# The Complexity of <br> Accurate Floating Point Computation and Symbolic Computing <br> Or 

# Can we do Numerical Linear Algebra In Polynomial Time? 

James Demmel<br>Mathematics and Computer Science UC Berkeley<br>Joint work with<br>Ben Diament, W. Kahan, Plamen Koev<br>Ming Gu, Stan Eisenstat, Ivan Slapničar, Kresimir Veselić, Zlatko Drmač

Supported by NSF and DOE

## Goals

- Def: Accurate floating point (FP) computation means with guaranteed relative error $<1$
$-10^{-2} \equiv 2$ digits, $10^{-16} \equiv 16$ digits,..
- zero must be exact
- Def: Efficient computation of an expression means in time poly(size of the expression, size of the input)
- Def: CAE means "compute accurately and efficiently"
- Goal: Understand cost of accurate FP computation
- What FP expressions can we CAE?
- Are there FP expressions that we cannot CAE?
- For what structured matrices
(i.e. with FP expressions as entries)
are there matrix computations that we can CAE?
* LU, QR, Inv, Pinv, SVD, Eig, ...


## Structure of Results

- Classes of FP expressions/matrices that we can CAE depends strongly on
- Set of Numbers

1. Positive real numbers
2. Real numbers
3. Complex numbers

- Model of FP Arithmetic

1. Traditional (" $1+\delta$ ") Model:
$f l(a \otimes b)=(a \otimes b)(1+\delta),|\delta|$ tiny
2. Bit model (IEEE) $f \cdot 2^{e}$, with "large exponents":
"natural" model for algorithms, analysis
3. Bit model (IEEE) $f \cdot 2^{e}$, with "small exponents": integers in disguise, well understood
4. Blum/Shub/Smale (BSS) model (not today)

- Classes described by factorizability properties of expressions/minors of matrices
- New algorithms can be exponentially faster than conventional algorithms that just use enough precision
- $\operatorname{Cost}($ CAE in Bit model with large exponents) $\geq$ Cost("symbolic computing")
- There are FP expressions that we cannot CAE

Example: 100 by 100 Hilbert Matrix

$$
H(i, j)=1 /(i+j-1)
$$

- Eigenvalues range from 1 down to $10^{-150}$
- Old algorithm, New Algorithm, both in 16 digits

- $D=\log \left(\lambda_{1} / \lambda_{n}\right)=\log \operatorname{cond}(A)$ (here $D=150$ digits)
- "Cost" of Old algorithm $=O\left(n^{3} D^{2}\right)$
- "Cost" of New algorithm $=O\left(n^{3}\right)$
- New algorithm cost independent of condition number


## Why bother computing tiny eigenvalues accurately?

- Aren't they too ill-conditioned?
- NO - they are determined accurately by the data
- Hilbert: $H(i, j)=1 /(i+j-1)$
- Cauchy: $C(i, j)=1 /\left(x_{i}+y_{j}\right)$
- Data are $x_{i}$ and $y_{j}, \operatorname{not} 1 /\left(x_{i}+y_{j}\right)$
- Changing $x_{i}$ or $y_{j}$ in $d$-th digit changes each eigenvalue in $d$-th digit (for Hilbert, analogous for Cauchy)
- Hilbert matrix is nearly perfectly conditioned!
- Algorithm works for Cauchy matrices
* complex numbers
* $1+\delta$ model
- In some applications, tiny eigenvalues matter most
- Quantum mechanics: want lowest energy levels
- Elasticity: want lowest frequencies of vibration
- Large eigenvalues are artifacts of discretization
- Computational geometry: what is $\operatorname{sign}(\operatorname{det}(A))$ ?
- Good to get accurate results if they cost about as much as inaccurate results


## Central Role of Minors

- Being able to CAE $\operatorname{det}(A)$ is necessary for CAE
- $A=L U$ with pivoting
- $A=Q R$
- Eigenvalues $\lambda_{i}$ of $A$
- Related factorizations ... * Proof: $\operatorname{det}(A)= \pm \Pi_{i} U_{i i}= \pm \Pi_{i} R_{i i}=\Pi_{i} \lambda_{i}=\cdots$
- Being able to CAE all minors of $A$ is sufficient for CAE
$-A^{-1}$
* Proof: Cramer's rule
* Only need $n^{2}+1$ minors
$-A=L U$ or $A=L D U$ with pivoting
* Proof: Each entry of $L, D, U$ a quotient of minors * Only need $O\left(n^{2}\right)$ or $O\left(n^{3}\right)$ minors
- Singular values
* Proof: new SVD algorithm for $A=L D U$ with pivoting
- Similar result for $\mathbf{Q R}$, pseudoinverse via $\left[\begin{array}{cc}I & A \\ A^{T} & 0\end{array}\right]$, etc.
- Examine which expressions (minors) we can CAE


# How do we CAE $A=L \cdot D \cdot U$ for a Hilbert (or Cauchy) Matrix? 

- How can we lose accuracy in computing?
$-1+\delta$ model: $f l(a \otimes b)=(a \otimes b)(1+\delta),|\delta| \leq \epsilon \ll 1$
- OK to multiply, divide, add positive numbers
- OK to subtract exact numbers (initial data)
- Cancellation when subtracting approximate results dangerous:

$$
\begin{array}{r}
.12345 x x x \\
-.12345 y y y \\
\hline .000000 z z z
\end{array}
$$

- Cauchy: $C(i, j)=1 /\left(x_{i}+y_{j}\right)$
- Fact 1: $\operatorname{det}(C)=\Pi_{i<j}\left(x_{j}-x_{i}\right)\left(y_{j}-y_{i}\right) / \Pi_{i, j}\left(x_{i}+y_{j}\right)$
- No bad cancellation $\Rightarrow$ good to most digits
- Fact 2 : Each minor of $C$ also Cauchy
- Fact 3 : Each entry of $L, D, U$ is a (quotient of) minors
- Change inner loop of Gaussian Elimination from

$$
C(i, j):=C(i, j)-C(i, k) * C(k, j)
$$

to

$$
C(i, j):=C(i, j) *\left(x_{i}-x_{k}\right) *\left(y_{j}-y_{k}\right) /\left(x_{k}+y_{j}\right) /\left(x_{i}+y_{k}\right)
$$

- Each entry of $L, D, U$ accurate to most digits!


## SVD Algorithm



- Examples of RRDs:
$-A=U \Sigma V^{T}$, SVD itself
$-A=Q D R$, QR decomposition with pivoting
$-A=L D U$, Gaussian Elimination with "complete" pivoting (GECP)
- Phase 1: GECP via (implicitly) computing accurate minors of $A$
- Depends on structure of $A$ (e.g. Cauchy)
- Phase 2: Works for any RRD in $O\left(n^{3}\right)$
- Independent of structure of $A$


## Accurate SVD of $A=X D Y^{T}$

- SVD is $A=U \Sigma V^{T}$
- Many accurate algorithms, here is simplest:

1. Compute SVD of $D Y^{T}=U_{1} \Sigma_{1} V_{1}^{T}$ using one-sided Jacobi
2. Multipy $W=X U_{1}$
3. Compute SVD of $W \Sigma_{1}=U \Sigma V_{2}^{T}$ using one-sided Jacobi
4. Multiply $V=V_{1} V_{2}$

- To guarantee efficiency, find eigenvalues of

$$
\begin{aligned}
{\left[\begin{array}{cc}
0 & A \\
A^{T} & 0
\end{array}\right] } & =\frac{1}{2^{1 / 2}} \cdot\left[\begin{array}{cc}
L & L \\
U^{T} & -U^{T}
\end{array}\right] \cdot\left[\begin{array}{cc}
D & 0 \\
0 & -D
\end{array}\right] \cdot\left[\begin{array}{cc}
L^{T} & U \\
L^{T} & -U
\end{array}\right] \cdot \frac{1}{2^{1 / 2}} \\
& \equiv Z \cdot \hat{D} \cdot Z^{T}
\end{aligned}
$$

by performing bisection on $\lambda \hat{D}-Z^{-1} Z^{-T}$

## Why roundoff is harmless

- $1+\delta$ model: $f l(a \otimes b)=(a \otimes b)(1+\delta)$
- We want $A=U \Sigma V^{T}$,
$U=\left[u_{1}, \ldots, u_{n}\right], \Sigma=\operatorname{diag}\left(\sigma_{1}, \ldots, \sigma_{n}\right)$
- But we compute $\bar{A}=\bar{U} \bar{\Sigma} \bar{V}^{T}$, $\bar{U}=\left[\bar{u}_{1}, \ldots, \bar{u}_{n}\right], \bar{\Sigma}=\operatorname{diag}\left(\bar{\sigma}_{1}, \ldots, \bar{\sigma}_{n}\right)$


## Absolute (additive) vs. Perturbations

$$
\bar{A}=A+\sigma_{\max } \cdot E \quad \bar{A}=(I+E) A
$$

$\|E\| \ll 1$

$$
\left|\sigma_{i}-\bar{\sigma}_{i}\right| \leq\|E\| \cdot \sigma_{\max }
$$

$$
\left|\sigma_{i}-\bar{\sigma}_{i}\right| \leq\|E\| \cdot \sigma_{i}
$$

Conventional error bound
Our error bound

## Sturm-Liouville Equations

- $-\left(p(x) y^{\prime}\right)^{\prime}+q(x) y=\lambda r(x) y$ on $[\mathbf{0 , 1}], p, q, r>0$
- Discretize: second centered differences on uniform grid
- Get $T x=\lambda D_{r} x$
- $D_{r}=\operatorname{diag}\left(r_{i}\right)$
$-T=\operatorname{tridiag}\left(-p_{i-.5}, \quad p_{i-.5}+p_{i+.5}+h^{2} q_{i}, p_{i+.5}\right)$
- Don't even form $T$ !
- Rewrite $T x=\lambda D_{r} x$ as $G G^{T} y=\lambda y($ SVD of $G)$
- Factor $T=L D_{p} L^{T}+h^{2} D_{q}$ where

$$
D_{p}=\operatorname{diag}\left(p_{1.5}, \ldots, p_{n-.5}\right), D_{q}=\operatorname{diag}\left(q_{1}, \ldots, q_{n}\right)
$$

$$
L=\left[\begin{array}{ccc}
1 & & \\
-1 & \ddots & \\
& \ddots & 1 \\
& & -1
\end{array}\right]
$$

$$
T=U \cdot K^{2} \cdot U^{T} \quad \text { where } U=[L, I] \text { and } K=\operatorname{diag}\left(D_{p}, h^{2} D_{q}\right)
$$

$$
-G=D_{r}^{-1 / 2} U K
$$

- Thm: (Poincaré) $U$ is totally unimodular,
i.e. all minors $\in\{+1,-1,0\}$
- Theorem: High relative accuracy from GE by changing

$$
G(j, k):=G(j, k)-G(j, i) * G(i, k)
$$

to

$$
\begin{aligned}
& \text { if } G(j, k), G(j, i), G(i, k) \text { all } \neq 0 \text { then } G(j, k):=0 \\
& \text { else } G(j, k):=G(j, k)-G(j, i) * G(i, k)
\end{aligned}
$$

## Other examples in $1+\delta$ model

- Sturm-Liouville trick extends to elliptic PDE
- Second centered differences on uniform square meshes
- Irregular boundaries ok
- Still get SVD of
$G=$ diagonal $\cdot$ totally unimodular $\cdot$ diagonal
- Cost $=O\left(n^{3}\right)$
- Sparse matrices with
- particular sparsity patterns, Cost $=O\left(n^{3}\right)$
- particular sparsity and sign patterns, Cost $=O\left(n^{4}\right)$
- Real Vandermonde, other unit displacement rank
- Reduce to Cauchy
$-\mathbf{C o s t}=O\left(n^{3}\right)$
- Totally positive matrices (but cost not always poly)
- More later ...
- What do these matrices have in common?


## $1+\delta$ Model with Complex Numbers What we CAN do

- Def: $1+\delta$ allowable expressions may only
- Multiply and divide
- Add or subtract initial data
- Proof: All $1+\delta$ factors can be factored out
- Def: A family $A_{n}(x)$ of $n$-by- $n$ rational matrices is fully polyfactorable if each minor $r(x)$ is a $1+\delta$ allowable expression of at most poly $(n)$ factors $x_{i}$ and $\left(x_{j} \pm x_{k}\right)$
- Thm: Suppose $A_{n}(x)$ is fully polyfactorable.

Then in the $1+\delta$ model we can CAE $L U$ with pivoting, $A^{-1}$, singular values.

- Enough for all examples so far (Cauchy, real Vandermonde, Sturm-Liouville, ...)
- Common conditioning analysis
- Relative uncertainty $\epsilon$ in input only magnified by computing $x_{i} \pm x_{j}$, yielding $\epsilon\left(\left|x_{i}\right|+\left|x_{j}\right|\right) /\left|x_{i} \pm x_{j}\right|$
- Condition number is largest $\left(\left|x_{i}\right|+\left|x_{j}\right|\right) /\left|x_{i} \pm x_{j}\right|$
- Hilbert matrix very well conditioned


## What we CANNOT $\quad \begin{aligned} & 1+\delta \\ & \text { Model }\end{aligned}$

- Thm: Can't compute $x+y+z$ accurately in $\mathrm{O}(1)$ time
- Assume only $\pm$, deterministic rounding, exact compare, branch
- Without branches, show $s=x+y+z+x \cdot f_{x}+y \cdot f_{y}+z \cdot f_{z}$ where $f_{a}$ a polynomial in rounding errors $\delta_{i} \mathrm{~S}$
- So if $x+y+z=0$, need $0=x \cdot f_{x}+y \cdot f_{y}+z \cdot f_{z}$
- Show ( $x, y, z$ ) cannot be orthogonal to $\left(f_{x}, f_{y}, f_{z}\right)$ for all independent choices of $x, y, z, \delta_{i}$ 's,
- Reduce case with branches to case without
- Will see $x+y+z$ is easy in bit model...


## Adding Sign Restrictions to $1+\delta$ Model

- Consider real numbers with fixed signs
- Fixed signs $\Rightarrow$ can add $x+y+z$ accurately if all positive
- Real $\Rightarrow$ can compute $x^{2}+y^{2}$ accurately
- New classes of matrices
- Total Sign Compound Matrices (Brualdi and Shader)
- each matrix entry $+x_{i j},-x_{i j}$ or 0 (all $x_{i j} \geq 0$ )
- each minor a sum of like-signed terms or zero
- Totally Positive Matrices
- Each minor nonnegative
- Many examples depending rationally on positive parameters (Karlin)
- Structure theorems (Brenti, Aiseen, Schoenberg, Whitney, Erdrei) show that all TP matrices can be built from simpler ones via matmul, inversion, Schur complementation, subsetting
$\Longrightarrow$ Can compute any minor accurately in $1+\delta$ model
- Possibly expensive!
- Concentrate on CAE TP Generalized Vandermonde matrices


## Facts about

TP Generalized Vandermonde Matrices

- TP Vandermonde Matrix:

$$
V=\left[\begin{array}{llll}
1 & x_{1} & \ldots & x_{1}^{n-1} \\
1 & x_{2} & \ldots & x_{2}^{n-1} \\
& & \ddots & \\
1 & x_{n} & \ldots & x_{n}^{n-1}
\end{array}\right]
$$

where $x_{1}>x_{2}>\cdots>x_{n}>0$.

- TP Generalized Vandermonde Matrix:

$$
G_{\lambda}=\left[\begin{array}{llll}
x_{1}^{\lambda_{1}} & x_{1}^{1+\lambda_{2}} & \ldots & x_{1}^{n-1+\lambda_{n}} \\
x_{2}^{\lambda_{1}} & x_{2}^{1+\lambda_{2}} & \ldots & x_{2}^{n-1+\lambda_{n}} \\
& & \ddots & \\
x_{n}^{\lambda_{1}} & x_{n}^{1+\lambda_{2}} & \ldots & x_{n}^{n-1+\lambda_{n}}
\end{array}\right]
$$

where
$-x_{1}>x_{2}>\cdots>x_{n}>0$
$-\lambda_{n} \geq \lambda_{n-1} \geq \cdots \geq \lambda_{0}$

- Def: $\lambda=\left(\lambda_{n}, \lambda_{n-1}, \ldots, \lambda_{0}\right)$ is partition of $|\lambda|=\lambda_{n}+\cdots+\lambda_{0}$
- Def: Young Diagrams $\equiv$ partitions:

$$
\lambda=(4,2,1)=
$$



- Def: Schur Function $s_{\lambda}\left(x_{1}, \ldots, x_{n}\right)=\operatorname{det}\left(G_{\lambda}\right) / \operatorname{det}(V)$.
- Thm: $s_{\lambda}$ is a polynomial with positive integer coefficients depending only on $\lambda$ (MacDonald)


## More facts about TP Generalized Vandermonde Matrices

- Recall: $\operatorname{det}(G)=\operatorname{det}(V) \cdot s_{\lambda}\left(x_{1}, \ldots, x_{n}\right)$
- Example:
$\operatorname{det}\left(\left[\begin{array}{ccc}1 & x_{1}^{2} & x_{1}^{4} \\ 1 & x_{2}^{2} & x_{2}^{4} \\ 1 & x_{3}^{2} & x_{3}^{4}\end{array}\right]\right)=$
$=\operatorname{det}\left(\left[\begin{array}{lll}1 & x_{1} & x_{1}^{2} \\ 1 & x_{2} & x_{2}^{2} \\ 1 & x_{3} & x_{3}^{2}\end{array}\right]\right) \cdot\left(2 x_{1} x_{2} x_{3}+x_{1}^{2} x_{2}+x_{1} x_{2}^{2}+x_{1}^{2} x_{3}+x_{1} x_{3}^{2}+x_{2}^{2} x_{3}+x_{2} x_{3}^{2}\right)$
- $\operatorname{det}(V)=\Pi_{i>j}\left(x_{i}-x_{j}\right)$ is CAE
- $s_{\lambda}$ computable accurately $\left(x_{i}>0\right)$, question is cost.
- Theorem:

$$
s_{\lambda}\left(x_{1}, \ldots, x_{n}, y_{1}, \ldots, y_{m}\right)=\sum_{\mu<\lambda} s_{\mu}\left(x_{1}, \ldots, x_{n}\right) s_{\lambda / \mu}\left(y_{1}, \ldots, y_{m}\right)
$$

Allows recursive computation and Divide-and-Conquer approach.

- Some $s_{\lambda}$ 's are CAE:

and


| Type of Matrix | $\operatorname{det}(A)$ | $A^{-1}$ | Any minor | $\begin{gathered} \hline \text { GEPP / } \\ \text { GENP } \end{gathered}$ | Bidiag <br> Decomp | GECP | SVD |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| Cauchy | $O\left(n^{2}\right)$ | $O\left(n^{2}\right)$ | $O\left(n^{2}\right)$ | $O\left(n^{3}\right)$ | $O\left(n^{2}\right)$ | $O\left(n^{3}\right)$ | $O\left(n^{3}\right)$ |
| Vandermonde | $O\left(n^{2}\right)$ | NONE | NONE | NONE | $O\left(n^{2}\right)$ | NONE | $O\left(n^{3}\right)$ |
| Totally <br> Positive (TP) <br> Vandermonde | $O\left(n^{2}\right)$ | $O\left(n^{3}\right)$ | EXP | $O\left(n^{3}\right)$ | $O\left(n^{2}\right)$ | EXP | $O\left(n^{3}\right)$ |
| TP Generalized Vandermonde, $\|\lambda\|=\lambda_{1}+O(1)$ | $O\left(\lambda_{1} n^{2}\right)$ | $O\left(\lambda_{1} n^{3}\right)$ | EXP | $O\left(\lambda_{1} n^{3}\right)$ | $O\left(\lambda_{1} n^{2}\right)$ | EXP | EXP |
| TP Generalized <br> Vandermonde, any $\lambda$ | $f(n, \lambda)$ | EXP | EXP | EXP | EXP | EXP | EXP |
| $f(n, \lambda)=O\left(n^{1+\log \lambda_{1}+\log \lambda_{2}+\cdots+\log \lambda_{n}}\right) \text { vs. } O\left(n^{\|\lambda\|}\right)=O\left(n^{\lambda_{1}+\lambda_{2}+\cdots+\lambda_{n}}\right)$ <br> (Symmetrica) |  |  |  |  |  |  |  |

## Models of FP Arithmetic

- Traditional $1+\delta$ model
$-f l(a \otimes b)=(a \otimes b)(1+\delta)$
- No over/underflow
$-|\delta| \leq \epsilon<1$, otherwise arbitrary
- Enough for many examples, but limited
- Bit model
- Inputs of form $f \cdot 2^{e}, e$ and $f$ integers
- Can accurately compute arbitrary rational FP expressions
- Question is cost
- BSS model (not today)


## Bit Model

- Inputs of form $f \cdot 2^{e}, e$ and $f$ integers
- $\operatorname{size}(X)=\#$ bits used to represent $X$
- $\operatorname{size}\left(f \cdot 2^{e}\right)=\# \operatorname{bits}(f)+\# \operatorname{bits}(e)$
- Can evaluate any rational expression accurately
- Convert to poly/poly, using high enough precision
- Question is cost
- Cost depends strongly on \# exponent bits
- Small Exponents (SE)
* \#bits $(e)=O(\log (\# \operatorname{bits}(f)))$
* Equivalent to integer arithmetic
* Can CAE many problems
- Large Exponents (LE)
* \#bits( $e$ ) and \#bits $(f)$ independent
* "Natural" model for algorithm design
* Algorithms work for any input magnitudes
* Like symbolic algebra, which is much harder


## Differences between SE and LE bit models - 1

- Recall definitions for size of $f \cdot 2^{e}$
- Small Exponents (SE): \#bits $(e)=O(\log (\# \operatorname{bits}(f)))$
- Large Exponents (LE): \#bits(e), \#bits $(f)$ indep.
- SE and "integer arithmetic" equivalent
- Represent $f \cdot 2^{e}$ as integer, not pair $(f, e)$
$-\# \operatorname{bits}\left(f \cdot 2^{e}\right)=\# \operatorname{bits}(f)+e \approx \# \operatorname{bits}(f)+2^{\# \operatorname{bits}(e)}=\operatorname{poly}(\# \operatorname{bits}(f))$
- LE and "integer arithmetic" not equivalent
$-2^{\# b i t s(e)}$ exponentially larger than \#bits(e)
- \# bits in FP expressions much bigger for LE than SE
- SE: $\operatorname{size}(x \cdot y) \leq \operatorname{size}(x)+\operatorname{size}(y)$
- LE: $\operatorname{size}(x \cdot y) \leq \operatorname{size}(x) \cdot \operatorname{size}(y)$

$$
\begin{aligned}
\operatorname{size}(x \cdot y) & =\operatorname{size}\left(\left(2^{x_{1}}+2^{x_{2}}+2^{x_{3}}\right) \cdot\left(2^{y_{1}}+2^{y_{2}}+2^{y_{3}}\right)\right) \\
& =\operatorname{size}\left(\sum_{i, j=1}^{3} 2^{x_{i}+y_{j}}\right) \\
& =\operatorname{size}(x) \cdot \operatorname{size}(y) \\
& =9, \operatorname{not} 6
\end{aligned}
$$

- LE can encode symblic algebra
$-2^{a} \cdot 2^{b}=2^{a+b}$ can "remember" $a$ and $b$
- Some symbolic algebra problems are very hard


## Differences between SE and LE bit models - 2

- Recall definitions for size of $f \cdot 2^{e}$
- Small Exponents (SE): \#bits $(e)=O(\log (\# \operatorname{bits}(f)))$
- Large Exponents (LE): \#bits $(e)$, \#bits $(f)$ indep.
- Cond $(A)$ in LE can be exponentially larger than in SE
- SE: $\log \operatorname{cond}(A)$ is $\operatorname{poly}(\operatorname{size}(A))$
* Conventional algorithms using $\log \operatorname{cond}(A)$ bits are polynomial
* Proof on next slide
- LE: $\log \operatorname{cond}(A)$ can be exponential in $\operatorname{size}(A)$
* $\operatorname{cond}\left(\operatorname{diag}\left(2^{e}, 1\right)\right)=2^{e} \approx 2^{2^{\# b i t s(e)}}$
* Conventional algorithms using $\log \operatorname{cond}(A)$ bits are not polynomial
- $\log \log \operatorname{cond}(A)$ is lower bound on complexity of any FP algorithm
- \# bits needed to print out exponent of answer


## Small Exponent (SE) Bit Model

- Consider set of FP expressions of form $P / Q, P$ and $Q$ polynomials
$-P$ or $Q=\Sigma_{i} \alpha_{i} \cdot x_{1}^{e_{i 1}} \cdots x_{k}^{e_{i k}}$
- Let $N$ bound sizes of $P$ and $Q$ * $N \geq \# x_{i}$, \# nonzero $\alpha_{i}$, \#bits $\left(\alpha_{i}\right), e_{i j}$
$-F \geq \#$ bits in each $x_{j}$
- Fact: \# bits $(P)=\operatorname{poly}(N, F)$, same for \# bits $(Q)$
- Computing $P$ and $Q$ costs poly $(N, F)$
- Consider $n$-by- $n$ matrix $A\left(x_{1}, \ldots, x_{k}\right)$ with entries $P_{i j} / Q_{i j}$
- Suppose $N=\operatorname{poly}(n)$
- Can compute each $P_{i j}, Q_{i j}$ in time poly $(n, F)$
- Can put over common denominator in time poly ( $n, F$ )
- Conclusion: $\log \operatorname{cond}(A)=\operatorname{poly}(n, F)$
- Conventional algorithms with $\log \operatorname{cond}(A)$ bits are ok
- Thm (Clarkson, 1992) Can CAE any minor in time $O(\operatorname{poly}(n, F))$
- Can CAE $A=L U$ with pivoting, $A^{-1}, A^{+}$, singular values of such matrices via minors


## Large Exponent (LE) Bit Model

- Several obstacles to CAE
- Clarkson's Thm does not work
$-N \geq$ size of polynomial $P$
$-F \geq$ \# fraction bits in any value
$-E \geq \#$ exponent bits in any value
- \# bits (P) not poly ( $N, F, E$ )
- Example: \#bits $\left(\Pi_{i=1}^{N}\left(1+x_{i}\right)\right)$ can grow like $2^{N}$
- Thm: It is PP-Hard to compute an arbitrary bit of $\Pi_{i=1}^{N}\left(1+x_{i}\right)$
- Reduce permanent to finding coeff $C$ of $\Pi_{i=1}^{n} u_{i} v_{i}$ in $\Pi_{i, j=1}^{n}\left(u_{i} v_{j} A_{i j}-1\right)$ where $A_{i j}=0,1$
- Reduce $C$ to finding a few bits of $\Pi_{i=1}^{n^{2}}\left(1+2^{n_{i}}\right)$
- Conjecture: We cannot CAE

$$
\prod_{i=1}^{N}\left(1+x_{i}\right)-\prod_{j=1}^{N}\left(1+y_{j}\right)
$$

- Justification: If many $x_{i}$ and $y_{j}$ the same, exponentially many leading bits of the two products can cancel. It seems hard to compute the first bit that does not cancel without finding the exponentially many that do.


## But isn't $\operatorname{det}(A)=? 0$ in NP?

- Not necessarily in LE model
- What is witness for singularity of $A$ ? A null vector
- But null vector for a matrix with LE entries can have exponentially many bits
- Even for a tridiagonal


# Sparse Arithmetic: Computing in Large Exponent Model 

- How much work does it take to compute $(B+s)-B$, where $B \gg s$ ?
- How many bits does it take to represent $B+s$ ?
- In usual "dense arithmetic" model, depends on relative sizes of $B$ and $s$
- Storing $2^{e}+1$ takes $e$ fraction bits
- In "sparse arithmetic", $B+s$ stored as $(B, s)$, exponentially smaller
- Widely used double-double arithmetic is special case of sparse arithmetic (Priest, Shewchuk, Bailey, Briggs, Bohlender, Kahan, Dekker, Pichat ...)
- Same idea very practical for higher precision
- Store number as array of "nonoverlapping" FP numbers
- Used in some exact inner product implementations


## Which FP Expressions can we CAE in the Large Exponent Model?

- Def: $r(x)$ is in factored form if

$$
r(x)=\prod_{i=1}^{n} p_{i}\left(x_{1}, \ldots, x_{k}\right)^{e_{i}}
$$

where

$$
p_{i}\left(x_{1}, \ldots, x_{k}\right)=\sum_{j=1}^{t} \alpha_{i j} \cdot x_{1}^{e_{i j 1}} \cdots x_{k}^{e_{i j k}}
$$

and

$$
\operatorname{size}(r)=\max \left(n, t, \log \left|e_{i}\right|, \operatorname{size}\left(\alpha_{i j}\right), \operatorname{size}\left(x_{i}\right), \operatorname{size}\left(e_{i j k}\right)\right)
$$

- Thm (mostly Priest) We can CAE $r$ in time poly( $\operatorname{size}(r)$ )
- Compute $p_{i}\left(x_{1}, \ldots, x_{k}\right)$ exactly, with sparse arithmetic
- CAE $p_{i}\left(x_{1}, \ldots, x_{k}\right)^{e_{i}}$ by repeated squaring
- CAE $\Pi_{i=1}^{n} p_{i}\left(x_{1}, \ldots, x_{k}\right)^{e_{i}}$ in conventional FP
- Def: A family $A_{n}(x)$ of $n$-by- $n$ rational matrices is polyfactorable if each minor $r(x)$ is in factored form of size $\operatorname{size}(r)=O(\operatorname{poly}(n))$
- Thm: Suppose $A_{n}(x)$ is polyfactorable.

Then in the Large Exponent model we can CAE $L U$ with pivoting, $A^{-1}$, singular values.

## Accurate and Efficient Matrix Computations in Large Exponent Model

- Thm: Suppose $A_{n}(x)$ is polyfactorable.

Then in the Large Exponent model we can CAE $L U$ with pivoting, $A^{-1}$, singular values.

- Recall Thm: Suppose $A_{n}(x)$ is fully polyfactorable.

Then in the $1+\delta$ model we can CAE $L U$ with pivoting, $A^{-1}$, singular values.

- What matrices can we do in LE model that we could not do in $1+\delta$ model?
- Complex Vandermonde matrices, not just real
- Green's matrices
* inverses of tridiagonals
* represented as $A_{i j}=x_{i} y_{j}, i<j$
- Any fully polyfactorable matrix where we substitute polynomials
* Substitute $x_{i}=p_{i}(z), y_{j}=q_{j}(z)$ in $C_{i j}=1 /\left(x_{i}+y_{j}\right)$
- What matrices can we do in SE model that we could not do in LE model?
- A lot
- Any matrix whose entries are reasonable rational functions of data
- Matrix of $n^{2}$ FP entries


## Cost comparison to symbolic algebra

- Cost(Accurate evaluation in Large Exponent Model) $\geq$ Cost(symbolic expression $\equiv 0$ ?)
- Proof idea: Simulate symbolic algebra using large exponents
$-\operatorname{Cost}($ Accurate evaluation of $p) \geq \operatorname{Cost}(p \equiv 0$ ?)
- Suppose $p\left(x_{0}, \ldots, x_{m-1}\right)$ a symbolic polynomial with max degree $D-1$, integer coeffs of max $\#$ bits $B-1$
- Let $X_{i}=2^{B \cdot D^{i}}$
- Then $p\left(X_{0}, \ldots, X_{m-1}\right)=0$ iff $p \equiv 0$
* Idea: bits in typical term $\alpha \cdot x_{1}^{e_{1}} \cdots x_{m-1}^{e_{m-1}}$ of $p$ do not "overlap" so cannot cancel in sum
- Example: determinant of $A$ each entry of which is rational


## Open Questions

- Are there FP expressions that we provably cannot CAE in Large Exponent (LE) model?
$-\Pi_{i=1}^{n}\left(1+x_{i}\right)-\Pi_{j=1}^{n}\left(1+y_{j}\right)$
- Determinant of general matrix
- Determinant of tridiagonal matrix
- Such an example could distinguish LE from SE
- Conversely, are there fast algorithms for these?
- What does symbolic computing complexity tell us about CAE in LE model, and vice versa?
- What changes if we have sign information?
- We have accurate algorithms for all

Totally Positive (TP) matrices, but not efficient

- How big a class of TP matrices can we do efficiently?
- Generalized Vandermondes $\equiv$ Schur Functions
- What changes if we have complex data?
- Differential equations
- Only simplest ones understood
- What about other discretizations?
- Conjecture: Accuracy depends only on geometry, not material properties
- What about nonsymmetric eigenproblem?
- Blum/Shub/Smale model


## Conclusions

- We have identified many classes of floating point expressions and matrix computations that permit
- Accurate solutions: relative error $<1$
- Efficient solutions: time $=$ poly(size)
- Classes depend strongly on model of FP arithmetic
$-1+\delta$ model: most limited classes, but still interesting
- Bit model with Large Exponents: strictly more, but limited by complexity of symbolic algebra
- Bit model with Small Exponents: strictly more again, since not "really" FP, just integer arithmetic
- Need new algorithms for Large Exponents
- Conventional algorithms with enough precision would be exponentially slower
- New algorithm much faster in practice!
- Lots of open problems
- Reports available
- www.cs.berkeley.edu/~ demmel/NASC.ps to appear Contemporary Mathematics soon
- SIMAX, v. 21, n. 2, pp 562-580, 1999
- Lin. Alg. Appl., vol 299, issue 1-3, pp 21-80, 1999
- These slides: www.cs.berkeley.edu/~demmel/ISSAC2001_2.ps

