The Art of Hybrid Computation

Erich L. Kaltofen
`google,bing->kaltofe`

Phillip Colella's 7 Dwarfs, Berkeley 13 Dwarfs

"A dwarf is an **algorithmic method** that captures **a pattern** of computation and communication" ["Killer-kernels"]

1. Structured Grids
2. Unstructured Grids
3. Fast Fourier Transform
4. Dense Linear Algebra
5. Sparse Linear Algebra
6. Particles
7. Monte Carlo

Phillip Colella's 7 Dwarfs, Berkeley 13 Dwarfs

"A dwarf is an **algorithmic method** that captures **a pattern** of computation and communication" ["Killer-kernels"]

1. Structured Grids
2. Unstructured Grids
3. Fast Fourier Transform
4. Dense Linear Algebra
5. Sparse Linear Algebra
6. Particles
7. Monte Carlo

http://view.eecs.berkeley.edu/wiki/Dwarf_Mine

1. Dense Linear Algebra
2. Sparse Linear Algebra
3. Spectral Methods
4. N-Body Methods
5. Structured Grids
6. Unstructured Grids
7. MapReduce
8. Combinational Logic
9. Graph Traversal
10. Dynamic Programming
11. Backtrack and Branch-and-Bound
12. Graphical Models
13. Finite State Machines

How about Logic Programming, Symbolic Computation?

My 7 Dwarfs of Symbolic Computation [SNSC 2008]

1. Exact linear algebra including algorithms for integer lattices
2. Exact polynomial and differential algebra, including polynomial arithmetic and computation of canonical forms such as Gröbner bases
3. Inverse symbolic problems such as sparse interpolation and curve and surface parameterization
4. Hybrid symbolic-numeric computation
5. Tarski's algebraic theory of real geometry
6. Computation of closed form solutions to, e.g., sums, integrals, differential equations
7. Rewrite rule systems (simplification and theorem proving) and computational group theory

Deep are the roots

First approximate GCD paper:
Donna K. Dunaway, "Calculation of Zeros of a Real Polynomial Through Factorization Using Euclid's Algorithm,"
SIAM J. Numer. Anal. vol. 11 (1974)

Deep are the roots

First approximate GCD paper:
Donna K. Dunaway, "Calculation of Zeros of a Real Polynomial Through Factorization Using Euclid's Algorithm,"
SIAM J. Numer. Anal. vol. 11 (1974)

Recommendations in Boyle/Caviness Report 1988:
Stimulate developments at the interface of symbolic and numeric computation by:

- *Funding research in defining the interface and on algorithms that employ both symbolic and numeric methods*
- *Funding course development that incorporates symbolic and numeric computing*
- *Funding workshops to attack a particular problem using symbolic and numeric methods*

What’s in a Name?

- Integrated Symbolic-Numeric Computing [ISSAC 1992]
- Symbolic-Numeric Algebra for Polynomials [SNAP’96, JSC special issue]
- Symbolic and Numerical Scientific Computation [SNSC’99]
- Hybrid Symbolic-Numeric Computation [Computer Algebra Handbook 2002]
- Symbolic-Numeric Computation [SNC 2005]
- Approximate Algebraic Computation [AAC@ACA’05]
- Approximate Commutative Algebra [ApCoA’06]

Famous Hybrids

- Sphinx: human + lion

Famous Hybrids

- Sphinx: human + lion

- Toyota Prius: electro + gasoline engine

Famous Hybrids

- Sphinx: human + lion

- Toyota Prius: electro + gasoline engine
- Marquis ("Manitoba gold")—Canada's most famous
  Charles Saunders's 1904 hybrid wheat: cross of
  early-ripening *Hard Red Calcutta* and Ontario farmer
  David Fife's *Galician Halychanka* ("*Red Fife*")
  Ripens 3–4 days earlier, short straw that does not flatten
  Doubled Canada's Red Fife wheat fields
  By 1918 constitutes 80% of North America's wheat crop

Approximate GCD: How to define?

Corless,Gianni,Trager,Watt'95 / Karmarkar,Lakshman'96
Nearest approximate GCD in the Euclidean norm

Let $f,g \in \mathbb{C}[z]$, *both monic,* $\deg(f) = m$ *and* $\deg(g) = n$.
Assuming that $\mathrm{GCD}(f,g) = 1$, *find* $\tilde{f}, \tilde{g} \in \mathbb{C}[z]$, *s.t.*
$\mathrm{GCD}(\tilde{f}, \tilde{g})$ *is non-trivial,* $\deg(\tilde{f}) \leq n$, $\deg(\tilde{g}) \leq m$, *and*
$\mathscr{N} = \|f - \tilde{f}\|^2 + \|g - \tilde{g}\|^2$ *is minimized.*

$\|f\|$ denotes a norm of the coefficient vector of f

Approximate GCD: How to define?

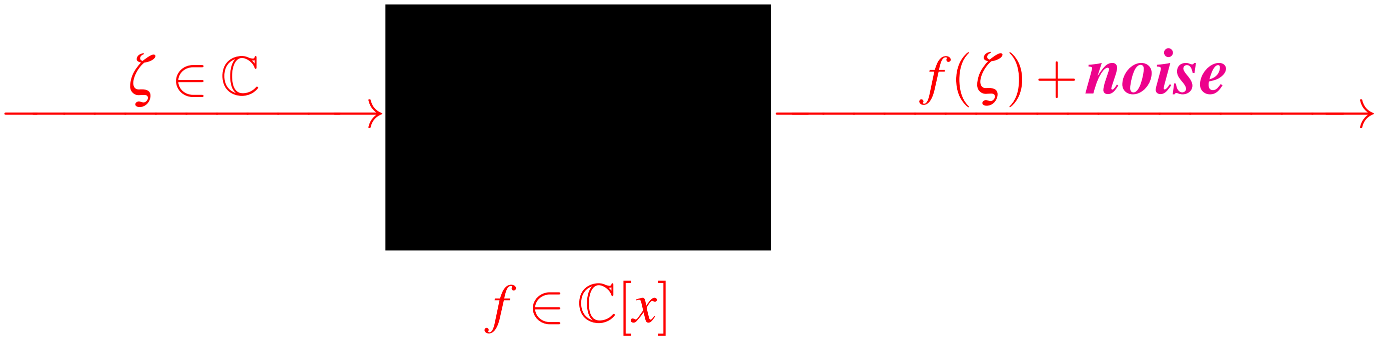
Corless,Gianni,Trager,Watt'95 / Karmarkar,Lakshman'96
Nearest approximate GCD in the Euclidean norm

Let $f, g \in \mathbb{C}[z]$, *both monic,* $\deg(f) = m$ *and* $\deg(g) = n$.
Assuming that $\mathrm{GCD}(f, g) = 1$, *find* $\tilde{f}, \tilde{g} \in \mathbb{C}[z]$, *s.t.*
$\mathrm{GCD}(\tilde{f}, \tilde{g})$ *is non-trivial,* $\deg(\tilde{f}) \leq n$, $\deg(\tilde{g}) \leq m$, *and*
$\mathscr{N} = \|f - \tilde{f}\|^2 + \|g - \tilde{g}\|^2$ *is minimized.*

$\|f\|$ denotes a norm of the coefficient vector of f

Kaltofen, Yang, Zhi '06 [unpublished]:
Minimum can be unattainable $\longrightarrow$ cf. Greuet,Safey El Din'11

Approx. Sparse Interpolation: How to define?

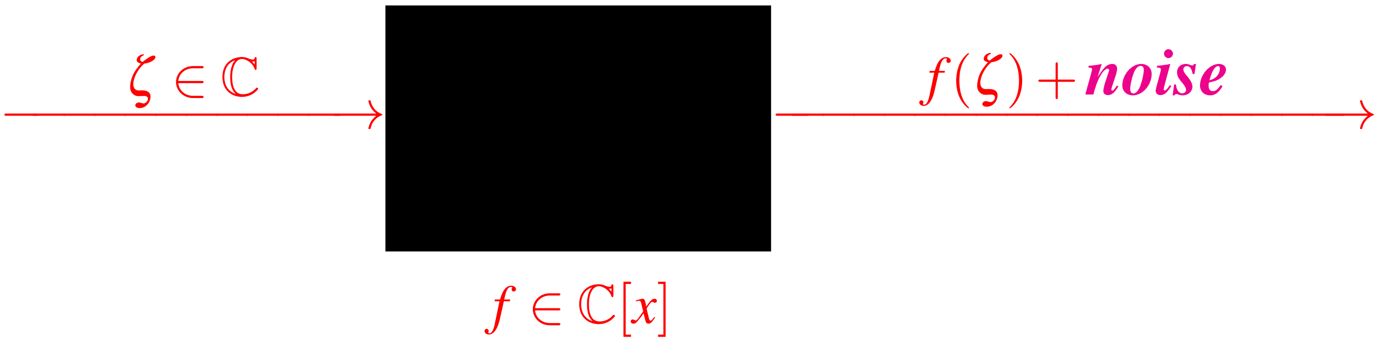


By sampling black box, compute t-sparse representation

$$f(x) = \sum_{j=1}^{t} c_j x^{d_j}, \quad 0 \neq c_j \in \mathbb{C}, d_j \in \mathbb{Z}_{\geq 0}$$

Note: t, d_j are not known (otherwise, a least squares problem)
Number of sample points $O(t)$, not $O(\deg(f))$

Approx. Sparse Interpolation: How to define?



By sampling black box, compute t-sparse representation

$$f(x) = \sum_{j=1}^{t} c_j x^{d_j}, \quad 0 \neq c_j \in \mathbb{C}, d_j \in \mathbb{Z}_{\geq 0}$$

Remark: Output is a trade-off between sparsity and backward error
By oversampling, can get sparse $\tilde{f}$ that is better fit than f

Show Maple Worksheet

Exact Algorithm: Early Termination [Kaltofen & Lee '03] in 1988 Ben-Or/Tiwari Sparse Interpolation

- Pick a **random** element $\omega \in S$
  Evaluate $f(x)$ at ω^k: $h_0 = f(\omega), \ldots, h_{k-1} = f(\omega^k), \ldots$
- Consider the $k \times k$ Hankel matrices:

$$H^{[k]} = \begin{bmatrix} h_0 & h_1 & h_2 & h_3 & \ldots & h_{k-1} \\ h_1 & h_2 & h_3 & h_4 & \iddots & h_k \\ h_2 & h_3 & h_4 & h_5 & \iddots & h_{k+1} \\ h_3 & h_4 & h_5 & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & \iddots & \iddots & \\ h_{k-1} & h_k & h_{k+1} & \ldots & & h_{2k-2} \end{bmatrix}$$

- **Theorem:** $\text{Prob}(\forall 1 \le k \le t:\ \det(H^{[k]}) \neq 0) \le 1 - \dfrac{O(t^3 \deg(f))}{|S|}$

Note: $H^{[k]}$ is singular for $k > t$

Numeric Zippel/Schwartz Lemma [Kaltofen,Yang,Zhi'07]

Let

$$0 \neq \Delta(z_1, \ldots, z_s) \in \mathbb{Z}[\boldsymbol{i}][z_1, \ldots, z_s], \quad \boldsymbol{i} = \sqrt{-1},$$

$\zeta_j = \exp(\frac{2\pi \boldsymbol{i}}{p_j}) \in \mathbb{C}$, $p_j \in \mathbb{Z}_{\geq 3}$ *distinct prime numbers* $\forall 1 \leq j \leq s$
[cf. Giesbrecht, Labahn, Lee 2006]

Suppose $\Delta(\zeta_1, \ldots, \zeta_s) \neq 0$ *(use algebraic lemma to enforce)*

Then for random integers r_j *with* $1 \leq r_j < p_j$

$$\textit{Expected value}\{ \quad \left|\Delta(\zeta_1^{r_1}, \ldots, \zeta_s^{r_s})\right| \quad \} \quad \geq \quad 1.$$

Numeric Zippel/Schwartz Lemma [Kaltofen,Yang,Zhi'07]

Let

$$0 \neq \Delta(z_1, \ldots, z_s) \in \mathbb{Z}[\boldsymbol{i}][z_1, \ldots, z_s], \quad \boldsymbol{i} = \sqrt{-1},$$

$\zeta_j = \exp(\frac{2\pi \boldsymbol{i}}{p_j}) \in \mathbb{C}$, $p_j \in \mathbb{Z}_{\geq 3}$ *distinct prime numbers* $\forall 1 \leq j \leq s$
[cf. Giesbrecht, Labahn, Lee 2006]

Suppose $\Delta(\zeta_1, \ldots, \zeta_s) \neq 0$ *(use algebraic lemma to enforce)*

Then for random integers r_j *with* $1 \leq r_j < p_j$

$$\textit{Expected value}\{ \quad \left|\Delta(\zeta_1^{r_1}, \ldots, \zeta_s^{r_s})\right| \quad \} \quad \geq \quad 1.$$

Can justify identification of those Δ with $\Delta \neq 0$

Problem with Numeric Zippel Approach: Identifying 0

$H^{[t+1]}$ is singular + noise: ill-conditioned

Rump 2003: distance to nearest singular Hankel matrix

$$= \|(H^{[t+1]})^{-1}\|_{\mathbf{2}}^{-1}$$

Main Question: how input-sensitive is $\det(H^{[t+1]})$?

2nd Question: Numeric Zippel Lemma with noisy ζ_j?

Problem with Numeric Zippel Approach: Identifying 0

$H^{[t+1]}$ is singular + noise: ill-conditioned
Rump 2003: distance to nearest singular Hankel matrix

$$= \|(H^{[t+1]})^{-1}\|_{\mathbf{2}}^{-1}$$

Main Question: how input-sensitive is $\det(H^{[t+1]})$?

2nd Question: Numeric Zippel Lemma with noisy ζ_j?

Note: $\kappa_{\det}(A) = \|\text{adjoint}(A)\|$

The zero matrix is well-conditioned for det (w.r.t. absolute error, but don't compute it unstably by elimination; use our division-free algorithm instead)

$\text{diag}(B, \ldots, B, 0)$ is not: $\det(\text{diag}(B, \ldots, B, \varepsilon)) = \varepsilon B^{n-1}$

Problem with Numeric Zippel Approach: Identifying 0

$H^{[t+1]}$ is singular + noise: ill-conditioned
Rump 2003: distance to nearest singular Hankel matrix

$$= \|(H^{[t+1]})^{-1}\|_{\mathbf{2}}^{-1}$$

Main Question: how input-sensitive is $\det(H^{[t+1]})$?

2nd Question: Numeric Zippel Lemma with noisy ζ_j?

Kaltofen, Lee, Yang SNC'11:

We use estimates for $\kappa_1(H^{[k]}) = \|H^{[k]}\|_{\mathbf{1}} \cdot \|(H^{[k]})^{-1}\|_{\mathbf{1}}$
$\longrightarrow$ give $O(t^2)$ algorithm for all estimates

(accounts for input sensitivity/noise)

Explicitly analyze expected condition numbers for $H^{[k]}$, $k \leq t$

(accounts for randomization)

Problem with Numeric Zippel Approach: Identifying 0

$H^{[t+1]}$ is singular + noise: ill-conditioned
Rump 2003: distance to nearest singular Hankel matrix

$$= \|(H^{[t+1]})^{-1}\|_{\mathbf{2}}^{-1}$$

Main Question: how input-sensitive is $\det(H^{[t+1]})$?

2nd Question: Numeric Zippel Lemma with noisy ζ_j?

Afterthought

Identify ill-conditioned submatrices by running a slightly perturbed problem in parallel and measure forward error ("Stochastic senstivity analysis")

Observations

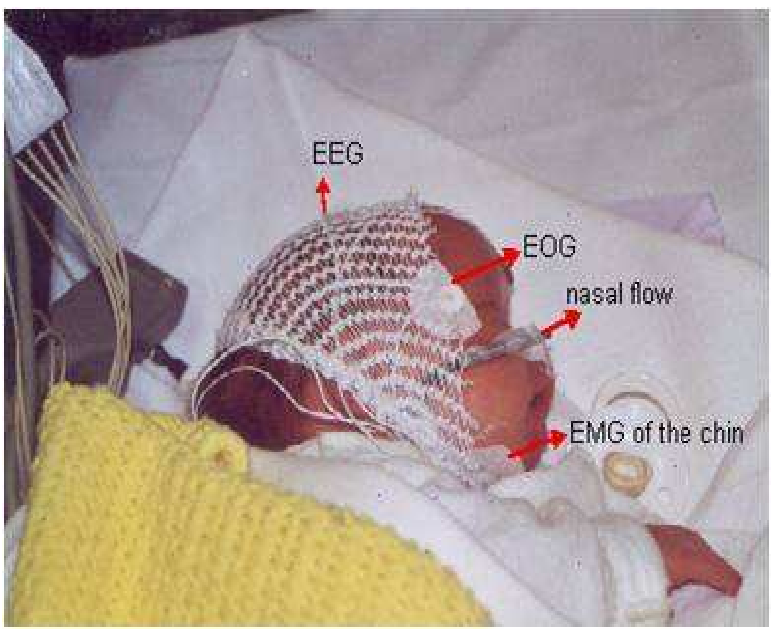
- Noise does not cause explosion of terms, as it would in exact arithmetic

Observations

- Noise does not cause explosion of terms, as it would in exact arithmetic
- Can also tolerate some outliers: interpolation with errors [Comer, Kaltofen, Pernet 2012]

Observations

- Noise does not cause explosion of terms, as it would in exact arithmetic
- Can also tolerate some outliers: interpolation with errors [Comer, Kaltofen, Pernet 2012]
- Very sparse signals occur: medical signal processing `http://smartcare.be` [Cuyt, Lee, et al. 2011]



brain seizures show up in EEG, but are rare
(photo courtesy Wen-shin Lee)

Sum-Of-Squares **certificates** in global optimization

For a real polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$:

$\boxed{f \succeq 0}$ (f is *positive semidefinite*)

$$\iff \forall \xi_1, \ldots, \xi_n \in \mathbb{R}\colon\ f(\xi_1, \ldots, \xi_i) \geq 0,$$

Note: $\mu = \inf_{\xi \in \mathbb{R}} f(\xi) \Longrightarrow f - \mu \succeq 0$

Sum-Of-Squares **certificates** in global optimization

For a real polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$:

$\boxed{f \succeq 0}$ (f is *positive semidefinite*)

$$\iff \forall \xi_1, \ldots, \xi_n \in \mathbb{R}\colon\ f(\xi_1, \ldots, \xi_i) \geq 0,$$

Note: $\mu = \inf_{\xi \in \mathbb{R}} f(\xi) \Longrightarrow f - \mu \succeq 0$

For a real **symmetric** matrix $W \in \mathbb{R}^{N \times N}$, all of whose eigenvalues are necessarily $\in \mathbb{R}$:

$\boxed{W \succeq 0}$ if W is positive semidefinite, i.e.,

all eigenvalues of W are ≥ 0;

Emil Artin's 1927 Theorem (Hilbert's 17th Problem)

$$f \in \mathbb{Q}[X_1, \ldots, X_n]: \quad f \succeq 0$$

$$\Updownarrow$$

$$\exists u_i, v_j \in \mathbb{Q}[X_1, \ldots, X_n]: f(X_1, \ldots, X_n) = \frac{\sum_{i=1}^{l} u_i^2}{\sum_{j=1}^{l'} v_j^2}$$

$$\Updownarrow$$

$$\exists \text{rational } W^{[1]} \succeq 0, W^{[2]} \succeq 0: f = \frac{m_d^T \, W^{[1]} \, m_d}{m_e^T \, W^{[2]} \, m_e}$$

with $m_d(X_1, \ldots, X_n)$, $m_e(X_1, \ldots, X_n)$ vectors of terms

$W \succeq 0$ (positive semidefinite)

$\Longleftrightarrow W = PL\,D\,L^T P^T$, D diagonal, $D_{i,i} \geq 0$ (Cholesky)

Emil Artin's 1927 Theorem (Hilbert's 17th Problem)

$$f \in \mathbb{Q}[X_1, \ldots, X_n]: \quad f \succeq 0$$

$$\Updownarrow$$

$$\exists u_i, v_j \in \mathbb{Q}[X_1, \ldots, X_n]: f(X_1, \ldots, X_n) = \frac{\sum_{i=1}^{l} u_i^2}{\sum_{j=1}^{l'} v_j^2}$$

$$\Updownarrow$$

$$\exists \text{rational } W^{[1]} \succeq 0, W^{[2]} \succeq 0: f = \frac{m_d^T \, W^{[1]} \, m_d}{m_e^T \, W^{[2]} \, m_e}$$

with $m_d(X_1, \ldots, X_n)$, $m_e(X_1, \ldots, X_n)$ vectors of terms

If $\deg(v_j) \leq e$ then we write $f \in \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2e}$

Theodore Motzkin's 1967 Polynomial

$$(3 \text{ arithm. mean} - 3 \text{ geom. mean})(x^4y^2, x^2y^4, z^6)$$
$$= x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$$

is positive semidefinite (AGM inequality) but $\notin$ SOS $(e = 0)$

However,

$$(x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2)(x^2 + y^2 + z^2) =$$
$$(z^4 - x^2y^2)^2 + 3\left(xyz^2 - \frac{xy^3}{2} - \frac{x^3y}{2}\right)^2 + \left(\frac{xy^3}{2} - \frac{x^3y}{2}\right)^2$$
$$+ (xz^3 - xy^2z)^2 + (yz^3 - x^2yz)^2$$

Theodore Motzkin's 1967 Polynomial

$$\begin{aligned}&(3 \text{ arithm. mean} - 3 \text{ geom. mean})(x^4y^2, x^2y^4, z^6)\\&= x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2\end{aligned}$$

is positive semidefinite (AGM inequality) but $\notin$ SOS $(e = 0)$

However,

$$\begin{aligned}&(x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2)(x^2+z^2) =\\&\quad \left(z^4 - x^2y^2\right)^2 + \left(xyz^2 - x^3y\right)^2 + \left(xz^3 - xy^2z\right)^2\end{aligned}$$

Semidefinite Programming: Block Form

$A^{[i,j]}, C^{[j]}, W^{[j]}$ are real **symmetric** matrices

$$\min_{W^{[1]},\ldots,W^{[k]}} \quad C^{[1]} \bullet W^{[1]} + \cdots + C^{[k]} \bullet W^{[k]} \qquad (\bullet \text{ is vector inner product})$$

$$\text{s. t.} \qquad \begin{bmatrix} A^{[1,1]} \bullet W^{[1]} + \cdots + A^{[1,k]} \bullet W^{[k]} \\ \vdots \\ A^{[m,1]} \bullet W^{[1]} + \cdots + A^{[m,k]} \bullet W^{[k]} \end{bmatrix} = b \in \mathbb{R}^m,$$

$$\boxed{W^{[j]} \succeq 0, W^{[j]} = (W^{[j]})^T, j = 1, \ldots, k}$$

Semidefinite Programming: Block Form

$A^{[i,j]}, C^{[j]}, W^{[j]}$ are real **symmetric** matrices

$$\min_{W^{[1]},\ldots,W^{[k]}} \quad C^{[1]} \bullet W^{[1]} + \cdots + C^{[k]} \bullet W^{[k]} \qquad (\bullet \text{ is vector inner product})$$

$$\text{s. t.} \qquad \begin{bmatrix} A^{[1,1]} \bullet W^{[1]} + \cdots + A^{[1,k]} \bullet W^{[k]} \\ \vdots \\ A^{[m,1]} \bullet W^{[1]} + \cdots + A^{[m,k]} \bullet W^{[k]} \end{bmatrix} = b \in \mathbb{R}^m,$$

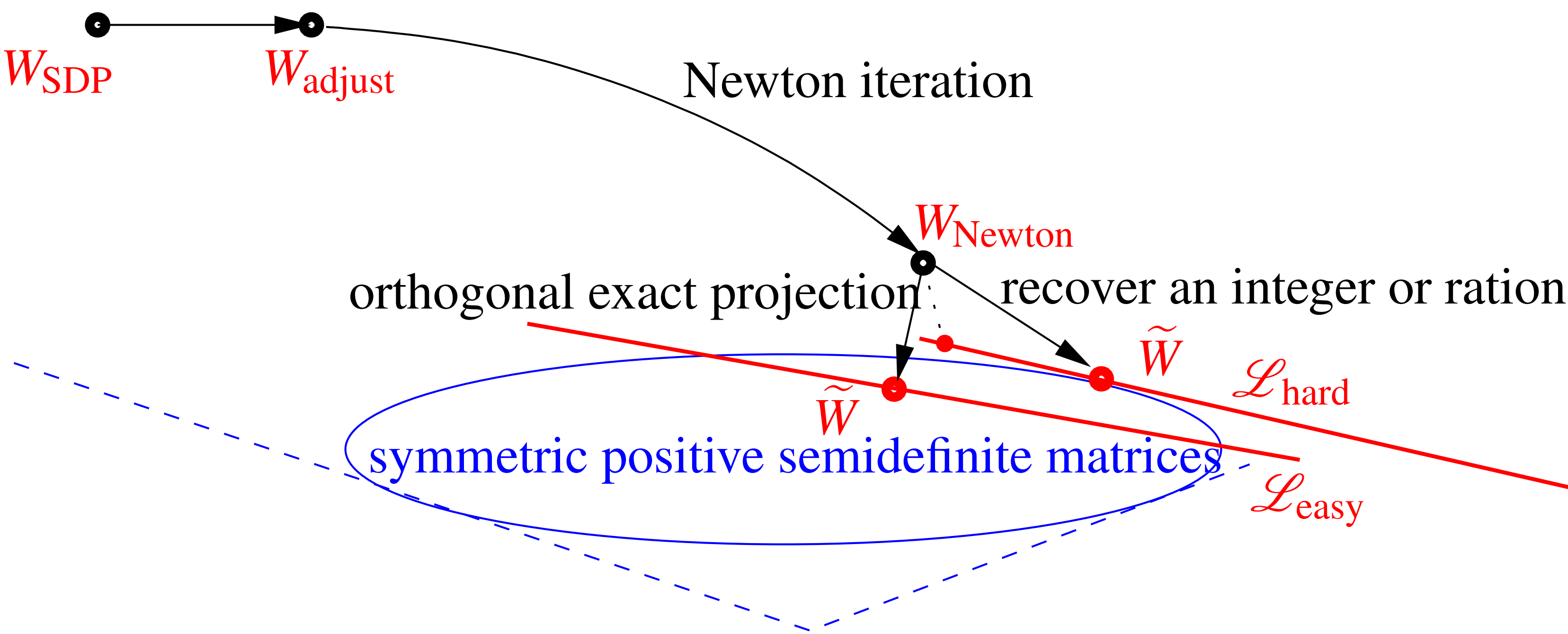
$$\boxed{W^{[j]} \succeq 0, W^{[j]} = (W^{[j]})^T, j = 1, \ldots, k}$$

Note: the Hilbert-Artin form $f \times (m_e^T\, W^{[2]}\, m_e) = m_d^T\, W^{[1]}\, m_d$ is a feasible solution for $k = 2$; (pure) SOS polynomial has $k = 1$

Software: SeDuMi, YALMIP, SOSTOOLS, SparsePOP, SDPT3, VSDP, GloptiPoly, SDPTools; soon to come(?) Maple

Exact Sum-Of-Squares: “Easy Case” Peyrl & Parrilo ’07,’08; “Hard Case” Kaltofen, Li, Yang, Zhi ’08,’09

Method in our *ArtinProver* software



where the affine linear hyperplane is given by

$$\mathscr{L} = \{A \text{ symmetric} \mid f(\mathbf{X}) = m_d(\mathbf{X})^T \cdot A \cdot m_d(\mathbf{X})\}$$

A "Hard Case" Example [Kaltofen, Li, Yang, Zhi'09]

$\mathit{Voronoi2}(a, \alpha, \beta, X, Y)$ [Everett,Lazard,Lazard,Safey El Din'07]
has 253 terms

$$a^{12}\alpha^6 + a^{12}\alpha^4 - 4\,a^{11}\alpha^5 Y + 10\,a^{11}\alpha^4\beta X + \underbrace{\cdots}_{\text{248 terms}} + 20\,a^{10}\alpha^2 X^2$$

A “Hard Case” Example [Kaltofen, Li, Yang, Zhi’09]

$\mathit{Voronoi2}(a,\alpha,\beta,X,Y)$ [Everett,Lazard,Lazard,Safey El Din’07] has 253 terms

$$a^{12}\alpha^6 + a^{12}\alpha^4 - 4a^{11}\alpha^5 Y + 10a^{11}\alpha^4\beta X + \underbrace{\cdots}_{\text{248 terms}} + 20a^{10}\alpha^2 X^2$$

$\mathit{Voronoi2} \succeq 0$ and 0 is attained on two manifolds defined by

$$\{Y + a\alpha, 2a\beta X + 4a^3\beta X + 4a^4\alpha^2 + 4a^4 + 4a^2\alpha^2 + 4a^2 - a^2X^2 - \beta^2\}$$

and

$$\{aX + \beta, -4\beta^2 - 4 - 2a^3\alpha Y - 4a\alpha Y + a^4\alpha^2 + a^2Y^2 - 4a^2\beta^2 - 4a^2\}$$

A “Hard Case” Example [Kaltofen, Li, Yang, Zhi’09]

$Voronoi2(a, \alpha, \beta, X, Y)$ [Everett,Lazard,Lazard,Safey El Din’07]
has 253 terms

$$a^{12}\alpha^6 + a^{12}\alpha^4 - 4a^{11}\alpha^5 Y + 10a^{11}\alpha^4\beta X + \underbrace{\cdots}_{\text{248 terms}} + 20a^{10}\alpha^2 X^2$$

Note: all $f(x) - \mu \succeq 0$ are numerically ill-posed at their optima

$$\mu = \inf_\xi f(\xi): \ f(x) - \mu - \varepsilon \not\succeq 0$$

But it’s worse: $\inf_{\xi,\eta} \quad \xi^2 - 2\xi\eta + \eta^2 = 0$, but

$$\inf_{\xi,\eta} (1-\varepsilon)\xi^2 - 2\xi\eta + \eta^2 = -\infty$$

$\longrightarrow$ Hutton, Kaltofen, Zhi ’10

SOS Certificate *Voronoi2* $\succeq 0$ (“It’s not hard! [Lihong]”)

- The singular values of YALMIPS’s Gram matrix $W_{118\times 118}$

  $196, 152.78, 152.29, 107.36, 68.64, 61.48, \underline{43.05}, 42.58, 25.06, \ldots$

- Compute the truncated Cholesky decomposition of $W \approx L_{\text{adj}} L_{\text{adj}}^T$ that is cut at the singular value 43 and obtain

$$\mathit{Voronoi2} \approx g_1^2 + g_2^2 + \cdots + g_7^2 \qquad (*)$$

- Apply Gauss-Newton iteration to refine $(*)$
  after 30 iterations, we obtain L_{Newton}

- Round $L_{\text{Newton}}\, L_{\text{Newton}}^T$ to an **integer matrix** $\widetilde{W} \succeq 0$ such that

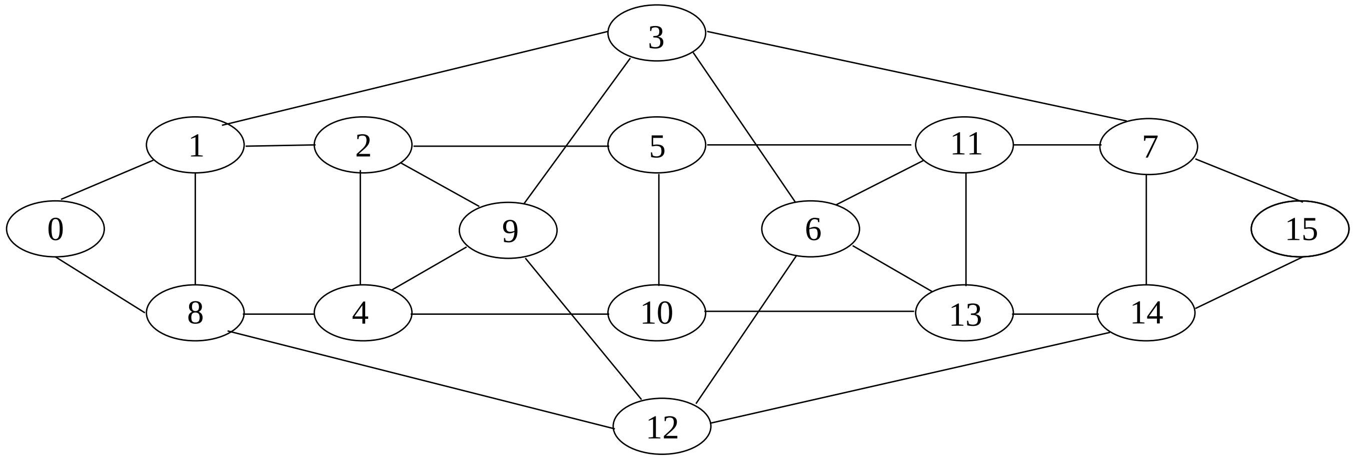
$$\mathit{Voronoi2} = m_d^T \widetilde{W} m_d \; (= f_1^2 + \frac{1}{16} f_2^2 + f_3^2 + \frac{1}{28} f_4^2 + \frac{7}{27} f_5^2,$$

$$\text{where } f_i \in \mathbb{Q}[a, \alpha, \beta, X, Y])$$

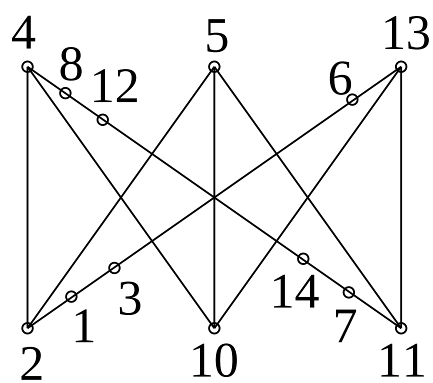
Show email

What actually is a certificate?

4-D De Bruijn graph



Kuratowski's 1930 certificate of non-planarity



Certificate Definition from Kaltofen, Li, Yang, Zhi'09

A *certificate for a problem* that is given by I/O specs is:

an input-dependent data structure and an algorithm that computes from that input and its certificate the specified output, and that has **lower computational complexity than any known algorithm** that does the same when only receiving the input.

Correctness of the data structure is not assumed but validated by the algorithm **(adversary-verifier model)**

WANTED: certificates for $W \succeq 0$ and $f \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 2e}$.

Certificate Definition from Kaltofen, Li, Yang, Zhi'09

A *certificate for a problem* that is given by I/O specs is:

an input-dependent data structure and an algorithm that computes from that input and its certificate the specified output, and that has **lower computational complexity than any known algorithm** that does the same when only receiving the input.

Correctness of the data structure is not assumed but validated by the algorithm **(adversary-verifier model)**

WANTED: certificates for $W \succeq 0$ and $f \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 2e}$.

Note difference to Blum's and Kannan's 1989 *programs that check their work:* programs are rerun, check eliminates bugs

Another classical certificate: The Farkas Lemma

Linear Programming: certificate of infeasibility

$$\forall x \in \mathbb{R}^k: \quad Ax \neq b \quad \Longrightarrow \quad \exists y \in \mathbb{R}^l: y^T A = 0 \text{ and } y^T b \neq 0$$

$$\forall x \in \mathbb{R}^k_{\geq 0}: Ax \neq b \quad \Longrightarrow \quad \exists y \in \mathbb{R}^l: y^T A \geq 0 \text{ and } b^T y < 0$$

Semidefininite Programming

$A^{[i]} \in \mathbb{SR}^{k \times k}$ such that $\exists x \in \mathbb{R}^l: \sum_i x_i A^{[i]} \succeq 0$

$$\forall W \in \mathbb{SR}^{k \times k}, W \succeq 0\ \exists i: A^{[i]} \bullet W \neq b_i$$

$$\Longrightarrow \quad \exists y: \sum_i y_i A^{[i]} \succeq 0 \text{ and } b^T y < 0$$

Can certify infeasibility by solving the dual LP or SDP

Example: Motzkin Polynomial

We prove that the well-known Motzkin polynomial

$$f(X,Y) = X^4Y^2 + X^2Y^4 + 1 - 3X^2Y^2$$

is not SOS. Otherwise, by exploiting sparsity, f can be written as $f(X) = \sum u_i(X,Y)^2$ where $\mathrm{supp}(u_i) \subseteq \{1, XY, X^2Y, XY^2\}$

The certificate is obtained from the dual semidefinite program

$$y = (y_{0,0} = \frac{22011}{55402}, y_{1,1} = 0, y_{2,1} = 0, y_{1,2} = 0, y_{2,2} = \frac{358944}{9403},$$
$$y_{3,2} = 0, y_{2,3} = 0, y_{4,2} = \frac{96310}{4693}, y_{3,3} = 0, y_{2,4} = \frac{96310}{4693})$$

Examples with $e > 1$
[with Feng Guo and Lihong Zhi 2011]

Even symmetric sextics [Choi, Lam, Reznick 1987]

$$M_{n,r}(X) \stackrel{\text{def}}{=} \sum_{i=1}^{n} X_i^r,$$
$$f_{n,0} \stackrel{\text{def}}{=} -nM_{n,6} + (n+1)M_{n,2}M_{n,4} - M_{n,2}^3,$$
$$f_{n,k} \stackrel{\text{def}}{=} (k^2+k)M_{n,6} - (2k+1)M_{n,2}M_{n,4} + M_{n,2}^3,\ 1 \le k \le n-1$$

$$\boxed{\begin{gathered} f_{n,2} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 2}, \quad n = 4,5,6 \\ f_{5,3}, f_{6,3}, f_{6,4} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 4} \\ \frac{f_{n,2}}{M_{n,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 4}, n = 4,5,6, \quad \frac{f_{5,3}}{M_{5,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 6} \end{gathered}}$$

Examples with $e > 1$ [with Feng Guo and Lihong Zhi 2011]

Even symmetric sextics [Choi, Lam, Reznick 1987]

$$M_{n,r}(X) \stackrel{\text{def}}{=} \sum_{i=1}^{n} X_i^r,$$
$$f_{n,0} \stackrel{\text{def}}{=} -nM_{n,6} + (n+1)M_{n,2}M_{n,4} - M_{n,2}^3,$$
$$f_{n,k} \stackrel{\text{def}}{=} (k^2+k)M_{n,6} - (2k+1)M_{n,2}M_{n,4} + M_{n,2}^3,\ 1 \le k \le n-1$$

$$\boxed{\begin{array}{c} f_{n,2} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 2}, \quad n = 4,5,6 \\ f_{5,3}, f_{6,3}, f_{6,4} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 4} \\ \frac{f_{n,2}}{M_{n,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 4}, n = 4,5,6, \quad \frac{f_{5,3}}{M_{5,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \le 6} \end{array}}$$

To our knowledge, they are the **first** polynomials $\succeq 0$ that cannot be written as $\sum_i u_i^2 / \sum_j v_j^2$ with $\deg(v_j) \le 1, 2$

Thank you!