CS 70 SPRING 2006 — LECTURE 2/28/2006

PROFESSOR VAZIRANI

1. Error Correcting Codes

Suppose A wants to send message $m = m_1 m_2 \cdots m_n$ across a noisy channel C to B. A sends message $c = f(m)$ (where f is some encoding function), and where $c = c_1 c_2 \cdots c_{n+l}$ (so f adds l more characters).

$$A \xrightarrow[C]{c_1 c_2 \cdots c_{n+l}} B$$

1.1. Erasure Channel.

B receives the message $c'_1 c'_2 \cdots c'_{n+l}$ where either $c'_i = c_i$ or $c'_i = \texttt{-}$ (message c_i was *erased* by the noisy channel). So, for example, B might receive $c_1\texttt{-}c_3 c_4 c_5 c_6 \texttt{-} \cdots c_{n+l}$. We assume that there are at most k erasures.

It turns out that for $l = k$, we can always recover the original message m. The way we will do this is similar to the secret sharing method we described in a previous lecture.

Work modulo some prime q. Construct the unique polynomial $P(x)$ of degree $n-1$ such that $P(i) = m_i$ for $1 \le i \le n$. Then we construct the message c by $c_j = P(j)$ for $1 \le j \le n + k$.

$$m_1 m_2 \cdots m_n \xrightarrow[f]{} c_1 c_2 \cdots c_{n+k} \xrightarrow[C]{} c'_1 c'_2 \cdots c'_{n+k}$$

If there are at most k erasures, then B receives at least n of the c_j values. Therefore he can interpolate to recover $P(x)$ and hence m.

1.2. General Errors.

B receives the message $c'_1 c'_2 \cdots c'_{n+l}$ where either $c'_i = c_i$ or $c'_i \ne c_i$ (the message c_i was corrupted by the noisy channel). We assume there are at most k errors.

In this case, it turns out that $l = 2k$ suffices to recover the original message m. Again we work modulo some prime q and find the unique polynomial $P(x)$ of degree $n-1$ such that $P(i) = m_i$ for $1 \le i \le n$. Again we construct the message c by $c_j = P(j)$ for $1 \le j \le n + 2k$.

$$m_1 m_2 \cdots m_n \xrightarrow[f]{} c_1 c_2 \cdots c_{n+2k} \xrightarrow[C]{} c'_1 c'_2 \cdots c'_{n+2k}$$

Now consider that at most k of the $n + 2k$ characters have been modified. Can we still reconstruct the original message? We make the following claim:

Claim 1. Suppose some polynomial $Q(x)$ of degree $n-1$ agrees with $n+k$ of the received values. Then $P(x) = Q(x)$.

Scribed by Chris Crutchfield — Last updated March 10, 2006.

The explanation is fairly intuitive. Suppose we have this polynomial $Q(x)$ of degree $n-1$ that agrees with $n+k$ of the received values. By the problem statement, we know that at least n of these points are uncorrupted (and hence come from $P(x)$). But then $Q(x)$ and $P(x)$ are both of degree $n-1$ and agree on at least n points. Therefore by uniqueness, $P(x) = Q(x)$.

Now all we have to do is just pick the correct $n+k$ values and recover the polynomial $Q(x) = P(x)$, right? Well, if you simply try all possibilities, this will take time exponential in k. So we need to do something a bit more clever.

1.3. **Berlekamp-Welch Decoding Algorithm.** As input, we're given pairs (i, c'_i) where $1 \le i \le n+2k$. For $n+k$ choices of j, $1 \le j \le n+2k$, $P(j) = c'_j$, $\deg P = n-1$. The errors are $e_1, e_2, \ldots, e_k$ for $1 \le e_i \le n+2k$.

Consider the "error polynomial" $E(x) = (x-e_1)(x-e_2)\cdots(x-e_k)$. Note that $E(e_i) = 0$ for all i. However, we cannot construct this polynomial because we don't know the error values e_i.

We want to be able to say $P(i) = c'_i$, but this is not possible. But we *can* say $P(i)E(i) = c'_i E(i)$, and this holds for $1 \le i \le n+2k$.

Let $Q(i) = c'_i E(i)$ for $1 \le i \le n+2k$. We define $Q(x) = P(x)E(x)$, and note that Q has degree $n+k-1$, and hence has $n+k$ coefficients.

$$\begin{aligned} Q(x) &= a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-k+1} x^{n-k+1} \\ E(x) &= b_0 + b_1 x + b_2 x^2 + \cdots + b_{k-1} x^{k-1} + x^k \end{aligned}$$

Hence we have $n+k$ unknowns for $Q(x)$ and k unknowns for $E(x)$. Furthermore, we know that

$$a_0 + a_1 i + a_2 i^2 + \cdots + a_{n+k-1} i^{n+k-1} = c'_i(b_0 + b_1 i + \cdots b_{k-1} i^{k-1} + i^k,$$

for $1 \le i \le n+2k$. Therefore we have $n+2k$ linear equations in $n+2k$ unknowns, and hence we can solve for the coefficients of $Q(x)$ and $E(x)$. Letting $P(x) = Q(x)/E(x)$, we recover $P(x)$ and hence the message m.