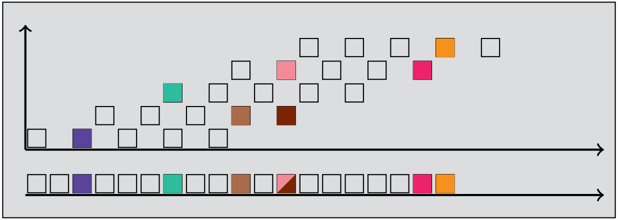
Multivariate sparse interpolation using randomized Kronecker substitutions



Andrew Arnold

Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada

Daniel S. Roche

Computer Science Department
United States Naval Academy
Annapolis, Maryland, USA

ISSAC 2014
Kobe, Japan
July 24, 2014

Overview

Our Main Result

A new **randomization** that improves
the **Kronecker substitution** trick
by **reducing the degree**
when the polynomial is **sparse**.

The initial application is sparse interpolation.

Kronecker

Definition

The *Kronecker Substitution* (1882) is a map:

multivariate polynomial → univariate polynomial

$$\mathsf{R}[x, y] \to \mathsf{R}[z]$$

defined by $f(x, y) \mapsto f(z, z^D)$, where $D > \deg_x(f)$.

This map is a homomorphism and
it is invertible given the degree bound D.

(Can also map polynomials to integers, or multivariate to univariate.)

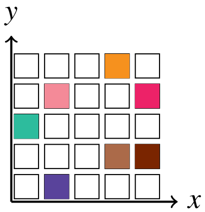
Kronecker Example

Example

$f(x, y) = \blacksquare x + \blacksquare x^3 y + \blacksquare x^4 y + \blacksquare y^2 + \blacksquare x y^3 + \blacksquare x^4 y^3 + \blacksquare x^3 y^4$

(colored boxes ■ represent coefficients in R)

Representation of $f(x, y)$:



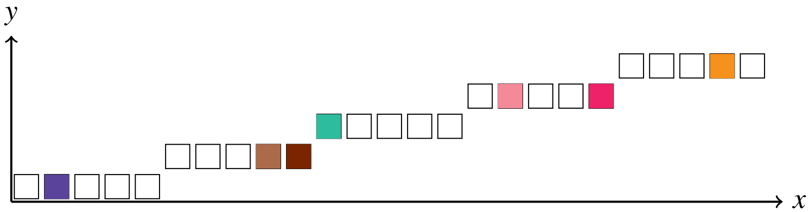
Kronecker Example

Example

$$f(x,y) = \blacksquare x + \blacksquare x^3 y + \blacksquare x^4 y + \blacksquare y^2 + \blacksquare x y^3 + \blacksquare x^4 y^3 + \blacksquare x^3 y^4$$

(colored boxes ■ represent coefficients in R)

Representation of $f(x, x^D y)$**:**



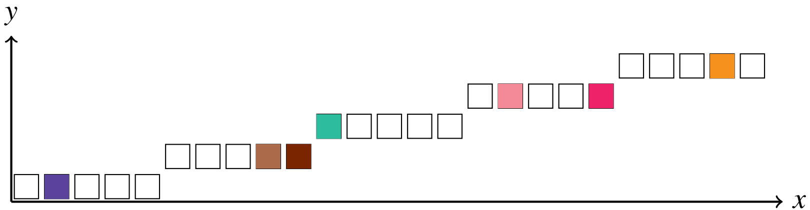
Kronecker Example

Example

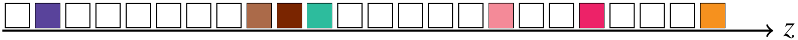
$$f(x,y) = \blacksquare x + \blacksquare x^3 y + \blacksquare x^4 y + \blacksquare y^2 + \blacksquare xy^3 + \blacksquare x^4 y^3 + \blacksquare x^3 y^4$$

(colored boxes ■ represent coefficients in R)

Representation of $f(x, x^D y)$**:**



Kronecker substitution: $f(z, z^D)$, degree 23



Applications of Kronecker

1. Multiplication

The Kronecker substitution is often used to multiply polynomials.

- Reducing $\mathbb{Z}[x]$ to $\mathbb{Z}$ (Schönhage '82, Harvey '09)
- Exponent packing for multivariate sparse polynomials (Monagan & Pearce '07)
- Reducing multivariate dense to bivariate multiplilcation (Moreno Maza & Xie '11)

Applications of Kronecker

2. Factorization

Kronecker substitutions can be used to discover the factorization of multivariate polynomials.

- Kronecker's original motivation! (1882)
- Reducing multivariate to bivariate factorization (Kaltofen 1982)
- Computing perfect roots of sparse polynomials (Giesbrecht & R. '11)

Randomized Kronecker substitution

Let $f \in R[x, y]$ with $\deg_x(f) = d_x$, $\deg_y(f) = d_y$ and $d_x, d_y < D$.

The Idea

Instead of a usual Kronecker substitution:

$$f(x, y) \mapsto f(z, z^D)$$

we choose random integers p, q and the homomorphism:

$$f(x, y) \mapsto f(z^p, z^q)$$

(Note: similar trick to Klivans & Spielman '01)

Challenge: How to choose p, q
so that f can be recovered from $f(z^p, z^q)$?

Randomized Kronecker substitution

Let $f \in \mathrm{R}[x, y]$ with $\deg_x(f) = d_x$, $\deg_y(f) = d_y$ and $d_x, d_y < D$.

The Idea

Instead of a usual Kronecker substitution:

$$f(x, y) \mapsto f(z, z^D) \qquad \longrightarrow \text{degree } d_x + Dd_y \approx D^2$$

we choose random integers $p, q \ll D$ and the homomorphism:

$$f(x, y) \mapsto f(z^p, z^q) \qquad \longrightarrow \text{degree } d_x p + d_y q \ll D^2$$

(Note: similar trick to Klivans & Spielman '01)

Challenge: How to choose p, q as small as possible
so that f can be recovered from $f(z^p, z^q)$?

Randomized Kronecker Example

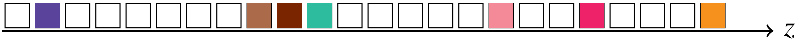
Example

$$f(x,y) = \blacksquare x + \blacksquare x^3y + \blacksquare x^4y + \blacksquare y^2 + \blacksquare xy^3 + \blacksquare x^4y^3 + \blacksquare x^3y^4$$

(colored boxes ■ represent coefficients in R)

Representation of $f(x,y)$:

Kronecker substitution: $f(z, z^D)$, degree 23



Randomized Kronecker Example

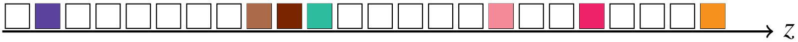
Example

$$f(x,y) = \blacksquare x + \blacksquare x^3y + \blacksquare x^4y + \blacksquare y^2 + \blacksquare xy^3 + \blacksquare x^4y^3 + \blacksquare x^3y^4$$

(colored boxes ■ represent coefficients in R)

Representation of $f(x^2, y)$**:**

Kronecker substitution: $f(z, z^D)$, degree 23



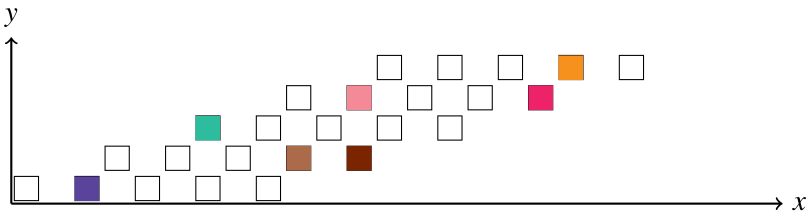
Randomized Kronecker Example

Example

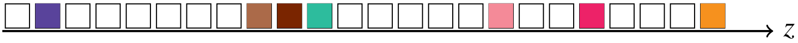
$$f(x,y) = \blacksquare x + \blacksquare x^3y + \blacksquare x^4y + \blacksquare y^2 + \blacksquare xy^3 + \blacksquare x^4y^3 + \blacksquare x^3y^4$$

(colored boxes ■ represent coefficients in R)

Representation of $f(x^2, x^3y)$**:**



Kronecker substitution: $f(z, z^D)$, degree 23



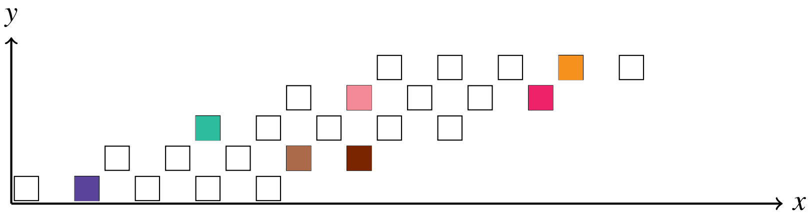
Randomized Kronecker Example

Example

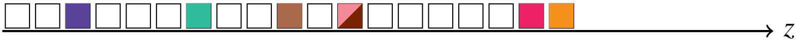
$$f(x,y) = \blacksquare x + \blacksquare x^3y + \blacksquare x^4y + \blacksquare y^2 + \blacksquare xy^3 + \blacksquare x^4y^3 + \blacksquare x^3y^4$$

(colored boxes ■ represent coefficients in R)

Representation of $f(x^2, x^3y)$:



Randomized Kronecker substitution: $f(z^2, z^3)$, degree 18



Less trivial example

Example

$$f = (x^{50} - x^{35} + x^{23} - 1) \circ (x^{127}y^2 + xy^{127} + x^3y^{102} + x^7y^{77} + x^{45}y^{27} + x^{17}y^{52})$$

This polynomial has $\deg_x = \deg_y = 6350$ and $\#f = 161\,778$ nonzero terms over $\mathbb{F}_{13}[x, y]$.

The usual Kronecker substitution $f(z, z^{6351})$ has degree $40\,328\,900$.

■=161 778 nonzero coeffs, □=40 167 122 zero coeffs

The substitution $f(z^{101}, z^{103})$ has degree $659\,100$ (61x smaller):

■=148 558 nonzero coeffs, ■=**6610 collisions**, □=503 932 zero coeffs

Probabilistic analysis, bivariate case

- We choose exponents p, q to be primes in this case, and evaluate the map $f(x,y) \mapsto f(z^p, z^q)$
- How large should p, q be to minimize collisions?

Theorem

Suppose $f \in \mathsf{R}[x,y]$ has degree $< D$ and at most T nonzero terms. If p, q are randomly chosen primes of size $O(\sqrt{T}\log D)$, then w.h.p. there will be fewer than $T/2$ collisions.

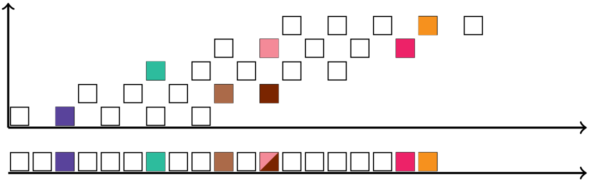
Proof trick:

If $z^{a_i p} z^{b_i q} = z^{a_j p} z^{b_j q}$, then
$(a_i - a_j)p = (b_j - b_i)q$, so
$p | (b_i - b_j)$ and $q | (a_i - a_j)$.

The two independent divisibility conditions give the $\sqrt{T}$ term in the size of the primes.

Challenges of randomized Kronecker

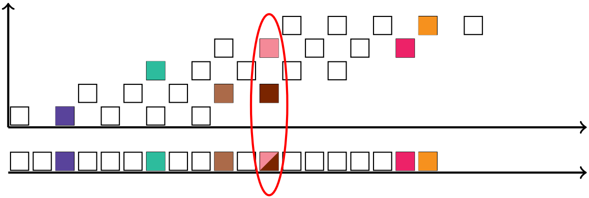
With the benefit of a smaller degree, comes two challenges:



Challenges of randomized Kronecker

With the benefit of a smaller degree, comes two challenges:

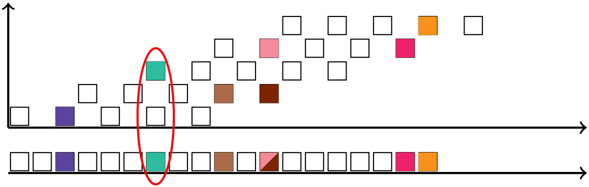
- There will be some collisions of terms



Challenges of randomized Kronecker

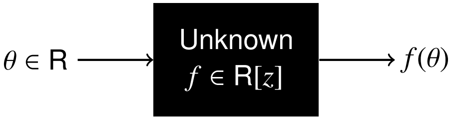
With the benefit of a smaller degree, comes two challenges:

- There will be some collisions of terms
- The map is no longer invertible



The way around these will depend on the application.

Background: Univariate Interpolation



Problem: determine the coefficients and exponents of f

Two flavors of univariate interpolation

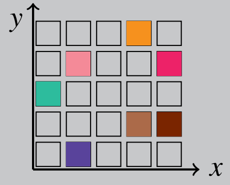
Say $\deg f < D$ and $\#f < T$.

- **Dense**: Requires D probes and $O(D \log D)$ computation. (Newton, Waring, Lagrange, FFT)
- **Supersparse**: Requires $O(T)$ probes and $O(T \log^2 D)$ computation. (Prony, Ben-Or & Tiwari '89, Garg & Schost '09)

More background: Zippel Interpolation

(Zippel '79, Kaltofen/Lee/Lobo '00)

Idea: Do a random projection to univariate, then interpolate up from each nonzero coefficient.

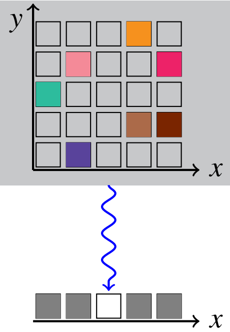


Total cost:

More background: Zippel Interpolation

(Zippel '79, Kaltofen/Lee/Lobo '00)

Idea: Do a random projection to univariate, then interpolate up from each nonzero coefficient.

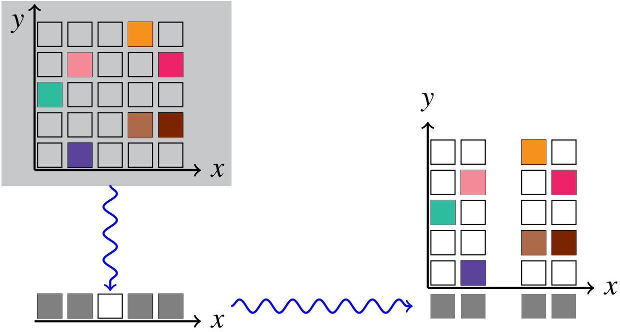


Total cost: 1 univariate interpolation, degree D

More background: Zippel Interpolation

(Zippel '79, Kaltofen/Lee/Lobo '00)

Idea: Do a random projection to univariate, then interpolate up from each nonzero coefficient.

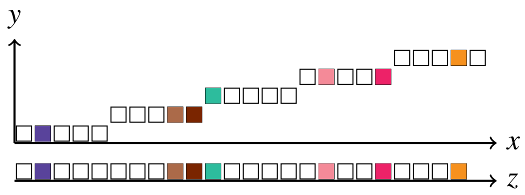


Total cost: At most $t + 1$ univariate interpolations, each degree D

Applications of Kronecker

3. Interpolation

Kronecker can also reduce multivariate to univariate interpolation.



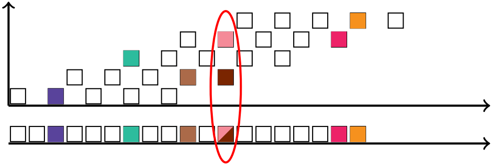
1. Evaluate $f(\theta, \theta^D)$ for many univariate evaluation points θ
2. Use univariate interpolation to discover $f(z, z^D)$
3. Invert the map to discover $f \in R[x, y]$

(Kaltofen, Lakshman, Wiley '90; Kaltofen & Lee '03; Javadi & Monagan '10; van der Hoeven & Lecerf '13)

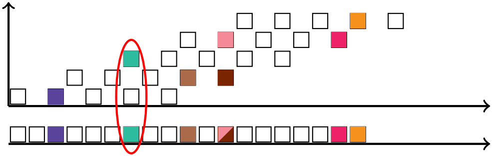
Our method for interpolation

We use the same idea, but must address the two challenges:

- There will be some collisions of terms



- The map is no longer invertible



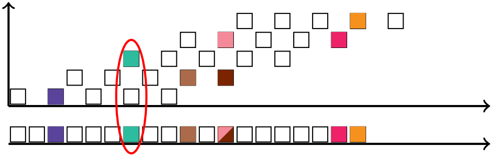
Our method for interpolation

We use the same idea, but must address the two challenges:

- There will be some collisions of terms

Our theorem guarantees *most* terms do not collide.
Use the technique from (A., Giesbrecht, R. '13) and
iterate $O(\log T)$ times

- The map is no longer invertible



Our method for interpolation

We use the same idea, but must address the two challenges:

- There will be some collisions of terms

Our theorem guarantees *most* terms do not collide.
Use the technique from (A., Giesbrecht, R. '13) and
iterate $O(\log T)$ times

- The map is no longer invertible

Get every term in at least two reductions, then solve:

$$\begin{bmatrix} p_1 & q_1 \\ p_2 & q_2 \end{bmatrix} \begin{bmatrix} e_x \\ e_y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix},$$

where u, v are the exponents in the two univariate images.

Multi- to Uni-variate methods comparison

n=# of variables, D=degree bound, T=sparsity bound

	# of reductions	degree of each
Kronecker '82	1	D^n
Zippel '88	nT	D
Klivans & Spielman '01	n	$O(n^2T^2D)$
Ours (bivariate)	$O(\log T)$	$O(\sqrt{T} \log D)$
Ours (≥ 3 variate)	$O(n + \log T)$	$O(TD)$

Multivariate interpolation complexity

n=# of variables, D=degree bound, T=sparsity bound

Using **dense** univariate interpolation

	# of probes *and* computation cost
Kronecker	D^n
Zippel	nTD
Ours (bivariate)	$\sqrt{T}D$
Ours (≥ 3 variate)	nTD

(All costs are soft-oh, ignoring logarithmic factors.)

Multivariate interpolation complexity

n=# of variables, D=degree bound, T=sparsity bound

Using **supersparse** univariate interpolation

	# of probes	computation cost
Kronecker	T	$n^2 T \log^2 D$
Zippel	nT^2	$nT^2 \log^2 D$
Ours (bivariate)	T	$T \log^2 D$
Ours (≥ 3 variate)	nT	$nT \log^2 D$

(All costs are soft-oh, ignoring logarithmic factors.)

Did I mention multivariate?

The trick with primes does not work when $n \geq 3$.

In this case we choose random integer exponents, but have a somewhat weaker result:

Theorem

Suppose $f \in \mathsf{R}[x_1, x_2, \ldots, x_n]$ *has degree* $< D$ *and at most* T *nonzero terms.*
If $s_1, s_2, \ldots, s_n$ *are random integers of size* $O(T)$*, then w.h.p. there will be fewer than* $T/2$ *collisions in the substitution*

$$f(z^{s_1}, z^{s_2}, \ldots, z^{s_n}).$$

Proof idea: Any vector $(s_1, \ldots, s_n)$ that makes two terms collide must lie in some $(n-1)$-dimensional null space.

Future work

- Strengthen probabilistic analysis, especially in the multivariate case
- Work on implementation
- Apply theoretical results to more problems
- Can we do better when we know (some of) the structure?

Thanks!

Back to example
Back to results