6.895 Essential Coding Theory	September 27, 2004

Lecture 6

Lecturer: Madhu Sudan — *Scribe: Kyomin Jung*

Remark: We defer the proof of the next statement to some later lecture.(it occurred in the proof of Plotkin bound in the last lecture):
if $x_1, \ldots, x_m \in \mathbb{R}^n$ satisfy $\forall\ i \neq j$, $< x_i, x_j > \leq 0$ then, $m \leq 2n$.

1 Overview

In this lecture we will examine some topics of decoding codes. Especially we will study Welch-Berlekamp algorithm, an error detecting decoding algorithm for Reed Solomon Codes(RS Codes).

2 Decoding linear codes

When we encode or decode linear codes, the some problems of finding efficient algorithm arise.

- Encoding codes: by multiplying the generator matrix, complexity of encoding any linear code is $O(n^2)$.[1]
- Detecting errors : For any linear codes, if the number of errors is less than d, we can detect errors in $O(n^2)$ since it only involves multiplication by H, the error check matrix.
- Decoding from erasures
- Decoding from erroneous codes: This is one of the main topics in codes decoding and in this lecture we will cover one algorithm for RS codes decoding.

3 Decoding from erasure

Given a generator matrix G, and a codeword $y \in (\sum \cup \{?\})^n$ where '$?'$ represents an erasure,
Goal: find x such that xG is consistent with y.
Note that if $y_i \neq ?$, $(xG)_i = x(G_i) = y_i$ because xG is consistent with y. (Here, G_i refers to the ith column of G)
Now construct G' consisting of such ith columns of G, and y' consisting of non ? elements of y. If the number of erasure is less than d, than because $d \leq n-k+1$, we can obtain unique x such that $xG' = y'$. Then this is the required x.

4 Welch-Berlekamp algorithm for RS codes decoding('86)

4.1 Brief history for RS codes decoding

- 1958,1959 - BCH codes were discovered.
- 1960 - Peterson gave a polynomial time algorithm for decoding BCH codes.
- 1963 - Gorenstein Zierler saw that BCH codes and RS codes have a common generalization. And the decoding algorithm extends to more general situation.
- 1968 - Berlekamp, Massey gave more efficient algorithm to decode BCH, RS codes.

[1] Some codes have lower encoding complexity. For example there exists an $O(n(logn)^{O(1)})$ algorithm for encoding RS codes. There even exist some linear-time encoding codes

4.2 Error-locator polynomial

Let's recall the RS decoding problem. In this problem inputs are pairwise distinct α_i's ($i = 1 \ldots n$) and a codeword $y = (y_1, \ldots, y_n) \in \mathbb{F}^n$. Now our goal is to find a polynomial P over $\mathbb{F}$ such that P has degree less than k and (the number of i's s.t. $P(\alpha_i) \neq y_i) \leq \frac{d-1}{2} = \frac{n-k}{2}$. Note that the coefficients of P are the encoded information.

To solve this problem, we may think of an indicator for the i's where error occurred. To this end, we will define a Error-locator polynomial $E(x)$. $E(x)$ will be a polynomial over $\mathbb{F}$ such that $E(\alpha_i) = 0$ if $y_i \neq P(\alpha_i)$ and the degree of E is less than or equal to $\frac{n-k}{2}$.

Claim 1 *Error locator polynomial exists.*

Proof
Let $S = \{\alpha_i | P(\alpha_i) \neq y_i\}$
Then let $E(x) = \prod_{\alpha_i \in S}(x - \alpha_i)$.♠

Now, define $N(x)$ a polynomial over $\mathbb{F}$ by $N(x) = E(x)P(x)$. Then $E(x)$ and $N(x)$ have following properties.

- $deg(E) \leq \frac{n-k}{2}$
- $E \neq 0$
- $deg(N) \leq \frac{n-k}{2} + (k-1) = \frac{n+k}{2} - 1$
- $\forall i \; N(\alpha_i) = E(\alpha_i)y_i$
- $\frac{N}{E} = P$

The proofs for the above properties are straightforward. Now we introduce **Welch-Berlekamp Algorithm**. it uses above properties of E and N.

4.3 Welch-Berlekamp Algorithm

Welch-Berlekamp Algorithm
Find two polynomials $E_0(x)$, $N_0(x)$ such that

1. $degE_0 = fracn - k2$, the highest coefficient of E_0 is 1.
2. $degN_0 \leq \frac{n-k}{2} + (k-1) = \frac{n+k}{2} - 1$
3. $\forall i \; N_0(\alpha_i) = E_0(\alpha_i)y_i$

We can find these E_0 and N_0 using n linear equations of 3) over $\frac{n-k}{2} + \frac{n+k}{2} = n$ unknown coefficients of E_0 and N_0. It can be performed in $O(n^3)$ time.

Let the output of this algorithm be $\frac{N_0}{E_0}$.

Lemma 2 *If (N_1, E_1) and (N_2, E_2) are two solutions satisfying above 1), 2), 3), then*

$$\frac{N_1}{E_1} = \frac{N_2}{E_2} \tag{1}$$

Proof

For all i, $N_j(\alpha_i) = E_j(\alpha_i)y_i$.
If $y_i \neq 0$, we obtain

$$N_1(\alpha_i)E_2(\alpha_i) = N_2(\alpha_i)E_1(\alpha_i) \tag{2}$$

by multiplying $N_1(\alpha_i) = E_1(\alpha_i)y_i$ and $E_2(\alpha_i)y_i = N_2(\alpha_i)$ side by side.
If $y_i = 0$, $N_1(\alpha_i) = N_2(\alpha_i) = 0$. So (2) still holds.
Therefore (2) holds for all i.
Then because N_1E_2 and N_2E_1 have degrees less than n, they must be identical.♠

Now, it can be easily checked that for some polynomial $R(x)$ with degree $\frac{n-k}{2} - deg(E)$, $(E(x)R(x), N(x)R(x))$ is one solution for 1), 2), 3). And by definition of $N(x)$, it also can be easily checked that $\frac{N \cdot R}{E \cdot R} = P$. So for any solution (N_0, E_0) of 1), 2), 3), $\frac{N_0}{E_0} = P$ as expected.

5 Abstracting the algorithm

In this section, we will try to generalize the condition given for the Welch-Berlekamp algorithm. When we consider E,N,P of Welch-Berlekamp algorithm, E is an element of set A of all the polynomials with degree $\frac{n-k}{2}$ or less. Similarly N is an element of set B of all the polynomials with degree $\frac{n+k}{2} - 1$ or less, and P is an element of set C of all the polynomials with degree $k-1$ or less.

Then the problem we need to solve is,

Given (A, B, C) and $y = (y_1, y_2, \ldots, y_n)$ such that y is (in some sense) close to some element of C, Find $E \in A$, $N \in B$ such that $E \neq 0$ and $\forall i \; E_i y_i = N_i$.

More precise description and analysis of this generalization will be given in the next lecture.