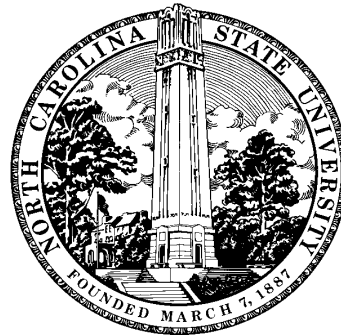


Early Termination in Ben-Or/Tiwari Sparse Interpolation and a Hybrid of Zippel's Algorithm

Erich Kaltofen
North Carolina State University
www.math.ncsu.edu/~kaltofen



Joint work with: Wen-shin Lee (North Carolina State)
Austin Lobo (Washington College, Maryland)

Zippel's (1979) theorem/sparse interpolation idea:

Let $f \in K[x_1, \dots, x_n]$ non-zero, $S \subseteq K$:

$$\text{Probability}(f(a_1, \dots, a_n) \neq 0 \mid a_i \in S \subseteq K) \leq 1 - \frac{\deg f}{\text{cardinality}S}$$

Interpolate $f(x, y) \in K[x, y]$:

1. *Pick random $a \in S$, interpolate $f(x, a)$.*

2. Suppose $f(x, y) = x^4 - 2x + 1$.

Assume that x^2, x^3 have a zero coefficients in y

Therefore, interpolate $f(x, y) = c_4(y)x^4 + c_2(y)x + c_0(y)$:

Pick p, b_0, b_1, \dots and compute $c_i(b_j)$ from

$$c_4(b_j)(p^4)^k + c_2(b_j)(p^2)^k + c_0(b_j) = f(p^k, b_j), k = 0, 1, 2$$

(transposed Vandermonde system).

3. Interpolate each c_i .

```

> with(combinat):
Warning, new definition for Chi
> for i from 0 to 10 do a[i]:=fibonacci(i); od;
      a[0] := 0
      a[1] := 1
      a[2] := 1
      a[3] := 2
      a[4] := 3
      a[5] := 5
      a[6] := 8
      a[7] := 13
      a[8] := 21
      a[9] := 34
      a[10] := 55

> read("BM.mpl");
> bermass(a,10);
"Delta[" , 1, "]" = " , 0
      1
"Delta[" , 2, "]" = " , 1
      1
"Delta[" , 3, "]" = " , 1
      1 - z
"Delta[" , 4, "]" = " , 1
      2
      1 - z - z
"Delta[" , 5, "]" = " , 0

```

$$\frac{1 - z - z^2}{2}$$

"Delta[" , 6, "]" = " , 0

$$\frac{1 - z - z^2}{2}$$

"Delta[" , 7, "]" = " , 0

$$\frac{1 - z - z^2}{2}$$

"Delta[" , 8, "]" = " , 0

$$\frac{1 - z - z^2}{2}$$

"Delta[" , 9, "]" = " , 0

$$\frac{1 - z - z^2}{2}$$

"Delta[" , 10, "]" = " , 0

$$\frac{1 - z - z^2}{2}$$

z - z - 1

> a[7] := 14;

a[7] := 14

> bermass(a, 10);

"Delta[" , 1, "]" = " , 0

$$1$$

"Delta[" , 2, "]" = " , 1

$$1$$

```

"Delta[" , 3, "]" = " , 1
      1 - z
"Delta[" , 4, "]" = " , 1
      2
      1 - z - z
"Delta[" , 5, "]" = " , 0
      2
      1 - z - z
"Delta[" , 6, "]" = " , 0
      2
      1 - z - z
"Delta[" , 7, "]" = " , 0
      2
      1 - z - z
"Delta[" , 8, "]" = " , 1
      2    6
      1 - z - z - z
"Delta[" , 9, "]" = " , -2
      2    6    3
1 + z - 3 z - z - 2 z
"Delta[" , 10, "]" = " , -5
      2    6    3    4
1 + z + 2 z - z - 7 z - 5 z
  6    5    4    3    2
z + z + 2 z - 1 - 7 z - 5 z

```

```
> f := x^2 - 3;
```

```

                2
                f := x  - 3
> p := 2;
                p := 2
> for i from 0 to 10 do b[i]:=subs(x=p^i,f); od;
                b[0] := -2
                b[1] := 1
                b[2] := 13
                b[3] := 61
                b[4] := 253
                b[5] := 1021
                b[6] := 4093
                b[7] := 16381
                b[8] := 65533
                b[9] := 262141
                b[10] := 1048573
> bermass(b, 10);
"Delta[" , 1, "]" = " , -2
                1
"Delta[" , 2, "]" = " , 1
                1 + 1/2 z
"Delta[" , 3, "]" = " , 27/2
                2
                1 + 1/2 z + 27/4 z
"Delta[" , 4, "]" = " , 297/4
                2

```

$$\frac{1 - 5z + 4z^2}{\text{"Delta["}, 5, \text{"}] = 0}$$

$$\frac{1 - 5z + 4z^2}{\text{"Delta["}, 6, \text{"}] = 0}$$

$$\frac{1 - 5z + 4z^2}{\text{"Delta["}, 7, \text{"}] = 0}$$

$$\frac{1 - 5z + 4z^2}{\text{"Delta["}, 8, \text{"}] = 0}$$

$$\frac{1 - 5z + 4z^2}{\text{"Delta["}, 9, \text{"}] = 0}$$

$$\frac{1 - 5z + 4z^2}{\text{"Delta["}, 10, \text{"}] = 0}$$

$$\frac{1 - 5z + 4z^2}{z^2 - 5z + 4}$$

> factor(%);

$$(z - 1) (z - 4)$$

Early termination in Newton interpolation

For $i \leftarrow 1, 2, \dots$ Do

Pick random p_i and from $f(p_i)$

compute

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

If $c_i = 0$ stop.

End For

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

Early termination theorem:

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

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

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

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

where t is the number of terms of f .

Threshold: in order to obtain a better probability, we require $\Delta = 0$ more than once before terminating.

Recovery of term exponents in Ben-Or/Tiwari:

1. Use prime numbers p_1, \dots, p_n .
2. Factor $\Lambda(z) \bmod q^k$ where $q^k > \max_{\mathbf{e}} p_1^{e_1} \cdots p_n^{e_n}$.
3. Decompose term values.

[Kaltofen, Lakshman, Wiley ISSAC 1990]

Idea of hybrid:

For $n = 1$, can search for e with $p^e \equiv b \pmod{q}$.

Do Zippel with univariate Ben-Or/Tiwari interpolation.

Guard against failure by concurrent Newton. In fact, race Newton against univariate Ben-Or/Tiwari

Term pruning during Zippel [Diaz and Kaltofen 1998]

Interpolate homogenized

$$f(x_0x_1, \dots, x_0x_n) = \sum_i c_i x_0^{e_{i,1} + \dots + e_{i,n}} x_1^{e_{i,1}} \dots x_n^{e_{i,n}}$$

The homogenizing variable tells when a term is complete during interpolation. It can be then subtracted from the interpolation process.

```

> read 'initpkg.mpl':
> with(protobox);
  [BM_step_mod, HybridInterp, NewtonInterp_step, bbpoly_mod,
    check_same, eval_mon_mod, eval_polyseq, eval_tmpprunelist_mod,
    find_max, find_true, heval_plist_mod, heval_pnt_mod,
    list_to_poly, prune, raising_pnts_mod, recover, relocate_c,
    relocate_shift_c, rev, rm_element, slice, spoly_to_slist,
    tmpprune, vansolve_kl_mod]
> bb:=bbpoly_mod(9*x[1]^2*x[3]*x[4]*x[6]^3*x[7]^2*x[8]*x[10]^4+17*x[1]^3
> *x[2]*x[5]^2*x[6]^2*x[7]*x[8]^3*x[9]^4*x[10]^3+17*x[2]^2*x[3]^4*x[4]^2
> *x[7]^4*x[8]^3*x[9]*x[10]^3+3*x[1]^3*x[2]^2*x[6]^3*x[10]^2+10*x[1]*x[3
> ]*x[5]^2*x[6]^2*x[7]^4*x[8]^4, [x[1], x[2], x[3], x[4], x[5], x[6], x[7], x[8]
> , x[9], x[10]]);
  bb := proc(pntsnf_i, modulusnf_i)
local polynf, inf, numvarsnf, varlistnf;
  polynf := 9*x[1]^2*x[3]*x[4]*x[6]^3*x[7]^2*x[8]*x[10]^4
    + 17*
    x[1]^3*x[2]*x[5]^2*x[6]^2*x[7]*x[8]^3*x[9]^4*x[10]^3
    + 17*x[2]^2*x[3]^4*x[4]^2*x[7]^4*x[8]^3*x[9]*x[10]^3
    + 3*x[1]^3*x[2]^2*x[6]^3*x[10]^2
    + 10*x[1]*x[3]*x[5]^2*x[6]^2*x[7]^4*x[8]^4;
  numvarsnf := 10;
  varlistnf := [x[1], x[2], x[3], x[4], x[5], x[6], x[7],
    x[8], x[9], x[10]];
  polynf := Eval(polynf, {seq(
    varlistnf[inf] = pntsnf_i[inf], inf = 1 .. numvarsnf)

```

```

    }) mod modulusnf_i;
    RETURN(polyfnf)
end
>
> for i from 1 to 2 do print(i, '-th');
> traperror(HybridInterp(bb,
> [x[1],x[2],x[3],x[4],x[5],x[6],x[7],x[8],x[9],x[10]],100,nextprime(10^
> 6),'test_thresh'=0,'BM_thresh'=1, 'N_thresh'=1,'rep_tresh'=6,
> 'mapmon_thresh'=6 ));
> od;

```

```

                1, -th
                Number of Black box calls:, 133
          2          3          2          4
9 x[1] x[3] x[4] x[6] x[7] x[8] x[10]
          3          2          2          3          4          3
+ 17 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10]
          2          4          2          4          3          3
+ 17 x[2] x[3] x[4] x[7] x[8] x[9] x[10]
          3          2          3          2
+ 3 x[1] x[2] x[6] x[10]
          2          2          4          4
+ 10 x[1] x[3] x[5] x[6] x[7] x[8]

```

```

                2, -th
                Number of Black box calls:, 133
          2          3          2          4
9 x[1] x[3] x[4] x[6] x[7] x[8] x[10]

```

$$\begin{aligned}
& + 17 x[1]^3 x[2]^2 x[5]^2 x[6]^3 x[7]^4 x[8]^3 x[9]^4 x[10]^3 \\
& + 17 x[2]^2 x[3]^4 x[4]^2 x[7]^4 x[8]^3 x[9]^3 x[10]^3 \\
& + 3 x[1]^3 x[2]^2 x[6]^3 x[10]^2 \\
& + 10 x[1]^2 x[3]^2 x[5]^4 x[6]^4 x[7]^4 x[8]^4
\end{aligned}$$

```

> read 'initpkg.mpl':
> with(protobox);
  [BM_step_mod, HybridInterp, NewtonInterp_step, bbpoly_mod,
    check_same, eval_mon_mod, eval_polyseq, eval_tmpprunelist_mod,
    find_max, find_true, heval_plist_mod, heval_pnt_mod,
    list_to_poly, prune, raising_pnts_mod, recover, relocate_c,
    relocate_shift_c, rev, rm_element, slice, spoly_to_slist,
    tmpprune, vansolve_kl_mod]
> bb:=bbpoly_mod(9*x[1]^2*x[3]*x[4]*x[6]^3*x[7]^2*x[8]*x[10]^4+17*x[1]^3
> *x[2]*x[5]^2*x[6]^2*x[7]*x[8]^3*x[9]^4*x[10]^3+17*x[2]^2*x[3]^4*x[4]^2
> *x[7]^4*x[8]^3*x[9]*x[10]^3+3*x[1]^3*x[2]^2*x[6]^3*x[10]^2+10*x[1]*x[3
> ]*x[5]^2*x[6]^2*x[7]^4*x[8]^4, [x[1], x[2], x[3], x[4], x[5], x[6], x[7], x[8]
> , x[9], x[10]]);
  bb := proc(pntsnf_i, modulusnf_i)
local polynf, inf, numvarsnf, varlistnf;
  polynf := 9*x[1]^2*x[3]*x[4]*x[6]^3*x[7]^2*x[8]*x[10]^4
    + 17*
    x[1]^3*x[2]*x[5]^2*x[6]^2*x[7]*x[8]^3*x[9]^4*x[10]^3
    + 17*x[2]^2*x[3]^4*x[4]^2*x[7]^4*x[8]^3*x[9]*x[10]^3
    + 3*x[1]^3*x[2]^2*x[6]^3*x[10]^2
    + 10*x[1]*x[3]*x[5]^2*x[6]^2*x[7]^4*x[8]^4;
  numvarsnf := 10;
  varlistnf := [x[1], x[2], x[3], x[4], x[5], x[6], x[7],
    x[8], x[9], x[10]];
  polynf := Eval(polynf, {seq(
    varlistnf[inf] = pntsnf_i[inf], inf = 1 .. numvarsnf)

```

```

    }) mod modulusnf_i;
    RETURN(polyfnf)
end
>
> for i from 1 to 100 do print(i, '-th');
> traperror(HybridInterp(bb,
> [x[1],x[2],x[3],x[4],x[5],x[6],x[7],x[8],x[9],x[10]],100,19,'test_thre
> sh'=0,'BM_thresh'=5, 'N_thresh'=5,'rep_tresh'=6, 'mapmon_thresh'=6 ));
> od;

```

```

1, -th

```

```

Warning: the range for random number or the modulus might not be\
enough

```

```

Interpolation Failure: dropped a non-zero term

```

```

2, -th

```

```

Warning: the range for random number or the modulus might not be\
enough

```

```

Interpolation Failure: dropped a non-zero term

```

```

3, -th

```

```

Warning: the range for random number or the modulus might not be\
enough

```

```

Interpolation Failure: dropped a non-zero term

```

```

4, -th

```

```

Warning: the range for random number or the modulus might not be\
enough

```

```

Interpolation Failure: dropped a non-zero term

```

```

5, -th

```


Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

6, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

7, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

8, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

9, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

10, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

11, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
12, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
13, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
14, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
15, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
16, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
17, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
18, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

19, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

20, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

21, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

22, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

23, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

24, -th

Warning: the range for random number or the modulus might not be

enough
Interpolation Failure: dropped a non-zero term
25, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
26, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
27, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
28, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
29, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
30, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term

31, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

32, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

33, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

34, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

35, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

36, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

37, -th

Warning: the range for random number or the modulus might not be\
enough

enough
In Zippel algorithm: different terms map to the same value, 6,
times
38, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
39, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
40, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
41, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
42, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
43, -th
Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term
44, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
45, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
46, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
47, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
48, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
49, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
50, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

51, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

52, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

53, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

54, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

55, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

56, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

57, -th

Warning: the range for random number or the modulus might not be\
enough

In Zippel algorithm: different terms map to the same value, 6,
times

58, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

59, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

60, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

61, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

62, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

63, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

64, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

65, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

66, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

67, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

68, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

69, -th

Warning: the range for random number or the modulus might not be\
enough

enough
Interpolation Failure: dropped a non-zero term
70, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
71, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
72, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
73, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
74, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
75, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term

76, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

77, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

78, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

79, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

80, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

81, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

82, -th

Warning: the range for random number or the modulus might not be\
enough

enough
Interpolation Failure: dropped a non-zero term
83, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
84, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
85, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
86, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
87, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
88, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term

89, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

90, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

91, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

92, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

93, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

94, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

95, -th

Warning: the range for random number or the modulus might not be\
enough

enough
Interpolation Failure: dropped a non-zero term
96, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
97, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
98, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
99, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term
100, -th
Warning: the range for random number or the modulus might not be\
enough
Interpolation Failure: dropped a non-zero term

```

> read 'initpkg.mpl':
> with(protobox);
  [BM_step_mod, HybridInterp, NewtonInterp_step, bbpoly_mod,
    check_same, eval_mon_mod, eval_polyseq, eval_tmpprunelist_mod,
    find_max, find_true, heval_plist_mod, heval_pnt_mod,
    list_to_poly, prune, raising_pnts_mod, recover, relocate_c,
    relocate_shift_c, rev, rm_element, slice, spoly_to_slist,
    tmpprune, vansolve_kl_mod]
> bb:=bbpoly_mod(9*x[1]^2*x[3]*x[4]*x[6]^3*x[7]^2*x[8]*x[10]^4+17*x[1]^3
> *x[2]*x[5]^2*x[6]^2*x[7]*x[8]^3*x[9]^4*x[10]^3+17*x[2]^2*x[3]^4*x[4]^2
> *x[7]^4*x[8]^3*x[9]*x[10]^3+3*x[1]^3*x[2]^2*x[6]^3*x[10]^2+10*x[1]*x[3
> ]*x[5]^2*x[6]^2*x[7]^4*x[8]^4, [x[1], x[2], x[3], x[4], x[5], x[6], x[7], x[8]
> , x[9], x[10]]);
  bb := proc(pntsnf_i, modulusnf_i)
local polynf, inf, numvarsnf, varlistnf;
  polynf := 9*x[1]^2*x[3]*x[4]*x[6]^3*x[7]^2*x[8]*x[10]^4
    + 17*
    x[1]^3*x[2]*x[5]^2*x[6]^2*x[7]*x[8]^3*x[9]^4*x[10]^3
    + 17*x[2]^2*x[3]^4*x[4]^2*x[7]^4*x[8]^3*x[9]*x[10]^3
    + 3*x[1]^3*x[2]^2*x[6]^3*x[10]^2
    + 10*x[1]*x[3]*x[5]^2*x[6]^2*x[7]^4*x[8]^4;
  numvarsnf := 10;
  varlistnf := [x[1], x[2], x[3], x[4], x[5], x[6], x[7],
    x[8], x[9], x[10]];
  polynf := Eval(polynf, {seq(
    varlistnf[inf] = pntsnf_i[inf], inf = 1 .. numvarsnf)

```



```

    }) mod modulusnf_i;
    RETURN(polyfnf)
end
>
> for i from 1 to 100 do print(i, '-th');
> traperror(HybridInterp(bb,
> [x[1],x[2],x[3],x[4],x[5],x[6],x[7],x[8],x[9],x[10]],100,29,'test_thre
> sh'=0,'BM_thresh'=5, 'N_thresh'=5,'rep_tresh'=6, 'mapmon_thresh'=6 ));
> od;

```

1, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

2, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

3, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

4, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

5, -th

Warning: the range for random number or the modulus might not be
enough

$$\begin{aligned} & \text{Number of Black box calls: , 321} \\ & \quad 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ 10 & x[1] x[3] x[5] x[6] x[7] x[8] + 3 x[1] x[2] x[6] x[10] \\ & \quad 2 \quad 3 \quad 2 \quad 4 \\ & + 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10] \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\ & - 12 x[2] x[3] x[4] x[7] x[8] x[9] x[10] \\ & \quad 3 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \\ & - 12 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10] \\ & \quad 6, \text{-th} \end{aligned}$$

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
7, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

8, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
9, -th

Warning: the range for random number or the modulus might not be

```
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
                10, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
                11, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
                12, -th
Warning: the range for random number or the modulus might not be\
    enough
        Interpolation Failure: dropped a non-zero term
                13, -th
Warning: the range for random number or the modulus might not be\
    enough
        Interpolation Failure: dropped a non-zero term
                14, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
```

15, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

16, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

17, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 326

$$\begin{aligned}
& 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\
10 \ x[1] \ x[3] \ x[5] \ x[6] \ x[7] \ x[8] \ + \ 3 \ x[1] \ x[2] \ x[6] \ x[10] \\
& \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\
& - \ 12 \ x[2] \ x[3] \ x[4] \ x[7] \ x[8] \ x[9] \ x[10] \\
& \quad 2 \quad 3 \quad 2 \quad 4 \\
& + \ 9 \ x[1] \ x[3] \ x[4] \ x[6] \ x[7] \ x[8] \ x[10]
\end{aligned}$$

18, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

19, -th

Warning: the range for random number or the modulus might not be
enough

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

23, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

24, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 324

10 x[1] x[3] x[5] x[6] x[7] x[8] + 3 x[1] x[2] x[6] x[10]

2 2 4 4 3 2 3 2
2 4 2 4 3 3
- 12 x[2] x[3] x[4] x[7] x[8] x[9] x[10]

2 3 2 4
+ 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10]

3 2 2 3 4 3
- 12 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10]

25, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 323

2 2 4 4 3 2 3 2

Warning: the range for random number or the modulus might not be
enough

$$\begin{aligned} & \text{Number of Black box calls: , 323} \\ & \quad 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ 10 \ x[1] \ x[3] \ x[5] \ x[6] \ x[7] \ x[8] \ + \ 3 \ x[1] \ x[2] \ x[6] \ x[10] \\ & \quad 2 \quad 3 \quad 2 \quad 4 \\ & \ + \ 9 \ x[1] \ x[3] \ x[4] \ x[6] \ x[7] \ x[8] \ x[10] \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\ & \ - \ 12 \ x[2] \ x[3] \ x[4] \ x[7] \ x[8] \ x[9] \ x[10] \\ & \quad 3 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \\ & \ - \ 12 \ x[1] \ x[2] \ x[5] \ x[6] \ x[7] \ x[8] \ x[9] \ x[10] \\ & \quad 31, \text{-th} \end{aligned}$$

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
32, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
33, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

34, -th

Warning: the range for random number or the modulus might not be\


```
    enough
      Interpolation Failure: dropped a non-zero term
          35, -th
Warning: the range for random number or the modulus might not be\
    enough
      Interpolation Failure: dropped a non-zero term
          36, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
          37, -th
Warning: the range for random number or the modulus might not be\
    enough
      Interpolation Failure: dropped a non-zero term
          38, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
          39, -th
Warning: the range for random number or the modulus might not be\
    enough
      Interpolation Failure: dropped a non-zero term
          40, -th
Warning: the range for random number or the modulus might not be\
```

```
    enough
      Interpolation Failure: dropped a non-zero term
        41, -th
Warning: the range for random number or the modulus might not be\
    enough
      Interpolation Failure: dropped a non-zero term
        42, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
        43, -th
Warning: the range for random number or the modulus might not be\
    enough
In Zippel algorithm: different terms map to the same value, 6,
    times
        44, -th
Warning: the range for random number or the modulus might not be\
    enough
      Interpolation Failure: dropped a non-zero term
        45, -th
Warning: the range for random number or the modulus might not be\
    enough
      Interpolation Failure: dropped a non-zero term
        46, -th
Warning: the range for random number or the modulus might not be\
```


51, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

52, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 321

$$\begin{aligned} & 10 x[1] x[3] x[5] x[6] x[7] x[8] + 3 x[1] x[2] x[6] x[10] \\ & \quad 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\ & + 5 x[2] x[3] x[4] x[7] x[8] x[9] x[10] \\ & \quad 2 \quad 3 \quad 2 \quad 4 \\ & + 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10] \end{aligned}$$

53, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 322

$$\begin{aligned} & 10 x[1] x[3] x[5] x[6] x[7] x[8] + 3 x[1] x[2] x[6] x[10] \\ & \quad 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ & \quad 2 \quad 3 \quad 2 \quad 4 \\ & + 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10] \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\ & - 12 x[2] x[3] x[4] x[7] x[8] x[9] x[10] \\ & \quad 3 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \\ & - 12 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10] \end{aligned}$$

54, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

55, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

56, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 321

$$\begin{aligned}
& 10 x[1] x[3] x[5] x[6] x[7] x[8] + 3 x[1] x[2] x[6] x[10] \\
& \quad 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\
& \quad 2 \quad 3 \quad 2 \quad 4 \\
& + 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10] \\
& \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\
& - 12 x[2] x[3] x[4] x[7] x[8] x[9] x[10] \\
& \quad 3 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \\
& - 12 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10]
\end{aligned}$$

57, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

58, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

59, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 321

$$\begin{aligned} & 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ 10 \ x[1] \ x[3] \ x[5] \ x[6] \ x[7] \ x[8] \ + \ 3 \ x[1] \ x[2] \ x[6] \ x[10] \\ & \quad 2 \quad \quad \quad 3 \quad 2 \quad \quad 4 \\ & + \ 9 \ x[1] \ x[3] \ x[4] \ x[6] \ x[7] \ x[8] \ x[10] \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad \quad 3 \\ & - \ 12 \ x[2] \ x[3] \ x[4] \ x[7] \ x[8] \ x[9] \ x[10] \\ & \quad 3 \quad \quad 2 \quad 2 \quad \quad 3 \quad 4 \quad 3 \\ & - \ 12 \ x[1] \ x[2] \ x[5] \ x[6] \ x[7] \ x[8] \ x[9] \ x[10] \end{aligned}$$

60, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

61, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 321

$$\begin{aligned} & 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ 10 \ x[1] \ x[3] \ x[5] \ x[6] \ x[7] \ x[8] \ + \ 3 \ x[1] \ x[2] \ x[6] \ x[10] \\ & \quad 2 \quad \quad \quad 3 \quad 2 \quad \quad 4 \end{aligned}$$

$$\begin{aligned}
& + 9 x[1]^2 x[3]^4 x[4]^2 x[6]^4 x[7]^3 x[8]^3 x[10]^3 \\
& - 12 x[2]^3 x[3]^2 x[4]^2 x[7]^3 x[8]^4 x[9]^3 x[10]^3 \\
& - 12 x[1]^3 x[2]^2 x[5]^2 x[6]^3 x[7]^4 x[8]^3 x[9]^4 x[10]^3
\end{aligned}$$

62, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term
63, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

64, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 357

$$\begin{aligned}
& 3 x[1]^3 x[2]^2 x[6]^3 x[10]^2 \\
& + 9 x[1]^2 x[3]^4 x[4]^2 x[6]^3 x[7]^2 x[8]^4 x[10]^3 \\
& - 12 x[2]^3 x[3]^2 x[4]^2 x[7]^3 x[8]^4 x[9]^3 x[10]^3 \\
& - 12 x[1]^3 x[2]^2 x[5]^2 x[6]^3 x[7]^4 x[8]^3 x[9]^4 x[10]^3
\end{aligned}$$

65, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

66, -th

Warning: the range for random number or the modulus might not be
enough

Number of Black box calls:, 324

$$\begin{aligned}
& 10 x[1]^2 x[3]^2 x[5]^4 x[6]^4 + 3 x[1]^3 x[2]^2 x[6]^3 x[10]^2 \\
& + 9 x[1]^2 x[3]^4 x[4]^2 x[6]^4 x[7]^3 x[8]^2 x[10]^4 \\
& - 12 x[2]^3 x[3]^4 x[4]^2 x[7]^4 x[8]^3 x[9]^3 x[10]^3 \\
& - 12 x[1]^3 x[2]^2 x[5]^2 x[6]^3 x[7]^4 x[8]^3 x[9]^3 x[10]^3
\end{aligned}$$

67, -th

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

68, -th

Warning: the range for random number or the modulus might not be
enough

In Zippel algorithm: different terms map to the same value, 6,
times

69, -th

Warning: the range for random number or the modulus might not be
enough

$$\begin{aligned} & \text{Number of Black box calls:}, 321 \\ & \quad 2 \quad 2 \quad 4 \quad 4 \quad 3 \quad 2 \quad 3 \quad 2 \\ 10 & x[1] x[3] x[5] x[6] x[7] x[8] + 3 x[1] x[2] x[6] x[10] \\ & \quad 2 \quad 3 \quad 2 \quad 4 \\ & + 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10] \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\ & - 12 x[2] x[3] x[4] x[7] x[8] x[9] x[10] \\ & \quad 3 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \\ & - 12 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10] \\ & \quad 70, \text{-th} \end{aligned}$$

Warning: the range for random number or the modulus might not be
enough

$$\begin{aligned} & \text{Number of Black box calls:}, 355 \\ & \quad 3 \quad 2 \quad 3 \quad 2 \\ 3 & x[1] x[2] x[6] x[10] \\ & \quad 2 \quad 3 \quad 2 \quad 4 \\ & + 9 x[1] x[3] x[4] x[6] x[7] x[8] x[10] \\ & \quad 2 \quad 4 \quad 2 \quad 4 \quad 3 \quad 3 \\ & - 12 x[2] x[3] x[4] x[7] x[8] x[9] x[10] \\ & \quad 3 \quad 2 \quad 2 \quad 3 \quad 4 \quad 3 \\ & - 12 x[1] x[2] x[5] x[6] x[7] x[8] x[9] x[10] \\ & \quad 71, \text{-th} \end{aligned}$$

Warning: the range for random number or the modulus might not be
enough

Interpolation Failure: dropped a non-zero term

72, -th

Warning: the range for random number or the modulus might not be\
enough

In Zippel algorithm: different terms map to the same value, 6,
times

73, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

74, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

75, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

76, -th

Warning: the range for random number or the modulus might not be\
enough

Interpolation Failure: dropped a non-zero term

77, -th

Warning: the range for random number or the modulus might not be\
enough

Warning, computation interrupted

Table 2-4: Algorithm Throughput on Smaller Moduli under Different Thresholds.

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

mod	13			17			19			23			29		
	=	≠	!	=	≠	!	=	≠	!	=	≠	!	=	≠	!
Default: test_thresh= 0 N_thresh= 1, BM_thresh= 1 rep_thresh= 0, mapmon_thresh= 0	0	11	89	3	17	80	0	4	96	1	4	96	2	4	94
test_thresh= 0 + 1, N_thresh= 1 + 1 BM_thresh= 1 + 1, rep_thresh= 0 + 2 mapmon_thresh= 0 + 2	0	0	100	9	0	91	0	0	100	8	0	92	10	2	90
test_thresh= 0 + 1, N_thresh= 1 + 1 BM_thresh= 1 + 1, rep_thresh= 0 + 4 mapmon_thresh= 0 + 4	0	0	100	15	1	84	0	0	100	24	0	76	17	0	83
test_thresh= 0 + 2, N_thresh= 1 + 2 BM_thresh= 1 + 2, rep_thresh= 0 + 4 mapmon_thresh= 0 + 4	0	0	100	21	0	79	0	0	100	26	0	74	22	0	78
test_thresh= 0 + 2, N_thresh= 1 + 2 BM_thresh= 1 + 2, rep_thresh= 0 + 6 mapmon_thresh= 0 + 6	0	0	100	14	0	86	0	0	100	28	0	72	19	0	81