The notion of a code and some examples

George McNinch

2024-02-14

The idea

We want to *transmit* information over a potentially noisy channel. So we want to *encode* our information in some way that permits us to later *decode* it even in the presence of transmission errors.

We want to exploit *algebra* to create our codes. We will use as our *alphabet* a finite field $K = \mathbb{F}_q$

Some recollections about finite fields

We pause to recall some information about finite fields. We plan to return to this topic.

First of all, any finite field K contains a copy of the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for some prime number $p > 0$. Moreover, K can then be viewed as a finite-dimensional vector space over $\mathbb{F}_p$; as such, if $d = \dim_{\mathbb{F}_p} K$ we see that $\#K = |K| = p^d$.

Thus every finite field has order a power of some prime number p.

On the other hand, for any prime power $q = p^d$ there is a finite field $\mathbb{F}_q$ which is *unique up to isomorphism*.

For example, $\mathbb{F}_9 = \mathbb{F}_3[i] = \mathbb{F}_3 + \mathbb{F}_3 i$ where $i^2 = -1 = 2 \in \mathbb{F}_3$. In fact,

$$\mathbb{F}_9 \simeq \mathbb{F}_3[T]/\langle T^2 + 1\rangle$$

(quotient of the *polynomial ring* $\mathbb{F}_3[T]$ by the principal ideal generated by the minimal polynomial $T^2 + 1$ of the element $i \in \mathbb{F}_9$. This isomorphism identifies i with the coset $T + \langle T^2 + 1\rangle$).

Codewords as vectors

We are going to study what are known as *linear codes* C. A linear code C is a linear subspace $C \subseteq \mathbb{F}_q^n$ for some natural number n.

Thus a *code word* is a vector $\mathbf{v} \in C$, and we can write $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ for elements v_i in our *alphabet* $k = \mathbb{F}_q$.

We write k for the *dimension* of C; i.e. $k = \dim_{\mathbb{F}_q} C$. We say that C is an $[n, k]$-code, or more precisely an $[n, k]_q$-code.

Specifying a code via a *generator matrix*.

Let C be an $[n, k]_q$-code, and choose a *basis* $b_1, \cdots, b_k$ for C as $\mathbb{F}_q$-vector space.

Since $C \subset \mathbb{F}_q^n = \mathbb{F}_q^{1\times n}$, we view elements of C as $1 \times n$ *row vectors*.

Now form the matrix $k \times n$ matrix G whose *rows* are the $1 \times n$ vectors $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_k$:

$$G = \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_k \end{bmatrix}.$$

G is known as a *generator matrix* for the code C.

Notice that we recover C from G as the *image* of the linear transformation $\mathbb{F}_q^k \to \mathbb{F}_q^n$ determined by *right-multiplication with* G:

$$C = \{\mathbf{x}G | \mathbf{x} \in \mathbb{F}_q^{1\times n}\} = \text{image}(\mathbf{x} \mapsto \mathbf{x}G).$$

Standard form

Let us write $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ for the *standard basis* for $\mathbb{F}_q^n$.

Lemma: Let C be an $[n,k]_q$-code, and let G be a generator matrix for C.

a. After possibly replacing the basis $\mathbf{e}_1, \cdots, \mathbf{e}_n$ with the basis $\mathbf{e}_{\sigma(1)}, \cdots, \mathbf{e}_{\sigma(n)}$ for some $\sigma \in S_n$, we may suppose that the first k-columns of the $k \times n$ matrix are linearly independent.

b. If the conclusion a. holds, then C has a generator matrix of the form

$$G' = \left[\ \mathbf{I}_k \mid A\ \right]$$

for some $k \times (n-k)$ matrix A, where $\mathbf{I}_k$ denotes the $k \times k$ identity matrix.

Proof of the Lemma:

a. By construction, G has k linearly independent rows (its rows are a *basis* for C). Since G is $k \times n$ it follows that the rank of G is equal to k.

   Since the *row rank* of a matrix is equal to the *column rank* of the matrix, it follows that G has k linearly independent columns. After possibly re-ordering the order of these columns, we may arrange that G has the required form.

b. Suppose that the first k-columns of G are linearly independent and consider the projection mapping

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q^k \quad \text{given by the rule} \quad \pi(x_1, \cdots, x_n) = (x_1, \cdots, x_k).$$

   Write $1, 2, \cdots, b_k \in \mathbb{F}_q^{1\times n}$ for the *rows* of G.
   Since the first k-columns of G are linearly independent, the rank of the $k \times k$ matrix whose rows are the $1 \times k$-vectors $\pi(1), \pi(2), \cdots, \pi(k)$ is equal to k.

   This shows that the dimension of $\pi(C)$ is $\geq k$, and hence that $\pi(C) = \mathbb{F}_q^k$. In other words, the restriction $\pi_{|C} : C \to \mathbb{F}_q^k$ of π to C is *surjective*.

   In view of the surjectivity, for $i = 1, 2, \cdots, k$ we may choose a vector $i' \in \pi^{-1}(\mathbf{e}_i) \cap C$.

   Let G' whose rows are the vectors i':

$$G' = \begin{bmatrix} 1' \\ 2' \\ \vdots \\ k' \end{bmatrix}.$$

   Since

$$\begin{bmatrix} \pi(1') \\ \pi(2') \\ \vdots \\ \pi(k') \end{bmatrix} = \mathbf{I}_k,$$

   G' has the required properties.

We say that a $(k \times n)$ generator matrix G for the $[n,k]_q$-code C is in *standard form* if it has the form

$$G = \left[\ \mathbf{I}_k \mid A\ \right]$$

for some $k \times (n-k)$ matrix A; thus the Lemma asserts that (after possibly changing the ordering of the coordinates on $\mathbb{F}_q^n$) every code C has a generator matrix in standard form.

Check matrices

The preceding discussion described the subspace C by giving *generators* for the vector space. In contrast, we may also specify a subspace using *linear equations*.

So: let C be an $[n,k]_q$-code.

Consider the quotient linear mapping $x \mapsto x + C$:

$$\mathbb{F}_q^n \to \mathbb{F}_q^n / C \simeq \mathbb{F}_q^{n-k}$$

There is an $(n-k) \times n$ matrix H which represents this linear mapping; then

$$C = \text{Null}(H) = \{x \in \mathbb{F}_q^{1 \times n} \mid Hx^T = 0\};$$

i.e. we see that C is the null space for some $(n-k) \times n$ matrix H.

We say that such a matrix is a *check matrix* for C. For a vector $x \in \mathbb{F}_q^{1\times n}$, we can check membership in C using H: we have $x \in C \iff Hx^T = 0$.

Proposition: Suppose that C is an $[n,k]_q$-code and that

$$G = [\ \mathbf{I}_k \mid A\ ]$$

is a generator matrix for C in standard form. Then the $(n-k) \times n$ matrix

$$H = [\ -A^T \mid \mathbf{I}_{n-k}\ ]$$

is a check matrix for C.

Proof: We observe that

$$H \cdot G^T = [\ -A^T \mid \mathbf{I}_{n-k}\ ] \left[\begin{array}{c} \mathbf{I}_k \\ \hline A^T \end{array} \right] = -A^T \cdot \mathbf{I}_k + \mathbf{I}_{n-k} \cdot A^T = -A^T + A^T = \mathbf{0}.$$

Since the rows of G are a basis for C, this shows that $Hx^T = 0$ for every $x \in C$, i.e. $C \subset \text{Null}(H)$.

Now, H clearly has rank $(n-k)$, so $\dim C = \dim \text{Null}(H)$ and hence $C = \text{Null}(H)$. This completes the proof.

Weights and distance

For a vector $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_q^n = \mathbb{F}_q^{1\times n}$ we define weight(v) to be the number of non-zero entries; i.e.

$$\text{weight}(v) = \#\{i \mid v_i \neq 0\}.$$

For two vectors $v, w \in \mathbb{F}_q^n$ the *distance* between v and w is defined to be

$$\text{dist}(v, w) = \text{weight}(v - w).$$

Thus dist(v,w) represents the number of coordinates in which v and w *differ*.

For a subspace $C \subset \mathbb{F}_q^n$ - i.e. a *code* - we define the *minimal distance* of C to be

$$d = \min\{\text{dist}(v, w) \mid v, w \in C, v \neq w\}.$$

The following lemma is immediate:

Lemma: $d = \min\{\text{weight}(v) \mid v \in C, v \neq 0\}$.

If d is the *minimal distance* of the $[n,k]_q$ code C, we say that C is an $[n,k,d]_q$-code.

Example

We investigate an example using `SageMath`.

Let's create the field `k` having 3 elements, and the standard vector space `V=k^9`

```
K = GF(27);
V = VectorSpace(k,9)
print(k)
print(V)

=>
Finite Field in z3 of size 3^3
Vector space of dimension 9 over Finite Field in z3 of size 3^3
```

Now let's create a certain 3 dimensional subspace `C` of `V` – a $[9, 3]_3$ *code* – essentially by giving its *generator matrix*.

```
C = V.subspace([V([1,0,0,1,1,0,1,1,2]),
                V([0,1,0,1,0,1,1,2,1]),
                V([0,0,1,0,1,1,2,1,1])])
C
=>
Vector space of degree 9 and dimension 3 over Finite Field in z3 of size 3^3
Basis matrix:
[1 0 0 1 1 0 1 1 2]
[0 1 0 1 0 1 1 2 1]
[0 0 1 0 1 1 2 1 1]
```

In order to manipulate the generator matrix *as a matrix*, we create the `MatrixSpace` of the right dimensions, and *coerce* the basis of `C` into a matrix:

```
MM = MatrixSpace(K,3,9)
G = MM.matrix(C.basis())
G
=>
[1 0 0 1 1 0 1 1 2]
[0 1 0 1 0 1 1 2 1]
[0 0 1 0 1 1 2 1 1]
```

We investigate the *weights* of non-zero vectors in `C`:

```
# count the non-zero entries in a vector
def weight(v):
    r = [x for x in v if x != 0]
    return len(r)

# we now find the minimum of the weight of v for non-zero vectors v in C
min([ weight(v) for v in C if v != 0 ])
=> 6
```

This shows that C is a $[9, 3, 6]_3$-code.

Notice that the generator matrix `G` is in standard form. Let's extract from `G` the matrix `A` which is the `3 x 6` matrix for which `G = [ I | A ]`

```
A = MatrixSpace(K,3,6).matrix([b[3:9] for b in G])
A
=>
[1 1 0 1 1 2]
[1 0 1 1 2 1]
[0 1 1 2 1 1]
```

We can now form the 6 × 9 *check matrix* `H = [ -A.T | I ]` as above.

```
# form the 6x6 identity matrix
i6=MatrixSpace(K,6,6).one()

# we construct H via *block_matrix*
H=block_matrix([[-A.transpose(),i6]],
               subdivide=False)

H
=>
[2 2 0 1 0 0 0 0 0]
[2 0 2 0 1 0 0 0 0]
[0 2 2 0 0 1 0 0 0]
[2 2 1 0 0 0 1 0 0]
[2 1 2 0 0 0 0 1 0]
[1 2 2 0 0 0 0 0 1]
```

We can confirm that `H * G.T == 0` and that `H` has rank 6:

```
H * G.T == 0
=>
True

rank(H)
=>
6
```

And indeed, if we use `SAGE` to check the `right_kernel` of the matrix `H`, we get exactly the subspace `C`.

```
H.right_kernel() == C
=>
True
```

So `H` is indeed a check-matrix for the code `C`.

Bibliography

Bibliography