8 The Dual code

The main idea here is to develop a dramatic speeding up of the previous decoding algorithm. The key concept here will be the use of the inner (or scalar) product on $F^{(n)}$, and the related notion of duality.

Inner product. For $\underline{u}, \underline{v} \in F^{(n)}$, the element of F

$$\underline{u} \cdot \underline{v} = \sum u_i v_i$$

is called the *inner product* of the vectors $\underline{u}$ and $\underline{v}$.

Properties of the inner product.

(1)

$$\begin{aligned} \underline{u} \cdot \underline{v} &= \sum u_i v_i \\ &= (u_1, \ldots, u_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \\ &= \underline{u}\, \underline{v}^T \end{aligned}$$

(matrix multiplication).

(2) $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$ (symmetry).

(3) For scalars $\lambda, \mu \in F$ we have

$$\begin{aligned} (\lambda \underline{u} + \mu \underline{w}) \cdot \underline{v} &= \lambda(\underline{u} \cdot \underline{v}) + \mu(\underline{w} \cdot \underline{v}), \\ \underline{u}(\lambda \underline{v} + \mu \underline{w}) &= \lambda(\underline{u} \cdot \underline{v}) + \mu(\underline{u} \cdot \underline{w}) \end{aligned}$$

(bilinearity).

Given a linear code $C \subset F^{(n)}$ we define the *dual code* (or orthogonal vector space) $C^\perp$ as

$$C^\perp = \{ \underline{v} \in F^{(n)} \mid \underline{v} \cdot \underline{c} = 0 \text{ for every } \underline{c} \in C \}$$

Proposition 15 *$C^\perp$ is a linear code.*

Proof. If $\underline{x}, \underline{y} \in C^{\perp}$ then

$\underline{x} \cdot \underline{c} = \underline{y} \cdot \underline{c} = 0$ for every $\underline{c} \in C$.

Thus

$$(\lambda \underline{x} + \mu \underline{y}) \cdot \underline{c} = \lambda(\underline{x} \cdot \underline{c}) + \mu(\underline{y} \cdot \underline{c}) = 0$$

for every $\underline{c} \in C$.

This implies $\lambda \underline{x} + \mu \underline{y} \in C^{\perp}$. □

Lemma 16 *Let C be a linear code in $F^{(n)}$ with generator matrix G. Then $\underline{x} \in C^{\perp}$ if and only if $\underline{x} G^T = \underline{0}$.*

Here G^T is the transpose of the matrix G.

Proof. Recall that

$$G = \begin{bmatrix} \underline{r}_1 \\ \vdots \\ \underline{r}_k \end{bmatrix},$$

where $\{\underline{r}_i\}$ is some basis of G. Also $\underline{x} G^T = (\underline{x} \cdot \underline{r}_1, \cdots, \underline{x} \cdot \underline{r}_n)$.

If $\underline{x} \in C^{\perp}$ then $\underline{x} \cdot \underline{r}_i = 0$ for every i, so $\underline{x} G^T = \underline{0}$.

If $\underline{x} G^T = \underline{0}$ then $\underline{x} \cdot \underline{r}_i = 0$ for every i. If $\underline{c} \in C$ then $\underline{c} = \sum_i \lambda_i \underline{r}_i$ for some $\lambda_i \in F$, so

$$\underline{x} \cdot \underline{c} = \underline{x} \cdot (\sum \lambda_i \underline{r}_i) = \sum_i \lambda_i (\underline{x}_i \cdot \underline{r}_i) = 0$$

and $\underline{x} \in C^{\perp}$. □

Theorem 17 $\dim(C) + \dim(C^{\perp}) = n$. *Thus if C is an $[n, k]$-code then $C^{\perp}$ is an $[n, n-k]$-code.*

Proof. It is a standard algebraic fact that for any non-degenerate bilinear form (such as our inner product) $\dim(C) + \dim(C^{\perp}) = n$. □

In Part 10 we shall give another proof of this theorem, which is more adapted to our point of view.