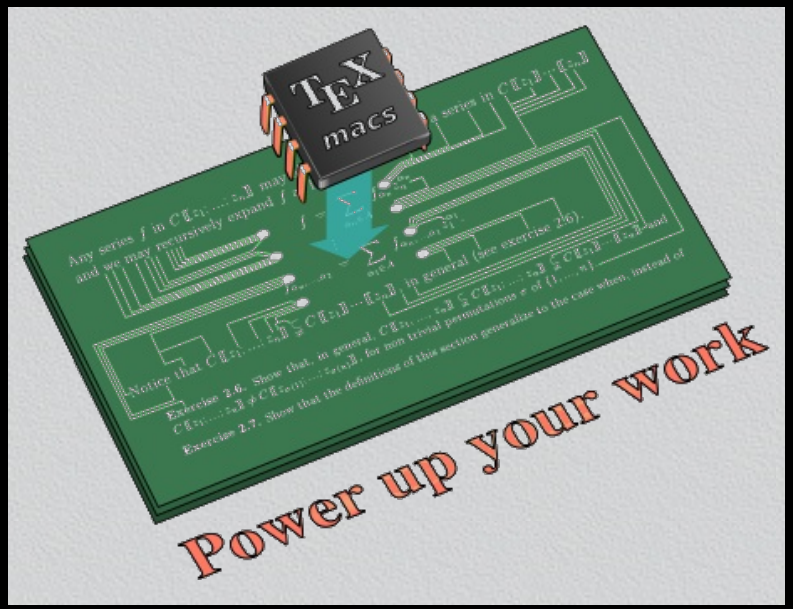
Sparse polynomial interpolation (part I)

Joris van der Hoeven

CNRS, visiting professor at PIMS and SFU

Joint work with Grégoire Lecerf



SFU, Vancouver

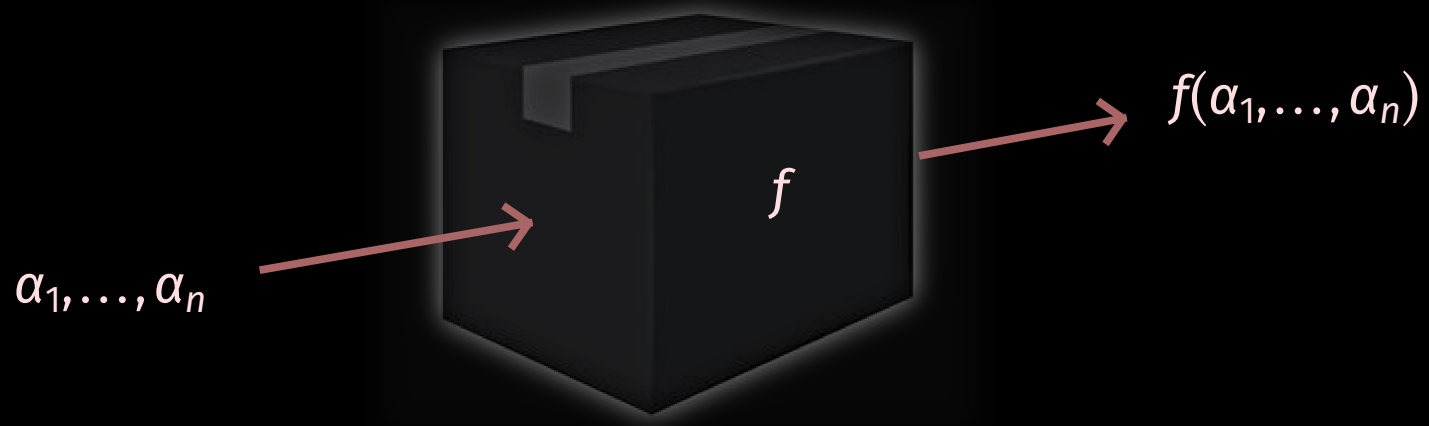
December 3, 2019

Part I

Statement of the problem

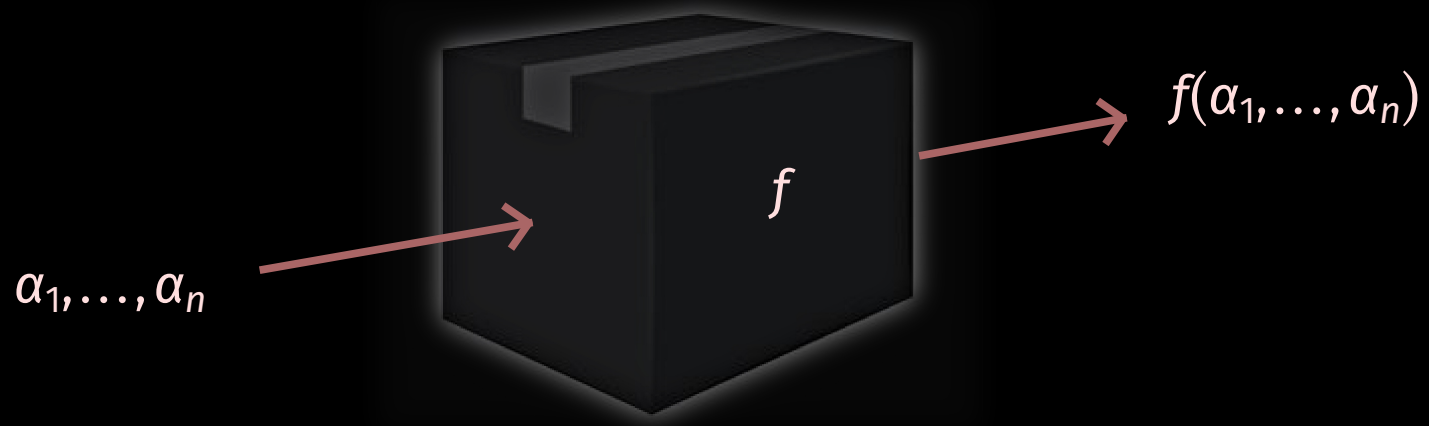
Black box functions and their interpolation

Input



Black box functions and their interpolation

Input

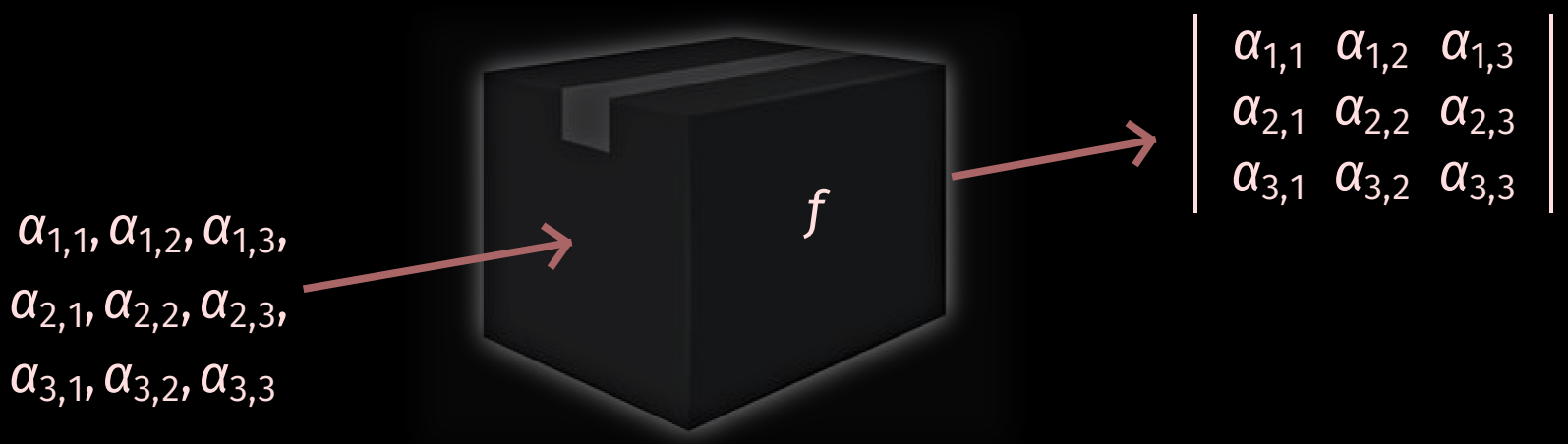


Output

$$f(x_1, \ldots, x_n) = c_1 x_1^{e_{1,1}} \cdots x_n^{e_{1,n}} + \cdots + c_t x_1^{e_{t,1}} \cdots x_n^{e_{t,n}}$$

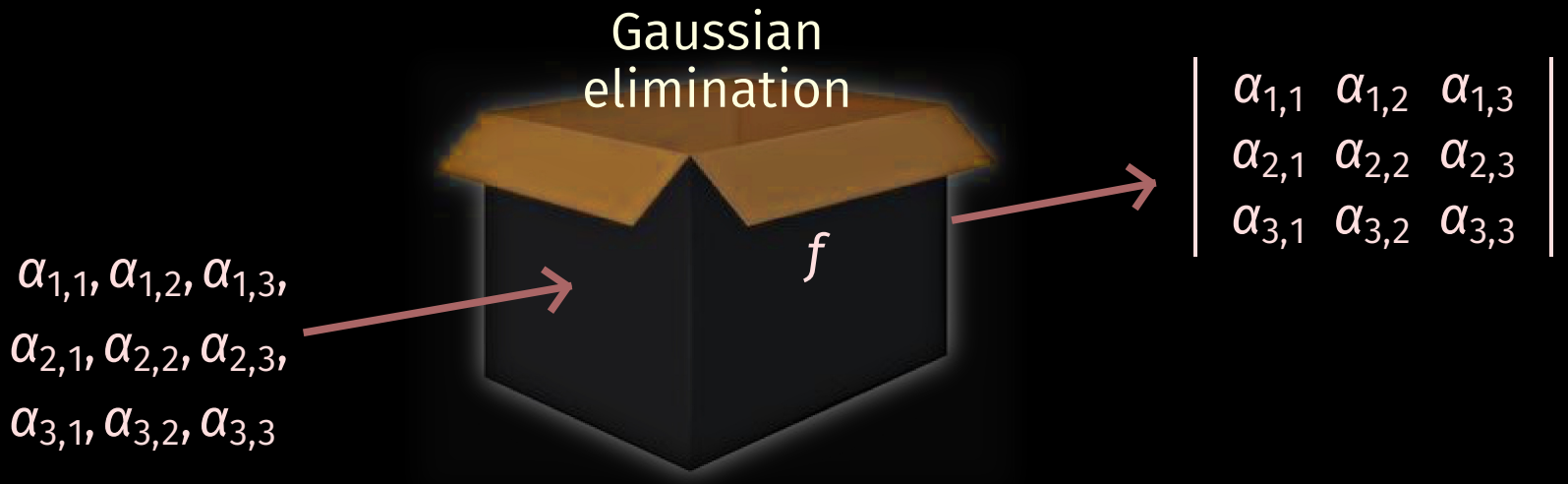
Example

Input



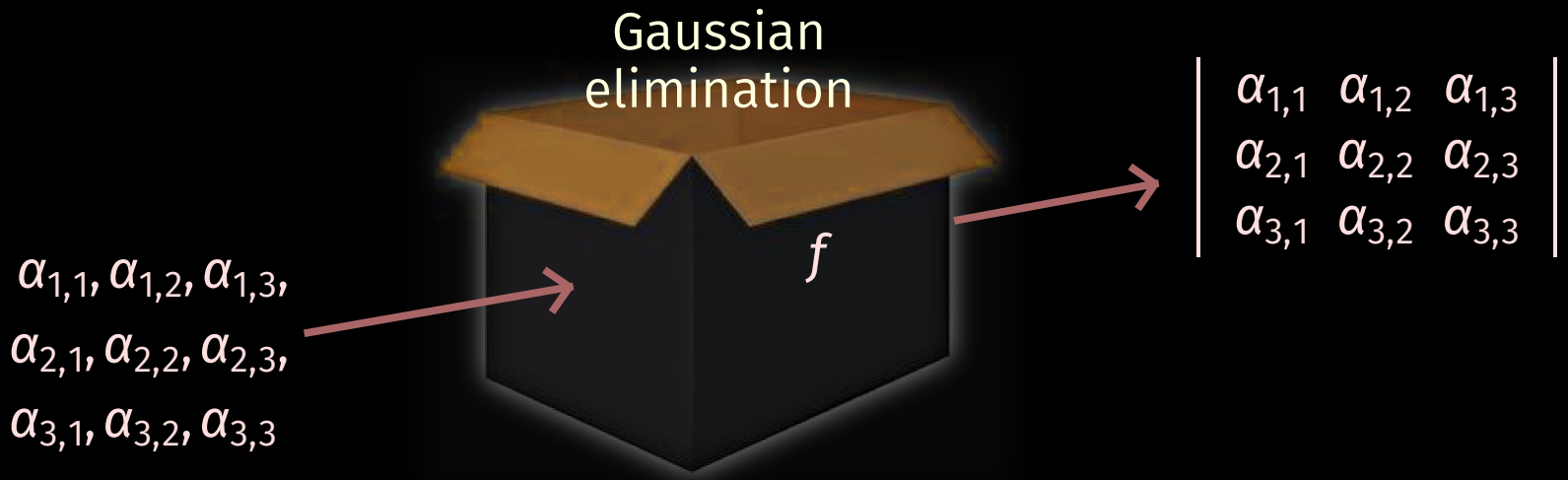
Example

Input



Example

Input



Output

$$x_{1,1}x_{2,2}x_{3,3} - x_{1,1}x_{2,3}x_{3,2} + x_{1,2}x_{2,3}x_{3,1} - x_{1,2}x_{2,1}x_{3,3} + x_{1,3}x_{2,1}x_{3,2} - x_{1,3}x_{2,2}x_{3,1}$$

Coefficients K

- A field from analysis such as $K = \mathbb{C}$.
- A discrete field such as $K = \mathbb{Q}$ or a finite field $K = \mathbb{F}_q$.
- Roots of unity ω of large smooth order in K?

Variants

Coefficients K

- A field from analysis such as $K = \mathbb{C}$.
- A discrete field such as $K = \mathbb{Q}$ or a finite field $K = \mathbb{F}_q$.
- Roots of unity ω of large smooth order in K?

Complexity model

- Algebraic *versus* bit complexity.
- Deterministic (needs bounds) *versus* probabilistic.
- Theoretic (asymptotic) *versus* practical complexity.
- Divisions in K allowed for evaluation of f?
- Allow evaluations at points in A^n for extension $A \supseteq K$?

Variants

Coefficients K

- A field from analysis such as $K = \mathbb{C}$.
- A discrete field such as $K = \mathbb{Q}$ or a finite field $K = \mathbb{F}_q$.
- Roots of unity ω of large smooth order in K?

Complexity model

- Algebraic *versus* bit complexity.
- Deterministic (needs bounds) *versus* probabilistic.
- Theoretic (asymptotic) *versus* practical complexity.
- Divisions in K allowed for evaluation of f?
- Allow evaluations at points in A^n for extension $A \supseteq K$?

How sparse?

- Weakly sparse: total degrees d of the order $O(\log t)$.
- Normally sparse: total degrees d of the order $t^{O(1)}$.
- Super sparse: total degrees of order d with $\log t = o(\log d)$.

Short history

Old work

- Prony [1795]
- Zippel [1979, 1990]

Short history

Old work

- Prony [1795]
- Zippel [1979, 1990]

Rediscovery and early work in computer algebra

- Ben-Or Tiwari [1988]
- Kaltofen-Yagati [1988], Canny-Kaltofen-Lakshman [1989], Kaltofen-Trager [1990], Kaltofen-Lakshman-Wiley [1990]
- Huang-Rao [1996], Murao-Fujise [1996]

Short history

Old work

- Prony [1795]
- Zippel [1979, 1990]

Rediscovery and early work in computer algebra

- Ben-Or Tiwari [1988]
- Kaltofen-Yagati [1988], Canny-Kaltofen-Lakshman [1989], Kaltofen-Trager [1990], Kaltofen-Lakshman-Wiley [1990]
- Huang-Rao [1996], Murao-Fujise [1996]

Early implementations

- Diaz-Kaltofen [1988] FOXFOX
- Freeman-Imirzian-Kaltofen-Lakshman [1988] Dagwood

Short history continued...

Recent work

- Garg-Schost [2009]
- Javadi-Monagan [2010], Hu-Monagan [2013, 2016], Monagan-Tuncer [2015, 2019], Monagan-Wong [2016]
- Giesbrecht-Roche [2011], Arnold-Giesbrecht-Roche [2014, 2016], Arnold-Roche [2014], Roche [2018]
- vdH-Lecerf [2009, 2013, 2015, 2019], Grenet-vdH-Lecerf [2015, 2016]
- Huang-Gao [2017], Huang [2019]

Short history continued...

Recent work

- Garg-Schost [2009]
- Javadi-Monagan [2010], Hu-Monagan [2013, 2016], Monagan-Tuncer [2015, 2019], Monagan-Wong [2016]
- Giesbrecht-Roche [2011], Arnold-Giesbrecht-Roche [2014, 2016], Arnold-Roche [2014], Roche [2018]
- vdH-Lecerf [2009, 2013, 2015, 2019], Grenet-vdH-Lecerf [2015, 2016]
- Huang-Gao [2017], Huang [2019]

Modern implementations

- Monagan [2010–] Maple
- vdH-Lecerf [2009, 2015–] Mathemagix

Part II

Generalities

Reduction to case with known bounds

Algorithm

Input: a polynomial black box function $f(x_1, \ldots, x_n)$
Output: the sparse interpolation f^* of f

1. Set initial bounds $T := 1$ and $D := 1$ for t and the total degree d of f
2. Determine the sparse interpolation f^* of f using these bounds
3. If $f = f^*$ with high probability, then return f^*
4. Increase T and/or D and return to step 2

Algorithm

Input: a polynomial black box function $f(x_1, \ldots, x_n)$
Output: the sparse interpolation f^* of f

1. Let $f^* := 0$ be an initial approximation of f
2. Determine the approximate sparse interpolation δ^* of $\delta := f - f^*$
3. Set $f^* := f^* + \delta^*$
4. If $f = f^*$ with high probability, then return f^*
5. Return to step 3

Finite fields

Unique finite field $\mathbb{F}_q$ of each size $q = p^n$, with p prime and $n \in \mathbb{N}$

Finite fields

Unique finite field $\mathbb{F}_q$ of each size $q = p^n$, with p prime and $n \in \mathbb{N}$

Defining equation

We have $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$, whence $f = f \operatorname{rem} (x_1^{q-1} - 1, \ldots, x_n^{q-1} - 1)$

Finite fields

Unique finite field $\mathbb{F}_q$ of each size $q = p^n$, with p prime and $n \in \mathbb{N}$

Defining equation

We have $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$, whence $f = f \operatorname{rem} (x_1^{q-1} - 1, \ldots, x_n^{q-1} - 1)$

Roots of unity

$\mathbb{F}_q^*$ is a cyclic group of order $q - 1 \Rightarrow \exists$ primitive root of unity of order $q - 1$

- Usually, $q - 1$ admits a few small prime divisors
- If n is smooth, then $q - 1$ usually admits many small prime divisors
  $2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$

Finite fields

Unique finite field $\mathbb{F}_q$ of each size $q = p^n$, with p prime and $n \in \mathbb{N}$

Defining equation

We have $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$, whence $f = f \bmod (x_1^{q-1} - 1, \ldots, x_n^{q-1} - 1)$

Roots of unity

$\mathbb{F}_q^*$ is a cyclic group of order $q-1 \Rightarrow \exists$ primitive root of unity of order $q-1$

- Usually, $q-1$ admits a few small prime divisors
- If n is smooth, then $q-1$ usually admits many small prime divisors
  $2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$

Frobenius automorphisms $(a\,b)^q = a^q\,b^q, (a+b)^q = a^q + b^q$

$$\begin{aligned} \phi : \mathbb{F}_{q^s} &\longrightarrow \mathbb{F}_{q^s} \\ a &\longmapsto a^q \end{aligned}$$

Part III

The cyclic extension approach

(Univariate case)

Idea

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$$

Idea

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$$

Main idea

For pairwise coprime $r = r_1, r_2, \ldots$, evaluate f at $\bar{x} \in K[x]/(x^r - 1)$, which yields

$$f \operatorname{rem} (x^r - 1) = c_1 x^{e_1 \operatorname{rem} r} + \cdots + c_t x^{e_t \operatorname{rem} r}$$

Match corresponding terms and reconstruct f using Chinese remaindering

Idea

$$f = c_1 x^{e_1} + \cdots + c_t x^{e_t}$$

Main idea

For pairwise coprime $r = r_1, r_2, \ldots$, evaluate f at $\bar{x} \in K[x]/(x^r - 1)$, which yields

$$f \operatorname{rem} (x^r - 1) = c_1 x^{e_1 \operatorname{rem} r} + \cdots + c_t x^{e_t \operatorname{rem} r}$$

Match corresponding terms and reconstruct f using Chinese remaindering

Diversification

Several ways to "match corresponding terms"

Easiest approach: assume that $c_1, \ldots, c_t$ are (almost all) pairwise distinct

α is random and $|K|$ large $\Rightarrow f(\alpha x)$ is diversified with high probability

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^2 - 1) = (2 + 7 + 11)x + (18 + 33 + 1 + 4 + 28)$$
$$f \bmod (x^3 - 1) = (2 + 1)x^2 + (18 + 33 + 7 + 4)x + (11 + 28)$$
$$f \bmod (x^5 - 1) = (4 + 11)x^3 + (33 + 2 + 1)x^2 + 7x + (18 + 28)$$
$$f \bmod (x^7 - 1) = 4x^6 + (18 + 1)x^5 + 7x^2 + (33 + 2)x + (11 + 28)$$
$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^9 + (18 + 4 + 11)x^8 + 33x + (28 + 7)$$
$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^9 + 7x^4 + 18x^3 + 2x^2 + 4x + 28$$
$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^2 + 28$$
$$f \bmod (x^{19} - 1) = (2 + 7)x^7 + 11x^6 + (33 + 4)x^4 + 18x^3 + (28 + 1)$$
$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^6 + 4x^3 + 33x^2 + 28$$
$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^7 + (7 + 11)x^5 + 4x^2 + (33 + 28)$$
$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^2 + 11x + 28$$
$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^7 + 1x^4 + 28$$
$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^4 + 28$$

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^2 - 1) = (2 + 7 + 11)x + (18 + 33 + 1 + 4 + 28)$$

$$f \bmod (x^3 - 1) = (2 + 1)x^2 + (18 + 33 + 7 + 4)x + (11 + 28)$$

$$f \bmod (x^5 - 1) = (4 + 11)x^3 + (33 + 2 + 1)x^2 + 7x + (18 + 28)$$

$$f \bmod (x^7 - 1) = 4x^6 + (18 + 1)x^5 + 7x^2 + (33 + 2)x + (11 + 28)$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^9 + (18 + 4 + 11)x^8 + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^9 + 7x^4 + 18x^3 + 2x^2 + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^2 + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^7 + 11x^6 + (33 + 4)x^4 + 18x^3 + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^6 + 4x^3 + 33x^2 + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^7 + (7 + 11)x^5 + 4x^2 + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^2 + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^7 + 1x^4 + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^4 + 28$$

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^2 - 1) = (2 + 7 + 11)x + (18 + 33 + 1 + 4 + 28)$$

$$f \bmod (x^3 - 1) = (2 + 1)x^2 + (18 + 33 + 7 + 4)x + (11 + 28)$$

$$f \bmod (x^5 - 1) = (4 + 11)x^3 + (33 + 2 + 1)x^2 + 7x + (18 + 28)$$

$$f \bmod (x^7 - 1) = 4x^6 + (18 + 1)x^5 + 7x^2 + (33 + 2)x + (11 + 28)$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^9 + (18 + 4 + 11)x^8 + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^9 + 7x^4 + 18x^3 + 2x^2 + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^2 + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^7 + 11x^6 + (33 + 4)x^4 + 18x^3 + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^6 + 4x^3 + 33x^2 + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^7 + (7 + 11)x^5 + 4x^2 + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^2 + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^7 + 1x^4 + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^4 + 28$$

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	0	0	0	0	0	0	0	0
modulo	1	1	1	1	1	1	1	1

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	0	1	10	9	0	0	0	0
modulo	1	11	11	11	1	1	1	1

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	3	1	54	9	4	1	0	0
modulo	13	11	143	143	13	13	1	13

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	3	45	197	9	121	1	0	0
modulo	13	187	2431	143	187	13	1	187

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	3	45	197	9	121	1	6	0
modulo	247	187	2431	143	187	13	19	187

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	250	232	197	153	121	118	63	0
modulo	5681	4301	55913	3289	4301	299	437	4301

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	250	232	197	153	121	118	63	0
modulo	164749	4301	$>10^6$	95381	4301	8671	437	4301

Example

$$f = 18x^{250} + 33x^{232} + 2x^{197} + x^{152} + 7x^{121} + 4x^{118} + 11x^{63} + 28$$

$$f \bmod (x^{11} - 1) = 2x^{10} + 1x^{9} + (18 + 4 + 11)x^{8} + 33x + (28 + 7)$$

$$f \bmod (x^{13} - 1) = (33 + 11)x^{11} + 1x^{9} + 7x^{4} + 18x^{3} + 2x^{2} + 4x + 28$$

$$f \bmod (x^{17} - 1) = (4 + 1)x^{16} + (18 + 11)x^{12} + 33x^{11} + 2x^{10} + 7x^{2} + 28$$

$$f \bmod (x^{19} - 1) = (2 + 7)x^{7} + 11x^{6} + (33 + 4)x^{4} + 18x^{3} + (28 + 1)$$

$$f \bmod (x^{23} - 1) = 18x^{20} + 11x^{17} + 1x^{14} + 2x^{13} + 7x^{6} + 4x^{3} + 33x^{2} + 28$$

$$f \bmod (x^{29} - 1) = 2x^{23} + 18x^{18} + 1x^{7} + (7 + 11)x^{5} + 4x^{2} + (33 + 28)$$

$$f \bmod (x^{31} - 1) = (1 + 7)x^{28} + 4x^{25} + 33x^{15} + 2x^{11} + 18x^{2} + 11x + 28$$

$$f \bmod (x^{37} - 1) = 18x^{28} + 11x^{26} + 2x^{12} + (33 + 7)x^{10} + 4x^{7} + 1x^{4} + 28$$

$$f \bmod (x^{41} - 1) = 7x^{39} + 4x^{36} + 2x^{33} + 1x^{29} + 33x^{27} + 11x^{22} + 18x^{4} + 28$$

coefficient	18	33	2	1	7	4	11	28
exponent	250	232	197	153	121	118	63	0
modulo	$>10^6$	133331	$>10^6$	95381	4301	268801	13547	133331

The algorithm

Algorithm

Input: a black box polynomial $f(x)$, a degree bound D, a sparsity bound T
Output: a partial sparse interpolation f^* of f

1. Determine suitable moduli $r_1, \ldots, r_l > T$ with $\operatorname{lcm}(r_1, \ldots, r_l) > D$
2. Evaluate f at x in $K[x]/(x^{r_i} - 1)$ for $i = 1, \ldots, l$
3. Determine matching terms in the expansions of $f^{[r_1]}, \ldots, f^{[r_l]}$ (likely from the same term $c_i x^{e_i}$ in the expansion of f)
4. Return the sum f^* of all terms $c_i x^{e_i}$ as above

Algorithm

Input: a diversified black box polynomial $f(x)$, suitable moduli $r_1, r_2, \ldots, r_l$

Output: an approximate sparse interpolation f^* of f

1. Compute $f^{[r_k]} = f \operatorname{rem} (x^{r_k} - 1)$ for $k = 1, \ldots, l$.
2. Let $f^* := 0$.
3. Let $\mathscr{C}_k :=$ set of all coefficients that occur once in $f^{[r_k]}$, for $k = 1, \ldots, l$.
4. For each $c \in \mathscr{C}_1 \cup \cdots \cup \mathscr{C}_l$ do:

   If $\mathscr{K} := \{k : c \in \mathscr{C}_k\}$ is such that $\operatorname{lcm}(r_k : k \in \mathscr{K}) > D$, then:

   Determine the unique exponent $e < D$ such that $c\,x^{e \operatorname{rem} r_k}$ occurs in $f^{[r_k]}$ for every $k \in \mathscr{K}$, and set $f^* := f^* + c\,x^e$.
5. Return f^*.

Heuristic assumption

When reducing $f(x)$ modulo $x^r - 1$, the modular reductions of exponents $e_i \operatorname{rem} r$ are uniformly distributed in $\{0, \ldots, r-1\}$

Heuristic assumption

When reducing $f(x)$ modulo $x^r - 1$, the modular reductions of exponents $e_i \operatorname{rem} r$ are uniformly distributed in $\{0, \ldots, r-1\}$

Throwing t balls in r boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = e^{\log\left(1-\frac{1}{r}\right)t} = e^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx e^{-t/r}$$

Heuristic assumption

When reducing $f(x)$ modulo $x^r - 1$, the modular reductions of exponents $e_i \operatorname{rem} r$ are uniformly distributed in $\{0, \ldots, r-1\}$

Throwing t balls in r boxes

- Probability that a ball ends up in a box of its own:

$$\left(1-\frac{1}{r}\right)^{t-1} \approx \left(1-\frac{1}{r}\right)^{t} = e^{\log\left(1-\frac{1}{r}\right)t} = e^{\left(-\frac{1}{r}-\frac{1}{2r^2}+\cdots\right)t} \approx e^{-t/r}$$

- On average, we obtain $e^{-t/r}\, t$ non-colliding terms when evaluating $f(x) \operatorname{rem} (x^r - 1)$.

Complexity analysis

- L: number of operations needed to evaluate f

Complexity analysis

- L: number of operations needed to evaluate f
- $M(n) = O^{\flat}(n \log n)$: cost to multiply two polynomials of degree $\leqslant n$

Complexity analysis

- L: number of operations needed to evaluate f
- $M(n) = O^{\flat}(n \log n)$: cost to multiply two polynomials of degree $\leqslant n$
- Cost of one evaluation $f(x) \operatorname{rem} (x^r - 1)$ is $O(L\,\mathsf{M}(r))$

Complexity analysis

- L: number of operations needed to evaluate f
- $M(n) = O^{\flat}(n \log n)$: cost to multiply two polynomials of degree $\leqslant n$
- Cost of one evaluation $f(x) \operatorname{rem} (x^r - 1)$ is $O(L\, \mathsf{M}(r))$
- Expected number of correct terms: $\mathrm{e}^{-t/r}\, t$

Complexity analysis

- L: number of operations needed to evaluate f
- $M(n) = O^{\flat}(n \log n)$: cost to multiply two polynomials of degree $\leqslant n$
- Cost of one evaluation $f(x) \operatorname{rem} (x^r - 1)$ is $O(L\, \mathsf{M}(r))$
- Expected number of correct terms: $\mathrm{e}^{-t/r}\, t$
- Cost per correct term proportional to $r\, \mathrm{e}^{t/r}$

Complexity analysis

- L: number of operations needed to evaluate f
- $M(n) = O^\flat(n \log n)$: cost to multiply two polynomials of degree $\leqslant n$
- Cost of one evaluation $f(x) \operatorname{rem} (x^r - 1)$ is $O(L\,\mathsf{M}(r))$
- Expected number of correct terms: $\mathrm{e}^{-t/r}\,t$
- Cost per correct term proportional to $r\,\mathrm{e}^{t/r}$
- Optimum obtained by taking $r_1 \approx \cdots \approx r_l \approx t$

Complexity analysis

- L: number of operations needed to evaluate f
- $M(n) = O^\flat(n \log n)$: cost to multiply two polynomials of degree $\leqslant n$
- Cost of one evaluation $f(x) \operatorname{rem} (x^r - 1)$ is $O(L\,\mathsf{M}(r))$
- Expected number of correct terms: $\mathrm{e}^{-t/r}\,t$
- Cost per correct term proportional to $r\,\mathrm{e}^{t/r}$
- Optimum obtained by taking $r_1 \approx \cdots \approx r_l \approx t$

Proposition (modulo heuristic hypothesis)

Given $0 < \eta < 1$ and a diversified polynomial $f \in \mathbb{F}_q[x]$ of degree $d \leqslant D$ and with $t \leqslant T$ terms, there exists a Monte Carlo probabilistic algorithm which computes at least $(1-\eta)\,t$ terms of f in time

$$O^\flat(L\,T \log D \log(q\,T)).$$