

Math 499C Worksheet #3: Codes, First Steps

Q1. Show that the Hamming distance satisfies the triangle inequality: $d(v, w) + d(w, z) \geq d(v, z)$ for $v, z, w \in A^n$.

Q2. For $A = \{0, 1\}$, suppose v, w, z are words in A^n forming an equilateral triangle i.e. $d(v, w) = d(w, z) = d(v, z)$ and call this common distance $2t$. Show that there is exactly one word $x \in A^n$ such that $d(v, x) = d(w, x) = d(z, x) = t$.

Q3. Suppose C is an (n, M, d) -code over $\{0, 1\}$. Let us “augment” C into a code \overline{C} by adding one parity check bit to each codeword as follows. If $v \in C$ has an odd number of 1s, we tack on an extra 1 at the end and otherwise we tack on a 0. For example, if $C = \{00, 01, 11\}$, then $\overline{C} = \{000, 011, 110\}$. Compute the parameters $(\overline{n}, \overline{M}, \overline{d})$ of \overline{C} .

Q4. Let C be a $(7, 16)$ code over $\mathbb{F}_2 = \{0, 1\}$ with the property that every word in \mathbb{F}_2^7 is at Hamming distance at most 1 from exactly one codeword in C . In other words, for all $v \in \mathbb{F}_2^7$ the set

$$\{x \in C \mid d(x, v) \leq 1\}$$

has size 1.

Can you compute the minimum distance of C ? (A little bird tells me it's 3; can I trust the bird?).

Q5. Let $v = (a_1, a_2, \dots, a_k) \in \mathbb{F}_q^k$ be a non-zero vector. Consider the map $\phi_v : \mathbb{F}_q^k \rightarrow \mathbb{F}_q$ defined by

$$\phi_v((x_1, \dots, x_k)) = a_1x_1 + \dots + a_kx_k.$$

Show that for each $a \in \mathbb{F}_q$, there are q^{k-1} elements of \mathbb{F}_q^k which map to a under ϕ_v .

Q6. Show that in every linear code over \mathbb{F}_2 , either all codewords have even Hamming weight or exactly half of the codewords have even Hamming weight.

Hint: Letting G be a generator matrix for the code, try to apply the previous problem to the map $x \mapsto xG(1, 1, \dots, 1)^t$.

Q7. The Plotkin Bound for Linear Codes. Show that every linear $[n, k, d]_q$ code satisfies

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

Hint: Using the NEXT problem show that the average Hamming weight of the $q^k - 1$ nonzero codewords is at most $n(q-1)(q^k-1)/(q^k-1)$. That will do it because the minimum distance is bounded above by that average (yes? why?).

Q8. Let C be a linear $[n, k, d]$ code over \mathbb{F}_q . Let T be a $q^k \times n$ array whose rows are the codewords of C . Show that each element of \mathbb{F}_q appears in every non-zero column in T exactly q^{k-1} times. (A column is non-zero if it has at least one non-zero element).

Hint: Use Q5.