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)

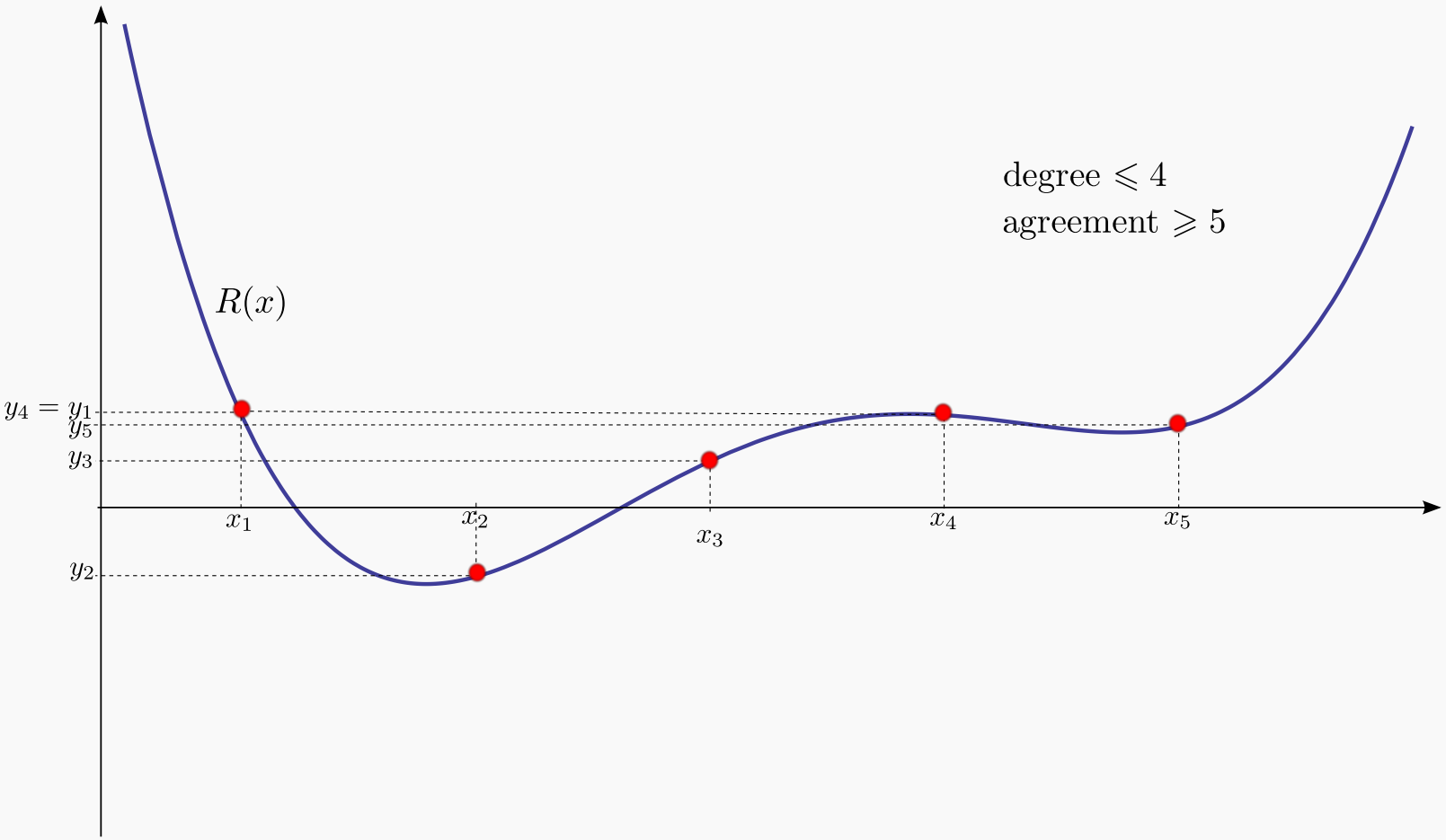


Figure: Polynomial reconstruction (Lagrange interpolation)

The problem of Polynomial Reconstruction (1/2)

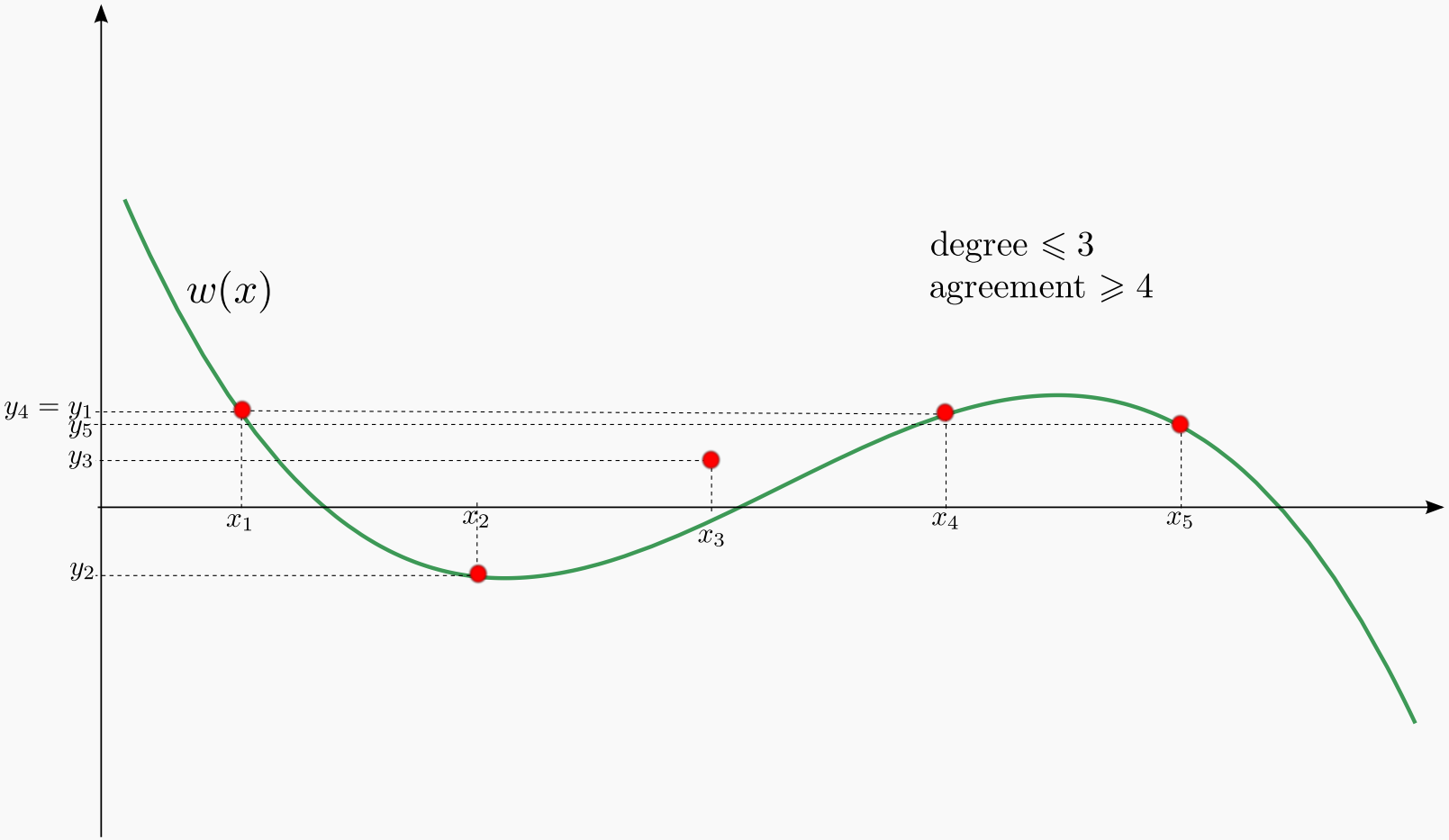


Figure: Polynomial reconstruction

The problem of Polynomial Reconstruction (1/2)

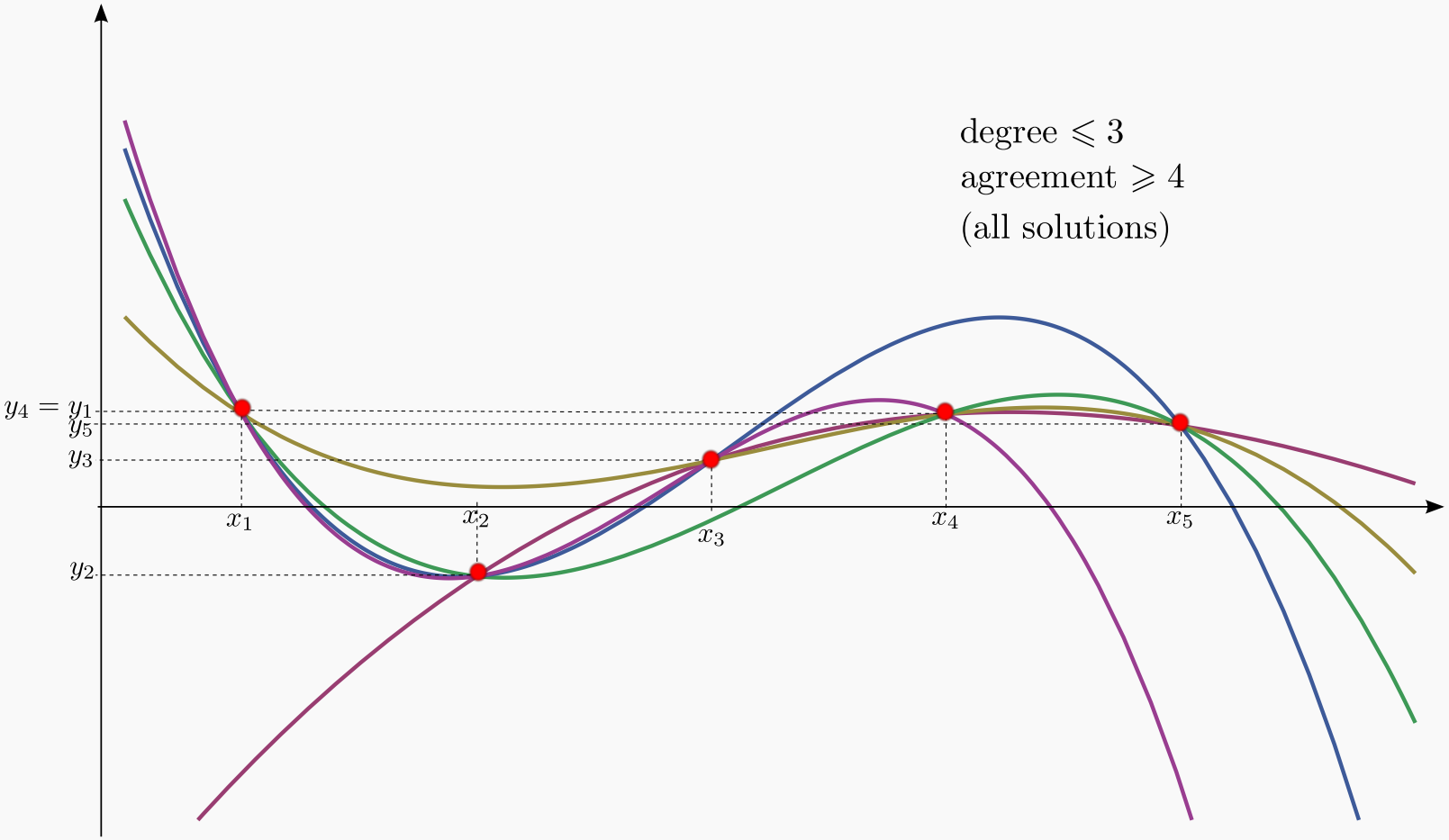


Figure: Polynomial reconstruction (all solutions)

The problem of Polynomial Reconstruction (2/2)

This is a generalization of Lagrange interpolation.

Polynomial Reconstruction

Input:

n points $\{(x_i, y_i)\}_{1 \leqslant i \leqslant n}$ 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

$$\deg w \leqslant k \qquad \text{and} \qquad \#\{i \mid w(x_i) = y_i\} \geqslant t.$$

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 $\{(x_i, y_i)\}_{1 \leqslant i \leqslant n}$ in $\mathbb{K}^2$, with the x_i's distinct

k the degree constraint, t the agreement

ℓ the list-size, m the multiplicity $(m \leqslant \ell)$

Output:

a polynomial Q in $\mathbb{K}[X, Y]$ such that

(i)	Q is nonzero,	
(ii)	$\deg_Y Q(X, Y) \leqslant \ell$,	(list-size condition)
(iii)	$\deg_X Q(X, X^k Y) < mt$,	(weighted-degree condition)
(iv)	$\forall i,\ Q(x_i, y_i) = 0$ with multiplicity m.	(vanishing condition)

Algorithms based on structured linear systems

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

Write

$$Q(X,Y) = \sum_{0 \leqslant j \leqslant \ell} Q_j(X) Y^j \qquad \text{(list-size condition)}$$

$$\text{where} \quad \deg Q_j(X) < mt - jk. \qquad \text{(weighted-degree condition)}$$

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:

$$\mathcal{O}(\ell m^4 n^2)$$

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

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

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:

$$\tilde{\mathcal{O}}(\ell^{\omega} mn)$$

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

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

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

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Contributions

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

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

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

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Univariate reformulation (1/2)

Defining

$$G(X) = \prod_{1 \leqslant i \leqslant n} (X - x_i)$$

and

$$R(X) \text{ such that } \forall i, R(x_i) = y_i,$$

the vanishing condition becomes a set of univariate modular equations.

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

$$\left(\forall i \in \{1, \ldots, n\},\ Q(x_i, y_i) = 0 \text{ with multiplicity } m \right)$$
$$\iff \quad \left(\forall i < m,\ \ Q^{[i]}(X, R(X)) = 0 \mod G(X)^{m-i} \right).$$

Univariate reformulation (2/2)

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: $\deg_Y Q \leqslant \ell$.

By definition of the Hasse derivative, the vanishing condition is

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \binom{j}{i} R(X)^{j-i} = 0 \pmod{G(X)^{m-i}}$$

Goal: derive a linear system directly from these equations

From the univariate reformulation to a linear system (1/3)

Vanishing condition + list-size condition:

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \underbrace{\binom{j}{i} R(X)^{j-i}}_{F_{i,j}(X)} = 0 \pmod{\underbrace{G(X)^{m-i}}_{P_i(X)}}$$

Cost for computing $F_{i,j}$ and P_i:

- computing $n(m-i)$ coefficients of $F_{i,j}$ for every i, j
  $\approx$ computing nm coefficients of $R(X)^j$ for $0 \leqslant j \leqslant \ell$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\boldsymbol{\ell \mathbf{m}^2 \mathbf{n}})$ **operations** $\in \mathcal{O}(\ell^{\omega-1} m^2 n)$
- computing P_i for every i
  $=$ computing the m polynomials $G(X), G(X)^2, \ldots, G(X)^m$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\mathbf{m}^2 \mathbf{n})$ **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:

$$\forall i < m, \qquad \sum_{i \leqslant j \leqslant \ell} \sum_{0 \leqslant r < N_j} Q_j^{(r)} X^r F_{i,j}(X) \;=\; 0 \pmod{P_i(X)}$$

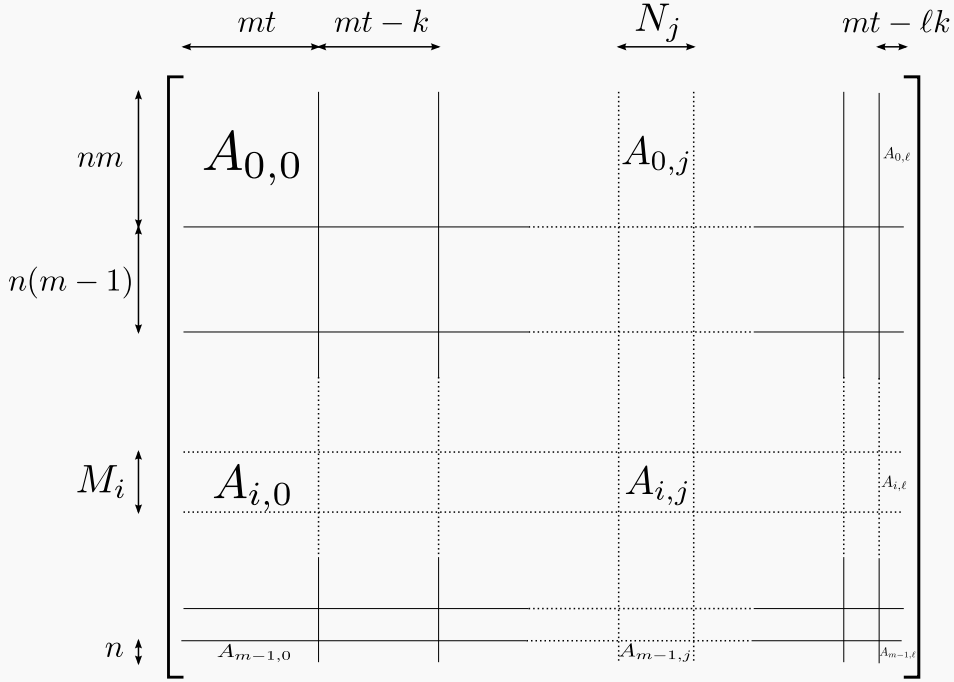
Define the companion matrix

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

Key property:
multiplication by $\mathcal{C}(P_i)$ on the left is multiplication by X modulo $P_i(X)$

From the univariate reformulation to a linear system (3/3)

Solution $\Longleftrightarrow$ nonzero vector in the nullspace of the matrix



where the block $A_{i,j} \in \mathbb{K}^{M_i \times N_j}$ 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 $c^{(r+1)} = \mathcal{C}(P_i) \cdot c^{(r)}$.

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
  $\approx$ computing the first and last column of each block $\rightsquigarrow \tilde{\mathcal{O}}(\ell m^2 n)$
  $+$ computing the first row of each block $\rightsquigarrow \tilde{\mathcal{O}}(\ell m^2 n)$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\ell \mathbf{m^2 n})$ **operations**
- solving the system
  at most $\ell + 1$ blocks on each row or column,
  the number of equations is $\sum_i n(m-i) = \mathcal{O}(m^2 n)$
  $\rightsquigarrow$ $\tilde{\mathcal{O}}(\ell^{\omega-1} \mathbf{m^2 n})$ **operations**

Complexity bound:

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

Which problem have we solved?

$$\forall i < m, \quad \sum_{i \leqslant j \leqslant \ell} Q_j(X) \underbrace{\binom{j}{i} R(X)^{j-i}}_{F_{i,j}(X)} = 0 \pmod{\underbrace{G(X)^{m-i}}_{P_i(X)}}$$

Simultaneous Polynomial Approximations

Input:

- Parameters: ℓ 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 $j \leqslant \ell$
- Degree bounds: N_j a positive integer, for every $j \leqslant \ell$

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

- (i') $Q_j(X)$ are not all zero,
- (ii') $\forall j \leqslant \ell$, $\deg Q_j(X) < N_j$,
- (iii') $\forall i < m$, $\sum_{j \leqslant \ell} Q_j(X) F_{i,j}(X) = 0 \pmod{P_i(X)}$.

Contributions

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

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

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

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Contributions

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

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

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

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Multivariate Interpolation with Multiplicities

Multivariate Interpolation With Multiplicities

Input:

s the number of variables

n points $\{(x_i, y_{i1}, \ldots, y_{is})\}_{1 \leqslant i \leqslant n}$ in $\mathbb{K}^{s+1}$, with the x_i's distinct

k the degree constraint, t the agreement

ℓ 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) $\deg_{\boldsymbol{Y}} Q(X, Y_1, \ldots, Y_s) \leqslant \ell$, (list-size condition)

(iii) $\deg_X Q(X, X^k Y_1, \ldots, X^k Y_s) < mt$, (weighted-degree condition)

(iv) $\forall i,\ Q(x_i, y_{i1}, \ldots, y_{is}) = 0$ with multiplicity m. (vanishing condition)

Application: list-decoding of folded Reed-Solomon codes

From univariate reformulation...

Defining

$$G(X) = \prod_{1 \leqslant i \leqslant n} (X - x_i)$$

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

$$\left(\text{for } i \in \{1, \ldots, n\} : \ Q(x_i, y_{i1}, \ldots, y_{is}) = 0 \text{ with multiplicity } m \right)$$

$$\iff \quad \left(\text{for } \boldsymbol{i} = (i_1, \ldots, i_s), \ |\boldsymbol{i}| < m : \right.$$

$$\left. Q^{[\boldsymbol{i}]}(X, R_1(X), \ldots, R_s(X)) = 0 \pmod{G(X)^{m-|\boldsymbol{i}|}} \right).$$

. . . to simultaneous polynomial approximations

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

$$\underbrace{\sum_{\boldsymbol{i} \preccurlyeq \boldsymbol{j}, |\boldsymbol{j}| \leqslant \ell} Q_{\boldsymbol{j}}(X) \binom{j_1}{i_1} R_1(X)^{j_1 - i_1} \cdots \binom{j_s}{i_s} R_s(X)^{j_s - i_s}}_{Q^{[\boldsymbol{i}]}(X, R_1(X), \ldots, R_s(X))} = 0 \pmod{G(X)^{m - |\boldsymbol{i}|}}$$

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

$$\text{for every } \boldsymbol{i}, |\boldsymbol{i}| < m : \quad \sum_{\boldsymbol{i} \preccurlyeq \boldsymbol{j}, |\boldsymbol{j}| \leqslant \ell} Q_{\boldsymbol{j}}(X) F_{\boldsymbol{i},\boldsymbol{j}}(X) = 0 \pmod{P_{\boldsymbol{i}}(X)}$$

Instance of Simultaneous Polynomial Approximations

- list-size $\binom{s+\ell}{s}$
- number of linear equations $mn\binom{s+m-1}{s}$

Complexity bound in the multivariate case

Cost for computing the polynomials $F_{i,j}$ and P_i:

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

$\rightsquigarrow$ Complexity bound in the multivariate case

$$\mathcal{O}^{\sim}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

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

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

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

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$

Contributions

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

$$\tilde{\mathcal{O}}(\ell^{\omega-1} m^2 n)$$

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

$$\tilde{\mathcal{O}}\left(\binom{s+\ell}{s}^{\omega-1} mn \binom{s+m-1}{s}\right)$$