

# Codes from points in projective space

George McNinch

2024-03-04

## Codes and vectors

From the usual perspective, an  $[n, k]_q$ -code  $C$  is given as a subspace  $C \subset \mathbb{F}_q^n$ . Rather than give the embedding, we are going to explain how the “additional coordinates” can instead be understood using points in  $\mathbb{P}^{k-1}$ .

So, let  $C$  be an  $[n, k]_q$ -code and let the  $k \times n$  matrix  $G$  be a generator matrix for  $C$ .

Let us view the *columns* of  $G$  as a multi-set  $S$  of vectors in  $\mathbb{F}_q^k$ .

**Proposition** The following are equivalent for the natural number  $d$ :

- $d$  is the minimal distance of  $C$
- each hyperplane of  $\mathbb{F}_q^k$  contains at most  $n - d$  vectors of  $S$ , and some hyperplane of  $\mathbb{F}_q^k$  contains exactly  $n - d$  vectors of  $S$ .

**Proof/sketch** Recall that the map  $v \mapsto vG$  gives an isomorphism  $\mathbb{F}_q^k \rightarrow C$ .

Write  $\langle \cdot, \cdot \rangle$  for the standard inner product on  $\mathbb{F}_q^k$ . For a vector  $\mathbf{u} \in \mathbb{F}_q^k$ , write  $\pi_{\mathbf{u}}$  for the hyperplane defined by

$$\pi_{\mathbf{u}} = \{\mathbf{v} \in \mathbb{F}_q^k \mid \langle \mathbf{v}, \mathbf{u} \rangle = 0\}.$$

Notice that  $\pi_{\mathbf{u}} = \pi_{\lambda \mathbf{u}}$  for any  $0 \neq \lambda \in \mathbb{F}_q$ . The  $\pi_{\mathbf{u}}$  for  $\mathbf{u} \neq 0$  are precisely the hyperplanes of  $\mathbb{F}_q^k$ .

Now, label the coordinates of  $vG$  by the points in  $S$ ; for  $s \in S$  the  $s$ -coordinate of  $vG$  is thus  $\langle v, s \rangle$ .

Now the proposition follows from the observation that for  $v \in \mathbb{F}_q^k$ , we have:

$$\langle v, s \rangle = 0 \iff s \in \pi_v.$$

## Points in projective space

We can reformulate the above discussion using the projective space  $\mathbb{P}^{k-1}$  determined by  $\mathbb{F}_q^k$ .

Assume that the generator matrix has no 0-columns. Let  $S$  be the set of points  $[x] \in \mathbb{P}^{k-1}$  where  $x$  is a column of the matrix  $G$ .

Now observe that each hyperplane  $\Pi_{\mathbf{u}}$  in  $\mathbb{P}^{k-1}$  has the form

$$\Pi_{\mathbf{u}} = \{[v] \in \mathbb{P}^{k-1} \mid \langle \mathbf{v}, \mathbf{u} \rangle = 0\}.$$

Repeating the proof given above we obtain:

**Proposition (Reformulation)** The following are equivalent for the natural number  $d$ :

- $d$  is the minimal distance of  $C$
- each hyperplane of  $\mathbb{P}^{k-1}$  contains at most  $n - d$  vectors of  $S$ , and some hyperplane of  $\mathbb{P}^{k-1}$  contains exactly  $n - d$  vectors of  $S$ .

Conversely, given a subset  $S \subset \mathbb{P}^{k-1}$ , we construct a code  $C(S)$  with generator matrix  $G$ , where the columns of  $G$  are vector representatives for the points in  $S$ .

## Polynomials on $\mathbb{P}^1$

Let  $g(X, Y) \in k[X, Y]_d$  be a *homogeneous polynomial of degree  $d$* . Thus  $g(X, Y)$  is a  $k$ -linear combination of *monomials* of the form  $X^i Y^{d-i}$ , say

$$(*) \quad g(X, Y) = \sum_{i=0}^d a_i X^{d-i} Y^i, \quad a_i \in \mathbb{F}_q.$$

Note that we can “evaluate”  $g(X, Y)$  at a point  $P = (x : y) \in \mathbb{P}^1$ ; we write

$$g(P) = g(x, y).$$

Note that since  $g$  is *homogeneous*, for a non-zero  $\lambda \in \mathbb{F}_q$  we have  $g(\lambda x, \lambda y) = \lambda^d g(x, y)$ . Thus, the *value* of  $g$  at  $P$  is not well-defined, but the condition  $g(P) = 0$  is independent of the choice of representative  $(x : y)$  for  $P$ .

If  $g(P) = 0$  for a point  $P \in \mathbb{P}^1$  we say that  $P$  is a *root* of  $g(X, Y)$ .

**Proposition** If  $g(X, Y) \neq 0$  then are  $\leq d$  roots of  $g(X, Y)$  in  $\mathbb{P}^1$ .

**Proof** Recall that  $\mathbb{P}^1 = \{(0 : 1)\} \cup \{(1 : t) \mid t \in \mathbb{F}_q\}$ .

Let's proceed by induction on  $d \geq 1$ .

If  $d = 1$ , then  $g(X, Y) = aX + bY$ , and there is exactly one solution in  $\mathbb{P}^1$ , namely the point  $(-b : a)$ .

Now suppose that  $d \geq 2$  and that every polynomial of degree  $d - 1$  is known to have no more than  $d - 1$  roots in  $\mathbb{P}^1$ . Let  $g(X, Y)$  have degree  $d$ .

First suppose that  $g(0, 1) = 0$  – i.e. that  $(0 : 1)$  is a root of  $g(X, Y)$ . Then

$$g(0, 1) = a_d = 0$$

so that

$$g(X, Y) = \sum_{i=0}^{d-1} a_i X^{d-i} Y^i = X \left( \sum_{i=0}^{d-1} a_i X^{d-i-1} Y^i \right) = X \cdot h(X, Y)$$

where

$$h(X, Y) = \sum_{i=0}^{d-1} a_i X^{d-i-1} Y^i$$

is homogeneous of degree  $d - 1$ . Now, by induction  $h(X, Y)$  has no more than  $d - 1$  roots in  $\mathbb{P}^1$ , and if  $(1 : t)$  is a root of  $g(X, Y)$  then it is also a root of  $h(X, Y)$ . This proves that  $g(X, Y)$  has no more than  $(d - 1) + 1 = d$  roots in  $\mathbb{P}^1$  in this case.

Finally, suppose that  $g(0, 1) \neq 0$ . Thus  $a_d \neq 0$ . In this case, for points of the form  $P = (1 : t)$  we see that

$$g(1, t) = \sum_{i=0}^d a_i t^i,$$

so  $P$  is a root of  $g(X, Y)$  just in case  $t$  is a root of the polynomial  $\sum_{i=0}^d a_i T^i \in \mathbb{F}_q[T]$ . Since this polynomial has degree  $d$ , there are no more than  $d$  such roots  $t \in \mathbb{F}_q$ .

**Construction** We give an example of a construction of a code by specifying points in projective space.

More precisely, let

$$\phi = \phi(T_0, T_1, T_2) \in \mathbb{F}_q[T_0, T_1, T_2]_m$$

be *irreducible* homogeneous of degree  $m$  and let

$$S = \{P \in \mathbb{P}^2 \mid \phi(P) = 0\}.$$

Now, a line  $L$  in  $\mathbb{P}^2$  is determined by a non-zero linear function  $\psi = aT_0 + bT_1 + cT_2$ . Note that  $L$  may be identified with  $\mathbb{P}^1$ . Since  $\phi$  is irreducible,  $\psi \nmid \phi$ ; thus  $\phi$  defines by restriction a non-zero homogeneous polynomial of degree  $m$  on  $L$ <sup>1</sup>. According to the previous Proposition,  $\phi$  has no more than  $m$  roots in  $L$ .

The code  $C(S)$  determined by  $S$  has parameters

$$[|S|, 3, d]_q$$

where  $d \geq |S| - \deg \phi$ . Indeed, the preceding discussion shows that  $|S \cap L| \leq \deg \phi$ .

**Example** Let  $\phi = T_0^2 - T_1T_2$  so that  $\phi$  has degree 2. Then  $|S| = q + 1$ . Indeed,

- $(1 : y : z) \in S \iff yz = 1$  so there are  $q - 1$  solutions of this form.
- $(0 : 1 : z) \in S \iff z = 0$  so there is 1 solution of this form.
- $(0 : 0 : 1) \in S$  gives another solution.

In this case, note that the line  $Y = Z$  has two roots of  $\phi$ , namely  $(1 : 1 : 1)$  and  $(1 : -1 : -1)$ . Since each line has no more than 2 roots of  $\phi$ , it follows that the code  $C(S)$  has minimal distance  $d = q + 1 - 2 = q - 1$  so that  $C(S)$  has parameters

$$[q + 1, 3, q - 2]_q.$$

## An “elliptic quadric”

Let  $f$  be a irreducible homogeneous polynomial of degree 2 in two variables.

**Example** If  $\alpha \in \mathbb{F}_q^\times$  is not a square, so that  $T^2 - \alpha$  is irreducible, we could take  $f(T, S) = T^2 - \alpha S^2$ .

Now form  $F(T_0, T_1, T_2, T_3) = T_0T_1 - f(T_2, T_3) \in k[T_0, T_1, T_2, T_3]_2$  and let

$$Q = \{P \in \mathbb{P}^3 \mid F(P) = 0\}.$$

**Proposition** If  $L$  is a line in  $\mathbb{P}^3$ , then  $Q$  contains no more than 2 points on  $L$ .

**Proof** Let  $L$  be a line in  $\mathbb{P}^3$ . Of course,  $L$  is determined by a 2 dimensional subspace  $W$  of  $\mathbb{F}_q^4$ . Thus there are  $\phi, \psi \in (\mathbb{F}_q^k)^*$  for which  $W = \ker \phi \cap \ker \psi$ ; i.e.

$$L = \{P \mid \phi(P) = \psi(P) = 0\}.$$

Let's write

$$\begin{aligned}\phi &= aX_0 + bX_1 + cX_2 + dX_3 \\ \psi &= a'X_0 + b'X_1 + c'X_2 + d'X_3\end{aligned}$$

for scalars  $a, b, c, a', b', c' \in \mathbb{F}_q$ .

Of course,  $\phi$  and  $\psi$  are linearly independent.

Let us first consider the case where  $\det \begin{bmatrix} a & b \\ a' & b' \end{bmatrix} \neq 0$ . Under this assumption, after replacing  $\phi$  and  $\psi$  by suitable linear combinations  $\alpha\phi + \beta\psi$ , we may suppose that

$$\begin{aligned}\phi &= X_0 - \alpha X_2 - \beta X_3 \\ \psi &= X_1 - \gamma X_2 - \delta X_3\end{aligned}$$

for scalars  $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ .

Thus on  $L$  we have  $X_0 = \alpha X_2 + \beta X_3$  and  $X_1 = \gamma X_2 + \delta X_3$ . For a point  $P = (x_0 : x_1 : x_2 : x_3) \in Q \cap L$  we have

$$Q(P) = (\alpha x_2 + \beta x_3)(\gamma x_2 + \delta x_3) - f(x_2, x_3).$$

<sup>1</sup>To be more precise, one knows that  $\phi$  doesn't vanish on the points of  $L$  in any extension field. Note that if  $m \geq q + 1$ , it is possible that  $\phi(P) = 0$  for every point  $P$  in  $L$ , though there will be some field extension  $\mathbb{F}_{q^r}$  and a point  $Q$  in “ $L$  over  $\mathbb{F}_{q^r}$ ” with  $\phi(Q) \neq 0$ . But in any event, it is still true that  $\phi$  can have no more than  $m$  roots in  $L$ .

i.e.  $(x_2 : x_3)$  is a root of the 2-variable homogeneous polynomial

$$h(X_2, X_3) = (\alpha X_2 + \beta X_3)(\gamma X_2 + \delta X_3) - f(X_2, X_3).$$

Since  $f$  is *irreducible*, the polynomial  $h$  is *non-zero*, and  $h$  thus has no more than 2 solutions in  $\mathbb{P}^1$  so that  $\phi$  has no more than 2 roots in  $L$ .

Next we suppose that  $\det \begin{bmatrix} a & b \\ a' & b' \end{bmatrix} = 0$ . Since one row is a multiple of the other, we may suppose - after replacing  $\psi$  by  $\phi - \lambda\psi$  for suitable  $\lambda \in \mathbb{F}_q$  - that we have

$$\begin{aligned} \phi &= aX_0 + bX_1 + & cX_2 + dX_3 \\ \psi &= & c'X_2 + d'X_3 \end{aligned}$$

If  $a = b = 0$ , then after replacing  $\phi$  and  $\psi$  by suitable linear combinations of  $\phi$  and  $\psi$  we may suppose that  $\phi = X_2$  and  $\psi = X_3$ . Then any point  $(x_0 : x_1 : x_2 : x_3) \in Q \cap L$  has  $x_2 = x_3 = 0$ . Now applying  $\phi$  we find

$$x_0x_1 = f(x_2, x_3) = f(0, 0) = 0$$

so that one of  $x_0, x_1$  must be zero. This leads to the two solutions  $(1 : 0 : 0 : 0)$  and  $(0 : 1 : 0 : 0)$ .

If one of  $a, b$  is non-zero, we may suppose WLOG that  $a \neq 0$  and even that  $a = 1$ . Now, at least one of  $c', d'$  is non-zero and WLOG we suppose that  $c' \neq 0$  and even that  $c' = 1$ .

So we have

$$\begin{aligned} \phi &= X_0 + bX_1 + & cX_2 + dX_3 \\ \psi &= & X_2 + d'X_3 \end{aligned}$$

Replacing  $\phi$  by a suitable  $\phi + t\psi$  we can arrange

$$\begin{aligned} \phi &= X_0 + bX_1 + & +dX_3 \\ \psi &= & X_2 + d'X_3 \end{aligned}$$

For a point

$$\mathbf{x} = (x_0 : x_1 : x_2 : x_3) \in Q \cap L$$

we have

$$\begin{aligned} x_2 &= -d'x_3 \\ x_0 &= -bx_1 - dx_3 \end{aligned}$$

Applying  $\phi$  we find that

$$(-bx_1 - dx_3)x_1 - f(-d'x_3, x_3) = 0.$$

Observe that the polynomial  $f(-d'X_3, X_3)$  is just a multiple of  $X_3^2$ ; say  $f(-d'X_3, X_3) = \alpha X_3^2$ . Now,  $\mathbf{x}$  is a root of the degree 2 homogeneous polynomial

$$H(X_1, X_3) = (-bX_1 - dX_3)X_1 - f(-d'X_3, X_3) = -bX_1^2 - dX_1X_3 - \alpha X_3^2 \in \mathbb{F}_q[X_1, X_3].$$

If either  $b$  or  $d$  is non-zero, then  $H$  is non-zero. If  $b = d = 0$ , the irreducibility of  $f$  shows that  $f(0, X_3)$  is a *non-zero* multiple of  $X_3$  - i.e.  $\alpha \neq 0$ . So in all cases,  $H \neq 0$ . Thus,  $H$  has no more than 2 roots in  $\mathbb{P}^1$ . This shows that  $\phi$  has no more than 2 roots in the line  $L$  determined by  $\phi, \psi$ .

This completes the proof.

The points in  $Q$  are easy to describe; they are as follows:

$$Q = \{(1 : f(x, y) : x : y) \mid x, y \in \mathbb{F}_q\} \cup \{(0 : 1 : 0 : 0)\}.$$

In particular, this shows that  $|Q| = q^2 + 1$ .

Now form the  $4 \times (q^2 + 1)$  matrix  $H$  whose columns are vector representatives for the points in  $Q$ .

The previous Proposition immediately implies:

**Corollary** Any 3 columns of  $H$  are linearly independent.

**Proof** Indeed, if  $P_1, P_2, P_3 \in Q$  are distinct points, the proposition shows that they are not co-linear. Hence if the vectors  $v_1, v_2, v_3$  are representatives of the  $P_i$ , the span  $\mathbb{F}_q v_1 + \mathbb{F}_q v_2 + \mathbb{F}_q v_3$  must have dimension 3.

On the other hand,  $H$  has 4 linearly dependent columns, at least if  $q \geq 3$ . For this it is enough to see that there is a plane in  $\mathbb{P}^3$  containing 4 points of  $Q$ . In fact, any three points  $P_1, P_2, P_3$  in  $Q$  determine a unique plane  $H$  in  $\mathbb{P}^3$ , and there are  $q + 1$  points of  $Q$  contained in  $H$ .

We write  $C^\perp$  of the code generated by the rows of  $H$  – i.e.  $C^\perp = C(Q)$ . Thus  $C^\perp$  is a  $[q^2 + 1, 4]_q$ -code.

Now, the code  $C$  dual to  $C^\perp$  has check matrix  $H$ . The corollary shows that the minimal distance  $d$  of  $C$  satisfies  $d = 4$  so that  $C$  is a  $[q^2 + 1, q^2 - 3, 4]_q$ -code.

In fact, one can describe the weight-enumerator polynomial of  $C^\perp$  geometrically, and then use the McWilliams identity to get the weight-enumerator polynomial for  $C$ ; see (Ball 2020, sec. 4.6, page 62)

## Bibliography

---

## Bibliography

Ball, Simeon. 2020. *A Course in Algebraic Error-Correcting Codes*. Compact Textbooks in Mathematics. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-030-41153-4>.