On the Complexity of Multivariate Interpolation and of Simultaneous Polynomial Approximations

Muhammad F. I. Chowdhury† Claude-Pierre Jeannerod§
Éric Schost† Vincent Neiger§ Gilles Villard§

†Computer Science Department, The University of Western Ontario, London, ON, Canada
§Laboratoire de l’Informatique du Parallélisme, École Normale Supérieure de Lyon, France

August 4, 2013
The problem of Polynomial Reconstruction (1/2)

Figure: Polynomial reconstruction (Lagrange interpolation)
The problem of Polynomial Reconstruction (1/2)

Figure: Polynomial reconstruction

degree ≤ 3
agreement ≥ 4
The problem of Polynomial Reconstruction (1/2)

Figure: Polynomial reconstruction (all solutions)
The problem of Polynomial Reconstruction (2/2)

This is a generalization of Lagrange interpolation.

Polynomial Reconstruction

**Input:**

- $n$ points $\{(x_i, y_i)\}_{1 \leq i \leq n}$ in $\mathbb{K}^2$, with the $x_i$’s distinct
- $k$ the degree constraint, $t$ the agreement

**Output:**

- all polynomials $w$ in $\mathbb{K}[X]$ such that
  
  \[
  \deg w \leq k \quad \text{and} \quad \# \{ i \mid w(x_i) = y_i \} \geq t. \]

Famous application in coding theory:
list-decoding Reed-Solomon codes [Guruswami and Sudan, 1999]
Several algorithms, one strategy

Most algorithms consist of two main steps,

- **Interpolation step**
  
  compute $Q(X, Y)$ such that: \( w(X) \) solution $\Rightarrow Q(X, w(X)) = 0$

- **Root-finding step**
  
  find all $Y$-roots of $Q(X, Y)$, keep those that are solutions

Here we are interested in the interpolation step

$\Rightarrow$ leads to the problem of **Interpolation with Multiplicities**.
The problem of Interpolation with multiplicities

Interpolation With Multiplicities

Input:

- $n$ points $\{(x_i, y_i)\}_{1 \leq i \leq n}$ in $\mathbb{K}^2$, with the $x_i$'s distinct
- $k$ the degree constraint, $t$ the agreement
- $\ell$ the list-size, $m$ the multiplicity ($m \leq \ell$)

Output:

- a polynomial $Q$ in $\mathbb{K}[X, Y]$ such that
  
  (i) $Q$ is nonzero,
  (ii) $\deg_Y Q(X, Y) \leq \ell$,  \hspace{1cm} (list-size condition)
  (iii) $\deg_X Q(X, X^k Y) < mt$,  \hspace{1cm} (weighted-degree condition)
  (iv) $\forall i, Q(x_i, y_i) = 0$ with multiplicity $m$. \hspace{1cm} (vanishing condition)
Algorithms based on structured linear systems

[Roth - Ruckenstein, 2000] [Zeh - Gentner - Augot, 2011]

Write

$$Q(X, Y) = \sum_{0 \leq j \leq \ell} Q_j(X) Y^j$$  \hspace{1cm} \text{(list-size condition)}

where $\deg Q_j(X) < mt - jk$. \hspace{1cm} \text{(weighted-degree condition)}

Then, rewrite the vanishing condition so that a solution $Q(X, Y)$ can be retrieved as a nontrivial solution of a homogeneous structured linear system (the unknown being the coefficient vector of $Q(X, Y)$).

Complexity bound for this method:

$$O(\ell m^4 n^2)$$

using a modified Feng-Tzeng’s linear system solver [Feng - Tzeng, 1991].
Algorithms based on polynomial lattices

[Alekhnovich, 2002] [Reinhard, 2003] [Beelen - Brander, 2010] [Bernstein, 2011] [Cohn - Heninger, 2011]

Build a polynomial lattice $\mathcal{L}$ such that

$$Q(X, Y) \in \mathcal{L} \iff \text{(list-size condition) + (vanishing condition)}.$$ 

Then, a solution to Interpolation With Multiplicities can be retrieved as a short vector in $\mathcal{L}$ (weighted-degree condition).

Complexity bound for this method:

$$O^\sim(\ell^\omega mn)$$

using the most efficient polynomial lattice basis reduction algorithm: [Gupta - Sarkar - Storjohann - Valeriote, 2012]
Contributions

1. New approach
   - Based on a more general problem
   - Solved using structured linear systems
   - Improved complexity bound
     \[ O^{\sim}(\ell^{\omega-1} m^2 n) \]

2. Extension to the multivariate case
   - Based on the same more general problem
   - Improved complexity bound
     \[ O^{\sim}\left( \left( \frac{s + \ell}{s} \right)^{\omega-1} mn \left( \frac{s + m - 1}{s} \right) \right) \]
Contributions

1. New approach
   - Based on a more general problem
   - Solved using structured linear systems
   - Improved complexity bound
     \[ O(\ell^{\omega-1} m^2 n) \]

2. Extension to the multivariate case
   - Based on the same more general problem
   - Improved complexity bound
     \[ O^\sim \left( \left( \frac{s + \ell}{s} \right)^{\omega-1} m n \left( \frac{s + m - 1}{s} \right) \right) \]
Univariate reformulation (1/2)

Defining

\[ G(X) = \prod_{1 \leq i \leq n} (X - x_i) \]

and

\[ R(X) \] such that \( \forall i, R(x_i) = y_i \),

the vanishing condition becomes a set of univariate modular equations.

Lemma of univariate reformulation [Zeh - Gentner - Augot, 2011]

\[
\left( \forall i \in \{1, \ldots, n\}, \; Q(x_i, y_i) = 0 \text{ with multiplicity } m \right) \iff \left( \forall i < m, \; Q[i](X, R(X)) = 0 \mod G(X)^{m-i} \right).
\]
Univariate reformulation: the vanishing condition is

\[ \forall i < m, \quad Q[i](X, R(X)) = 0 \pmod{G(X)^{m-i}} \]

Assume that \( Q \) satisfies the list-size condition: \( \deg_Y Q \leq \ell \).

By definition of the Hasse derivative, the vanishing condition is

\[ \forall i < m, \quad \sum_{i \leq j \leq \ell} Q_j(X) \binom{j}{i} R(X)^{j-i} = 0 \pmod{G(X)^{m-i}} \]

Goal: derive a linear system directly from these equations
From the univariate reformulation to a linear system (1/3)

Vanishing condition + list-size condition:

\[ \forall i < m, \quad \sum_{i \leq j \leq \ell} Q_j(X) \binom{j}{i} R(X)^{j-i} = 0 \pmod{G(X)^{m-i} \cdot P_i(X)} \]

Cost for computing \( F_{i,j} \) and \( P_i \):

- computing \( n(m - i) \) coefficients of \( F_{i,j} \) for every \( i, j \)
  \[ \approx \text{computing } nm \text{ coefficients of } R(X)^j \text{ for } 0 \leq j \leq \ell \]
  \[ \leadsto \mathcal{O}^\sim(\ell m^2 n) \text{ operations } \in \mathcal{O}(\ell^{\omega-1} m^2 n) \]
- computing \( P_i \) for every \( i \)
  \[ = \text{computing the } m \text{ polynomials } G(X), G(X)^2, \ldots, G(X)^m \]
  \[ \leadsto \mathcal{O}^\sim(m^2 n) \text{ operations } \in \mathcal{O}(\ell^{\omega-1} m^2 n) \]
From the univariate reformulation to a linear system (2/3)

Vanishing condition + list-size condition + weighted-degree condition:

\[ \forall i < m, \quad \sum_{i \leq j \leq \ell} \sum_{0 \leq r < N_j} Q_j^{(r)} X^r F_{i,j}(X) = 0 \pmod{P_i(X)} \]

Define the companion matrix

\[
C(P_i) = \begin{bmatrix}
0 & 0 & \cdots & 0 & -P_i^{(0)} \\
1 & 0 & \cdots & 0 & -P_i^{(1)} \\
0 & 1 & \cdots & 0 & -P_i^{(2)} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & -P_i^{(M_i-1)}
\end{bmatrix} \in \mathbb{K}^{M_i \times M_i}
\]

Key property:

multiplication by \( C(P_i) \) on the left is multiplication by \( X \) modulo \( P_i(X) \)
Solution $\iff$ nonzero vector in the nullspace of the matrix

$\begin{array}{cccc}
& m_{t} & m_{t-k} & N_{j} & m_{t-\ell k} \\
\hline
n_{m} & A_{0,0} & & A_{0,j} & A_{0,t} \\
n(m-1) & & & & \\
M_{i} & A_{i,0} & A_{i,j} & & A_{i,t} \\
\hline
n & m_{i-1,0} & & A_{m-1,j} & \hspace{1cm} m_{i-1,t} \\
\end{array}$

where the block $A_{i,j} \in K^{M_{i} \times N_{j}}$ is defined by its first column

$c^{(0)} = \begin{bmatrix} F_{i,j}^{(0)} \\ \vdots \\ F_{i,j}^{(M_{i}-1)} \end{bmatrix}$ and the subsequent columns $c^{(r+1)} = C(P_{i}) \cdot c^{(r)}$. 
Improved cost via Simultaneous Polynomial Approximations

Complexity bound for this approach

Solving the structured linear system [Bitmead - Anderson, 1980] [Morf, 1980] [Kaltofen, 1994] [Pan, 2001] [Bostan - Jeannerod - Schost, 2007]

Two main operations:

- Computing generators
  - Computing the first and last column of each block $\sim O(\ell m^2 n)$
  - Computing the first row of each block $\sim O(\ell m^2 n)$
  $\sim O(\ell m^2 n)$ operations

- Solving the system
  - At most $\ell + 1$ blocks on each row or column,
  - The number of equations is $\sum_i n(m - i) = O(m^2 n)$
  $\sim O(\ell^{\omega-1} m^2 n)$ operations

Complexity bound:

$O(\ell^{\omega-1} m^2 n)$
Which problem have we solved?

\[
\forall i < m, \quad \sum_{i \leq j \leq \ell} Q_j(X) \binom{j}{i} R(X)^{j-i} = 0 \pmod{G(X)^{m-i}} \]

Simultaneous Polynomial Approximations

**Input:**

- **Parameters:** \(\ell\) the list-size, \(m\) the number of equations
- **Moduli:** \(P_i \in \mathbb{K}[X]\) monic of degree \(M_i\), for every \(i < m\)
- **Polynomials:** \(F_{i,j} \in \mathbb{K}[X]\) of degree less than \(M_i\), for \(i < m\) and \(j \leq \ell\)
- **Degree bounds:** \(N_j\) a positive integer, for every \(j \leq \ell\)

**Output:** \(Q_0, \ldots, Q_\ell \in \mathbb{K}[X]\) satisfying

1. \(Q_j(X)\) are not all zero,
2. \(\forall j \leq \ell, \deg Q_j(X) < N_j\),
3. \(\forall i < m, \sum_{j \leq \ell} Q_j(X) F_{i,j}(X) = 0 \pmod{P_i(X)}\)
Contributions

1. New approach
   - Based on a more general problem
   - Solved using structured linear systems
   - Improved complexity bound
     \[ \mathcal{O}^\sim(\ell^{\omega-1} m^2 n) \]

2. Extension to the multivariate case
   - Based on the same more general problem
   - Improved complexity bound
     \[ \mathcal{O}^\sim \left( \left( \frac{s + \ell}{s} \right)^{\omega-1} m n \left( \frac{s + m - 1}{s} \right) \right) \]
Contributions

1. New approach
   - Based on a more general problem
   - Solved using structured linear systems
   - Improved complexity bound
     \[ O(\ell^{\omega-1} m^2 n) \]

2. Extension to the multivariate case
   - Based on the same more general problem
   - Improved complexity bound
     \[ O(\left(\left(\frac{s + \ell}{s}\right)^{\omega-1} mn\left(\frac{s + m - 1}{s}\right)\right) \]
Multivariate Interpolation with Multiplicities

**Input:**
- $s$ the number of variables
- $n$ points $\{(x_i, y_{i1}, \ldots, y_{is})\}_{1 \leq i \leq n}$ in $\mathbb{K}^{s+1}$, with the $x_i$’s distinct
- $k$ the degree constraint, $t$ the agreement
- $\ell$ the list-size, $m$ the multiplicity

**Output:** a polynomial $Q$ in $\mathbb{K}[X, Y_1, \ldots, Y_s]$ such that

(i) $Q$ is nonzero,
(ii) $\deg_Y Q(X, Y_1, \ldots, Y_s) \leq \ell$, \hspace{1cm} (list-size condition)
(iii) $\deg_X Q(X, X^k Y_1, \ldots, X^k Y_s) < mt$, \hspace{1cm} (weighted-degree condition)
(iv) $\forall i, Q(x_i, y_{i1}, \ldots, y_{is}) = 0$ with multiplicity $m$. \hspace{1cm} (vanishing condition)

Application: list-decoding of folded Reed-Solomon codes
From univariate reformulation...

Defining

\[ G(X) = \prod_{1 \leq i \leq n}(X - x_i) \]

and

\[ R_1(X), \ldots, R_s(X) \text{ such that } R_r(x_i) = y_{ir}, \]

the vanishing condition becomes a set of univariate modular equations.

**Lemma of univariate reformulation**

\[ \begin{aligned}
    \left( &\text{for } i \in \{1, \ldots, n\} : Q(x_i, y_{i1}, \ldots, y_{is}) = 0 \text{ with multiplicity } m \right) \\
    \iff &\left( \text{for } i = (i_1, \ldots, i_s), \ |i| < m : \right. \\
    &\left. Q^{[i]}(X, R_1(X), \ldots, R_s(X)) = 0 \pmod{G(X)^{m-|i|}} \right) .
\end{aligned} \]
Vanishing condition + list-size condition + weighted-degree condition:

\[
\sum_{i \leq j, |j| \leq \ell} Q_j(X) \binom{j_1}{i_1} R_1(X)^{j_1-i_1} \cdots \binom{j_s}{i_s} R_s(X)^{j_s-i_s} = 0 \pmod{G(X)^{m-|i|}}
\]

for \( i = (i_1, \ldots, i_m) \) such that \( |i| < m \). Rewrite this as

\[
\text{for every } i, |i| < m : \sum_{i \leq j, |j| \leq \ell} Q_j(X) F_{i,j}(X) = 0 \pmod{P_i(X)}
\]

Instance of Simultaneous Polynomial Approximations

- list-size \( \binom{s+\ell}{s} \)
- number of linear equations \( mn\binom{s+m-1}{s} \)
Cost for computing the polynomials $F_{i,j}$ and $P_i$:

$$\mathcal{O}\left(\left(\binom{s + \ell}{s} m n \binom{s + m - 1}{s}\right) \right) + \mathcal{O}(m^2 n)$$

Improves on [Busse, 2008] and [Brander, 2010]
Contributions

1. New approach
   - Based on a more general problem
   - Solved using structured linear systems
   - Improved complexity bound

\[ \mathcal{O}^\sim(\ell^\omega - 1 m^2 n) \]

2. Extension to the multivariate case
   - Based on the same more general problem
   - Improved complexity bound

\[ \mathcal{O}^\sim \left( \left( \frac{s + \ell}{s} \right)^{\omega - 1} m n \left( \frac{s + m - 1}{s} \right) \right) \]
Contributions

1. New approach
   - Based on a more general problem
   - Solved using structured linear systems
   - Improved complexity bound
     \[ \mathcal{O}^\sim(\ell^{\omega-1} m^2 n) \]

2. Extension to the multivariate case
   - Based on the same more general problem
   - Improved complexity bound
     \[ \mathcal{O}^\sim \left( \left( \begin{array}{c} s + \ell \\ s \end{array} \right)^{\omega-1} mn \left( \begin{array}{c} s + m - 1 \\ s \end{array} \right) \right) \]