Massively parallel algorithms in symbolic computing

Erich Kaltofen
North Carolina State University
www.math.ncsu.edu/~kaltofen

Properties of algorithms distributable over the Internet

- Small input for parallel tasks
- Small code for parallel talks
- Highly parallel, i.e., many tasks
- Tasks are independent, i.e., no spacial or temporal barriers
- Tasks are non-trivial, i.e., coarse grain size

Example: number field sieve, prime number triples

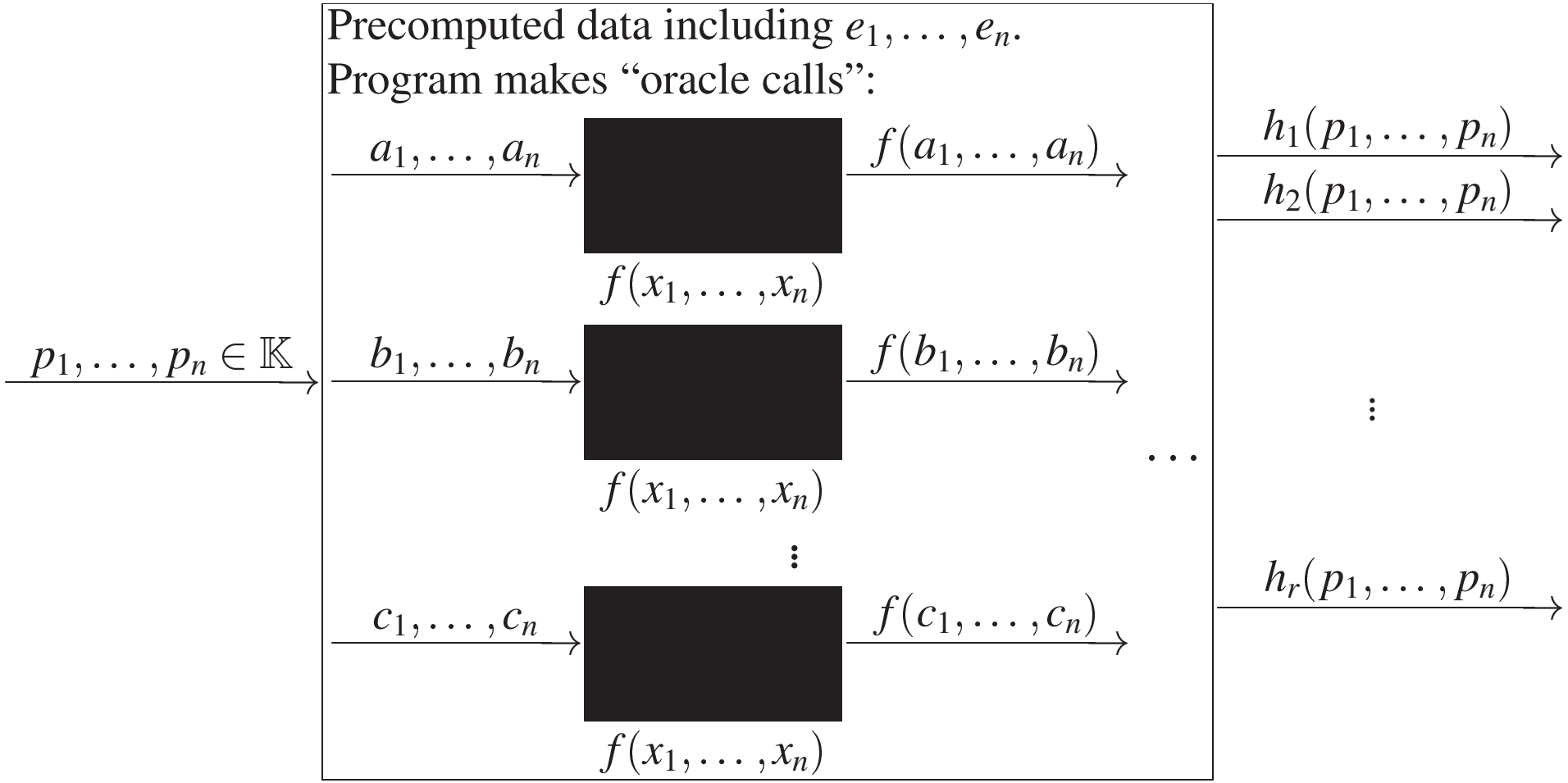
Black box polynomials

$\mathbb{K}$ an arbitrary field, e.g., rationals, reals, complexes

Perform polynmial algebra operations, e.g., factorization with

$n^{O(1)}$	black box calls,
$n^{O(1)}$	arithmetic operations in $\mathbb{K}$ and
$n^{O(1)}$	randomly selected elements in $\mathbb{K}$

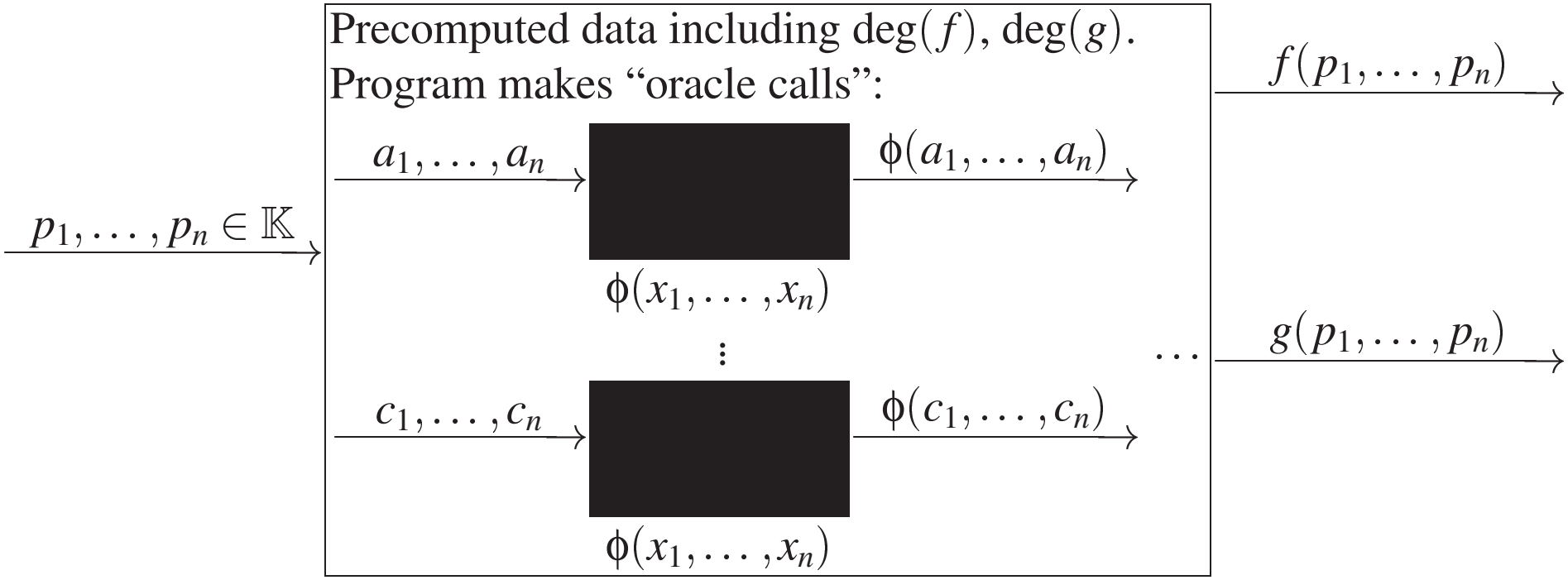
K and TRAGER (1988) efficiently construct the following efficient program:



$$f(x_1, \ldots, x_n) = h_1(x_1, \ldots, x_n)^{e_1} \cdots h_r(x_1, \ldots, x_n)^{e_r}$$

$h_i \in \mathbb{K}[x_1, \ldots, x_n]$ irreducible.

Numerator and denominator separation [K and TRAGER 1988]



$$\phi(x_1, \ldots, x_n) = \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}, f, g \in \mathbb{K}[x_1, \ldots, x_n], \gcd(f, g) = 1.$$

Given a black box

$f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$
$\mathbb{K}$ a field of characteristic 0

compute by multiple evaluation of this black box the sparse representation of f

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{t} a_i x_1^{e_{i,1}} \cdots x_n^{e_{i,n}}, \quad a_i \neq 0$$

Several solutions that are polynomial-time in n and t:

ZIPPEL (1979, 1988), BEN-OR, TIWARI (1988)
K, LAKSHMAN (1988), GRIGORIEV, KARPINSKI, SINGER (1988)
MANSOUR (1992)

Sparsity with non-standard basis

In place of x^e use

$(x-a)^e$	shifted basis
$x(x+1)\cdots(x+e-1)$	Pochhammer basis
$T_e(x)$	Chebyshev basis

Solutions (not all polynomial-time):

LAKSHMAN, SAUNDERS (1992, 1994): Chebyshev, Pochh., shifted
GRIGORIEV, KARPINSKI (1993): shifted
GRIGORIEV, LAKSHMAN (1995): shifted

Example: determinant of Cauchy matrix

$$\det\left(\begin{bmatrix} \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \cdots & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \cdots & \frac{1}{x_2+y_n} \\ \vdots & \vdots & & \vdots \\ \frac{1}{x_n+y_1} & \frac{1}{x_n+y_2} & \cdots & \frac{1}{x_n+y_n} \end{bmatrix}\right) = \frac{\prod_{1\le i<j\le n}(x_j-x_i)(y_j-y_i)}{\prod_{1\le i,j\le n}(x_i+y_j)}.$$

Compute sparse factors of numerators and denominators

FoxBox [Díaz and K 1998] example: determinant of symmetric Toeplitz matrix

$$\det\left(\begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_1 & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2} & a_{n-3} & \dots & a_0 & a_1 \\ a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \end{bmatrix}\right)$$

$$= F_1(a_0, \dots, a_{n-1}) \cdot F_2(a_0, \dots, a_{n-1}).$$

over the integers.

```
> readlib(showtime):
> showtime():
O1 := T := linalg[toeplitz]([a,b,c,d,e,f]):
time   0.03   words   7701
O2 := factor(linalg[det](T));
```

$$
\begin{aligned}
&-(2dca-2bce+2c^2a-a^3-da^2+2d^2c+d^2a+b^3+2abc-2c^2b\\
&\quad+d^3+2ab^2-2dcb-2cb^2-2ec^2+2eb^2+2fcb+2bae\\
&\quad+b^2f+c^2f+be^2-ba^2-fdb-fda-fa^2-fba+e^2a-2db^2\\
&\quad+dc^2-2deb-2dec-dba)(2dca-2bce-2c^2a+a^3\\
&\quad-da^2-2d^2c-d^2a+b^3+2abc-2c^2b+d^3-2ab^2+2dcb\\
&\quad+2cb^2+2ec^2-2eb^2-2fcb+2bae+b^2f+c^2f+be^2-ba^2\\
&\quad-fdb+fda-fa^2+fba-e^2a-2db^2+dc^2+2deb-2dec\\
&\quad+dba)
\end{aligned}
$$

```
time   27.30   words   857700
```

FoxBox timings for symmtric Toeplitz deteriminant challenge

N	CPU Time	Degree	# Terms
10	$1^h20'$	5	931
11	$1^h34'$	5	847
12	$10^h14'$	6	5577
13	$15^h24'$	6	4982

CPU times (hours^{h}minutes$'$) to retrieve the distributed representation of a factor from the factors black box of a symmetric Toeplitz determinant black box. Construction is over $\mathbb{Q}$, evaluation is over GF(10^8+7) for $N = 10, 11$, and 12 (Pentium 133, Linux 2.0) and GF$(2^{30}-35)$ for $N = 13$ (Sun Ultra 2 168MHz, Solaris 2.4).

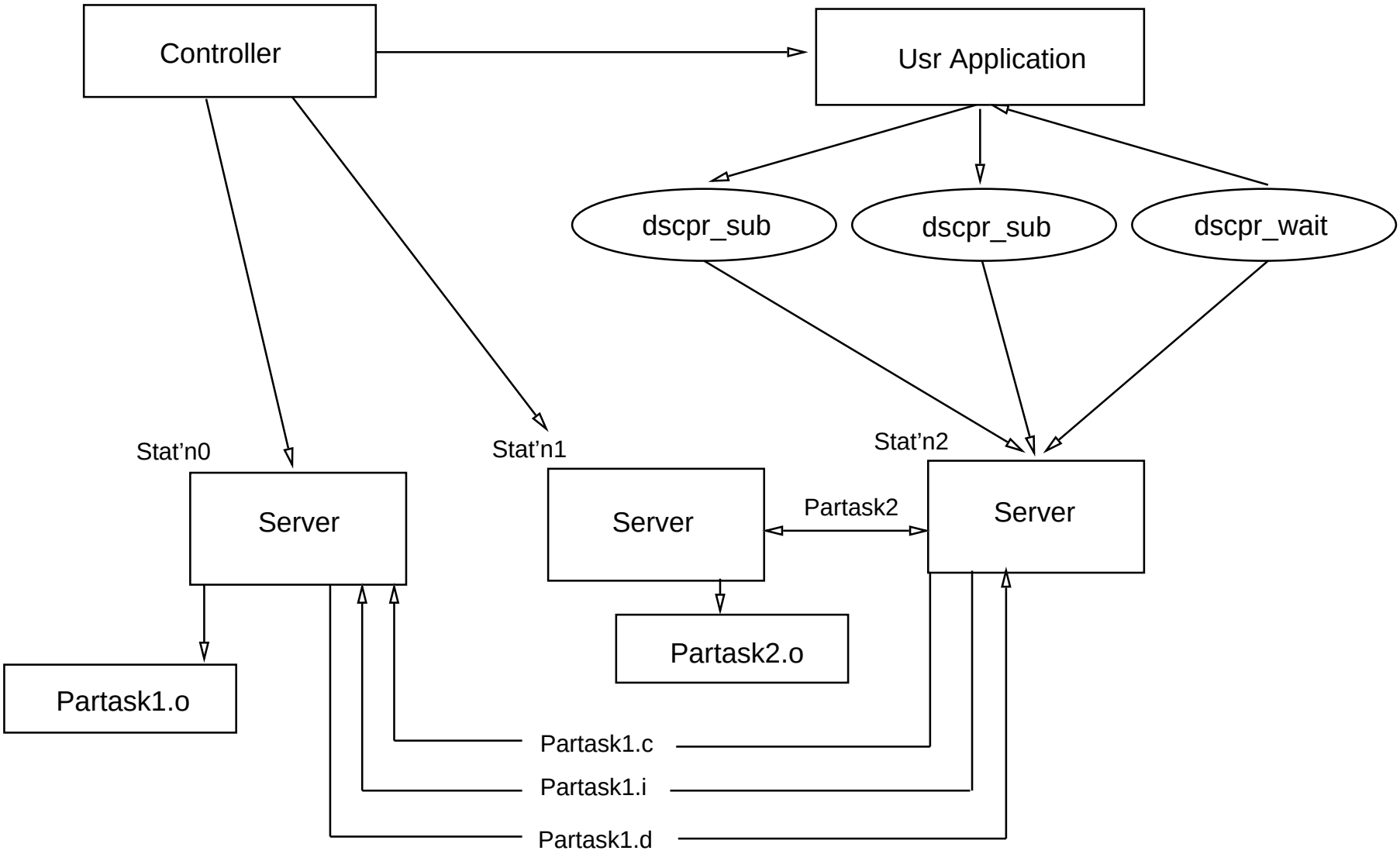
Serialization of **factors box** of 8 by 8 symmetric Toeplitz matrix modulo 65521

15,8,-1,1,2,2,-1,8,1,7,1,1,20752,-1,1,39448,33225,984,17332,53283,
35730,23945,13948,22252,52005,13703,8621,27776,33318,2740,
4472,36959,17038,55127,16460,26669,39430,1,0,1,4,20769,16570,
58474,30131,770,4,25421,22569,51508,59396,10568,4,20769,16570,
58474,30131,770,8,531,55309,40895,38056,34677,30870,397,59131,
12756,3,13601,54878,13783,39334,3,41605,59081,10842,15125,
3,45764,5312,9992,25318,3,59301,18015,3739,13650,3,23540,44673,
45053,33398,3,4675,39636,45179,40604,3,49815,29818,2643,16065,
3,46787,46548,12505,53510,3,10439,37666,18998,32189,3,38967,
14338,31161,12779,3,27030,21461,12907,22939,3,24657,32725,
47756,22305,3,44226,9911,59256,54610,3,56240,51924,26856,52915,
3,16133,61189,17015,39397,3,24483,12048,40057,21323

Serialization of **checkpoint** during sparse interpolation

28, 14, 9, 64017, 31343, 5117, 64185, 47755, 27377, 25604, 6323, 41969, 14, 3, 4, 0, 0, 3, 4, 0, 1, 3, 4, 0, 2, 3, 4, 0, 3, 3, 4, 0, 4, 3, 4, 1, 0, 3, 4, 1, 1, 3, 4, 1, 2, 3, 4, 1, 3, 3, 4, 2, 0, 3, 4, 2, 1, 3, 4, 2, 2, 3, 4, 3, 0, 3, 4, 3, 1, 14, 59877, 1764, 59012, 44468, 1, 19485, 25871, 3356, 2, 58834, 49014, 65518, 15714, 65520, 1, 2, 4, 4, 1, 1

DSC system [1991]



Black box matrices

$A \in \mathbb{K}^{n \times n}$ singular

$\mathbb{K}$ an arbitrary, e.g., finite field

Perform linear algebra operations, e.g., $A^{-1}b$ [Wiedemann 86] with

$O(n)$	black box calls and
$n^2(\log n)^{O(1)}$	arithmetic operations in $\mathbb{K}$ and
$O(n)$	intermediate storage for field elements

Flurry of recent results

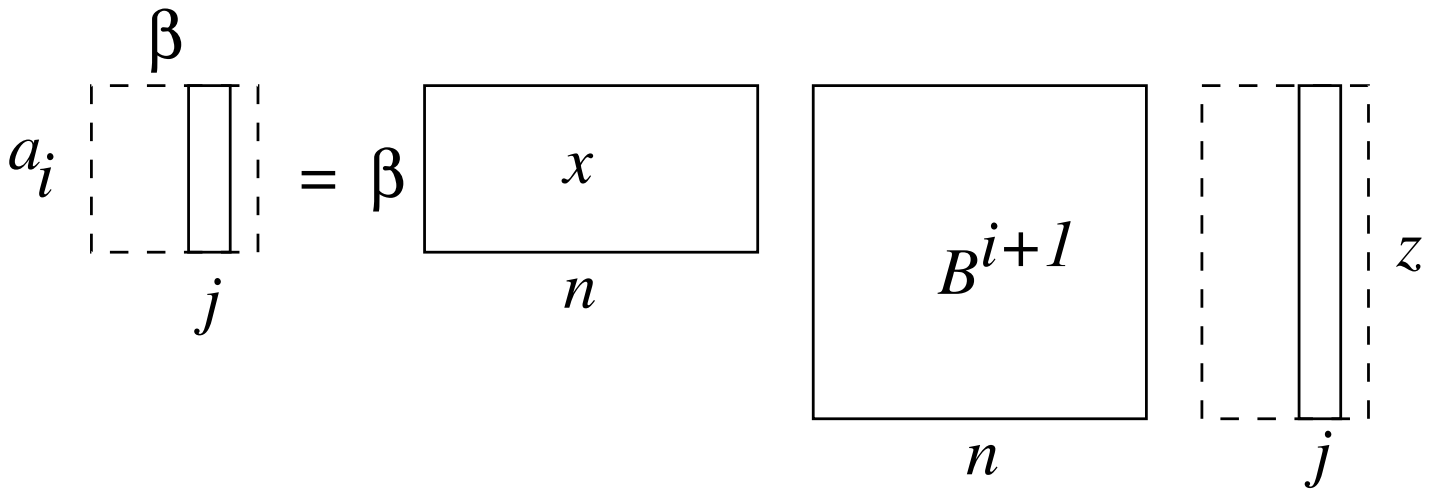
Lambert [1996], Teitelbaum [1997], Eberly & K [1997]	relationship of Wiedemann and Lanczos approach
Villard [1997]	analysis of *block* Wiedemann algorithm
Giesbrecht [1997]	computation of integral solutions
Giesbrecht & Lobo & Saunders [1997]	certificates for inconsistency

Diophantine solutions
by Giesbrecht:
Find several rational solutions.

$$A(\tfrac{1}{2}x^{[1]}) = b, \quad x^{[1]} \in \mathbb{Z}^n$$
$$A(\tfrac{1}{3}x^{[2]}) = b, \quad x^{[2]} \in \mathbb{Z}^n$$

$$\gcd(2,3) = 1 = 2 \cdot 2 - 1 \cdot 3$$
$$A(2x^{[1]} - x^{[2]}) = 4b - 3b = b$$

Parallel coarse-grain block Wiedemann



The j^{th} processor computes the j^{th} column of the sequence of (small) matrices.

Example of massively parallel problem

$$\begin{bmatrix} 1 & \cdots & & \cdots & \frac{1}{n} \\ & \vdots & & & \\ & \frac{1}{i+j-1} & & & \\ & \vdots & & & \\ \frac{1}{n} & \cdots & & \cdots & \frac{1}{2n-1} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

(Hilbert matrix)

K and Lobo (1994) implemented Berlekamp's polynomial factorization algorithm with black box Petr matrix

LINBOX project

U. Calgary:	Wayne Eberly
U. Delaware:	David Saunders
IMAG Grenoble:	Jean-Guillaume Dumas,
	Jean-Louis Roch, Gilles Villard
NC State U.:	Erich Kaltofen, Wen-shin Lee
Washington College:	Austin Lobo
U. Western Ontario:	Mark Giesbrecht

Design, analyze and implement black box matrix algorithms

- early termination criterion for block Wiedemann
- rank certificates over characteristic 0 fields
- new Smith normal form algorithm
- "plug-and-play" generic design for library

Random search and test

What is the largest known prime?

$$x^{1055} + x^{1054} + x^2 + x + 1 \bmod 2 \qquad \text{is a prime}$$

Fast algorithms for constructing irreducible polynomials modulo 2 are known.

Search in parallel for those that have few terms.

Can use fast polynomial remaindering.

Parallel software design issues

- Application interface must be stable: Cilk, Jade, Athapascan, Java threads
- Checkpoints: must be able to continue after crash
- Usage of existing libraries: initialization must persist over several calls; co-routines
- Symbolic objects are shipped as procedures
  - for remote construction
  - for black box evaluation
  - checkable for illegal memory access/operations?

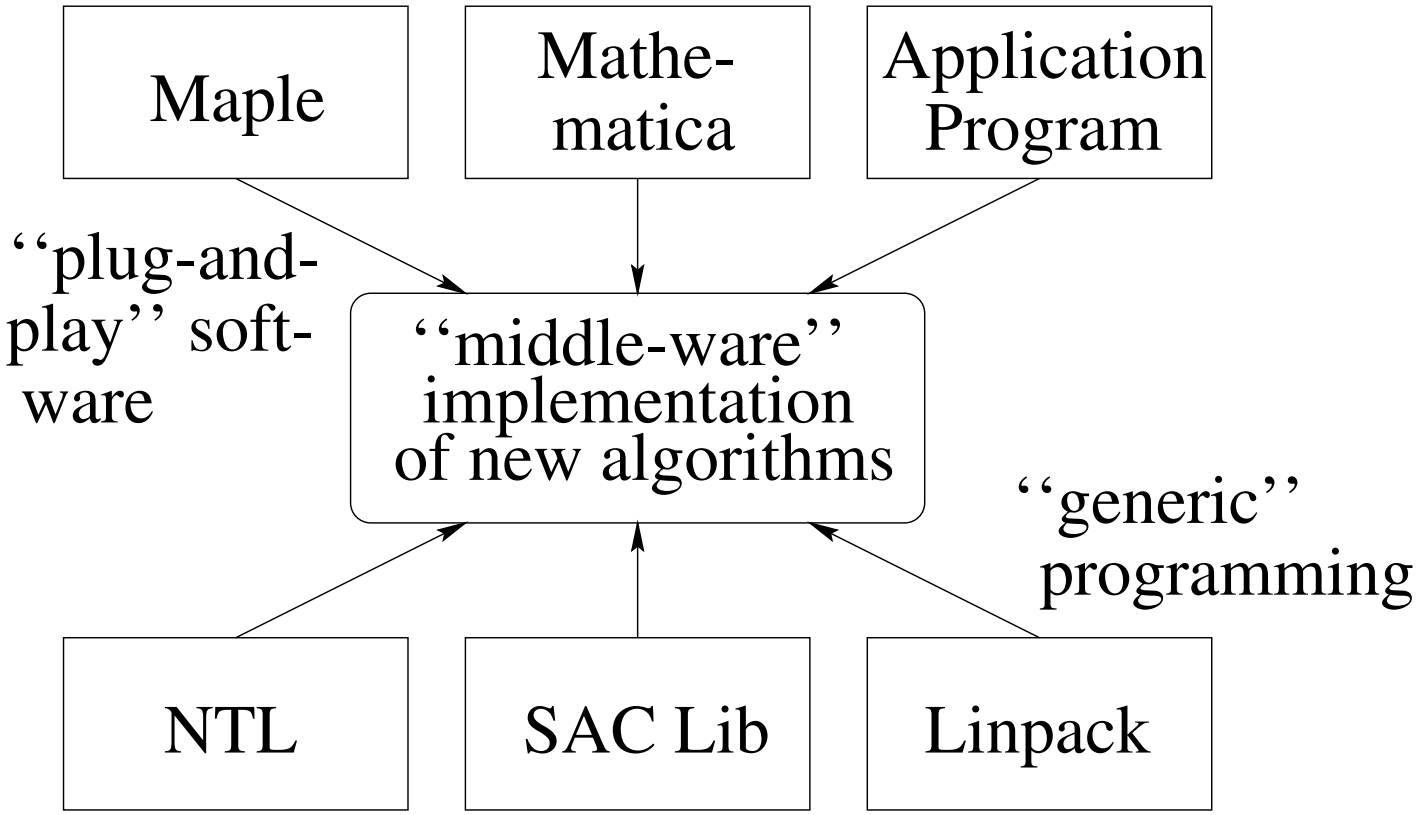
OpenMath programming standard

```
<Comment> Programmer: Leslie Jones, NCSU, Sep 28, 1998 </Comment>
<Function> FIBO <Parameters> <equal> NUM Integer </equal></Parameters>
                <TypeToken>Integer</Typetoken>
<Block>
     <Declaration>
          <equal> <list> N TEMP NEXT PREV COUNT </list> Integer </equal>
     </Declaration>

     <Assign> COUNT 0 </Assign>
     <Assign> NEXT 0 </Assign>
     <Assign> TEMP 1 </Assign>
     <Assign> PREV 0 </Assign>

     <if> <greater> NUM 0 </greater>
          <TBlock>
               <ForLoop>
                    <LoopVariable> COUNT </LoopVariable>
                    <InitialValue> 2 </InitialValue>
                    <Increment> 1 </Increment>
                    <LastValue> NUM </LastValue>
```

```
                    <Block>
                         <Assign> NEXT
                              <plus> TEMP PREV </plus> </Assign>
                         <Assign> PREV TEMP </Assign>
                         <Assign> TEMP NEXT </Assign>
                    </Block>
               </ForLoop>
          </TBlock>

          <FBlock>
               <assign>N<minus>NUM</minus></assign>
               <assign> NEXT <times> <power> -1 <minus> N 1 </minus>
                    </power><FIBO>N</FIBO></times></assign>
          </FBlock>
     </if>
     <Return> NEXT </Return>
</Block>
</Function>
```

Ms. Jones and I are building an “OpenMath virtual machine”

Plug-and-play components



```
From kaltofen@pams.ncsu.edu  Thu Oct  8 13:07:48 1998
Received: from eos01mh.eos.ncsu.edu (eos01mh.eos.ncsu.edu [152.1.9.16])
by eos00mh.eos.ncsu.edu (8.8.7/8.8.7) with ESMTP id NAA01130
for <kaltofen@eos00mh.eos.ncsu.edu>; Thu, 8 Oct 1998 13:07:47 -0400 (EDT)
Received: from math.ncsu.edu (math.ncsu.edu [152.1.30.3])
by eos01mh.eos.ncsu.edu (8.8.7/8.8.7) with SMTP id NAA07270
for <kaltofen@eos.ncsu.edu>; Thu, 8 Oct 1998 13:07:46 -0400 (EDT)
Received: from vega.math.ncsu.edu by math.ncsu.edu (8.6.11/PC07mar95)
id NAA00566; Thu, 8 Oct 1998 13:07:45 -0400
Received: (from kaltofen@localhost)
          by vega.math.ncsu.edu (8.8.4/UC02Jan97)
  id NAA07512; Thu, 8 Oct 1998 13:07:41 -0400 (EDT)
From: "Erich Kaltofen" <kaltofen@eos.ncsu.edu>
Message-Id: <9810081307.ZM7510@eos.ncsu.edu>
Date: Thu, 8 Oct 1998 13:07:40 -0400
In-Reply-To: Petr Lisonek <lisonek@cecm.sfu.ca>
        "irreducible trinomials" (Oct  6,  7:12pm)
References: <199810070212.TAA15883@bb.cecm.sfu.ca>
X-Mailer: Z-Mail (3.2.1 10oct95)
To: Laurent.Bernardin@inf.ethz.ch, kaltofen@math.ncsu.edu, lisonek@cecm.sfu.ca
Subject: Re: irreducible trinomials
Cc: monagan@cecm.sfu.ca
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Status: OR

On Oct 6,  7:12pm, Petr Lisonek wrote:
> Subject: irreducible trinomials
>
> Dear Erich,
>
> In your talk at MSRI last Saturday you posed the challenge
> to find high degree but sparse polynomials, irreducible over GF(2).
> Since I returned to Vancouver, I've spent quite a few machine and brain
cycles
> on this stuff and eventually came up with trinomials x^(2*3^k)+x^(3^k)+1
> as the most promising candidates.  Just before starting to prove the
> irreducibility I decided to do a thorough literature check using
> MathSciNet (the on-line version of Math Reviews), and came across the paper
>
> Blake, Ian F.; Gao, Shuhong; Lambert, Robert:
```

> Constructive problems for irreducible polynomials over finite fields.
> Information theory and applications (Rockland, ON, 1993),
> pages 1--23, Lecture Notes in Comput. Sci., 793, Springer, Berlin, 1994.

Got it! In fact, x^(2*3^k) + x^(3^k) + 1 is cyclotomic(3^(k+1), x)
and 2 is a primitive root modulo 3^(k+1) [Knuth, vol. 2, sec. 3.2.1.2],
which proves the example.

More interestingly, cyclotomic(7^(k+1), x) has exactly 2 irred. factors
which are trinomials of
equal degree modulo 2. This is an example where the DDF algorithm will
take the maximum time. I believe J. Gerhard was looking for such
examples, and I didn't know one then. I still have to prove this claim,
but I think it follows as before.

>
> In this paper the authors prove the GF(2)-irreducibility of "my" trinomials
> as well as several other constructions. They also give lots of
> references on irreducible fewnomials. Anyway, I enjoyed this.
>
> Best regards,
> Petr
>

OK, so my example for a search procedure was somewhat ill chosen. It would
still be a nice problem to find an irred. poly. mod 2 for a given degree,
say 10^6. But this just doesn't seem as interesting as finding the
largest prime.

Yours, Erich

>
> --
> Petr Lisonek   e-mail: lisonek@cecm.sfu.ca
> CECM   http://www.cecm.sfu.ca/~lisonek
> Department of Mathematics and Statistics
> Simon Fraser University   phone: (604)291-5617
> Burnaby, BC   fax: (604)291-5614
> CANADA V5A 1S6
> --
>-- End of excerpt from Petr Lisonek