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 $m \geq 1$ and consider the projective space $\mathbb{P}^{m-1} = \mathbb{P}^{m-1}_{\mathbb{F}_q}$.

List the elements

$$p_1, p_2, \cdots, p_n \quad \text{of } \mathbb{P}^{m-1}$$

so that $n = \dfrac{q^m - 1}{q - 1}$.

For each point $p_i \in \mathbb{P}^{m-1}$, choose a (column) vector h_i in $\mathbb{F}_q^m$ representing p_i, and let H be the $m \times n$ matrix whose columns are the h_i:

$$H = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}.$$

If $b_1, \ldots, b_m$ is a basis for $\mathbb{F}_q^m$, the lines $\mathbb{F}_q b_j$ determine points $p_{i_j} \in \mathbb{P}^{m-1}$, and the corresponding vectors $h_{i_1}, h_{i_2}, \cdots, h_{i_m}$ are again a basis for $\mathbb{F}_q^m$.

This shows that H has m linearly independent columns, since H is $m \times n$ it follows that H has *rank* m.

If we set

$$C = \mathrm{Null}(H) = \{v \in \mathbb{F}_q^n \mid Hv^T = 0\}$$

then the rank-nullity theorem implies that $\dim C = n - m = \dfrac{q^m - 1}{q - 1} - m$.

Proposition C is a $[n, n - m, 3]_q$-code. In particular, the minimal distance of C is $d = 3$.

Proof If p, q are distinct points of $\mathbb{P}^{m-1}$ and if $p = \mathbb{F}_q v$ and $q = \mathbb{F}_q w$ then v and w are linearly independent. In particular, any two distinct columns of H are linearly independent.

On the other hand, let p, q as above and let r be the point determined by the vector $v + w$. Then $\{p, q, r\}$ consists of 3 distinct points of $\mathbb{P}^{m-1}$, say $p = p_i$, $q = p_j$, $r = p_k$. Since $v, w, v + w$ are linearly dependent, it follows that h_i, h_j, h_k are linearly dependent. Thus there are 3 columns of H that are linearly dependent. This shows that C has minimal distance $d = 3$.

Some recollections on finite fields

Proposition Let k be a finite field. Then k contains the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for some prime number p, and $|k|$ is a power of p, say $|k| = p^n$ where $n = \dim_{\mathbb{F}_p} k$.

Proof If k is a finite field, consider the additive subgroup generated by $1 = 1_k$. This additive subgroup is cyclic of some order n, and is in fact a subring of k isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

If n were *composite* this subring would contain zero divisors, which is impossible since k is a field. Thus $n = p$ is *prime* and we see that k contains a copy of $\mathbb{Z}/p\mathbb{Z}$ as required.

We may choose a basis for k as a vector space over $\mathbb{F}_p$, and this basis is finite, say $\dim_{\mathbb{F}_p} k = n$. Writing $\mathbf{b}_1, \cdots, \mathbf{b}_n$ for the elements of this basis, we know that every element of k may be written uniquely in the form

$$s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \cdots + s_n\mathbf{b}_n$$

for scalars $s_i \in \mathbb{F}_p$. Since there are p choices for each scalar s_i, conclude that $|k| = p^n$.

Proposition Let k be a finite field having $q = p^n$ elements. For any $x \in k$ we have $x^q = x$ in k.

Proof We may suppose $x \neq 0$. Then $k = kx$ and thus

$$\prod_{a \in k\ \{0\}} a = \prod_{\alpha \in kx\ \{0\}} \alpha = \prod_{a \in k\ \{0\}} ax = \left(\prod_{a \in k\ \{0\}} a \right) x^{q-1}.$$

Canceling the common non-zero factor, we find that

$$1 = x^{q-1}$$

so that indeed $x = x^q$.

We recall that if F is a field and if $f \in F[T]$, we may find an extension field $F \subset E$ such that f splits over E; i.e. there are elements $a_1, \cdots, a_r \in E$ and $\alpha \in F$ such that

$$f = \alpha(T - a_1)(T - a_2) \cdots (T - a_r).$$

The field $F(a_1, a_2, \cdots, a_r)$ is called a *splitting field* for f.

If $q = p^n$, we write $\mathbb{F}_q$ for a splitting field over $\mathbb{F}_p$ for the polynomial $T^q - T$.

Theorem $\mathbb{F}_q$ is a field having q elements, and any field having q elements is isomorphic to $\mathbb{F}_q$.

Proof The previous Proposition shows that each element of $\mathbb{F}_q$ is a root of $f(T) = T^q - T$. Since the degree of $f(T)$ is q, this shows that $|\mathbb{F}_q| \leq q$. Since the formal derivative satsfies $f'(T) = -1$, one knows that $\gcd(f(T), f'(T)) = 1$ so that $f(T)$ has distinct roots in a splitting field. Thus $f(T)$ has *exactly* q roots, and it follows that $|\mathbb{F}_q| \geq q$ so that indeed $|\mathbb{F}_q| = q$.

The uniqueness assertion follows since any two splitting fields for the polynomial $f(T) \in \mathbb{F}_p[T]$ are isomorphic (this is a general fact about splitting fields).

Proposition Suppose that $a, b \in \mathbb{N}$ and that $a \mid b$. Then $T^a - 1 \mid T^b - 1$ in the polynomial ring $\mathbb{Z}[T]$.

Proof First suppose that $a = 1$. Then

$$\frac{T^b - 1}{T - 1} = T^{b-1} + T^{b-2} + \cdots + T + 1$$

so indeed $T - 1 \mid T^b - 1$ in $\mathbb{Z}[T]$.

Now in general set $U = T^a$ so that $T^b = U^m$ where $m = b/a$.

The preceding discussion shows that $U - 1 \mid U^m - 1$; we have

$$\frac{U^m - 1}{U - 1} = U^{m-1} + U^{m-2} + \cdots + U + 1.$$

Thus

$$\frac{T^b - 1}{T^a - 1} = T^{a(m-1)} + T^{a(m-2)} + \cdots + T^a + 1$$

so indeed $T^a - 1$ divides $T^b - 1$ in $\mathbb{Z}[T]$.

Proposition Let $a, b \in \mathbb{N}$. Then $T^{p^a-1} - 1$ divides $T^{p^b-1} - 1$ in $\mathbb{F}_p[T]$ if and only if $a \mid b$.

Proof $(\Leftarrow)$: Assume that $a \mid b$. The previous proposition shows that $T^a - 1 \mid T^b - 1$ in $\mathbb{Z}[T]$, and it then follows (by evaluation of the polynomials at p) that $p^a - 1 \mid p^b - 1$ in $\mathbb{Z}$.

Now a second application of the previous proposition shows that $T^{p^a-1} - 1$ divides $T^{p^b-1} - 1$ in $\mathbb{Z}[T]$ and *a fortiori* $T^{p^a-1} - 1$ divides $T^{p^b-1} - 1$ in $\mathbb{F}_p[T]$

$(\Rightarrow)$: If $T^{p^a-1} - 1$ divides $T^{p^b-1} - 1$, then it is clear that $T^{p^a-1} - 1$ *splits* over $\mathbb{F}_{p^b}$. In particular, $\mathbb{F}_{p^b}$ contains a splitting field for $T^{p^a-1} - 1$ and hence $\mathbb{F}_{p^b}$ contains (a copy of) $\mathbb{F}_{p^a}$.

Now, notice that the multiplicativity of extension degrees gives

$$b = [\mathbb{F}_{p^b} : \mathbb{F}_p] = [\mathbb{F}_{p^b} : \mathbb{F}_{p^a}] \cdot [\mathbb{F}_{p^a} : \mathbb{F}_p] = [\mathbb{F}_{p^b} : \mathbb{F}_{p^a}] \cdot a$$

so that indeed $a \mid b$.

Example Let's find the irreducible factors of $f(T) = T^8 - 1$ in $\mathbb{F}_{13}[T]$.

Since $8 \nmid 13 - 1 = 12$, $\mathbb{F}_{13}^\times$ does not contain an element of order 8, so $f(T)$ doesn't split over $\mathbb{F}_{13}$.

But $\mathbb{F}_{13}^\times$ does contain an element of order 4, since $4 \mid 12$. Some investigation shows that in fact 5 is an element of order 4 (since $5^2 = 25 = 26 - 1 \equiv -1 \pmod{13}$).

In fact, we know that $T^4 - 1 \mid T^8 - 1$, and we now know that

$$T^4 - 1 = (T - 1)(T + 1)(T - 5)(T + 5).$$

In particular, ± 1 and ± 5 are the (only) roots of $f(T)$ in $\mathbb{F}_{13}$.

If we consider the field $\mathbb{F}_{13^2}$, we see that $\mathbb{F}_{13^2}^\times$ has order $13^2 - 1$. We know that

$$13^2 - 1 \equiv 5^2 - 1 \equiv 24 \equiv 0 \pmod{8}$$

i.e. $8 \mid 13^2 - 1$. Thus $\mathbb{F}_{13^2}^\times$ contains an element of order 8, so $T^8 - 1$ splits over $\mathbb{F}_{13^2}$.

We know that $T^2 - 5$ is irreducible over $\mathbb{F}_{13}$, since if α is a root, then $\alpha^2 = 5 \implies \alpha^8 = 1$ while $\alpha^4 = -1$. Thus $\pm\alpha \notin \mathbb{F}_{13}$ so $T^2 - 5$ has no roots in $\mathbb{F}_{13}$.

We've just seen that each root of $T^2 - 5$ is a root of $T^8 - 1$. Thus $T^2 - 5$ divides $T^8 - 1$.

Similarly, $T^2 + 5$ is irreducible and divides $T^8 - 1$ and we find that

$$\begin{aligned} T^8 - 1 &= (T - 1)(T + 1)(T - 5)(T + 5)(T^2 - 5)(T^2 + 5) \\ &= (T - 1)(T - 12)(T - 5)(T - 8)(T^2 - 5)(T^2 - 8) \end{aligned}$$

is the factorization of $T^8 - 1$ as a product of irreducibles over $\mathbb{F}_{13}$.

`SAGE` agrees:

```
k = GF(13)
k.<T> = PolynomialRing(k)

f = (T-1)*(T-12)*(T-5)*(T-8)*(T^2 - 5)*(T^2 - 8)
f

=>
T^8 + 12

[f.is_irreducible() for f in [ T^2 - 5, T^2 -8 ]]
=>
[True, True]

## in fact, we could have just asked SAGE to factor the polynomial

(T^8  - 1).factor()
=>
(T + 1) * (T + 5) * (T + 8) * (T + 12) * (T^2 + 5) * (T^2 + 8)
```

Bibliography