Coding Theory - Homework 4

Kishlaya Jaiswal

November 22, 2019

Exercise 1

Proof. First we show that

$$max_3(r,2) = 1 + max_2(r-1,2)$$

$$\begin{aligned} n &\leq max_3(r,2) \\ &\iff \exists (n,3) \text{ set in } \mathbb{F}_2^r \\ &\iff \exists [n, n-r, \geq 4] code \\ &\iff \exists [n-1, n-r, \geq 3] code \\ &\iff \exists (n-1,2) \text{ set in } \mathbb{F}_2^{r-1} \\ &\iff n \leq 1 + max_2(r-1,2) \end{aligned}$$

But since we know that $max_2(r-1,2) = 2^{r-1} - 1$ (no. of lines in $\mathbb{F}_2^{r-1}$), we get that $max_3(r,2) = 2^{r-1}$ □

Exercise 2

Proof. Let $V = \mathbb{F}_2^{r+1}$ and
Since every line passing through origin has exactly one more point on it (in V), we get that $V \setminus \{0\} \cong PG(r,2)$.
We can identify any $S \subseteq PG(r,2)$ as $S \subseteq V$.
Now, if S is a maximal $n-cap$ then we know that any 3 vectors in S are linearly independent and hence by the previous problem we know that $|S| = max_3(r+1,2) = 2^r$.
Let $T = V \setminus S$. Clearly $|T| = 2^r$ as $|\mathbb{F}_2^{r+1}| = 2^{r+1}$
We shall show that T is a linear subspace of V.

- $0 \in T$. This is clear as the pullback of S doesn't contain 0 by definition.

- $v \in T \implies \lambda v \in T \forall \lambda \in \mathbb{F}_2$. If $\lambda = 0$ then we are done otherwise if $\lambda v \in S$ then since $v \sim \lambda v \implies v \in S$ which is a contradiction.
- $v, w \in T \implies v + w \in T$. Fix a $s \in S$ and consider the map

$$\begin{aligned} f : V &\longrightarrow V \\ x &\longmapsto s + x \end{aligned}$$

  First note that f is injective and hence it's a bijection. Now for any $s' \in S$, $f(s') = s + s' \in T$ because any 3 points in S are non-collinear (and $s, s', s + s'$ are collinear points). So $f(S) \subseteq T$. But since $|S| = |T| = 2^r$, therefore $f(S) = T$ and so any point in T is of the form $s + x$ for some $x \in S$.

  So let $v = s + s_1$ and $w = s + s_2$, where $s_1, s_2 \in S$.

  Furthermore, since s in the definition of f was arbitrary, we get that $S + S \subseteq T$.

  Hence, $v + w = (s + s_1) + (s + s_2) = s_1 + s_2 \in T$ as required.

It follows that, T' (projection of T in $PG(r, 2)$ and so $|T'| = 2^r - 1$ as T' doesn't contain 0) is a $r - 1$ dimensional subspace of $PG(r, 2)$. Clearly, S and T are disjoint in their images in $PG(r, 2)$ and furthermore, $|S| + |T'| = 2^r + (2^r - 1) = 2^{r+1} - 1 = |PG(r, 2)|$. And therefore, S is obtained from the complement of some hyperplane in $PG(r, 2)$. □

Exercise 3

Proof. Let $\mathbb{F}_q^* = \{a_1, a_2, \ldots a_{q-1}\}$. Consider

$$H = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ a_1 & a_2 & a_3 & \ldots & a_{q-1} & 0 & 1 & 0 \\ a_1^2 & a_2^2 & a_3^2 & \ldots & a_{q-1}^2 & 0 & 0 & 1 \end{pmatrix}$$

We will show that H when considered as a parity check matrix, gives a $[q + 2, q - 1, 4]$ code iff q is even prime power. Otherwise if q is odd prime power, then we get $[q + 2, q - 1, \geq 5]$ code.
First, it is clear that $n = q + 2$ and that the rank of H is 3 and so $k = q - 1$.
Now, if we consider the following submatrix H' of H:

$$H' = \begin{pmatrix} 1 & 1 & 0 \\ a_i & a_j & 1 \\ a_i^2 & a_j^2 & 0 \end{pmatrix}$$

Then $|H'| = (a_j^2 - a_i^2)$.
If q is even prime power, then $|H'| = (a_j^2 - a_i^2) = (a_j - a_i)^2 \neq 0$ as $a_i \neq a_j$.
But if q is odd prime power, then $|H'| = (a_j^2 - a_i^2) = (a_j - a_i)(a_j + a_i) = 0$, whenever a_i and a_j are additive inverses of each other, which are distinct.
(Note that, for characteristic 2 fields, additive inverse of x is x itself).

□