Error Correcting Codes: Combinatorics, Algorithms and Applications **(Spring 2011)**

Lecture 7: Dual of a linear subspace

Feb 4, 2011

Lecturer: Atri Rudra *Scribe: Atri Rudra*

In today's lecture we will study the notion of a null/dual space of a linear subspace and prove some properties of the dual spaces.

1 The Inner Product

Recall that for vectors $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$, $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u} \cdot \mathbf{v}^T = \sum_{i=1}^n u_i \cdot v_i$.

The following follows from the definition of the inner product:

Proposition 1.1. *The following properties hold for vectors $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v} \in \mathbb{F}_q^n$ and scalar $\alpha \in \mathbb{F}_q$:*

$$\langle \mathbf{u}_1 + \mathbf{u}_2, \mathbf{v} \rangle = \langle \mathbf{u}_1, \mathbf{v} \rangle + \langle \mathbf{u}_2, \mathbf{v} \rangle,$$

and

$$\langle \alpha \cdot \mathbf{u}_1, \mathbf{u}_2 \rangle = \alpha \cdot \langle \mathbf{u}_1, \mathbf{u}_2 \rangle.$$

2 The Null Space

We begin with the definition of a dual/null space of a linear subspace.

Definition 2.1. *Let $S \subseteq \mathbb{F}_q^n$ be a linear subspace. The* null/dual *space of S, denoted by $S^\perp$, is defined as*

$$S^\perp = \left\{ \mathbf{u} \in \mathbb{F}_q^n \mid \langle \mathbf{u}, \mathbf{v} \rangle = 0 \text{ for every } \mathbf{v} \in S \right\}.$$

Proposition 1.1 and Definition 2.1 imply the following:

Proposition 2.2. *For every linear subspace S, $S^\perp$ is also a linear subspace.*

The following theorem requires more work and we will not prove it in this course:

Theorem 2.3. *For any linear subspace $S \subseteq \mathbb{F}_q^n$,*

$$\dim(S) + \dim(S^\perp) = n.$$

Finally, Definition 2.1 implies the following fact:

Proposition 2.4. *For any linear subspace S, $\left(S^\perp\right)^\perp = S$.*

3 The Parity Check Matrix

As Proposition 2.2 states that $S^\perp$ is a linear subspace, it must have a generator matrix H. (Note that by Theorem 2.3, H is an $(n-k) \times n$ matrix.) This matrix has a special name:

Definition 3.1. *Let S be a linear subspace and let H be a generator matrix of $S^\perp$. Then H is a* parity check matrix *of S.*

The parity check matrix uniquely characterizes its linear subspace. More specifically,

Proposition 3.2. *Let $S \subseteq \mathbb{F}_q^n$ be a linear subspace with a parity check matrix H. Then*

$$S = \{\mathbf{u} | H \cdot \mathbf{u}^T = \mathbf{0}\}.$$

Proof. We begin by proving the inclusion $S \subseteq \{\mathbf{u} | H \cdot \mathbf{u}^T = \mathbf{0}\}$. To this end, let $\mathbf{u} \in S$. Recall that by definition, H has as its ith row the vector $\mathbf{h}_i \in \mathbb{F}_q^n$ such that $\mathbf{h}_1, \ldots, \mathbf{h}_{n-k}$ forms a basis for $S^\perp$. In particular, $\mathbf{h}_i \in S^\perp$. Thus, by Definition 2.1, $\langle \mathbf{h}_i, \mathbf{u} \rangle = 0$. Thus, $H \cdot \mathbf{u}^T = (\langle \mathbf{h}_1, \mathbf{u} \rangle, \ldots, \langle \mathbf{h}_{n-k}, \mathbf{u} \rangle) = \mathbf{0}$, as desired.

We now prove the inclusion $\{\mathbf{u} | H \cdot \mathbf{u}^T = \mathbf{0}\} \subseteq S$. To this end, fix a $\mathbf{u} \in \mathbb{F}_q^n$ such that $H \cdot \mathbf{u}^T = \mathbf{0}$. Consider an arbitrary $\mathbf{x} \in \mathbb{F}_q^{n-k}$. By the associativity of vector-matrix-vector multiplication, we have

$$\langle \mathbf{u}, \mathbf{x}H \rangle = (\mathbf{x}H) \cdot \mathbf{u}^T = \mathbf{x}(H \cdot \mathbf{u}^T) = 0,$$

where the last equality follows from the fact that $H \cdot \mathbf{u}^T = \mathbf{0}$. Recall that as H is the generator matrix of $S^\perp$, we have

$$S^\perp = \{\mathbf{x}H | \mathbf{x} \in \mathbb{F}_q^n\}.$$

The above two equalities along with Definition 2.1 implies that

$$\mathbf{u} \in \left(S^\perp\right)^\perp = S,$$

where the equality follows from Proposition 2.4. This completes the proof. □