Linear codes

George McNinch

2024-02-28

Dual codes and weight enumerators

Consider a $[n,k]_q$-code C, and write
$$\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$$
for the *standard inner product*; if $\mathbf{e}_1, \cdots, \mathbf{e}_n$ are the standard basis vectors, then we have
$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij}.$$

We write $C^\perp$ for the *dual code* to C defined by the rule
$$C^\perp = \{\mathbf{w} \in \mathbb{F}_q^n \mid \langle \mathbf{w}, C \rangle = 0\} = \{\mathbf{w} \in \mathbb{F}_q^n \mid \langle \mathbf{w}, x \rangle = 0 \quad \forall x \in C\}.$$

Observe that the natural mapping
$$\mathbb{F}_q^n \to C^*$$
given by $\mathbf{w} \mapsto \langle \cdot, \mathbf{w} \rangle = (x \mapsto \langle x, \mathbf{w} \rangle)$ is a surjection with kernel $C^\perp$. It thus follows that
$$\dim C^\perp = n - \dim C^* = n - \dim C = n - k.$$

In particular, $C^\perp$ is an $[n, n-k]_q$-code.

Remark If $C = C^\perp$, we say that C is *self-dual*. Note that if C is self dual we must have $k = n - k$ so that $n = 2k$ is *even*.

For example, the following is a self-dual $[8,4]_2$ code.

```
k = GF(2)
V = VectorSpace(k,8)

C = V.subspace([V([1,0,0,0,1,1,1,0]),
                V([0,1,0,0,1,1,0,1]),
                V([0,0,1,0,1,0,1,1]),
                V([0,0,0,1,0,1,1,1])])

# generator matrix
G = MatrixSpace(k,4,8).matrix(C.basis())

G * G.T
=>

[0 0 0 0]
[0 0 0 0]
[0 0 0 0]
[0 0 0 0]
```

We see for this example that $C \subset C^\perp$ and thus $C = C^\perp$ since $\dim C = 4 = 8 - 4 = \dim C^\perp$.

Weight enumerators

Consider the polynomial with natural-number coefficients

$$A(T) = \sum_{\mathbf{u} \in C} T^{\text{weight}(\mathbf{u})} \in \mathbb{N}[T].$$

We evidently have

$$A(T) = \sum_{i=0}^{n} A_i T^i = 1 + \sum_{i=1}^{n} A_i T^i$$

where $A_i = \#\{\mathbf{u} \in C \mid \text{weight}(\mathbf{u}) = i\}$ (note that $A_0 = 1$). We call $A(T)$ the *weight-enumerator* polynomial of C.

Example Consider the self-dual $[8,4]_2$-code C introduced above; namely:

```
k = GF(2)
V = VectorSpace(k,8)

C = V.subspace([V([1,0,0,0,1,1,1,0]),
                V([0,1,0,0,1,1,0,1]),
                V([0,0,1,0,1,0,1,1]),
                V([0,0,0,1,0,1,1,1])])
```

We compute its weight-enumerator:

```
R.<T> = PolynomialRing(ZZ)

## compute the weight enumerator, as an element of R
def WE(C):
    return sum([ T^weight(c) for c in C ])

WE(C)
=>
T^8 + 14*T^4 + 1
```

Write $A^{\perp}(T)$ for the weight enumerator. We are going to prove a formula relating $A(T)$ and $A^{\perp}(T)$ due to McWilliams.

The proof involves some *character theory*. We need a few extra tools.

Characters of $\mathbb{F}_q$-vector spaces.

Let tr : $\mathbb{F}_q \to \mathbb{F}_p$ be the *trace map*.

For any finite degree field extension $E \supset F$ we have a trace mapping tr : $E \to F$; for $\alpha \in E$, tr(α) is the trace of the F-linear mapping $E \to E$ given by $x \mapsto \alpha x$.

Proposition If $E \supset F$ is a finite Galois extension, and if $\Gamma = \text{Gal}(E/F)$ is the *galois group*, then for $\alpha \in E$ we have

$$\text{tr}(\alpha) = \sum_{\sigma \in \Gamma} \sigma(\alpha).$$

Proposition If $q = p^2$, then tr : $\mathbb{F}_q \to \mathbb{F}_p$ is given by the formula

$$\text{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{s-1}}.$$

The importance to us of the trace mapping is this: we know how to describe complex characters of $\mathbb{F}_p$, and we use these together with the trace to describe complex characters of $\mathbb{F}_q$.

Fix $\zeta_p = \exp\left(\frac{2\pi i}{p}\right) \in \mathbb{C}^{\times}$.

For a vector $\mathbf{u} \in \mathbb{F}_q^n$, we define a group homomorphism ("character")

$$\chi_{\mathbf{u}} : \mathbb{F}_q^n \to \mathbb{C}^{\times}$$

by the rule

$$\chi_{\mathbf{u}}(\mathbf{v}) = \zeta_p^{\mathrm{tr}(\langle \mathbf{u},\mathbf{v}\rangle)} = \exp\left(\frac{2\pi i}{p}\,\mathrm{tr}(\langle \mathbf{u},\mathbf{v}\rangle)\right)$$

Observe that since $\mathrm{tr}(\alpha) \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for $\alpha \in \mathbb{F}_q$, the complex number $\zeta_p^{\mathrm{tr}(\alpha)}$ is always *well-defined*.

Remark Arguing as in an earlier homework exercise, it is easy to see that $\widehat{\mathbb{F}_q^n} = \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{C}^\times) = \{\chi_{\mathbf{u}} \mid \mathbf{u} \in \mathbb{F}_q^n\}$.

For a finite abelian group A, recall that we write

$$\langle \chi, \phi\rangle_A = \frac{1}{|A|}\sum_{a\in A}\chi(a)\overline{\phi(a)}$$

for the *character inner product*; here $\chi, \phi \in \widehat{A} = \mathrm{Hom}(A, \mathbb{C}^\times)$.

We have the following result from *character theory*:

Proposition For $\mathbf{x} \in \mathbb{F}_q^n$, we have

$$\sum_{\mathbf{u}\in C}\chi_{\mathbf{u}}(\mathbf{x}) \begin{cases} 0 & \text{if } \mathbf{x} \notin C^\perp \\ |C| & \text{if } \mathbf{x} \in C^\perp \end{cases}$$

Proof We know that $\chi_{\mathbf{u}}\mid_C$ is a character of C; i.e. an element of $\widehat{C}$.

Now,

$$\begin{aligned} \sum_{\mathbf{u}\in C}\chi_{\mathbf{u}}(\mathbf{x}) = \sum_{\mathbf{u}\in C}\zeta_p^{\mathrm{tr}(\langle \mathbf{u},\mathbf{x}\rangle)} &= \sum_{u\in C}\chi_{\mathbf{x}}(\mathbf{u}) \\ &= |C|\langle \chi_{\mathbf{x}}, \mathbf{1}_C\rangle_C \\ &= \begin{cases} |C| & \text{if } \chi_{\mathbf{x}} = \mathbf{1}_C \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

where $\mathbf{1}_C$ denotes the trivial homomorphism $C \to \mathbb{C}^\times$.

Now the result follows from the observation that $\chi_{\mathbf{x}} = \mathbf{1}_C$ if and only $\langle \mathbf{x}, \mathbf{u}\rangle = 0 \quad \forall \mathbf{u} \in C$ if and only if $\mathbf{x} \in C^\perp$.

Theorem *(McWilliams' Identity)* If C is an $[n,k]_q$-code, then

$$q^k A^\perp(T) = (1 + (q-1)T)^n \cdot A\left(\frac{1-T}{1+(q-1)T}\right).$$

Proof see (Ball 2020, Theorem 4.13 page 56)

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.