Notes on an Efficient Solution to the Rational Function Interpolation Problem

Madhu Sudan*

March 23, 1999

These notes outline how a rational function interpolation problem may be reduced (in nearly linear time) to a "rational approximation problem". The writeup assumes that polynomial interpolation, multiplication and division can be solved in nearly linear time. (This part can be read up from [1].) Combined with Michael Rosenblum's notes [3] on the rational approximation problem, this should give a pretty good idea on how to implement the "Welch-Berlekamp decoder" [4, 2] for Reed-Solomon codes in nearly linear time.

Definition 1 *Degree of rational function* $a(x)/b(x)$ *is defined to be* $\deg_a - \deg_b$.

Problem 1
[Rational interpolation] Given n *points* $\{(x_1, y_1), \ldots, (x_n, y_n)\}$ *and degree bounds* d_1, d_2, *find a rational function* $a(x)/b(x)$ *such that for all* $i \in \{1, \ldots, n\}$ $a(x_i) = y_i b(x_i)$ *and* $\deg a(x) \leq d_1$ *and* $\deg b(x) \leq d_2$.

Problem 2
[Absolute approximation] Given rational function $\alpha(x)$ *and degree bound* d, *find a rational function* $a(x)/b(x)$ *with* $\deg b \leq d$, *minimizing* $\deg(\alpha(x) - a(x)/b(x))$.

Problem 3
[Relative approximation] Given rational function $\alpha(x) = A(x)/B(x)$ *and degree bound* d, *find a rational function* $a(x)/b(x)$ *with* $\deg b \leq d$, *minimizing* $\deg(\alpha(x) - a(x)/b(x)) + \deg(b(x))$. *Notice that this is equivalent to minimizing the degree of the cross product* $\deg(A(x)b(x) - B(x)a(x))$.

Definition 2 *Given a rational function* $\alpha(x)$ *with* $\deg(\alpha(x)) < 0$, *its continued fraction representation is given by a unique sequence of polynomials* $q_1(x), q_2(x), \ldots, q_l(x)$, *with* $\deg q_i(x) > 0$, *satisfying*

$$\alpha(x) = \frac{1}{q_1(x) + \frac{1}{q_2(x) + \frac{1}{\cdots + \frac{1}{q_l(x)}}}}. \tag{1}$$

Denote $(q_1(x), \ldots, q_l(x)) = \mathrm{CF}(\alpha(x))$. *Conversely, given any sequence of rational functions* $(q_1(x), q_2(x), \ldots, q_l(x))$, *let* $\alpha(x) = \mathrm{CF}^{-1}(q_1(x), \ldots, q_l(x))$ *be the rational function satisfying Eq. (1).*

*MIT Laboratory for Computer Science, 200 Technology Square, Cambridge, MA 02139, USA. madhu@mit.edu

Problem 4
[Continued fraction approximation] Given rational function $\alpha(x)$ and degree bound d, find a rational function $a(x)/b(x)$ with $\deg b \leq d$, such that $a(x)/b(x) = \mathrm{CF}^{-1}(q_1(x), \ldots, q_k(x))$, where $(q_1(x), \ldots, q_l(x)) = \mathrm{CF}(\alpha(x))$ and k is the largest index such that $\mathrm{CF}^{-1}(q_1(x), \ldots, q_k(x))$ has degree of denominator at most d.

The three relevant claims are summarized below:

Lemma 3 *1. The continued fraction approximation problem is solvable in $\tilde{O}(n)$ time.*

2. The solution to the continued fraction approximation problem is also a solution to the absolute approximation problem and the relative approximation problem (for same inputs).

3. The rational interpolation problem reduces to the relative approximation problem.

(Actually we don't ever need the absolute approximation problem, but it is so close to what we need, so I mentioned it anyway.)

Proof: Part 1 follows from [1, Chapter 8] and binary search for the right index k.

Part 3 is obtained as follows: Given $\{(x_1, y_1), \ldots, (x_n, y_n)\}$, and d_1, d_2 (and assuming w.l.o.g. that x_i's are distinct), let $Y(x)$ be a polynomial of degree at most $n-1$ such that for every i, $Y(x_i) = y_i$, and let $Z(x) = \prod_{i=1}^{n}(x - x_i)$. Then the rational interpolation condition is equivalent to to

$$a(x) = b(x).Y(x) - c(x).Z(x)$$

for some polynomial $c(x)$. Dividing by $b(x).Z(x)$ we get:

$$Y(x)/Z(x) - c(x)/b(x) = a(x)/(Z(x).b(x)).$$

Thus the rational interpolation problem reduces to that of finding $a(x), b(x), c(x)$, given $Y(x), Z(x)$, such that the condition above holds. We invoke the relative approximation problem on inputs $\alpha(x) = Y(x)/Z(x)$ and $d = d_2$ to get polynomials $c(x)$ and $b(x)$ with $\deg b(x) \leq d$ and with $\deg(Y(x)b(x) - c(x)Z(x))$ as small as possible. Setting $a(x) = Y(x)b(x) - c(x)Z(x)$, we get an $a(x)$ of the smallest possible degree satisfying the interpolation conditions, and thus if a solution with $\deg a(x) \leq d_1$ and $\deg b(x) \leq d_2$ exists, then our solution will have the same properties.

Now for Part 2. (To make notation simpler we'll just ignore the "(x)" part everywhere.) Let $\alpha_0 = \alpha$ and let $\alpha_i = \frac{1}{\alpha_{i-1}} - q_i$. Notice that α_i's are the fractional part of what remains: i.e., for every i, $\alpha = \mathrm{CF}^{-1}(q_1, \ldots, q_{i-1}, q_i + \alpha_i)$, where $(q_1, \ldots, q_l) = \mathrm{CF}(\alpha)$. Notice further that $\deg \alpha_i < 0$.

Let $g_i/h_i = \mathrm{CF}^{-1}(q_1, \ldots, q_i)$. Recall (from, Lovasz's book) that $g_i = g_{i-2} + q_i g_{i-1}$ and $h_i = h_{i-2} + q_i h_{i-1}$. (If you wish to verify, best is to try induction using the identities: $g_i/h_i = \mathrm{CF}^{-1}(q_1, \ldots, q_i) = \frac{1}{q_1 + \mathrm{CF}^{-1}(q_2, \ldots, q_i)}$.) Notice that the degrees of h_i's are monotone increasing (strictly); and that they satisfy the identity: $h_i g_{i-1} - g_i h_{i-1} = \pm 1$. In particular this implies that g_i is relatively prime to h_i. Now comes the crucial observation:

$$\alpha = \mathrm{CF}^{-1}(q_1, \ldots, q_{i-1}, q_i + \alpha_i) = \frac{g_{i-2} + (q_i + \alpha_i)g_{i-1}}{h_{i-2} + (q_i + \alpha_i)h_{i-1}}.$$

We first bound the degree of $\alpha - \frac{g_i}{h_i}$:

$$\begin{aligned}
\alpha - \frac{g_i}{h_i} &= \frac{g_{i-2} + (q_i + \alpha_i) g_{i-1}}{h_{i-2} + (q_i + \alpha_i) h_{i-1}} - \frac{g_{i-2} + q_i g_{i-1}}{h_{i-2} + q_i h_{i-1}} \\
&= \frac{\alpha_i (g_{i-1} h_{i-2} - h_{i-1} g_{i-2})}{(h_{i-2} + (q_i + \alpha_i) h_{i-1})(h_{i-2} + q_i h_{i-1})} \\
&= \frac{\pm \alpha_i}{(h_i + \alpha_i h_{i-1})(h_i)} \\
&= \frac{\pm 1}{(\alpha_i^{-1} h_i + h_{i-1})(h_i)} \\
&= \frac{\pm 1}{((q_{i+1} + \alpha_{i+1} h_i + h_{i-1})(h_i)} \\
&= \frac{\pm 1}{(h_{i+1} + \alpha_{i+1} h_i)(h_i)}
\end{aligned}$$

Thus we find that $\deg \alpha - \frac{g_i}{h_i}$ is at most $-(\deg h_i + \deg h_{i+1})$ as expected. Now we go on to prove that this is the best absolute and relative approximation.

Let k be such that $\deg h_k \leq d < \deg h_{k+1}$. Let a/b be a candidate for the absolute (relative) approximation with $\deg b \leq d$. We need to verify that $\deg(\alpha - a/b) \geq -(\deg h_k + \deg h_{k+1})$ (resp. $\deg(\alpha - a/b) + \deg b \geq -\deg h_{k+1}$).

$$\begin{aligned}
\delta \stackrel{\text{def}}{=} \alpha - \frac{a}{b} &= \frac{g_k}{h_k} + \frac{1}{h_k (h_{k+1} + \alpha_{k+1} h_k)} - \frac{a}{b} \\
&= \frac{(h_{k+1} + \alpha_{k+1} h_k)[b g_k - a h_k] + b}{h_k (h_{k+1} + \alpha_{k+1} h_k) b}
\end{aligned}$$

We now have two cases: If $b g_k - a h_k \neq 0$, then δ above has degree at least $-(\deg h_k + \deg b) > -(\deg h_k + \deg h_{k+1})$, so it is not a candidate for the best absolute approximation. Further $\deg \delta + \deg b \geq -\deg h_k > -\deg h_{k+1}$, so a/b is not a candidate for the best relative approximation either. Now if $b g_k - a h_k = 0$, then $\delta = \alpha - \frac{g_k}{h_k}$, and thus a/b is no better an absolute approximant than g_k/h_k; and further, since $\deg b \geq \deg h_k$ (here we use the fact that g_k and h_k are relatively prime), a/b is not a better relative approximant either. ▮

References

[1] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Anaylsis of Computer Algorithms*. Addison Wesley Publishing Company, 1974.

[2] Elwyn Berlekamp. Bounded distance +1 soft-decision Reed-Solomon decoding. *IEEE Transactions on Information Theory*, 42(3):704–720, 1996.

[3] Michael Rosenblum. A fast algorithm for rational function approximations. Available from `http://theory.lcs.mit.edu/~madhu/FT01/notes/rosenblum.ps`, November 1999.

[4] Lloyd R. Welch and Elwyn R. Berlekamp. Error correction of algebraic block codes. *US Patent Number 4,633,470*, December 1986.