EE5583 Error Correcting Codes	October 3, 2013

Lecture 10

Instructor: Arya Mazumdar — *Scribe: Arya Mazumdar*

Reed Solomon Codes

- q-ary Code.
- Length $n \leq q-1$, dimension k.
- Distance $d = n-k+1$.

Decoding: Berlekamp-Welch

Suppose the defining set is $\mathcal{P} = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, $\alpha_i \in \mathbb{F}_q, i = 1, 2, \dots, n$. Let the received vector is $\boldsymbol{r} = (r_1, r_2, \dots, r_n)$. The transmitted vector is $\text{eval}(f) = \boldsymbol{c} = (c_1, \dots, c_n)$ and the error vector is $\boldsymbol{e} = (e_1, \dots, e_n)$, and $\text{wt}(\boldsymbol{e}) \leq t = \frac{n-k}{2}$.

Find a polynomial $Q(x, y) \in \mathbb{F}_q[x, y]$ with the following properties:

1. $Q(x, y) = Q_0(x) + yQ_1(x)$.
2. $\deg(Q_0) \leq n-t-1$ and $\deg(Q_1) \leq n-t-1-(k-1)$.
3. $Q(\alpha_i, r_i) = 0$ for $i = 1, 2, \dots n$.

Lemma 1 *It is always possible to find a polynomial $Q(x, y) \in \mathbb{F}_q[x, y]$ with the above properties.*

Proof The number of unknown coefficients are at most $n-t+n-t-(k-1) = 2n-2t-(k-1) = 2n-n+k-k+1 = n+1$. On the other hand the third condition gives n linear equation involving them. Hence it is always possible to find a solution. ■

Theorem 2 *For a $Q(x, y)$ with the above properties, $f(x) = -\frac{Q_0(x)}{Q_1(x)}$ where $\boldsymbol{c} = \text{eval}(f)$.*

Proof Note, $\deg(Q(x, f(x)) \leq \max(\deg(Q_0), \deg(Q_1)+\deg(f)) = \max(n-t-1, n-t-1-(k-1)+k-1) = n-t-1$. Hence, if there exist $n-t$ or more points where $Q(x, f(x))$ evaluates to zero, $Q(x, f(x)) = 0$.

Now, $r_i = f(\alpha_i) + e_i$. As $\text{wt}(\boldsymbol{e}) = t$, there exists $n-t$ such is, that $r_i = f(\alpha_i)$. Therefore, for at least $n-t$ is, $Q(\alpha_i, f(\alpha_i)) = 0$. Hence, $Q(x, f(x)) = 0 \Rightarrow f(x) = -\frac{Q_0(x)}{Q_1(x)}$. ■

Error-locator polynomial

Q_1 is called error-locator polynomial as its roots give the locations of errors. Indeed,

$$Q(x, y) = Q_0(x) + yQ_1(x) = -Q_1(x)f(x) + yQ_1(x) = Q_1(x)(y - f(x)).$$

Hence, $Q(\alpha_i, r_i) = 0$ implies $Q_1(\alpha_i)(r_i - f(\alpha_i)) = Q_1(\alpha_i)e_i = 0$. Whenever, $e_i \neq 0$, $Q_1(\alpha_i) = 0$.

Interpolation

Given, n points $(\alpha_1, r_1), \dots, (\alpha_n, r_n) \in \mathbb{F}_q^2$, find a polynomial $f(x)$ of degree at most $k-1$ that goes through at least $n-t = \frac{n+k}{2}$ points $\implies$ RS decoding.

List Decoding of RS codes (Sudan)

Consider the following generalization of BW algorithm. Suppose the defining set is $\mathcal{P} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $\alpha_i \in \mathbb{F}_q, i = 1, 2, \ldots, n$. Let the received vector is $\boldsymbol{r} = (r_1, r_2, \ldots, r_n)$. The transmitted vector is $\mathrm{eval}(f) = \boldsymbol{c} = (c_1, \ldots, c_n)$ and the error vector is $\boldsymbol{e} = (e_1, \ldots, e_n)$, and $\mathrm{wt}(\boldsymbol{e}) = t$ (some number).

Find a polynomial $Q(x, y) \in \mathbb{F}_q[x, y]$ with the following properties:

1. $Q(x, y) = Q_0(x) + yQ_1(x) + y^2Q_2(x) + \cdots + y^L Q_L(x)$.
2. $\deg(Q_j) \leq n - t - 1 - j(k-1), j = 0, \ldots L$.
3. $Q(\alpha_i, r_i) = 0$ for $i = 1, 2, \ldots n$.

Theorem 3 *It is possible to find a polynomial* $Q(x, y) \in \mathbb{F}_q[x, y]$ *with the above properties if*

$$t < \min\Big(\frac{nL}{L+1} - \frac{(k-1)L}{2}, n - L(k-1)\Big).$$

Proof Number of coefficients in the polynomial $Q(x, y)$ is

$$(L+1)(n-t) - (k-1)\sum_{j=0}^{L} j = (L+1)(n-t) - (k-1)\frac{L(L+1)}{2} = (L+1)(n - t - (k-1)L/2).$$

If this is greater than or equal to n then the set of equations can be solved to find the polynomial Q. That is, Q can be found if,

$$t < n - \frac{n}{L+1} - (k-1)L/2.$$

At the same time $\deg(Q_j)$ must be nonnegative, i.e.,

$$n - t - 1 - L(k-1) \geq 0.$$

■

Theorem 4 $(y - f(x))$ *divides* $Q(x, y)$.

Proof This will be proved, if $Q(x, f(x)) = 0$.

Note, $\deg(Q(x, f(x))) \leq n - t - 1$. However, just as before, $r_i = f(\alpha_i) + e_i$. As $\mathrm{wt}(\boldsymbol{e}) = t$, there exists $n - t$ such is, that $r_i = f(\alpha_i)$. Therefore, for at least $n - t$ is, $Q(\alpha_i, f(\alpha_i)) = 0$. Hence, $Q(x, f(x)) = 0$. ■

Note that, there are at most L different polynomials f possible that are y-roots of $Q(x, y)$.

Theorem 5 *Given any vector* $\boldsymbol{r}$*, Sudan's algorithm finds all codewords that are within distance* t *from* $\boldsymbol{r}$*. When*

$$t < \min\Big(\frac{nL}{L+1} - \frac{(k-1)L}{2}, n - L(k-1)\Big),$$

there exist at most L *such codewords.*

This is called List Decoding.

Example: Say, $L = 2$. Hence, $t < \min\Big(\frac{2n}{3} - (k-1), n - 2(k-1)\Big)$. When $\frac{k}{n} < \frac{1}{3}$, the decoding radius is $t = \frac{2n}{3} - (k-1) - 1$, say. This is greater than the radius for unique decoding $\frac{n-k}{2}$.