Hamming codes; and generalities on finite fields

George McNinch

2024-02-21

A result on check-matrices.

We resume our discussion from the previous lecture. An $m \times n$ matrix H with entries in $\mathbb{F}_q$ determines a subspace $C \subset \mathbb{F}_q^n$ by the rule

$$C = \{x \mid Hx^T = 0\} = \text{Null}(H).$$

Proposition Suppose that every collection of $d-1$ columns of H is linearly independent and that some collection of d columns of H is linearly dependent.

Then the minimal distance of the code C is d.

Proof Let $x = (x_1, x_2, \cdots, x_n) \in C \subset \mathbb{F}_q^n$.

Let $D = D(x) = \{i \mid x_i \neq 0\}$ so that the weight of x is given by $|D|$.

If we denote by $\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_n$ the *columns* of the matrix H, then we have

$$x_1\mathbf{h}_1 + x_2\mathbf{h}_2 + \cdots + x_n\mathbf{h}_n = 0$$

and thus

$$\sum_{i \in D} x_i \mathbf{h}_i = 0$$

so that the there are $|D|$ columns that are linearly dependent.

If d' denotes the *minimal distance* of the code C, and if x' has weight d' then the indices $D(x')$ define a collection of d' linearly dependent columns. Moreover, any smaller collection of columns is linearly independent; thus $d' = d$.

Remark Given a check matrix H with coefficients in $\mathbb{F}_q$, one can construct a code C_a over the field $\mathbb{F}_{q^a}$ for any natural number a - i.e.

$$C_a = \{x \in \mathbb{F}_{q^a}^n \mid Hx^T = 0\}.$$

This Proposition shows that the *minimal distance* of the code C_a is independent of a, since the minimal distance can be determined from the matrix H.

Projective spaces over $\mathbb{F}_q$ and the Hamming Codes

Projective spaces over a finite field and their size

Definition For a natural number n, the projective space $\mathbb{P}^n$ is defined to be the set lines through the origin in the vector space $\mathbb{F}_q^{n+1}$.

If $0 \neq \mathbf{v} = (v_0, v_1, \cdots, v_n) \in k^{n+1}$, then $\mathbb{F}_q\mathbf{v}$ is a line, and we denote this line using the symbol

$$\mathbb{F}_q\mathbf{v} = [v_0 : v_1 : \cdots : v_n] \in \mathbb{P}^n = \mathbb{P}^n_{\mathbb{F}_q}.$$

For $\lambda \neq 0$ note that $\mathbb{F}_q\mathbf{v} = \mathbb{F}_q\lambda v$, and it follows that

$$[v_0 : v_1 : \cdots : v_n] = [\lambda v_0 : \lambda v_1 : \cdots : \lambda v_n].$$

Example Let's consider $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}_q}$. An arbitrary point has the form $[a : b]$. If $a \neq 0$, this point may be written $[a : b] = [1 : b/a]$. There are exactly q points of the form $[1 : c]$.

If $a = 0$, then b is non-zero and $[0 : b] = [0 : 1]$.

Thus $\mathbb{P}^1 = \{[1 : c] : c \in \mathbb{F}_q\} \cup \{[0 : 1]\}$ so that $|\mathbb{P}^1| = q + 1$.

Proposition: For $n \geq 1$ we have $\mathbb{P}^n = \{[1 : u_1 : u_2 : \cdots : u_n] \mid u_i \in \mathbb{F}_q\} \cup \{[0 : \beta] : \beta \in \mathbb{P}^{n-1}\}$.

In particular,

$$|\mathbb{P}^n| = q^n + |\mathbb{P}^{n-1}|.$$

Sketch: If $v_0 \neq 0$ then $[v_0 : v_1 : \cdots : v_n] = [1 : v_1/v_0 : \cdots : v_n/v_0] = [1 : u_1 : \cdots : u_n]$ where $u_i = v_i/v_0$. Moreover, if $[1 : u_1 : \cdots : u_n] = [1 : u_1' : \cdots : u_n']$ then $u_i = u_i'$ for each i.

On the other hand, points for which $v_0 = 0$ are in one-to-one correspondence with points $\beta = [v_1 : \cdots : v_n]$ in $\mathbb{P}^{n-1}$.

Proposition For $n \geq 1$, we have

$$|\mathbb{P}^n| = \frac{q^{n+1} - 1}{q - 1} = q^n + q^{n-1} + \cdots + q + 1.$$

Proof We proceed by induction on n. When $n = 1$ we have already seen that

$$|\mathbb{P}^1| = q + 1 = \frac{q^2 - 1}{q - 1}.$$

Now let $n > 1$. We have seen that

$$|\mathbb{P}^n| = q^n + |\mathbb{P}^{n-1}|$$

and we know by induction that

$$|\mathbb{P}^{n-1}| = \frac{q^n - 1}{q - 1}.$$

Thus

$$|\mathbb{P}^n| = q^n + \frac{q^n - 1}{q - 1} = \frac{q^{n+1} - q^n + q^n - 1}{q - 1} = \frac{q^{n+1} - 1}{q - 1}.$$

Hamming codes

Let $m \geq 1$.

Bibliography