18.413: Error-Correcting Codes Lab March 2, 2004

Lecture 8

Lecturer: Daniel A. Spielman

8.1 Vector Spaces

A set $\mathcal{C} \in \{0,1\}^n$ is a vector space if for all $x \in \mathcal{C}$ and $y \in \mathcal{C}$, $x + y \in \mathcal{C}$, where we take addition to be component-wise modulo 2. We note that over $0, 1$, we do not need to state the property that $cx \in \mathcal{C}$ for all $c \in \{0,1\}$, as it is obvious. Note that the all-0 vector is always in $\mathcal{C}$, as it equals $x+x$.

Given vector $x_1, \ldots, x_k$, we define

$$\operatorname{span}(x_1, \ldots, x_k) = \{a_1 x_1 + \cdots + a_k x_k : a_1, \ldots, a_k \in \{0,1\}\}.$$

We say that $x_1, \ldots, x_k$ span $\mathcal{C}$ if $\mathcal{C} = \operatorname{span}(x_1, \ldots, x_k)$.

The following definition is fundamental.

Definition 8.1.1. *The vectors $x_1, \ldots, x_k$ are a basis for $\mathcal{C}$ if they span $\mathcal{C}$ and no proper subset of these vectors spans $\mathcal{C}$.*

Lemma 8.1.2. *The vectors $x_1, \ldots, x_k$ are a basis for $\mathcal{C}$ if and only if they span $\mathcal{C}$ and for each i,*

$$x_i \notin \operatorname{span}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k).$$

Proof. If some subset of $x_1, \ldots, x_k$ spans $\mathcal{C}$, then there exists i such that $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ spans $\mathcal{C}$. As $x_i \in \mathcal{C}$ for all i, we then have

$$x_i \in \operatorname{span}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k).$$

On the other hand, if

$$x_i \in \operatorname{span}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k),$$

then we will show that $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ span $\mathcal{C}$. To see this, let $x_i = \sum_{j \neq i} b_j x_j$. We will now show that every vector in $\operatorname{span}(x_1, \ldots, x_k)$ can be expressed without using x_i. Let

$$x = \sum_j a_j x_j.$$

If $a_i = 0$, then $x \in \operatorname{span}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$. If $a_i = 1$, then

$$x = x_i + \sum_{j \neq i} a_j x_j = \sum_{j \neq i} b_j x_j + \sum_{j \neq i} a_j x_j = \sum_{j \neq i} (a_j + b_j) x_j,$$

and so $x \in \operatorname{span}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$. $\square$

Lemma 8.1.3. *Every vector space $\mathcal{C} \in \{0,1\}^n$ has a basis.*

Proof. We first note that $\mathcal{C}$ spans $\mathcal{C}$. Now, if we have a set S of vectors that spans $\mathcal{C}$, but which is not a basis, then we can find a proper subset of S that spans $\mathcal{C}$. If we replace S by this propert subset, and repeat, we will eventually find a basis. The process cannot go on forever because initially S is finite and at each step is gets smaller. □

Lemma 8.1.4. *Let $\{x_1, \ldots, x_k\}$ be a basis for $\mathcal{C}$. Then, for $(a_1, \ldots, a_k) \in \{0,1\}^k$ and $(b_1, \ldots, b_k) \in \{0,1\}^k$, if there exists a j for which $a_j \neq b_j$, then*

$$\sum_i a_i x_i \neq \sum_i b_i x_i.$$

Proof. We may assume without loss of generality that $a_j = 0$ and $b_j = 1$. Assume by way of contradiction that

$$\sum_i a_i x_i = \sum_i b_i x_i.$$

Then,

$$\sum_{i \neq j} (a_i + b_i) x_i = x_j,$$

so

$$x_j \in \operatorname{span}(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k),$$

contradicting the assumption that $x_1, \ldots, x_k$ is a basis. □

Lemma 8.1.5. *If $x_1, \ldots, x_k$ is a basis of $\mathcal{C}$, then $|\mathcal{C}| = 2^k$.*

Proof. There are 2^k vectors of the form

$$\sum a_i x_i,$$

and by the previous lemma they are all distinct. □

Corollary 8.1.6. *Each basis of a vector space has the same number of elements.*

If $\mathcal{C}$ has a basis of k vectors, then we say that $\mathcal{C}$ has dimension k.

8.2 Dual

Definition 8.2.1. *If $\mathcal{C}$ is a vector space in $\{0,1\}^n$, then the dual of $\mathcal{C}$ is*

$$\mathcal{D} = \left\{ y \in \{0,1\}^n : \forall x \in \mathcal{C}, y^T x = 0 \right\}.$$

This is where we will see a difference between vector spaces over the reals and $\{0,1\}$: we can have vectors in both $\mathcal{C}$ and $\operatorname{dual}(\mathcal{C})$. For example, consider

$$\mathcal{C} = \{0000, 0011, 1100, 1111\}.$$

In this case, we have $\operatorname{dual}(\mathcal{C}) = \mathcal{C}$.

Proposition 8.2.2. *The dual of a vector space is a vector space.*

Proposition 8.2.3. *If $x_1, \ldots, x_k$ is a basis of $\mathcal{C}$ and $\mathcal{D} = \text{dual}(\mathcal{C})$, then*

$$\mathcal{D} = \left\{ y \in \{0,1\}^n : y^T x_1 = 0, \ldots, y^T x_k = 0 \right\}.$$

The remainder of this section is devoted to the proof of:

Lemma 8.2.4. *Let $\mathcal{C}$ be a vector space and let $\mathcal{D} = \text{dual}(\mathcal{C})$. Let $\mathcal{C}$ have dimension k and $\mathcal{D}$ have dimension j. Then, $k + j = n$. Moreover, $\text{dual}(\mathcal{D}) = \mathcal{C}$.*

We first prove that bases can be extended:

Lemma 8.2.5. *Let $x_1, \ldots, x_k$ be the basis of $\mathcal{C} \subseteq \{0,1\}^n$. Then, there exist vector $x_{k+1}, \ldots, x_n$ such that $x_1, \ldots, x_n$ is a basis of $\{0,1\}^n$.*

Proof. It suffices to show that if $k < n$, then there is a vector x_{k+1} such that $x_1, \ldots, x_{k+1}$ is a basis. We may obtain such a vector by choosing any $x_{k+1} \in \{0,1\}^n - \mathcal{C}$, which must be non-empty because $|\mathcal{C}| = 2^k < 2^n$. To prove that $x_1, \ldots, x_{k+1}$ is a basis, we first note that it spans a vector space strictly larger than $\mathcal{C}$, so it's span must have dimension $k+1$. It then follows that no proper subset of these vectors can span this space, as any proper subset would have at most k vectors. $\square$

Proposition 8.2.6. *The dual of $\{0,1\}^n$ is $\left\{\vec{0}\right\}$.*

Lemma 8.2.7. *If $y_1, y_2 \in \{0,1\}^n$ are distinct, and $x_1, \ldots, x_n$ is a basis of $\{0,1\}^n$, then there exists an i such that*

$$x_i^T y_1 \neq x_i^T y_2.$$

Proof. Assume by way of contradiction that this does not hold. Let $y = y_1 - y_2$. As these are distinct, y is non-zero. But, we have

$$x_i^T y = x_i^T (y_1 - y_2) = x_i^T y_1 - x_i^T y_2 = 0,$$

for all i. Thus, $y \in \text{dual}(\text{span}(x_1, \ldots, x_n))$, which contradicts Propositions 8.2.6 and 8.2.3. $\square$

Lemma 8.2.8. *Let $x_1, \ldots, x_n$ be a basis of $\{0,1\}^n$. Then, there exists another basis $y_1, \ldots, y_n$ of $\{0,1\}^n$ such that*

$$x_i^T y_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases} \tag{8.1}$$

Proof. For any $y \in \{0,1\}^n$, let

$$f(y) = (x_1^T y, \ldots, x_n^T y).$$

By Lemma 8.2.7, for $y_1 \neq y_2$, $f(y_1) \neq f(y_2)$. As there are 2^n possible values for y and 2^n possible values for $f(y)$, for each possible $z \in \{0,1\}^n$, there must be some y for which $f(y) = z$. Thus, there must exist $y_1, \ldots, y_n$ that satisfy (8.1).

To show that these span $\{0,1\}^n$, we will show that the only vector in their dual is $\vec{0}$. To see this, consider any $x \neq 0$, express $x = \sum_i a_i x_i$. As some a_i must be non-zero, we have $y_i^T x = 1$ for that i. $\square$

We can now prove the lemma that we set out to prove.

proof of Lemma 8.2.4. Let $x_1, \ldots, x_k$ be a basis of $\mathcal{C}$. By Lemma 8.2.5, there exist $x_{k+1}, \ldots, x_n$ for which $x_1, \ldots, x_n$ is a basis of $\{0,1\}^n$. Let $y_1, \ldots, y_n$ be the inverse basis shown to exist in Lemma 8.2.8. We claim that $y_{k+1}, \ldots, y_n$ is a basis for dual$(\mathcal{C})$. From (8.1), it is clear that each of these vectors is in dual$(\mathcal{C})$. To show that they span dual$(\mathcal{C})$, let $z \in$ dual$(\mathcal{C})$. Express

$$z = \sum_i b_i y_i.$$

If b_i is 1 for some $i \leq k$, then we will have

$$x_i^T z = x_i^T y_i = 1,$$

contradicting the assumption that $z \in$ dual$(\mathcal{C})$. Thus, each vector in dual$(\mathcal{C})$ is spanned by $y_{k+1}, \ldots, y_n$. □

8.3 Codes and Matrices

Let $\mathcal{C}$ be a linear code over $\{0,1\}$. Then, $\mathcal{C}$ can be expressed either as the output of a generator matrix:

$$\mathcal{C} = \left\{ wG : w \in \{0,1\}^k \right\},$$

where G is a k-by-n matrix whose rows form a basis of $\mathcal{C}$, or as those words satisfying a check matrix

$$\mathcal{C} = \left\{ x : Hx = \vec{0} \right\},$$

where H is a $n-k$-by-n matrix whose rows form a basis of the dual space of $\mathcal{C}$.

It turns out that particular matrices are more useful that others. For example, consider the case in which G has the form

$$G = [I_k P],$$

where I_k is the k-by-k identity matrix. In this case, the first k bits of wG are w. Thus, the message that we are encoding appears in the codeword. An encoding matrix that has this property is called *systematic*, and this property is particularly useful if we are trying to estimate the w_is from corrupted versions of x. In general, any encoding matrix whose columns can be permuted into this special form is called *systematic*. One can prove:

Lemma 8.3.1. *If G is a matrix whose rows are a basis, then there is a systematic matrix G' such that*

$$\{wG\} = \left\{wG'\right\}.$$

Sketch. One can obtain G' from Gaussian elimination. You begin by finding some column that has a 1 in the first row. You then add this row to every other row that has a 1 in that column. After you do this, that will be the only row with a 1 in that column. You then move on to do the same for the next row, etc. □

Lemma 8.3.2. *If the span of the rows of G is $\mathcal{C}$, and G has the form*

$$G = [I_k P],$$

then the span of the rows of

$$H = \left[P^T I_{n-k}\right],$$

is $\operatorname{dual}(\mathcal{C})$.