Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 6: Linear Codes

January 26, 2009

Lecturer: Atri Rudra *Scribe: Steve Uurtamo*

1 Vector Spaces

A vector space V over a field F is an abelian group under "+" such that for every $\alpha \in F$ and every $v \in V$ there is an element $\alpha v \in V$, and such that:

i) $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$, for $\alpha \in F, v_1, v_2 \in V$.

ii) $(\alpha + \beta)v = \alpha v + \beta v$, for $\alpha, \beta \in F, v \in V$.

iii) $\alpha(\beta v) = (\alpha\beta)v$ for $\alpha, \beta \in F, v \in V$.

iv) $1v = v$ for all $v \in V$, where 1 is the unit element of F.

We can think of the field F as being a set of "scalars" and the set V as a set of "vectors".

If the field F is a finite field, and our alphabet Σ has the same number of elements as F, we can associate strings from Σ^n with vectors in F^n in the obvious way, and we can think of codes C as being subsets of F^n.

2 Linear Subspaces

Assume that we're dealing with a vector space of dimension n, over a finite field with q elements. We'll denote this as: $\mathbb{F}_q^n$.

Linear subspaces of a vector space are simply subsets of the vector space that are closed under vector addition and scalar multiplication:

In particular, $S \subseteq \mathbb{F}_q^n$ is a linear subspace of $\mathbb{F}_q^n$ if:

i) For all $v_1, v_2 \in S, v_1 + v_2 \in S$.

ii) For all $\alpha \in \mathbb{F}_q, v \in S, \alpha v \in S$.

Note that the vector space itself is a linear subspace, and that the zero vector is always an element of every linear subspace.

3 Properties of Linear Subspaces

We say that a set of vectors $\{v_1, v_2, ..., v_n\} \in V$ is linearly independent over the field F if there is no way to form a scalar multiple of any one of them as a sum of nonzero scalar multiples of the rest of them:

$\sum_{i \neq j} c_i v_i = c_j v_j \implies c_k = 0$ for all $k \in \{1, 2, .., n\}$.

We define the dimension of a linear subspace as the maximum size of a linearly independent subset of that subspace, over the scalar field. Such a maximum linearly independent set is called a basis for the subspace, because every vector in the subspace can be written as a linear combination of vectors from the basis.

Note that such a basis is not unique.

We define the dual subspace $S^{\perp}$ of S to be the set of vectors all of whose standard inner products with vectors from S are zero.

Recall that $S^{\perp}$ is also a linear subspace, and that any basis for the whole vector space can be decomposed into a basis for S and a basis for $S^{\perp}$, where the two bases are disjoint, implying:

dim(S)+ dim$(S^{\perp})$ =dim(V)

Treating linear operators over the vector space as matrices, recall that for every linear subspace $S \subseteq \mathbb{F}_q^n$ of dimension k, there exists a $k \times n$ matrix G over $\mathbb{F}_q$ (which we'll refer to as a generator matrix) such that $S = \{mG | m \in \mathbb{F}_q^k\}$. (Just take G to be any set of basis vectors of S.)

This immediately implies that for $S^{\perp}$, the dual subspace to S, there exists a $(n-k) \times n$ matrix which "generates" $S^{\perp}$. We call this matrix the generator matrix of $S^{\perp}$ and equivalently the parity check matrix of S.

4 Properties of Linear Codes

Define $C \subseteq F_q^n$ to be a linear code if it is a linear subspace of F_q^n.

Because the generator matrix for such a linear code is enough to generate any codeword in the code, we note that the representation of such a code only requires $O(nk)$ symbols from F_q.

As an example, C_{HAM} is a linear code from $\{0,1\}^4 \rightarrow \{0,1\}^7$.

$$G_{HAM} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H_{HAM} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Note that encoding can be accomplished in $O(nk)$ time. For any message vector $m \in \mathbb{F}_q^k$, we can compute $y = C(m)$ as mG.

Error detection, similarly, can be performed in $O(n(n-k))$ time, as we simply check to see if $Hy^T = 0$.

For error correction, note that we can decode any linear code over q symbols in $O(q^k kn)$ time by simply cycling through all possible messages, encoding them, and comparing with our received codeword.

If we assume that the number of errors is small, is there a better algorithm for decoding linear codes?

If the number of errors is e, we can cycle through all possible error vectors of weight e or less, checking to see if any of them represents the error vector for our received message. Because there are $\binom{n}{e}$ ways to choose e locations for an error, and each error can take one of $q-1$ values, we can accomplish this in $O(\binom{n}{e}(q-1)^e kn)$ time. If q is a constant polynomial in n (namely, $q \in n^{O(1)}$), then this results in a polynomial time algorithm whose degree is $O(e)$ (time $\in n^{O(e)}$).

For future reference, we refer to Hy^T as the syndrome of a received word y.

Question for next lecture: Can you construct a linear code such that correcting ≤ 1 error takes $O(n^2)$ time?

5 References

I.N. Herstein (1990), Abstract Algebra, Macmillan