Cauchy Interpolation with Errors in the Values*

Erich L. Kaltofen[1] and Clément Pernet[2]

[1]Dept. of Mathematics, North Carolina State University,
Raleigh, North Carolina 27695-8205, USA
{kaltofen}@math.ncsu.edu; http://www.kaltofen.us

[2]INRIA-MOAIS, LIG, Université Joseph Fourier
Grenoble, France
clement.pernet@imag.fr; http://membres-liglab.imag.fr/pernet/

1. The Main Lemma

Lemma 1.1 *Let d and e be non-negative integers, and let $H(X) \in \mathsf{K}[X]$, K an arbitrary field, $\deg(H) \leq d+e$; furthermore, let ξ_i, $1 \leq i \leq d+e+1$, be not necessarily distinct elements in K.*
1. Define $f_0(X) := (X-\xi_1)\cdots(X-\xi_{d+e+1})$, $\deg(f_0) = d+e+1$, and $f_1(X) := H(X)$. Now let $f_\ell(X), q_\ell(X) \in \mathsf{K}[X]$ be the ℓ-th remainders and quotients respectively, in the Euclidean polynomial remainder sequence

$$f_{\ell-2}(X) = q_\ell(X) f_{\ell-1}(X) + f_\ell(X), \quad \deg(f_\ell) < \deg(f_{\ell-1}) \text{ for } \ell \geq 2.$$

In the exceptional case $H = 0$ the sequence is defined to be empty.
Finally, let $h_\ell(X), g_\ell(X) \in \mathsf{K}[X]$ be the multipliers in the extended Euclidean scheme $g_\ell f_1 + h_\ell f_0 = f_\ell$, namely,

$$h_0 := g_1 := 1, \quad h_1 := g_0 := 0,$$
$$h_\ell := h_{\ell-2} - q_\ell h_{\ell-1}, \quad g_\ell := g_{\ell-2} - q_\ell g_{\ell-1} \quad \text{for } \ell \geq 2.$$

Then there exists an index j, $1 \leq j$, such that $\deg(f_j) \leq d < \deg(f_{j-1})$. For that index we have

$$f_j \equiv g_j H \pmod{(X-\xi_1)\cdots(X-\xi_{d+e+1})} \quad \text{and} \quad \deg(g_j) \leq e. \tag{1}$$

2. Let $F(X), G(X) \in \mathsf{K}[x]$ be another solution of (1), namely

$$F \equiv G\,H \pmod{(X-\xi_1)\cdots(X-\xi_{d+e+1})}, \quad d \geq \deg(F) \text{ and } e \geq \deg(G).$$

Then $g_j F = f_j G$. If furthermore $\mathrm{GCD}(F,G) = 1$ then $F = \lambda f_j$, $G = \lambda g_j$ for some $\lambda \in \mathsf{K}$.

*This material is based on work supported in part by the National Science Foundation under Grants CCF-0830347 and CCF-1115772.

The proof of this lemma is in [Kaltofen and Trager 1990, Lemma 1]. We repeat it now:

$$g_jF - h_jG = (F - GH)g_j - (h_j - g_jH)G \equiv 0 \pmod{f_0},$$

but $\deg(g_j) = \deg(f_0) - \deg(f_{j-1}) \leq e$ and $\deg(h_j) = \deg(f_1) - \deg(f_{j-1}) \leq d$ and therefore $\deg(g_jF - h_jG) \leq d + e$, which by divisibily by f_0 of degree $d + e + 1$ means $g_jF - f_jG = 0$. Note that the Lemma does not stipulate that f_j, g_j are necessarily relatively prime. The last statement for relative prime F, G is proven as the case $k = 0$ of Lemma 2.1 below.

2. Cauchy Rational Function Interpolation With Errors

Let $\widehat{F}(x), \widehat{G}(x) \in \mathsf{K}[x]$, $\widehat{G} \neq 0$, $\deg(\widehat{F}) \leq d_{\widehat{F}}$, $\deg(\widehat{G}) \leq d_{\widehat{G}}$, $\mathrm{GCD}(\widehat{F}, \widehat{G}) = 1$. We are given $d_{\widehat{F}}$, $d_{\widehat{G}}$, an $E \geq 0$, the upper bound of the number of erroneous values, and for $i = 1, 2, \ldots$, $n = d_{\widehat{F}} + d_{\widehat{G}} + 2E + 1$,

$$\xi_i \in \mathsf{K} \left(\xi_{i_1} \neq \xi_{i_2} \text{ for all } i_1 \neq i_2 \text{ and } \widehat{G}(\xi_i) \neq 0 \right), \; b_i = a_i + a'_i \; \left(a_i = \frac{\widehat{F}(\xi_i)}{\widehat{G}(\xi_i)} \right),$$

where $a'_{\lambda_\kappa} \neq 0$ exactly at the $k \leq E$ unknown indices $1 \leq \lambda_1 < \lambda_2 < \cdots < \lambda_k \leq n$, that is, $a'_i = 0$ for all $i \notin \{\lambda_1, \ldots, \lambda_k\}$. We wish to recover the rational function $\widehat{F}/\widehat{G} \in \mathsf{K}(X)$.

1. Compute the polynomial interpolant $H(x)$, $\deg(H) \leq n - 1$, for the argument/value pairs $(\xi_1, b_1), \ldots, (\xi_n, b_n)$.

2. Compute f_j, g_j as in Lemma 1.1 with $d = d_{\widehat{F}} + E$, $e = d_{\widehat{G}} + E$, $\xi_1, \ldots, \xi_n$, and H.

3. Let $\Lambda(X) = (X - \xi_{\lambda_1}) \cdots (X - \xi_{\lambda_k})$ be the error locator polynomial. Then

$$\underbrace{\widehat{F}\Lambda}_{F} \equiv \underbrace{\widehat{G}\Lambda}_{G} H \pmod{(x - \xi_1) \ldots (x - \xi_n)} \quad \left((\widehat{F}\Lambda)(\xi_i) = (\widehat{G}\Lambda)(\xi_i) H(\xi_i) \text{ for all } i \right),$$

with $\deg(F) \leq d_{\widehat{F}} + k \leq d$ and $\deg(G) \leq d_{\widehat{G}} + k \leq e$. Thus Lemma 1.1 applies, and $\widehat{F}/\widehat{G} = F/G = f_j/g_j$.

Lemma 2.1 $\mathrm{GCD}(f_j, g_j) = \Lambda$.

Proof. We have $f_j = g_jH + h_j(x - \xi_1) \ldots (x - \xi_n)$ so $f_j(\xi_{\lambda_\kappa}) = g_j(\xi_{\lambda_\kappa})H(\xi_{\lambda_\kappa})$. Also $\widehat{F}(\xi_{\lambda_\kappa}) = a_{\lambda_\kappa}\widehat{G}(\xi_{\lambda_\kappa})$ and $f_j(\xi_{\lambda_\kappa})\widehat{G}(\xi_{\lambda_\kappa}) = g_j(\xi_{\lambda_\kappa})\widehat{F}(\xi_{\lambda_\kappa}) = g_j(\xi_{\lambda_\kappa})a_{\lambda_\kappa}\widehat{G}(\xi_{\lambda_\kappa})$. Since $\widehat{G}(\xi_{\lambda_\kappa}) \neq 0$ we must have $f_j(\xi_{\lambda_\kappa}) = g_j(\xi_{\lambda_\kappa})a_{\lambda_\kappa} = g_j(\xi_{\lambda_\kappa})H(\xi_{\lambda_\kappa})$. But $H(\xi_{\lambda_\kappa}) \neq a_{\lambda_\kappa}$, so $g_j(\xi_{\lambda_\kappa}) = 0$ and consequently $f_j(\xi_{\lambda_\kappa}) = 0$. Thus Λ must divide f_j and g_j.

Now let $w = \mathrm{GCD}(f_j/\Lambda, g_j/\Lambda)$. We have $\widehat{F}\Lambda = f_j/w$ and $\widehat{G}\Lambda = g_j/w$, so

$$\widehat{F}\Lambda - \widehat{G}\Lambda H = \frac{f_j}{w} - H\frac{g_j}{w} = \frac{h_j(x - \xi_1) \ldots (x - \xi_n)}{w}.$$

But $(\widehat{F}\Lambda - \widehat{G}\Lambda H)(\xi_i) = 0$ for all i, so $(\widehat{F}\Lambda - \widehat{G}\Lambda H)/((x - \xi_1) \ldots (x - \xi_n))$ is a polynomial. This means that w divides h_j and because $\mathrm{GCD}(g_j, h_j) = 1$, w is a scalar. ⊠

For $d_{\widehat{G}} = 0$ one gets the Welch-Berlekamp decoding [Welch and Berlekamp 1986] of Reed-Solomon codes. For $E = 0$ one gets Cauchy rational function recovery. The approach generalizes to Herminte rational function interpolation with error correction [Kaltofen et al. 2020].

References

Kaltofen, Erich L. , Pernet, Clément, and Yang, Zhi-Hong. Hermite rational function interpolation with error correction. pages 335–357, 2020. URL: http://users.cs.duke.edu/~elk27/bibliography/20/KPY20.pdf, https://doi.org/10.1007/978-3-030-60026-6_19.

Kaltofen, Erich and Trager, Barry M. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symbolic Comput.*, 9(3):301–320, 1990. URL: http://users.cs.duke.edu/~elk27/bibliography/90/KaTr90.pdf.

Welch, Lloyd R. and Berlekamp, Elwyn R. Error correction of algebraic block codes. US Patent 4,633,470, 1986. Filed 1983; see http://patft.uspto.gov/.