# MATH 797AP HOMEWORK PROBLEMS

FARSHID HAJIR

(1) (a) Prove or Disprove: If $q$ is a prime number, then a subset $\mathcal{C}$ of $\mathbf{F}_q^n$ is a linear code if and only if $\mathcal{C}$ is non-empty and closed under addition.

(b) Prove or Disprove: If $q = p^f$ with $p$ a prime and $f > 1$, then a subset $\mathcal{C}$ of $\mathbf{F}_q^n$ is a linear code if and only if $C$ is non-empty and closed under addition.

(2) Suppose $k, n$ are integers satisfying $0 \leq k \leq n$.

(a) Give a formula for the number $S_q(n)$ of subspaces of $\mathbf{F}_q^n$.

(b) Give a formula for the number $S_q(n, k)$ of $k$-dimensional subspaces of $\mathbf{F}_q^n$.

(c) If you answered (a) before you answered (b), now take the sum of your formula for (b) over all $k$ to get another answer for (a) and see if they seem to match. If you didn't answer (a) yet, now you have!

(d) Compute the total number $N_q(n, k)$ of *all* codes of length $n$ over $\mathbf{F}_q$ of size $q^k$, not just the linear ones. How does this number compare with the number you computed in (b)? What percentage of codes of length $n$ and size $q^k$ are linear?

(3) Show that the Hamming metric $d_H$ is a metric on $\mathbf{F}_q^n$ in the sense that for all $v, v', v'' \in \mathbf{F}_q^n$,

(a) $d_H(v, v') = 0$ if and only if $v = v'$;

(b) $d_H(v, v') = d_H(v', v)$;

(c) $d_H(v, v') + d_H(v', v'') \geq d_H(v, v'')$.

(4) (a) Suppose $\mathcal{C}$ is a code of length $n$ and $\sigma$ is a permutation on $n$ letters, i.e. an element of the symmetric group $S_n$. Let $\widehat{\mathcal{C}} = \mathcal{C}^\sigma$ be the code obtained by applying $\sigma$ to all the words in $\mathcal{C}$. Show that $\mathcal{C}^\sigma$ has the same dimension and minimum distance as $\mathcal{C}$.

(b) Consider the proposal that we say two linear codes of length $n$ over $\mathbf{F}_q$ are isomorphic as codes if and only if they are isomorphic as vector spaces. Is this a good proposal? Discuss.

(c) Now consider the proposal that we say two linear codes, $\mathcal{C}, \mathcal{C}'$ of length $n$ over $\mathbf{F}_q$ are isomorphic as codes if and only if there exists a permutation $\sigma \in S_n$ such that $\mathcal{C}' = \mathcal{C}^\sigma$. Is this a good proposal? Discuss. Can you think of a better notion of code isomorphism?

(5) (a) Show that if $G = [I_k \mid A]$ is a systematic $k \times n$ generator matrix for a linear code $\mathcal{C}$ (so that $A$ is a $k \times (n-k)$ matrix), then $H = [-A^T \mid I_{n-k}]$ is a parity check matrix for $\mathcal{C}$. Here $I_j$ is of course the $j \times j$ identity matrix for every positive integer $j$ and $A^T$ is the transpose of $A$. State and prove a similar statement starting from the parity check matrix which "ends with" an identity matrix.

(b) If the generator matrix $G$ of a code $\mathcal{C}$ is not systematic, show that some permutation of the columns of $G$ yields a systematic generator matrix for a code $\widehat{\mathcal{C}}$. Can you then use (a) to describe a procedure for computing the parity check matrix for a code given by a not-necessarily-systematic generator matrix?

(6) Go to the library (and/or bookstore, and/or catalogue of online library materials) and find a book on Coding Theory. Read the first chapter or two of your chosen book.

(7) Let $\mathcal{C}$ be a binary linear code of length $n$.

(a) Show that the proportion of codewords of even weight to all codewords is either 1 or 1/2.

(b) Assume for the moment that $n \geq 17$. Show that the proportion of codewords whose 17th coordinate is 0 to all codewords is either 1 or 1/2.

(c) Generalize (b).

(d) Suppose $G$ is an abelian group (under an operation $+$) with a subset $A$ satisfying (i) If $a, a' \in A$, then $a - a' \in A$; (ii) if $b, b' \notin A$, then $b - b' \in A$; (iii) if $a \in A, b \notin A$, then $a + b \notin A$. Show that either $A = G$ or $A$ is a subgroup of $G$ of index 2.

(e) Explain how one can prove (a), (b), (c) using (d).

(8) Let $\mathcal{C}$ be an $[n, k]_q$-code. Show that the number of distinct generator matrices for $\mathcal{C}$ is the same as the size of the group of $k \times k$ invertible matrices over $\mathbf{F}_q$, which is

$$|GL_k(\mathbf{F}_q)| = \prod_{i=0,k} (q^k - q^i).$$

(9) Consider *puncturing* an $[n, k, d]_q$-code $\mathcal{C}$ by choosing a column index $1 \leq j \leq n$ and punching that column out, meaning letting $\mathcal{C}_j$ be the length $n-1$ code obtained by removing the $j$th coordinate from each codeword.

(a) Show that $\mathcal{C}_j$ in an $[n, k_j, d_j]_q$-code where $k_j \geq k - 1$ and $d_j \geq d - 1$.

(b) Show that there are at least $n - k$ indices $j$ for which $k_j = k$.

(10) This is a guided problem for establishing the *Plotkin Bound.*

(a) Consider a map $T : \mathbf{F}_q^k \to \mathbf{F}_q$ defined by $T(x_1, \ldots, x_k) = \sum_{i=0}^k a_i x_i$, where $(a_1, a_2, \ldots, a_k)$ is a fixed *non-zero* vector in $\mathbf{F}_q^k$. Show that this this is a surjective map with fibers of uniform size $q^{k-1}$.

(b) Suppose $\mathcal{C}$ is an $[n, k, d]_q$-code and let $B$ be a $q^k \times n$ matrix whose rows are the distinct codewords of $\mathcal{C}$ (in some arbitrary order). Show that for each column of $B$, either the entire column is 0 or each element of $\mathbf{F}_q$ appears in it $q^{k-1}$ times.

(c) Prove the Plotkin Bound: If $\mathcal{C}$ is an $[n, k, d]_q$-code, then

$$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}.$$

Hint: Compute the average weight of the non-zero codewords of $\mathcal{C}$; be sneaky. Now, even more sneakily, compare the minimum distance of the code with the average you just computed.

(d) Does the Simplex Code attain the Plotkin bound? Prove or disprove.