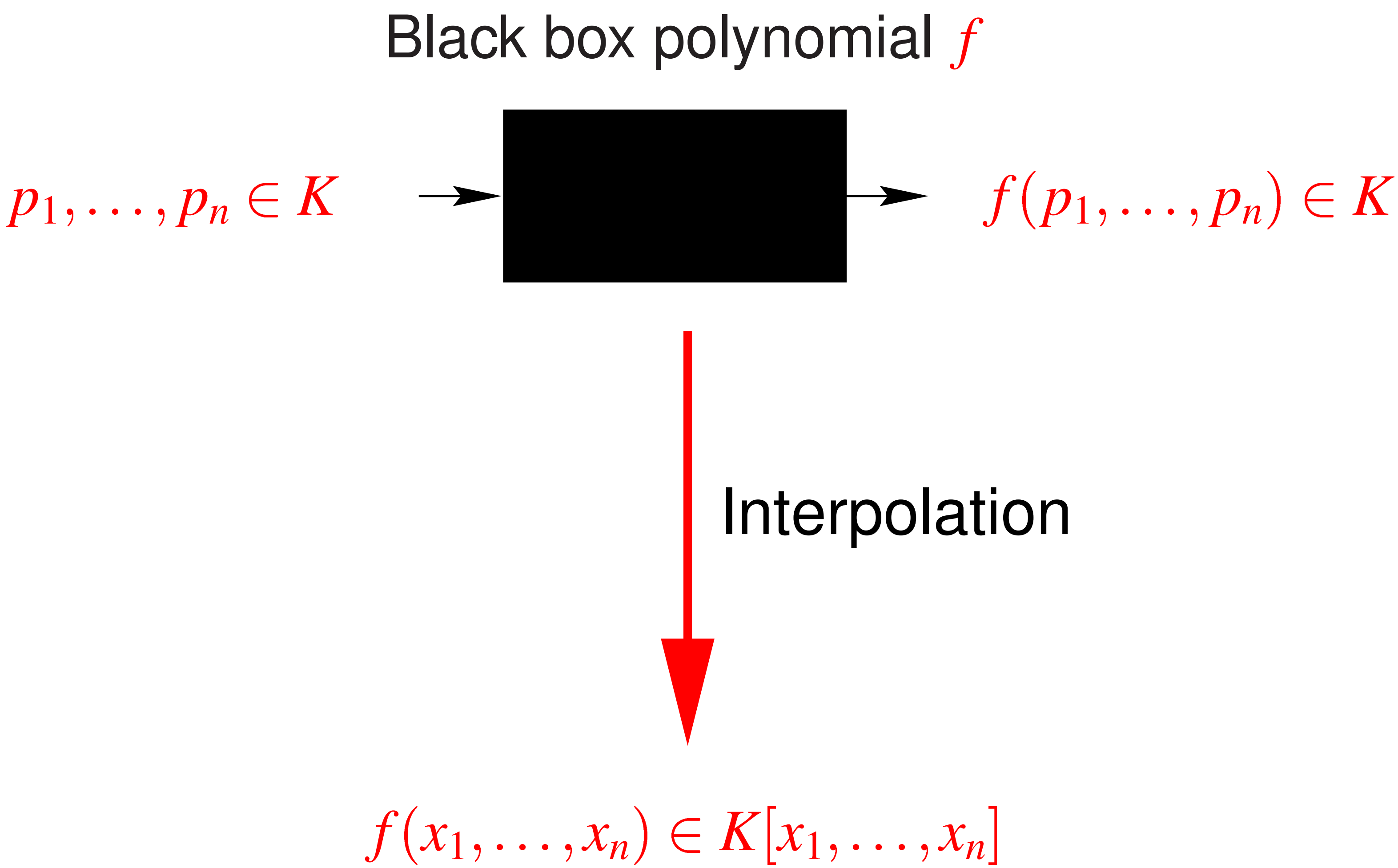
Early Termination Strategies in Sparse Interpolation and Sparse Shift Algorithms

Wen-shin Lee

ORCCA
Ontario Research Centre for Computer Algebra

December 7, 2001

Black box polynomial interpolation



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

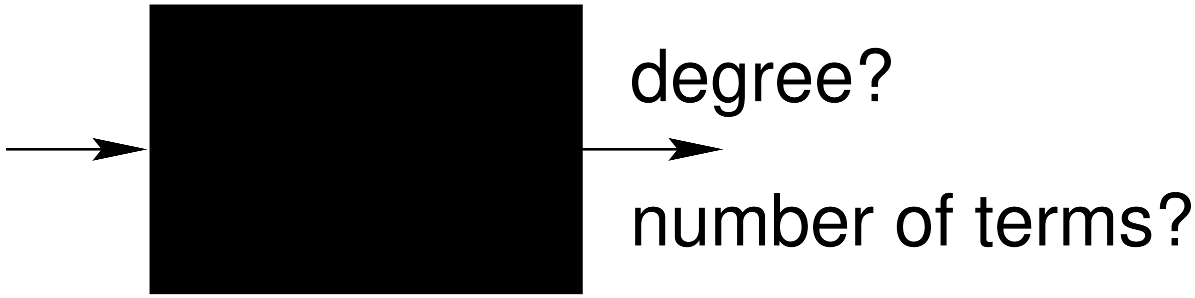
Zippel's probabilistic interpolation.

Needs an upper bound for the degree in each variable.

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

Needs an upper bound for the number of non-zero terms.

Early termination strategy



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 strategy.***

  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 (univariate)

- – Interpolate $f(x)$ on a random value sequence $p_0,\ p_1,\ p_2,\ldots$
  $f^{[i]} = c_0 + c_1(x - p_0) + \cdots + c_i(x - p_0)\cdots(x - p_{i-1})$
  – $\boxed{\text{When } c_i = 0,}$ f is interpolated with high probability.
  $(i = \deg f + 2)$
- Threshold $\eta > 1$ can improve the probability of correctness.

$f(x)$ is interpolated in the mixed power basis:

$$1,\ (x - p_0),\ (x - p_0)(x - p_1),\ \ldots$$

Early termination in the Ben-Or/Tiwari algorithm (multivariate)

- – Perform the Berlekamp/Massey algorithm on
  $$f(p),\ f(p^2),\ f(p^3),\ \dots,\ f(p^i),\ \dots$$ with p random.
  $\boxed{\text{When } \Delta = 0 \text{ at } 2L < i,}$ generator $\Lambda(z)$ is determined with high probability.
  $(i = 2t+1,\ t$ the number of non-zero terms in $f)$
  – Recover non-zero terms in f via finding roots for $\Lambda(z)$.
  – Locate coefficients for non-zero terms in f.
- Threshold $\zeta > 1$ can improve the probability, but its analysis is complicated.

$f(x)$ is interpolated in the standard power basis:
$$1,\ x,\ x^2,\ x^3,\ \dots$$ in the univariate case.

Early termination in sparse interpolations with respect to

Pochhammer basis:

$x^{\overline{n}} = x(x+1)\cdots(x+n-1)$

$f(x) = \sum_{j=1}^{t} c_j x^{\overline{e}_j}$

Pick random $p > 0$, evaluate $f(p), f(p+1), f(p+2), \ldots$

Chebyshev basis:

$T_0(x) = 1, \quad T_1(x) = x$

$i \geq 2: \quad T_i(x) = 2xT_{i-1}(x) - T_{i-2}(x)$

$f(x) = \sum_{j=1}^{t} c_j T_{\delta_j}(x)$

Pick random $p > 1$, evaluate $f(T_0(p)), f(T_1(p)), f(T_2(p)), \ldots$

Sparse shifts for polynomials

For univariate polynomials (Lakshman and Saunders)

- Need $f(x) = \sum_{i=0}^{d} c_i x^i$, its first 2τ derivatives, and an upper bound τ for the number of terms in the sparse shift.
- Need to evaluate $f(x)$ and its first 2τ derivatives at 2 points for a total of $4\tau + 2$ evaluations.

Grigoriev and Lakshman extended to multivariate polynomials.

Generalized early termination Ben-Or/Tiwari algorithm

- The shift s is given as input.
- – Perform the Berlekamp/Massey algorithm on
  $$f(p-s),\ f(p^2-s),\ \ldots,\ f(p^i-s),\ \ldots \text{ with } p \text{ random.}$$
  $\boxed{\text{When } \Delta = 0 \text{ at } 2L < i,}$ generator $\Lambda(z)$ is determined with high probability.
  $(i = 2t+1,\ t$ the term number of f in the basis shifted by $s)$
  – Recover non-zero terms in f via finding roots for $\Lambda(z)$.
  – Locate coefficients for non-zero terms in f.
- Threshold $\zeta \cdots$

$f(x)$ is interpolated in the shifted power basis:

$$1,\ x+s,\ (x+s)^2,\ (x+s)^3,\ \ldots \text{ in the univariate case.}$$

Early termination in sparse shifts

- To determine a most sparse shift α

  $f = \sum_{i=1}^{\tau} c_i (x+\alpha)^{e_i}, \quad c_i \neq 0$ and τ the minimum.

- – Perform the Berlekamp/Massey algorithm on

  $$f(p-\alpha),\ f(p^2-\alpha),\ \ldots,\ f(p^i-\alpha),\ \ldots$$ with p random.

  Now $\Delta(\alpha) \in \mathbb{K}(\alpha)$,

  $\boxed{\text{find the first } \alpha \text{ such that } \Delta(\alpha) = 0 \text{ at } 2L < i,}$

  $(i = 2\tau + 1)$

  ...

  – ...

  – ...

How to find α efficiently?

☹ Factorize numer$(\Delta(\alpha))$

$2\tau+1$ black box probes:

until $\Delta_{2\tau+1}(\alpha)$

😐 Compute the polynomial GCD of numer$(\Delta_i(\alpha))$ and numer$(\Delta_{i+1}(\alpha))$

$2\tau+2$ black box probes:

until GCD(numer$(\Delta_{2\tau+1}(\alpha))$, numer$(\Delta_{2\tau+2}(\alpha))$)

☺ Compute the GCD of numer$(\Delta_i(0))$ and numer$(\Delta_{i+1}(0))$

?

☺ ???