Hermite Interpolation with Error Correction Zero or Large Characteristic and High Error Rate

Erich Kaltofen

NC STATE UNIVERSITY and DUKE UNIVERSITY

https://users.cs.duke.edu/~elk27

Joint with Clément Pernet and Zhi-Hong Yang

A brief history of dense univariate interpolation (exclusive list-decoding)

	Polynomial	*Rational Function*
at values	Sun-Tzu/Lagrange, Guo Shoujing/Newton	Cauchy
at values of derivatives	Hermite, Birkhoff	Padé/Kronecker, Warner 1974
at values with errors	Reed and Solomon 1960	Beelen, Høholdt, Nielsen, Wu 2013
at values of derivatives with errors	Rosenbloom and Tsfasman 1997 (multiplicity codes)	Kaltofen, Pernet, Zhi-Hong Yang CASC 2020
	Higher error capacity: *This paper*	

Polynomial Interpolation with Error Correction
Decoding the Reed-Solomon Code

Arguments $\xi_1, \ldots, \xi_n \in \mathsf{K}$, distinct
Values $\hat{a}_1, \ldots, \hat{a}_n \in \mathsf{K}$
Bounds $E, D \in \mathbb{Z}_{\geq 0}$

Compute a polynomial $f \in \mathsf{K}[x]$ satisfying

1. $\deg(f) \leq D$
2. there are $\leq E$ errors: $\hat{a}_i$ is an error if $\hat{a}_i \neq f(\xi_i)$

Or determine that there is no such polynomial

If $n \geq D + 2E + 1$ there is a unique interpolant or none

Reed-Solomon's uniqueness argument

If f and $f^{[2]}$ are interpolants, there are

$$\geq n - \underbrace{E}_{\geq \text{ nr. of errors of } f} - \underbrace{E}_{\geq \text{ nr. of errors of } f^{[2]}}$$

$= D+1$ non-error locations with $\hat{a}_i = f(\xi_i) = f^{[2]}(\xi_i)$

$$\Longrightarrow f = f^{[2]}$$

Reed-Solomon's uniqueness argument

If f and $f^{[2]}$ are interpolants, there are

$$\geq n - \underbrace{E}_{\geq \text{ nr. of errors of } f} - \underbrace{E}_{\geq \text{ nr. of errors of } f^{[2]}}$$

$= D+1$ non-error locations with $\hat{a}_i = f(\xi_i) = f^{[2]}(\xi_i)$

$$\Longrightarrow f = f^{[2]}$$

$n = D+2E$ are too few values:

$$D = 0, \quad f = 1, f^{[2]} = 0, \quad [\hat{a}_1, \ldots \hat{a}_{2E}] = [\underbrace{1, \ldots, 1}_{E}, \underbrace{0, \ldots, 0}_{E}]$$

Welch-Berlekamp 1986 Decoding Algorithm
[US Patent 4,633,470 filed 1983]

Error locator polynomial for all $k \le E$ errors

$$\Lambda(x) = (x - \xi_{\lambda_1}) \cdots (x - \xi_{\lambda_k}), \quad f(\xi_{\lambda_\kappa}) \neq \hat{a}_{\lambda_\kappa}$$

Solve the linear equations

$$\underbrace{\Phi(\xi_i)}_{f(\xi_i)\Lambda(\xi_i)} = \underbrace{\hat{a}_i \Psi(\xi_i)}_{\hat{a}_i \Lambda(\xi_i)}, \qquad \begin{array}{l} \deg(\Phi) \le D+E,\ \deg(\Psi) \le E \\ i = 1, \ldots, n \end{array}$$

in coefficients of Φ, Ψ with $\text{lead-coeff}(\Psi) = 1$

$$\Longrightarrow D + 2E + 1 \text{ unknows and equations}$$

$\dfrac{f\Lambda}{\Lambda}$ is a rational function interpolant of all $\hat{a}_i$ with poles at errors

Welch-Berlekamp = Cauchy Rational Function Interpolation

$D = 0,\ E = 3$

Decode single element $1 \in \mathsf{K}$ from $D + 1 + 2E = 7$ values

$$[(i, \hat{a}_i)] = [(1,1),(2,1),(3,1),(4,1),(5,0),(6,0),(7,0)]$$

Error rate $= 3/7 > 42.8\%$

Cauchy interpolant $\dfrac{f}{g}$, $\deg(f) \leq 6, \deg(g) \leq 0$

$$-\frac{x^6}{72} + \frac{13x^5}{40} - \frac{107x^4}{36} + \frac{323x^3}{24} - \frac{2269x^2}{72} + \frac{2143x}{60} - 14$$

No errors

Welch-Berlekamp = Cauchy Rational Function Interpolation

$D = 0,\ E = 3$

Decode single element $1 \in \mathsf{K}$ from $D + 1 + 2E = 7$ values

$$[(i, \hat{a}_i)] = [(1,1),(2,1),(3,1),(4,1),(5,0),(6,0),(7,0)]$$

Error rate $= 3/7 > 42.8\%$

Cauchy interpolant $\dfrac{f}{g}$, $\deg(f) \leq 5, \deg(g) \leq 1$

$$\frac{3x^5 - 55x^4 + 355x^3 - 1025x^2 + 1922x - 3360}{600x - 2760}$$

No errors

Welch-Berlekamp = Cauchy Rational Function Interpolation

$D = 0,\ E = 3$

Decode single element $1 \in \mathsf{K}$ from $D + 1 + 2E = 7$ values

$$[(i, \hat{a}_i)] = [(1,1),(2,1),(3,1),(4,1),(5,0),(6,0),(7,0)]$$

Error rate $= 3/7 > 42.8\%$

Cauchy interpolant $\dfrac{f}{g}$, $\deg(f) \leq 4, \deg(g) \leq 2$

$$\frac{-x^4 + 10x^3 + 37x^2 - 646x + 1680}{72x^2 - 696x + 1704}$$

No errors

Welch-Berlekamp = Cauchy Rational Function Interpolation

$D = 0,\ E = 3$

Decode single element $1 \in \mathsf{K}$ from $D + 1 + 2E = 7$ values

$$[(i, \hat{a}_i)] = [(1,1),(2,1),(3,1),(4,1),(5,0),(6,0),(7,0)]$$

Error rate $= 3/7 > 42.8\%$

Cauchy interpolant $\dfrac{f}{g}$, $\deg(f) \leq 3 = D + E, \deg(g) \leq 3 = E$

$$1$$

3 errors

Welch-Berlekamp = Cauchy Rational Function Interpolation

$D = 0,\ E = 3$

Decode single element $1 \in \mathsf{K}$ from $D + 1 + 2E = 7$ values

$$[(i, \hat{a}_i)] = [(1,1),(2,1),(3,1),(4,1),(5,0),(6,0),(7,0)]$$

Error rate $= 3/7 > 42.8\%$

Cauchy interpolant $\dfrac{f}{g}$, $\deg(f) \leq 2, \deg(g) \leq 4$

$$0$$

4 errors

Application of Reed-Solomon error-correcting codes New Horizons's 2015 images of Pluto



Hermite Interpolation with Error Correction = Multiplicity Codes [Rosenbloom and Tsfasman 1997]

Non-erroneous $\hat{a}_{i,j} = f^{(j)}(\xi_i) = \left.\dfrac{\mathrm{d}^j f(x)}{\mathrm{d}x^j}\right|_{x=\xi_i}$, $1 \le i \le n$, $0 \le j \le \ell$

$\Longrightarrow N = (\ell+1)n$ values

$$f(x) \equiv \sum_{j=0}^{\ell} \underbrace{\frac{f^{(j)}(\xi_i)}{j!}}_{\ell!\neq 0 \text{ in } \mathsf{K}} (x-\xi_i)^j = \underbrace{\sum_{j=0}^{\ell} \frac{\hat{a}_{i,j}}{j!}(x-\xi_i)^j}_{\hat{R}^{[i]}(x)} \pmod{\underbrace{(x-\xi_i)^{\ell+1}}_{\text{multiplicity}}}$$

Chinese remainder the $\hat{R}^{[i]}(x)$ [Spitzbart's Hermite Formula 1960], but with error correction [Watson and Hastings 1966]

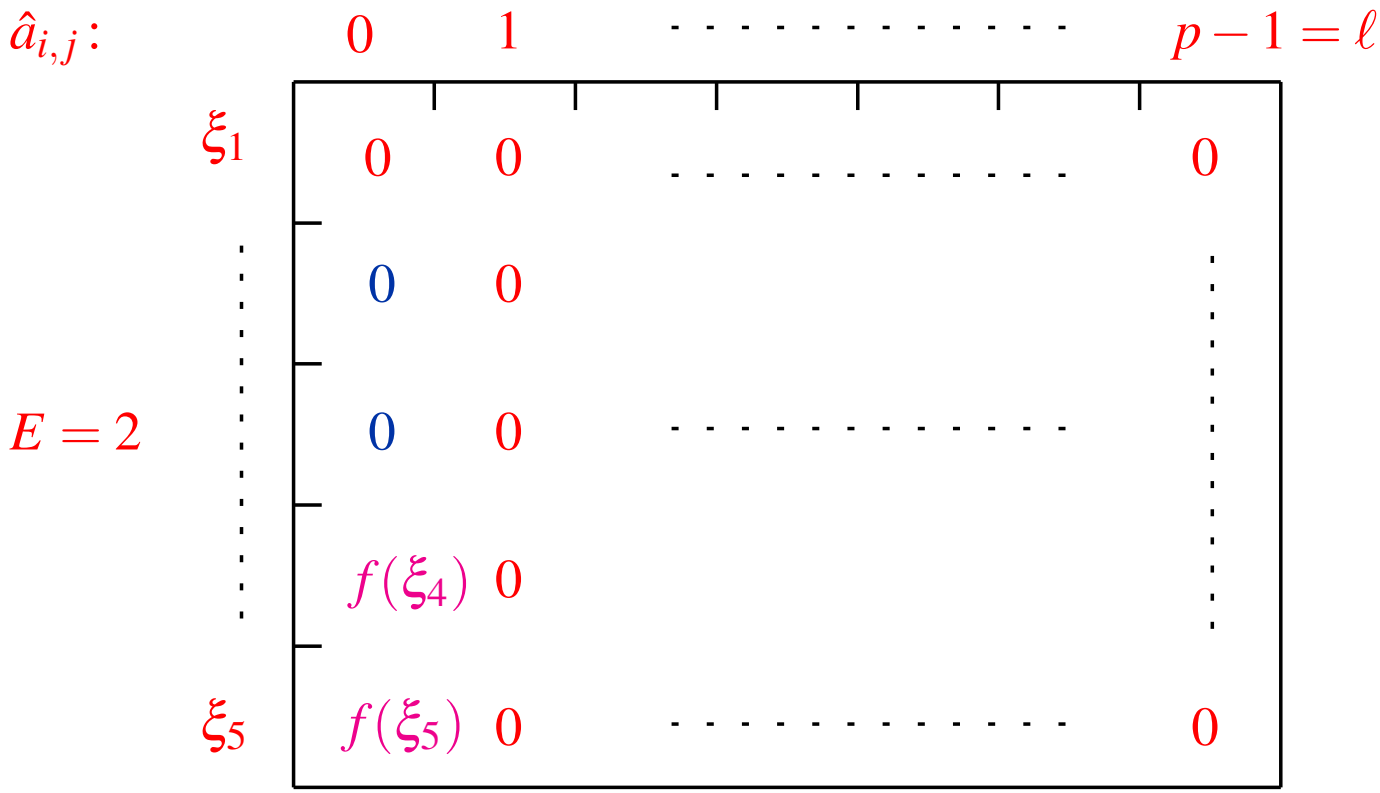
Every faulty residue $\hat{R}^{[i]}(x)$ requires a redundant good one

If $\le E$ erroneous $\hat{R}^{[\lambda_\kappa]}(x) \Longrightarrow N \ge \underbrace{D+1}_{\text{Hermite}} + \underbrace{2E(\ell+1)}_{\text{fault redundance}}$

Example

$\mathrm{char}(\mathsf{K}) = p$, $D = p$, $\ell = p-1$, $n = 2E+1$ $(|\mathsf{K}| \geq n+1)$

$f(x) = (x-\xi_1)^p \Longrightarrow f'(x) = 0$



With $D+2E(\ell+1)$ values, f and 0 have only E errors.

$\Longrightarrow$ the count $N = D+1+2E(\ell+1)$ is minimal for this example

Example

$\mathsf{K} = \mathbb{R}$, $\ell = 1$

$$f(x) = \prod_{i=1}^{D} (x - \xi_{2E+i})$$

$2E = D - 1$

$\xi_1, \ldots, \xi_{2E}$ are the roots of $f'(x)$

$\hat{a}_{i,j}$:

		0	$1 = \ell$
roots of f'	ξ_1	0	0
	$\vdots$	$\vdots$	$\vdots$
	ξ_E	0	0
	ξ_{E+1}	$f(\xi_{E+1})$	0
	$\vdots$	$\vdots$	$\vdots$
	ξ_{2E}	$f(\xi_{2E})$	0
roots of f	ξ_{2E+1}	0	
	$\vdots$	$\vdots$	
	ξ_{2E+D}	0	

With $D + 4E$ values, f and 0 have E errors

$\Longrightarrow$ the count $N = D + 4E + 1$ is minimal for this example

Birkhoff Problem in Hermite Interpolation

Example (CASC 2020)

$\mathsf{K} = \mathbb{R}$, $\ell = 1$, $\boxed{N = 2D + 2E}$ $\quad (2E \geq D \Longrightarrow N < D + 4E + 1)$

$\hat{a}_{1,0}, \ldots, \hat{a}_{n,0}$ values of $f(\xi_i)$, $\quad n \geq N/2$

$\hat{a}_{1,1}, \ldots, \hat{a}_{N-n,1}$ values of $f'(\xi_i)$, $\quad N - n \leq N/2$

$n \geq 2E + 1$

If $n \leq 2E$ then $\int f'$ and $\int f' + 1$ can both have $= E$ errors

Example (CASC 2020)

$\mathsf{K} = \mathbb{R}$, $\ell = 1$, $\boxed{N = 2D + 2E}$ $\quad (2E \geq D \Longrightarrow N < D + 4E + 1)$

$\hat{a}_{1,0}, \ldots, \hat{a}_{n,0}$ values of $f(\xi_i)$, $\quad n \geq N/2$

$\hat{a}_{1,1}, \ldots, \hat{a}_{N-n,1}$ values of $f'(\xi_i)$, $\quad N - n \leq N/2$

$n \geq 2E + 1$

f and $f^{[2]}$ two interpolants with $\leq E$ errors

k_0 the number of errors of $f(\xi_i)$ and $f^{[2]}(\xi_i)$

k_1 the number of errors of $f'(\xi_i)$ and $(f^{[2]})'(\xi_i)$

$k_0 + k_1 \leq 2E$

Case $n - k_0 \geq D + 1$:

f and $f^{[2]}$ interpolate the same $\geq D + 1$ good values

$\Longrightarrow f = f^{[2]}$

Example (CASC 2020)

$\mathsf{K} = \mathbb{R}$, $\ell = 1$, $\boxed{N = 2D + 2E}$ $\quad (2E \geq D \Longrightarrow N < D + 4E + 1)$

$\hat{a}_{1,0}, \ldots, \hat{a}_{n,0}$ values of $f(\xi_i)$, $\quad n \geq N/2$

$\hat{a}_{1,1}, \ldots, \hat{a}_{N-n,1}$ values of $f'(\xi_i)$, $\quad N - n \leq N/2$

$n \geq 2E + 1$

f and $f^{[2]}$ two interpolants with $\leq E$ errors

k_0 the number of errors of $f(\xi_i)$ and $f^{[2]}(\xi_i)$

k_1 the number of errors of $f'(\xi_i)$ and $(f^{[2]})'(\xi_i)$

$k_0 + k_1 \leq 2E$

Case $n - k_0 \leq D \Longrightarrow (N - n) - k_1 \geq D$

f' and $(f^{[2]})'$ interpolate the same $\geq D$ good values

$\Longrightarrow f' = (f^{[2]})' = c_{D-1}x^{D-1} + \cdots + c_0$

$\Longrightarrow \int f' + C = c_{D-1}\frac{1}{D}x^D + \cdots + c_0 x + C$

interpolate $n - E \geq E + 1$ good $\hat{a}_{i,0}$ for at most one C

$\Longrightarrow f = f^{[2]}$

Example (continued: decoding)

$D! \neq 0$ in K, $\ell = 1$, $N = 2D + 2E$

$\hat{a}_{1,0}, \ldots, \hat{a}_{n,0}$ values of $f(\xi_i)$, $n \geq N/2$

$\hat{a}_{1,1}, \ldots, \hat{a}_{N-n,1}$ values of $f'(\xi_i)$, $N - n \leq N/2$

$n \geq 2E + 1$

Reed-Solomon interpolated $\hat{a}_{i,0} = f(\xi_i)$ with $\leq E_0 = \lfloor \frac{n-(D+1)}{2} \rfloor$ errors;
if f exists and interpolates all values with $\leq E$ errors, return f

Example (continued: decoding)

$D! \neq 0$ in K, $\ell = 1$, $N = 2D + 2E$

$\hat{a}_{1,0}, \ldots, \hat{a}_{n,0}$ values of $f(\xi_i)$, $n \geq N/2$

$\hat{a}_{1,1}, \ldots, \hat{a}_{N-n,1}$ values of $f'(\xi_i)$, $N - n \leq N/2$

$n \geq 2E + 1$

Reed-Solomon interpolated $\hat{a}_{i,0} = f(\xi_i)$ with $\leq E_0 = \lfloor \frac{n-(D+1)}{2} \rfloor$ errors;
if f exists and interpolates all values with $\leq E$ errors, return f

Else Reed-Solomon interpolate $\hat{a}_{i,1} = f'(\xi_i)$
with $\leq E_1 = E - (E_0 + 1)$ errors
Note: $(N - n) - 2E_1 \geq D \Longrightarrow$ unique interpolant f'
If no interpolant, return "no interpolant"

Else compute C so that $f = \int f' + C$ interpolates with $\leq E$ errors, or there is "no interpolant"

ISSAC 2021

Arbitrary derivative order $\ell \leq D$ $\quad$ ($D! \neq 0$ in K)

$$N = (\ell+1)D + 1 - \frac{(\ell+1)\ell}{2} + 2E$$

$$n \geq 2E + 1$$

Condition $n \geq 2E+1$ may be false for values of $f'(\xi_i), \ldots, f^{(\ell)}(\xi_i)$, but $f^{(\ell)}$ is unique for all interpolants (if existent)

Second recursive call: interpolate
$\underbrace{\int \cdots \int}_{\ell} f^{(\ell)} + C_{\ell-1}x^{\ell-1} + \cdots + C_0$ from values $f(\xi_i), \ldots, f^{(\ell-1)}(\xi_i)$

ISSAC 2021

Arbitrary derivative order $\ell \le D$ ($D! \neq 0$ in K)

$$N = (\ell+1)D + 1 - \frac{(\ell+1)\ell}{2} + 2E$$

$$n \ge 2E+1$$

Example

$\mathsf{K} = \mathbb{R}$, $\ell = 3$, $D = 4$

16 values

$f(x) = (x^2-1)(x^2-5)$

$f'(x) = 4x(x^2-3)$

$f''(x) = 12(x^2-1)$

$f^{(3)}(x) = 24x$

f and 0 have $E = 3$ errors

$\Longrightarrow$ need $N = 17 =$

$4 \cdot 4 + 1 - 6 + 2 \cdot 3$ values

$\hat{a}_{i,j}$:

	0	1	2	$3 = \ell$
$\xi_1 = 0$	0	0	$f''(0)$	0
$\xi_2 = 1$	0	$f'(1)$	0	
$\xi_3 = -1$	0	$f'(-1)$	0	
$\xi_4 = \sqrt{3}$	0	0		
$\xi_5 = -\sqrt{3}$	0	0		
$\xi_6 = \sqrt{5}$	0			
$\xi_7 = -\sqrt{5}$	0			

ISSAC 2021

Arbitrary derivative order $\ell \leq D$ ($D! \neq 0$ in K)

$$N = (\ell+1)D + 1 - \frac{(\ell+1)\ell}{2} + 2E$$

$$n \geq 2E + 1$$

We have no example of minimality of N for $\mathsf{K} = \mathbb{R}$, $\ell = 4$

List-decoding à la [Guruswami-Wang 2011, Koparty 2015]
is also possible

New algorithm is numerically stable [my upcoming ACA 2021 talk]

Conclusion

As the saying goes, *"You can't teach an old dog a new trick"*

Conclusion

As the saying goes, *"You can't teach an old dog a new trick"*

The question is, of course, *"How old?"*

Thank you!

”End Key” wrong!