Dual Codes (Duale Kodes)

Definitions: Let $\underline{u} = u_1 u_2 \cdots u_n$ and $\underline{v} = v_1 v_2 \cdots v_n$ be vectors of $V(n,q)$. The **inner product** (binneproduk) of $\underline{u}$ and $\underline{v}$ is the scalar

$$\underline{u} \cdot \underline{v} = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n .$$

$\underline{u}$ and $\underline{v}$ are **orthogonal** if $\underline{u} \cdot \underline{v} = 0$.

If C is a q-ary $[n,k]$-code, then the **dual of C** is defined by

$$C^{\perp} = \{ \underline{v} \in V(n,q) : \underline{u} \cdot \underline{v} = 0 \text{ for all } \underline{u} \in C \},$$

that is, $C^{\perp}$ consists of all vectors of $V(n,q)$ that are orthogonal to every codeword of C.

Question: Is $C^{\perp}$ a linear code?

Lemma 3.5 For any $\underline{u}, \underline{v}, \underline{w} \in V(n,q)$ and $\lambda, \mu \in GF(q)$,

1. $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$
2. $(\lambda \underline{u} + \mu \underline{v}) \cdot \underline{w} = \lambda(\underline{u} \cdot \underline{w}) + \mu(\underline{v} \cdot \underline{w})$.

Proof: See the notes.

Lemma 3.6

Suppose C is a q-ary $[n,k]$-code with generator matrix G. Then $\underline{v} \in C^{\perp}$ if and only if $\underline{v} G^T = \underline{0}$, that is, $\underline{v}$ is in the dual of C if and only if $\underline{v}$ is orthogonal to every row of G.

Proof: Suppose $\underline{v} \in C^{\perp}$. Then $\underline{v} \cdot \underline{u} = 0$ for all $\underline{u} \in C$. Therefore $\underline{v} \cdot \underline{r} = 0$ for every row $\underline{r}$ of G, since the rows of G are codewords.

Conversely, suppose $\underline{r}_1, \underline{r}_2, \ldots, \underline{r}_k$ are the rows of G and that $\underline{v} \cdot \underline{r}_i = 0$ for $i = 1, 2, \ldots, k$.

Consider any $\underline{u} \in C$. Then there are scalars $\lambda_1, \lambda_2, \ldots, \lambda_k \in GF(q)$ such that $\underline{u} = \lambda_1 \underline{r}_1 + \lambda_2 \underline{r}_2 + \cdots + \lambda_k \underline{r}_k$. Therefore

$$\begin{aligned} \underline{v} \cdot \underline{u} &= \underline{v} \cdot (\lambda_1 \underline{r}_1 + \lambda_2 \underline{r}_2 + \cdots + \lambda_k \underline{r}_k) \\ &= \lambda_1 (\underline{v} \cdot \underline{r}_1) + \lambda_2 (\underline{v} \cdot \underline{r}_2) + \cdots + \lambda_k (\underline{v} \cdot \underline{r}_k) \quad \leftarrow \text{(by Lemma 3.5)} \\ &= \lambda_1 0 + \lambda_2 0 + \cdots + \lambda 0 \\ &= 0. \end{aligned}$$

It follows that $v \in C^{\perp}$. ∎

Theorem 3.7 If C is a q-ary $[n,k]$-code, then $C^\perp$ is a q-ary $[n, n-k]$-code.

Proof: Let C be a q-ary $[n,k]$-code.

Suppose that $\underline{v}_1, \underline{v}_2 \in C^\perp$ and $\lambda, \mu \in GF(q)$.

For every $\underline{u} \in C$,

$$(\lambda \underline{v}_1 + \mu \underline{v}_2) \cdot \underline{u} = \lambda(\underline{v}_1 \cdot \underline{u}) + \mu(\underline{v}_2 \cdot \underline{u}) \quad \text{(by Lemma 3.5)}$$

$$= \lambda 0 + \lambda 0 = 0,$$

and therefore $\lambda \underline{v}_1 + \mu \underline{v}_2 \in C^\perp$.

This shows that $C^\perp$ is a linear code.

We must still show that $C^\perp$ has dimension $n-k$.

By equivalence of codes, we may assume that C has a standard form generator matrix

$$G = \begin{bmatrix} 1 & & 0 & a_{1,1} & \cdots & a_{1,n-k} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & a_{k,1} & \cdots & a_{k,n-k} \end{bmatrix}$$

By Lemma 3.6, the elements of $C^\perp$ are precisely those vectors $\underline{v} = v_1 v_2 \cdots v_n$ satisfying

$$v_1 = -a_{1,1} v_{k+1} - \cdots - a_{1,n-k} v_n$$

$$\vdots \qquad\qquad \vdots$$

$$v_k = -a_{k,1} v_{k+1} - \cdots - a_{k,n-k} v_n$$