Early Termination in Ben-Or/Tiwari Sparse Interpolation and a Hybrid of Zippel's Algorithm

Wen-shin Lee
North Carolina State University
www.wen-shin.com

Joint work with

Erich Kaltofen
North Carolina State University
www.kaltofen.net

Austin Lobo
Washington College
www.austin.lobo.washcoll.edu

Objective Black box polynomial interpolation

Black box polynomial f

$p_1, \ldots, p_n \in K$

$f(p_1, \ldots, p_n) \in K$

Interpolation

$f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$

Question What if $f(x_1, \ldots, x_n)$ is sparse?

Previous Research 1 An algorithm sensitive to the sparsity of the target polynomial

Zippel's probabilistic interpolation (1979).

- 😐 Interpolate variable by variable.
- ☺ Sensitive to the sparsity after each variable is interpolated.
- ☺ Sensitive to the degree bound in every variable.
- ☹ Still interpolates each variable densely.
- ☹ Might falsely drop non-zero coefficients.
- ☹ Needs an upper bound of the degree in each variable.
- ☺ Does not need a large modulus for the recovery of polynomial terms. $O(\max_i \deg(f(x_i)))$

Previous Research 2

Another algorithm sensitive to the sparsity of the target polynomial

Ben-Or's/Tiwari's deterministic algorithm.

- :| Interpolate all the variables at once.
- :) Sensitive to the sparsity of the terms in the target polynomial.
- :) A deterministic algorithm that always interpolates correctly.
- :(Needs an upper bound of the number of terms.
- :(Might need a very large modulus for the recovery of polynomial terms. $O(\max_{\mathbf{e}} p_1^{e_1} \cdots p_n^{e_n})$, p_i the i-th prime, $e_i = \deg(f(x_i))$.

Idea # 1 Early termination

What if ***an upper bound of degree*** and ***an upper bound of the number of terms*** of the target polynomial are ***not known?***

- Guess and check.

  And double the guess if fails.

- ***Early termination.***

  Interpolate the polynomial at a random point, when the polynomial stops changing, it is done with high probability.

Why early termination?

- Save time and space.

- A useful tool for controlling intermediate expression swell in computer algebra.

- Sensitive to the sparsity of the target polynomial without knowing any bounds on degree or number of terms.

Early termination in Newton interpolation

For $i \leftarrow 1, 2, \ldots$ *Do*

Pick random p_i *and from* $f(p_i)$

compute

$$f^{[i]}(x) \leftarrow c_0 + c_1(x - p_1) + c_2(x - p_1)(x - p_2) + \cdots \\ \equiv f(x) \pmod{(x - p_1)\cdots(x - p_i)}$$

If $c_i = 0$ *stop.*

End For

Threshold η

In order to obtain a better probability, we require $c_i = 0$ more than once before terminating.

Analysis with thresholds

Let $p_0, p_1, p_2, \ldots$ be chosen randomly and uniformly from a subset S of the domain of values, and $f^{[i]}$ denote the interpolation polynomial that interpolates $f(p_0), \ldots, f(p_i)$.

If $f^{[d]} = f^{[d+1]} = \cdots = f^{[d+\eta]}$, then $f^{[d]}$ correctly interpolates f with probability at least

$$1 - (d+1)\left(\frac{\deg(f)}{\#(S)}\right)^{\eta}.$$

Early termination of Ben-Or/Tiwari

If $p_1, \ldots, p_n$ are chosen randomly and uniformly from a subset S of the domain of values, then for the sequence

$$a_i = f(p_1^i, \ldots, p_n^i), i = 1, 2, \ldots$$

the Berlekamp/Massey algorithm encounters $\Delta = 0$ and $2L < r$ the first time for $r = 2t+1$ with probability no less than

$$1 - \frac{t(t+1)(2t+1)\deg(f)}{6 \cdot \#(S)},$$

where t is the number of terms of f.

Threshold ζ

In order to obtain a better probability, we require $\Delta = 0$ (when $2L < r$) more than once before terminating.

Idea # 2 Zippel with univariate Ben-Or/Tiwari

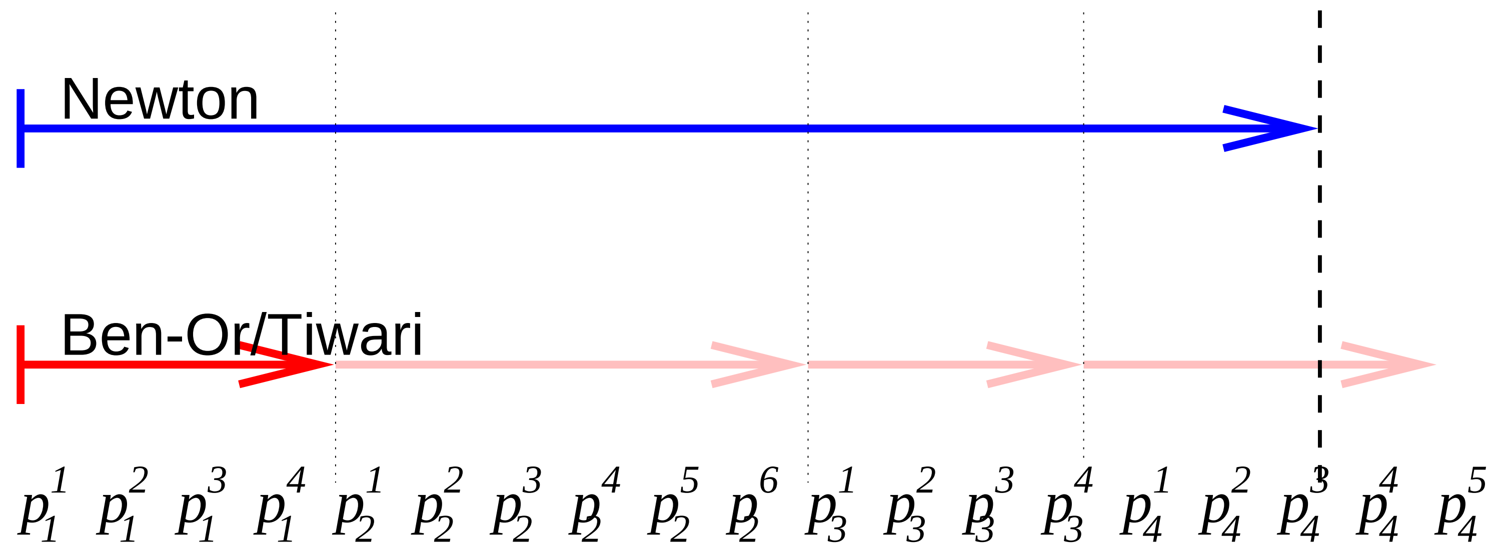
Implement Ben-Or/Tiwari on a single variable, and embed it as the univariate interpolation algorithm into Zippel's algorithm.

☺ Univariate interpolations within Zippel are now also sparse.

☺ Reduce the magnitude of the modulus needed for the recovery of all the terms. $O(\max_{\mathbf{e}} p_1^{e_1} \cdots p_n^{e_n}) \longrightarrow O(\max_{e_i} 2^{e_i})$

Racing Newton against Ben-Or/Tiwari

A likely racing scenario in univariate interpolations.



We embed this "racing" algorithm into Zippel's algorithm.

Why Racing?

- Terminate earlier when there are few terms.
  (Ben-Or/Tiwari)

- Newton outraces Ben-Or/Tiwari, e.g., in the dense case.
  (Newton)

- Algorithms can cross check their results.
  (Ben-Or/Tiwari $+$ Newton)

Implementation *protobox* package

The *protobox* package is our Maple V.5.1 implementation of this new hybrid algorithm.

Minimum black box probes needed under different embedded univariate interpolations in *protobox*

	mod	Newton	Ben-Or/Tiwari	"Racing"
f_1	100003	147	137	126
f_2	100003	146	143	124
f_3	100003	209	143	133
f_4	100003	188	149	133
f_5	100000007†	2652	251	251
f_6	100000007†	965	1256	881
f_7	100003	94	46	41

† This is tested in Maple 6

Throughputs under different modulus and thresholds

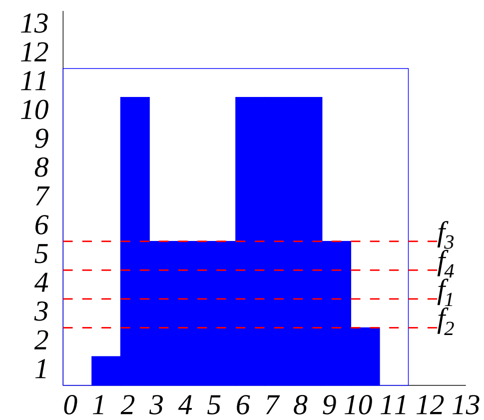
$$f_1 = x_1^2x_3^3x_4x_6x_8x_9^2 + x_1x_2x_3x_4^2x_5^2x_8x_9 + x_2x_3x_4x_5^2x_8x_9 + x_1x_3^3x_4^2x_5^2x_6^2x_7x_8^2 + x_2x_3x_4x_5^2x_6x_7x_8^2$$
$$f_2 = x_1x_2^2x_4^2x_8x_9^2x_{10}^2 + x_2^2x_4x_5^2x_6x_7x_9x_{10}^2 + x_1^2x_2x_3x_5^2x_7^2x_9^2 + x_1x_3^2x_4^2x_7^2x_9^2 + x_1^2x_3x_4x_7^2x_8^2$$
$$f_3 = 9x_2^3x_3^3x_5^2x_6^2x_8^3x_9^3 + 9x_1^3x_2^2x_3^3x_5^2x_7^2x_8^2x_9^3 + x_1^4x_3^4x_4^2x_5^4x_6^4x_7x_8^5x_9 + 10x_1^4x_2x_3^4x_4^4x_5^4x_7x_8^3x_9 + 12x_2^3x_4^3x_6^3x_7^2x_8^3$$
$$f_4 = 9x_1^2x_3x_4x_6^3x_7^2x_8x_{10}^4 + 17x_1^3x_2x_5^2x_6^2x_7x_8^3x_9^4x_{10}^3 + 17x_2^2x_3^4x_4^2x_7^4x_8^3x_9x_{10}^3 + 3x_1^3x_2^2x_6^3x_{10}^2 + 10x_1x_3x_5^2x_6^2x_7^4x_8^4$$

	Thresholds			mod 31			mod 37			mod 41			mod 43			mod 47			mod 53		
	η, ζ	τ	κ, γ	$=$	$\neq$	!	$=$	$\neq$	!	$=$	$\neq$	!	$=$	$\neq$	!	$=$	$\neq$	!	$=$	$\neq$	!
f_1	1	0	0	8	2	90	7	1	92	15	3	82	11	5	84	25	3	72	20	2	78
	2	1	2	30	0	70	38	1	61	44	0	56	55	0	45	71	0	29	52	0	48
	3	2	4	38	0	62	36	0	64	50	0	50	60	0	40	79	0	21	70	0	30
f_2	1	0	0	4	3	93	4	3	93	5	3	92	7	5	88	22	4	74	23	1	76
	2	1	2	22	0	78	36	0	64	38	0	62	48	1	51	61	0	39	66	0	34
	3	2	4	41	0	59	45	0	55	51	0	49	57	0	43	83	0	17	81	0	19
f_3	1	0	0	0	2	98	0	6	94	3	3	94	4	0	96	6	5	89	9	1	90
	2	1	2	3	1	96	8	0	92	16	0	84	10	0	90	37	0	63	27	0	73
	3	2	4	9	0	91	8	0	92	26	0	74	15	0	85	52	0	48	54	0	46
f_4	1	0	0	1	4	95	0	2	98	4	2	94	8	3	89	18	2	80	5	3	92
	2	1	2	8	0	92	5	0	95	20	0	80	22	0	78	63	0	37	44	0	56
	3	2	4	10	0	90	10	0	90	33	0	67	32	0	68	80	0	20	47	0	53

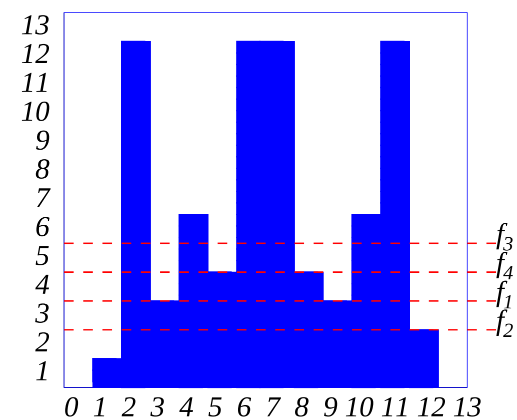
Performance on small moduli

$$f_1 = x_1^2x_3^3x_4x_6x_8x_9^2 + x_1x_2x_3x_4^2x_5^2x_8x_9 + x_2x_3x_4x_5^2x_8x_9 + x_1x_3^3x_4^2x_5^2x_6^2x_7x_8^2 + x_2x_3x_4x_5^2x_6x_7x_8^2$$
$$f_2 = x_1x_2^2x_4^2x_8x_9^2x_{10}^2 + x_2^2x_4x_5^2x_6x_7x_9x_{10}^2 + x_1^2x_2x_3x_5^2x_7^2x_9^2 + x_1x_3^2x_4^2x_7^2x_9^2 + x_1^2x_3x_4x_7^2x_8^2$$
$$f_3 = 9x_2^3x_3^3x_5^2x_6^2x_8^3x_9^3 + 9x_1^3x_2^2x_3^3x_5^2x_7^2x_8^2x_9^3 + x_1^4x_3^4x_4^2x_5^4x_6^4x_7x_8^5x_9 + 10x_1^4x_2x_3^4x_4^4x_5^4x_7x_8^3x_9 + 12x_2^3x_4^3x_6^3x_7^2x_8^3$$
$$f_4 = 9x_1^2x_3x_4x_6^3x_7^2x_8x_{10}^4 + 17x_1^3x_2x_5^2x_6^2x_7x_8^3x_9^4x_{10}^3 + 17x_2^2x_3^4x_4^2x_7^4x_8^3x_9x_{10}^3 + 3x_1^3x_2^2x_6^3x_{10}^2 + 10x_1x_3x_5^2x_6^2x_7^4x_8^4$$

	Thresholds			mod 11			mod 13		
	η, ζ	τ	κ, γ	$=$	$\neq$	!	$=$	$\neq$	!
f_1	2	2	6	28	2	70	28	0	72
Average black box probes: $=$				151.3928571			196.2142857		
Average black box probes: $=,\neq$				151.1666667			196.2142857		
f_2	2	2	6	8	1	91	26	0	74
Average black box probes: $=$				162.			164.3076923		
Average black box probes: $=,\neq$				161.6666667			164.3076923		
f_3	2	2	6	7	1	92	2	0	98
Average black box probes: $=$				167.2857143			167.		
Average black box probes: $=,\neq$				167.1250000			167.		
f_4	2	2	6	5	0	95	0	1	99
Average black box probes: $=$				170.					
Average black box probes: $=,\neq$				170.			180.		



The order of elements in $\mathrm{mod}\ 11$



The order of elements in $\mathrm{mod}\ 13$

For further developments
see
www.wen-shin.com

Thresholds

η: (default 1) Newton interpolation threshold.

ζ: (default 1) Ben-Or/Tiwari interpolation threshold.

τ: (default 0) number of points used for post test.

κ: (default 0) number of random numbers retried before abort the interpolation if two terms map to a same value and cause the interpolation failure.

γ: (default 0) extends the upper bound of each univariate interpolation loop. This regards the delay in updating Newton interpolants.

Polynomials tested

$$f_1(x_1,\ldots,x_{10}) = x_1^2x_3^3x_4x_6x_8x_9^2 + x_1x_2x_3x_4^2x_5^2x_8x_9 + x_2x_3x_4x_5^2x_8x_9 + x_1x_3^3x_4^2x_5^2x_6^2x_7x_8^2 + x_2x_3x_4x_5^2x_6x_7x_8^2$$

$$f_2(x_1,\ldots,x_{10}) = x_1x_2^2x_4^2x_8x_9^2x_{10}^2 + x_2^2x_4x_5^2x_6x_7x_9x_{10}^2 + x_1^2x_2x_3x_5^2x_7^2x_9^2 + x_1x_3^2x_4^2x_7^2x_9^2 + x_1^2x_3x_4x_7^2x_8^2$$

$$f_3(x_1,\ldots,x_{10}) = 9x_2^3x_3^3x_5^2x_6^2x_8^3x_9^3 + 9x_1^3x_2^2x_3^3x_5^2x_7^2x_8^2x_9^3 + x_1^4x_3^4x_4^2x_5^4x_6^4x_7x_8^5x_9 + 10x_1^4x_2x_3^4x_4^4x_5^4x_7x_8^3x_9 + 12x_2^3x_4^3x_6^3x_7^2x_8^3$$

$$f_4(x_1,\ldots,x_{10}) = 9x_1^2x_3x_4x_6^3x_7^2x_8x_{10}^4 + 17x_1^3x_2x_5^2x_6^2x_7x_8^3x_9^4x_{10}^3 + 17x_2^2x_3^4x_4^2x_7^4x_8^3x_9x_{10}^3 + 3x_1^3x_2^2x_6^3x_{10}^2 + 10x_1x_3x_5^2x_6^2x_7^4x_8^4$$

$$f_5(x_1,\ldots,x_{50}) = \sum_{i=1}^{50} x_i^{50}$$

$$f_6(x_1,\ldots,x_5) = \sum_{i=1}^{5}(x_1+x_2+x_3+x_4+x_5)^i$$

$$f_7(x_1,x_2,x_3) = x_1^{20} + 2x_2 + 2x_2^2 + 2x_2^3 + 2x_2^4 + 3x_3^{20}$$