb{F}_q$ as the set of all univariate polynomials $\mathbb{F}[z]$ of degree at most $k-1$, where all the arithmetic happens modulo an irreducible polynomial $g(z) \in \mathbb{F}_p[z]$ of degree equal to $k$. Observe that from the description of $\mathbb{F}_q$ above, there is a very natural bijective $\mathbb{F}_p$ linear map $\Phi$ from $\mathbb{F}_q$ to $\mathbb{F}_p^k$. We will work with this map $\Phi$ for the rest of this problem.

(a) **(5 points)**. For any non-zero $a \in \mathbb{F}_q$, consider the $\mathbb{F}_p$ linear map $M_a : \mathbb{F}_p^k \to \mathbb{F}_p^k$, defined as $M_a(\alpha) = \Phi(a \odot \Phi^{-1}(\alpha))$, where $\odot$ denotes multiplication of two field elements in $\mathbb{F}_q$. Show that every non-zero matrix in the $\mathbb{F}_p$ linear space spanned by $\{M_a : a \in \mathbb{F}_q \setminus \{0\}\}$ is of full rank.

(b) **(15 points)**. Consider the map $\psi : \mathbb{F}_p^k \times \mathbb{F}_p^k \to \mathbb{F}_p^k$, where for every $\alpha \in \mathbb{F}_p^k$ and $\beta \in \mathbb{F}_p^k$, $\psi(\alpha, \beta) = \Phi(\Phi^{-1}(\alpha) \odot \Phi^{-1}(\beta))$, where $\odot$ denotes multiplication of two field elements in $\mathbb{F}_q$. Let $T_\Phi$ be the corresponding $k \times k \times k$ tensor. Adapt the proof of the tensor rank lower bound on the rank of the polynomial multiplication tensor (and the properties of $M_a$ defined above) to deduce a similar lower bound on the rank of the tensor $T_\Phi$.

Note that while the polynomial multiplication tensor was a $k \times k \times (2k-1)$ tensor, $T_\Phi$ is a $k \times k \times k$ tensor, but the lower bound obtained for both the tensors is the same. In this sense, this bound is qualitatively better.