ENEE626: Error-Correcting Codes

Instructor: Alexander Barg | Notes by: Sung Hyun Chun,Randolph Baden

Lectures 20-21 (11/15, 11/19/05). RS Decoding

The Guruswami-Sudan algorithm http://www.ece.umd.edu/~abarg/626

Goal: Construct a list decoding algorithm of RS Codes with the error correction radius τ greater than for the Sudan algorithm. We will think of Sudan's algorithm as of polynomial interpolation, i.e., constructing a polynomial $\mathcal{Q}(x, y)$ such that it "passes" through the n points $(x_i, r_i), i = 1, 2, \dots, n$. This gave us n independent linear conditions. The error correcting radius is restricted by the degree condition and the solvability condition (Conditions 1 and 2 in the previous lecture). It is possible to increase τ if we can have more than n independent linear conditions. The idea that we will pursue in this lecture is to interpolate the polynomial through the given n points so that at each of them it has a root of multiplicity $s > 1$.

Guruswami-Sudan Decoding

Let $\mathcal{Q}(x, y) = \sum_{i,j} \mathcal{Q}_{ij} x^i y^j \in \mathbb{F}_q[x, y]$.

Let us make ourselves comfortable with the idea of $\mathcal{Q}$ having a root of multiplicity s at $(a, b), a, b \in \mathbb{F}_q$.

Begin with an example: The polynomial $f(x) = x^2 - 4x + 3 \in \mathbb{R}[x]$ has a root at 1. Expanding it into a "series" in the neighborhood of $x = 1$, we obtain $f(x) = f_0 + f_1(x - 1) + f_2(x - 1)^2$, where $f_0 = 0, f_1 = -2, f_2 = 1$. Since $f(1) = 0$, we got $f_0 = 0$. Taking $f(x) = 2x^3 - 9x^2 + 12x - 5$ and expanding it in the neighborhood of $x = 1$, we obtain $f(x) = -3(x - 1)^2 + 2(x - 1)^3$. Thus, $x = 1$ is a zero of f of multiplicity $s = 2$. Not only the term $f_0 = 0$, but also $f_1 = 0$, i.e., $f'(1) = 0$.

Let $\overline{\mathcal{Q}}(x, y) = \mathcal{Q}(x + a, y + b) = \sum_{i,j} \overline{\mathcal{Q}}_{ij} x^i y^j$. Then

$$\begin{aligned}
\overline{\mathcal{Q}}(x, y) &= \sum_{i,j} \mathcal{Q}_{ij} \sum_{\alpha} \binom{i}{a} x^{\alpha} a^{i-\alpha} \sum_{\beta} \binom{j}{\beta} y^{\beta} b^{j-\beta} \\
&= \sum_{\alpha,\beta} x^{\alpha} y^{\beta} \sum_{i,j} \mathcal{Q}_{ij} \binom{i}{\alpha}\binom{j}{\beta} a^{i-\alpha} b^{j-\beta} \\
&= \sum_{\alpha,\beta} \overline{\mathcal{Q}}_{\alpha\beta} x^{\alpha} y^{\beta}
\end{aligned}$$

(We relied upon $(x + a)^i = (a + x)^i = \sum_{\alpha} \binom{i}{\alpha} a^{i-\alpha} x^{\alpha}$)

Definition: The point (a, b) is called a zero of $\mathcal{Q}(x, y)$ of multiplicity s if the coefficients of the power series $\overline{\mathcal{Q}}_{ij} = 0$ for $0 \le i + j < s$

(The expression $\overline{\mathcal{Q}}_{\alpha\beta}(x, y) = \sum_{ij} \mathcal{Q}_{ij} \binom{i}{\alpha}\binom{j}{\beta} x^{i-\alpha} y^{j-\beta}$ is called a *Hasse derivative* of $\mathcal{Q}(x, y)$)

Example : Let $\mathcal{Q} \in \mathbb{F}_2[x, y]$ have the form $\mathcal{Q}(x, y) = x^2 y + x^2 + y + 1$. Then $\mathcal{Q}$ a zero of multiplicity 2 at (1,1), since $\mathcal{Q}(x + 1, y + 1) = x^2 y$.

Idea: Fit $\mathcal{Q}(x, y)$ through the points $\{(x_i, r_i), i = 1, 2, \cdots, n\}$ so that at each point (x_i, r_i), $\mathcal{Q}(x, y)$ has a zero of multiplicity s for some $s \ge 1$.

Let $\mathcal{Q}(x, y) = \sum_{j=0}^{l} \mathcal{Q}_j(x) y^j$ be a polynomial such that

1. (x_i, r_i) is a zero of multiplicity $s, i = 1, 2, \cdots, n$
2. deg $\mathcal{Q}_j(x) \le s(n - \tau) - 1 - j(k - 1), j = 0, 1, \cdots, l$

Definition: The weighted degree is defined as $\deg_{1,k-1} x^g y^h = g + (k - 1)h$

Then $\deg_{1,k-1} \mathcal{Q}_j(x) y^j \le s(n - \tau) - 1, j = 0, 1, \dots, l$.

Lemma: Let $\mathbf{c} = \mathrm{eval}(f)$, deg$f \le k - 1$. Let $\mathcal{Q}$ be chosen to satisfy Conditions 1-2. Then $(y - f(x)) | Q(x, y)$.

Proof: (a) First we will show that if i is such that $f(x_i) = r_i$ then $(x - x_i)^s \mid \mathcal{Q}(x, f(x))$. Let $p(x) = f(x + x_i) - r_i$, then $p(0) = 0$ or $x \mid p(x)$. Consider the polynomial $P(x) = \mathcal{Q}(x + x_i, p(x) + r_i)$. By definition of $\mathcal{Q}$, 0 is its zero of multiplicity s, or $x^s \mid P(x)$, therefore $(x - x_i)^s \mid P(x - x_i)$. Finally, $P(x - x_i) = \mathcal{Q}(x, f(x))$, therefore $(x - x_i)|Q(x, f(x))$.
(b) Compute the degree $\deg(\mathcal{Q}(x, f(x)) \le s(n - \tau) - 1$. On the other hand, $(x - x_i)^s \mid \mathcal{Q}(x, f(x))$ for $\ge n - \tau$ values of i. The number of zeros (counted with multiplicities) is greater than the degree, therefore, $\mathcal{Q}(x, f(x)) \equiv 0$ ∎

We again have 2 conditions on the parameters:

Condition 1: The degree of Q_j is positive, i.e., $s(n - \tau) - l(k - 1) > 0$. We will assume that

$$s(n - \tau) = l(k - 1) + 1 \qquad (*)$$

Condition 2: The system $\mathcal{Q}(x_i, r_i) = 0, i = 1, 2, \ldots, n$ has a nonzero solution for the coefficients of $\mathcal{Q}$, which means that the number of unknowns should be greater than the number of coefficients.

For a given point x_i the polynomial $\mathcal{Q}$ has a zero of multiplicity s at the point (x_i, r_i). This means that in the expression $\bar{\mathcal{Q}}(x, y) = \mathcal{Q}(x + x_i, y + r_i)$ the coefficients $\bar{\mathcal{Q}}_{\alpha,\beta}$ with $0 \le \alpha + \beta < s$ are zero. Their number is $\binom{s+1}{2}$. Therefore, the system has $n\binom{s+1}{2}$ equations.

On the other hand, the polynomial has $(l + 1)s(n - \tau) - (k - 1)\frac{l(l+1)}{2}$ coefficients. So the condition is

$$(l + 1)s(n - \tau) - (k - 1)\frac{l(l + 1)}{2} > n\binom{s + 1}{2} \qquad (**).$$

Solving for τ, we obtain

$$\frac{\tau}{n} < -\frac{k}{n}\frac{l}{2s} + \frac{2l - s + 1}{2(l + 1)} + \frac{l}{2sn}.$$

Lemma: If $s < l$ then $\tau > \frac{n-k+1}{2}$, if $\frac{k}{n} < \frac{s}{l+1} + \frac{1}{n}$
Proof: Exercise.

Before formulating the algorithm, let us examine a few examples that detail the error correction radius τ of the algorithm as a function of the list size l and the multiplicity s.

1. $l = 2, s = 1, \frac{k}{n} < \frac{1}{3} + \frac{1}{n}, \frac{\tau}{n} < -\frac{k}{n} + \frac{2}{3}$
2. $l = 3, s = 1, \frac{k}{n} < \frac{1}{4}, \frac{\tau}{n} < -\frac{3}{2}\frac{k}{n} + \frac{3}{4}$
$l = 3, s = 2, \frac{k}{n} < \frac{1}{2}, \frac{\tau}{n} < -\frac{3}{4}\frac{k}{n} + \frac{5}{8}$
3. $l = 4, s = 1, \frac{k}{n} < \frac{1}{5}, \frac{\tau}{n} < -2\frac{k}{n} + \frac{8}{10}$
$l = 4, s = 2, \frac{k}{n} < \frac{2}{5}, \frac{\tau}{n} < -\frac{k}{n} + \frac{7}{10}$
$l = 4, s = 3, \frac{k}{n} < \frac{3}{5}, \frac{\tau}{n} < -\frac{2}{3}\frac{k}{n} + \frac{6}{10}$

These functions are shown in the figure. Notice that for a given l we have freedom in choosing $s < l$. The whole spectrum of choices $s = 0, 1, \ldots, l - 1$ provides an increase of the decoding radius over the list size $l - 1$ for almost all values of the rate k/n (except for a finite number of its values).

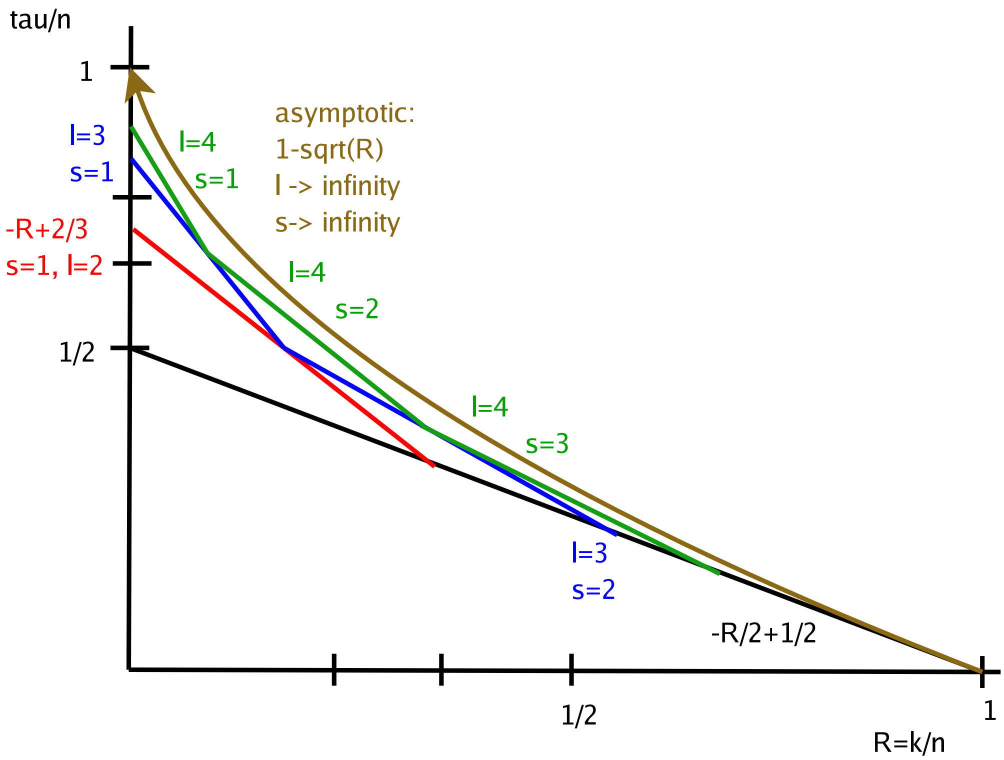

Figure 1: The behavior of the relative error correction radius τ/n as a function of the code rate k/n for $l = 1, 2, 3, 4$, and $l, s \to \infty$.

The Guruswami-Sudan decoding algorithm

Let C be an $[n, k]$ RS code over $\mathbb{F}_q$. Let $\mathbf{c} = \text{eval}(f)$ be the transmitted codeword, $\mathbf{r}$ be the received codeword. Choose l and find the maximum s and τ that satisfy the conditions

$$s(n-\tau) = l(k-1) + 1$$

$$s > \frac{n(k-1) + \sqrt{n^2(k-1)^2 + 4((n-\tau)^2 - n(k-1))}}{2(n-\tau)^2 - n(k-1)}$$

1. Solve the following system for $\mathcal{Q}_{\rho,\sigma}$

$$\sum_{\sigma=0}^{\ell} \sum_{\rho=\alpha}^{\ell_\sigma} \binom{\rho}{\alpha} \binom{\sigma}{\beta} x_i^{\rho-\alpha} r_i^{\sigma-\beta} Q_{\sigma,\rho} = 0$$

   for all $\alpha + \beta < s$, $i = 1, 2, ..., n$.

2. Form the polynomial:

$$\mathcal{Q}(x, y) = \sum_{j=0}^{l} \Big(\sum_{i=0}^{l_j} \mathcal{Q}_{j,i} x^i \Big) y^j$$

3. Find all y-roots of $\mathcal{Q}$, that is, find all $f(x)$ where $(y - f(x)) | \mathcal{Q}(x, y)$

4. Output the codewords $\mathbf{c} = \text{eval}(f)$ such that $d(\mathbf{c}, \mathbf{r}) \leq \tau$.

The implementation complexity of the most efficient version of the GS algorithm is $O(n^2m^4)$.

Let us justify the choice of s.

Lemma: If $(n-\tau)^2 > n(k-1)$, s is chosen as described above and l is chosen from $s(n-\tau) = l(k-1)+1$ then

$$(l+1)s(n-\tau) - (k-1)\frac{l(l+1)}{2} > n\binom{s+1}{2}.$$

Proof: Let us transform the inequality in question to a more convenient form.

$$(l+1)(l(k-1)+1) - (k-1)\frac{l(l+1)}{2} = (l+1)\Big[l(k-1)+1-\frac{l(k-1)}{2}\Big]$$

$$= \frac{(l+1)(l(k-1)+2)}{2} > \frac{l}{2}(l(k-1)+2).$$

Thus if

$$\frac{l}{2}(l(k-1)+2) > n\frac{s(s+1)}{2} \qquad (***)$$

then we will have proved the lemma. We have chosen

$$l = \frac{(n-\tau)s-1}{k-1}, \quad l(k-1)+2 = s(n-\tau)+1.$$

Thus, by $(***)$ we need to check the inequality

$$\frac{(n-\tau)s-1}{k-1}(s(n-\tau)+1) > n\frac{s(s+1)}{2}.$$

Solving this for s, we obtain the inequality

$$s > \frac{n(k-1)+\sqrt{n^2(k-1)^2+4((n-\tau)^2-n(k-1))}}{2((n-\tau)^2-n(k-1))}.$$

∎

The inequality $(n-\tau)^2 > n(k-1)$ implies for large n

$$\frac{\tau}{n} \le 1-\sqrt{R}.$$

This is the asymptotic (relative) *error correcting radius* of the GS algorithm. Observe that this is always better than $(n-k)/(2n)$ (the list-of-one error correction radius) because

$$\frac{1-R}{2} - 1 + \sqrt{R} = \sqrt{R} - \frac{1+R}{2} < 0$$

the last step by the arithmetic mean-geometric mean inequality.

Soft-decision decoding

Suppose that instead of $r_i \in \mathbf{F}_q$ we receive a signal r_i and can find $P(a|r_i)$ for all $a \in \mathbf{F}_q$.

What we see is a matrix:

	1	2	...	j	...	n
0	$P(0\|r_1)$	$P(0\|r_2)$		$P(0\|r_j)$		$P(0\|r_n)$
1	$P(1\|r_1)$	$P(1\|r_2)$		$P(1\|r_j)$		$P(1\|r_n)$
.						
.						
.						
a	$P(a\|r_1)$	$P(a\|r_2)$		$P(a\|r_j)$		$P(a\|r_n)$
.						
.						
.						
$q-1$	$P(q-1\|r_1)$	$P(q-1\|r_2)$		$P(q-1\|r_j)$		$P(q-1\|r_n)$

Suppose that this matrix is transformed to a $q \times n$ matrix W with nonnegative integer entries, for instance, by multiplying its entries by the largest denominator (under the assumption that the probabilities above are rational numbers). We would like to decode to a codeword $\mathbf{c} = (c_1, \ldots, c_n)$ that maximizes the quantity

$$\sum_{i=1}^{n} W_{c_i,i}$$

It is possible to modify the GS algorithm so that it outputs, in polynomial time (as a function s and n), a list of codewords of the RS code $C[n,k,d]$, such that these codewords $\{\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_l\}$ satisfy

$$\sum_{i=1}^{n} W_{i,c_{j,i}} \geq \sqrt{(n-d) \sum_{i=1}^{n} \sum_{a=0}^{q-1} W_{i,a}^2}$$

for $j = 1, 2, ..., l$. This condition guarantees that the system of equations for the coefficients of the interpolation polynomial has a nonzero solution.

Moreover, the matrix W does not have to be associated with transmission. For instance, given n subsets $S_1, \ldots, S_n \subset \mathbb{F}_q$, the GS algorithm can be employed to solve the problem of finding the codewords $\mathbf{c} \in C$ such that $c_i \in S_i$.