Fast algorithms for factoring polynomials

Erich Kaltofen
North Carolina State University
`google->kaltofen`

NORTH CAROLINA STATE UNIVERSITY
FOUNDED MARCH 7, 1887

Factorization of $f(x) \in \mathbb{F}_q[x]$, $n = \deg(f)$

Run-time comparisons (field arithmetic operations)

	$q = O(1)$	$\log q = O(n)$
Berlekamp ’70 $O(n^{\omega} + n^{1+o(1)} \log q)$	$O(n^{2.38})$	$O(n^{2.38})$
Cantor & Zassenhaus ’81 $O(n^{2+o(1)} \log q)$	$O(n^{2+o(1)})$	$O(n^{3+o(1)})$
von zur Gathen & Shoup ’91 $O(n^{2+o(1)} + n^{1+o(1)} \log q)$	$O(n^{2+o(1)})$	$O(n^{2+o(1)})$
Kaltofen & Shoup ’94 $O(n^{(\omega+1)/2+(1-\gamma)(\omega-1)/2} +$ $n^{1+\gamma+o(1)} \log q)$ for any $0 \leq \gamma \leq 1$	$O(n^{1.81})$	$O(n^{2.5})$

ω = matrix multiplication exponent

The high algebraic extension case (Kaltofen & Shoup ’96)

Let $q = 2^{\lceil n^{1.5} \rceil}$, and consider factorization over $\mathbb{F}_q$ in terms of bit complexity.

von zur Gathen & Shoup ’91: $O(n(\log q)^2)$.

Kaltofen & Shoup ’96: $O(n(\log q)^{1.69})$.

Generalizes to $q = p^k$ where k grows superlinearly with n.

Distinct degree factorization (C. F. Gauss)

Fact: $x^{q^i} - x = \prod_{\substack{f \text{ irreducible over } \mathbb{F}_q \\ \deg(f) \text{ divides } i}} f(x)$

Write $f^{[i]} = \prod_{\substack{g \text{ irred. factor of } f \\ \deg(g) = i}} g$

```
$f^* \leftarrow f$; /* squarefree */
   for $i \leftarrow 1, \ldots, \lfloor n/2 \rfloor$ do
         $\{ f^{[i]}(x) \leftarrow \mathrm{GCD}(-x + x^{q^i} \bmod f^*(x), f^*(x))$;
           $f^* \leftarrow f^* \big/ f^{[i]}$;
         $\}$
$f^{[\deg(f^*)]} \leftarrow f^*$; /* factor with degree $> \lfloor n/2 \rfloor$*/
```

Suppose $f(x) \in \mathbb{F}_q[x]$ has degree n, $g(x)$, $h(x)$ are remainders. All counts are in terms of arithmetic operations in $\mathbb{F}_q$.

Problem	Complexity	Inventors of algorithm
1. $g \cdot h \pmod f$	$O(n(\log n)\log\log n)$	Schönhage&Strassen 1969 Schönhage 1977 ($p = 2$)
2. $\mathrm{GCD}(f, g)$	$O(n(\log n)^2\log\log n)$	Knuth 1971/Moenck 1973
3. $g^q \pmod f$	$O((\log q)n^{1+o(1)})$	Pingala 200 b.c.
4. $g(h(x)) \pmod{f(x)}$	$O(n^{1.69})$	Brent&Kung 1978 Coppersmith&Winograd 1987
5. $x^{q^n} \pmod{f(x)}$ given $x^q \pmod{f(x)}$	$O(n^{1.69})$	von zur Gathen&Shoup 1991

6. $g(h_1), \ldots, g(h_n) \pmod{f}$ $O(n^{2+o(1)})$ Moenck&Borodin 1972

7. $x^{q^2}, \ldots, x^{q^n} \pmod{f(x)}$ $O(n^{2+o(1)})$ von zur Gathen&Shoup 1991
given $x^q \pmod{f(x)}$

Fast computation of $x^{q^n} \bmod f(x)$

$$x^{q^i} \equiv (\underbrace{x^{q^{i-1}}}_{h_{i-1}(x)})^q$$

$$\equiv h_{i-1}(\underbrace{x^q}_{h_1(x)})$$

$$\equiv h_{i-1}(\,h_1(x)\,)$$

$$\equiv h_{\lfloor i/2 \rfloor}(\,h_{\lfloor i/2 \rfloor}(\,h_{i \bmod 2}(x)\,)\,) \pmod{f(x)}$$

(modular polynomial composition)

Fast modular polynomial composition

Compute $g(h(x)) \pmod{f(x)}$ with $O(n^{1.69})$ field operations.

$$g(x) = \sum_{j=0}^{\lceil\sqrt{n}\rceil} \left(\sum_{l=0}^{\lfloor\sqrt{n}\rfloor-1} c_{j,l} x^l \right) \cdot x^{\lfloor\sqrt{n}\rfloor \cdot j}$$

$$[c_{j,l}] \qquad \cdot \qquad \begin{bmatrix} \overrightarrow{h^0 \bmod f} \\ \overrightarrow{h^1 \bmod f} \\ \overrightarrow{h^2 \bmod f} \\ \vdots \\ \overrightarrow{h^{\lfloor\sqrt{n}\rfloor-1} \bmod f} \end{bmatrix}$$

$$\lfloor\sqrt{n}\rfloor \times \lfloor\sqrt{n}\rfloor \qquad \lfloor\sqrt{n}\rfloor \times n \qquad\qquad \Rightarrow O(\sqrt{n}(\sqrt{n})^{2.38})$$

Baby step-giant step algorithm (Kaltofen & Shoup 1994)

Fact: $x^{q^J} - x^{q^i} = \left(x^{q^{J-i}} - x\right)^{q^i} = \left(\prod_{\substack{f \text{ irreducible over } \mathbb{F}_q \\ \deg(f) \text{ divides } J-i}} f(x) \right)^{q^i}$

Let $l = \lceil n^\beta \rceil$ with $0 \le \beta \le 1$:

$$\text{GCD}\left(\prod_{i=0}^{l-1} (\underbrace{x^{q^{jl}}}_{\substack{||| \\ H_j}} - \underbrace{x^{q^i}}_{\substack{||| \\ h_i}}) \bmod f(x), \;\; f(x) \right)$$

has all those factors of f whose degree is in the interval $[(j-1)l+1, jl]$.

Step 1 (*baby steps*): Let $l = \lceil n^{\beta} \rceil$.

```
for $i \leftarrow 1,\ldots,l-1$ do $h_i(x) \leftarrow x^{q^i} \bmod f(x)$.
```

Cost: $O(n^{1+\beta+o(1)} \log q)$

Step 2 (*giant steps*):

```
for $j \leftarrow 1,\ldots,\lceil n/(2l) \rceil$ do $H_j(x) \leftarrow x^{q^{jl}} \bmod f(x)$.
```

Cost: $O(n^{1.69+(1-\beta)})$

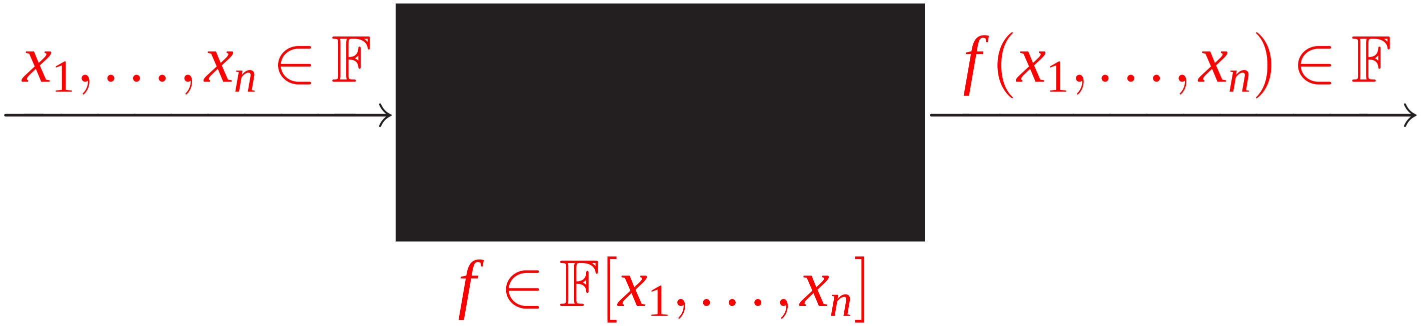
Step 3 (*coarse distinct degree factorization*):

```
for $j \leftarrow 1,\ldots,\lceil n/(2l) \rceil$ do $I_j \leftarrow \prod_{i=0}^{l-1} (H_j - h_i) \bmod f$.
$f^* \leftarrow f$;
for $j \leftarrow 1,\ldots,\lceil n/(2l) \rceil$ do
        $\{F_j \leftarrow \mathrm{GCD}(I_j, f^*); f^* \leftarrow f^* \big/ F_j\}$
```

Step 4 (*fine distinct degree factorization*):

Split $F_j = f^{[(j-1)l+1]} \cdot f^{[(j-1)l+2]} \cdots f^{[jl]}$ á la Gauss.

Black box polynomials



$x_1, \ldots, x_n \in \mathbb{F}$

$f(x_1, \ldots, x_n) \in \mathbb{F}$

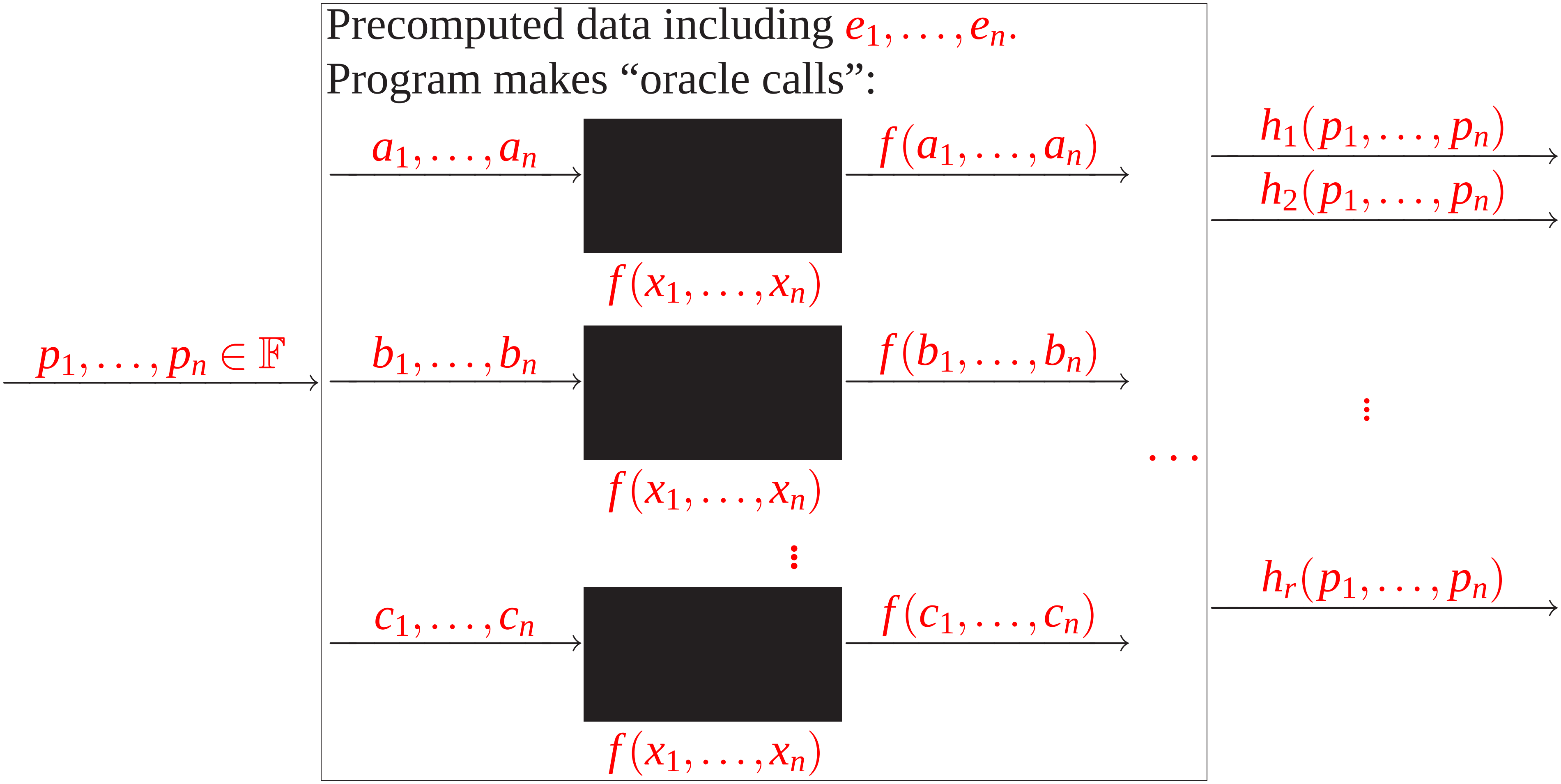
$f \in \mathbb{F}[x_1, \ldots, x_n]$

$\mathbb{F}$ 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 $\mathbb{F}$ and
$n^{O(1)}$ randomly selected elements in $\mathbb{F}$

Kaltofen and Trager (1988) efficiently construct the following efficient program:



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

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

Characterization of Factor Evaluation Program

- Always evaluates the same associate of each factor

$$x\,y \quad \text{vs.} \quad (\frac{1}{2}x)\,(2y)$$

- Construction of program is Monte-Carlo (might produce incorrect program with probability $\le \varepsilon$), and requires a factorization procedure for $\mathbb{F}[y]$, but the program itself is deterministic
- Program contains positive integer constants of value bounded by

$$\frac{2^{\deg(f)^{1+o(1)}}}{\varepsilon}$$

- Program makes

$$O(\deg(f)^2) \text{ oracle calls,}$$

none of whose inputs depends on another one's output, → parallel version

- Furthermore, program performs $\deg(f)^{2+o(1)}$ arithmetic operations in $\mathbb{F}$

Homotopy Method for Solving $F(X) = 0$

Known: Solution to $G(X) = 0$	Wanted: Solution to $F(X) = 0$
$x_1(0)$ ●	● $x_1(1)$
$x_2(0)$ ●	● $x_2(1)$
$x_3(0)$ ●	● $x_3(1)$
$\vdots$	$\vdots$
$x_n(0)$ ●	● $x_n(1)$

Follow from $y = 0$ to $y = 1$ the solutions of

$$H(X(y)) = (1-y)G(X(y)) + yF(X(y))$$

Our Homotopy

For $f(x_1,\ldots,x_n) \in \mathbb{F}[x_1,\ldots,x_n]$ consider

$$\begin{aligned}\bar{f}(X,Y) = f(&X+b_1, Y(p_2-a_2(p_1-b_1)-b_2)+a_2X+b_2,\\ &\ldots, Y(p_n-a_n(p_1-b_1)-b_n)+a_nX+b_n)\end{aligned}$$

The field elements $a_2,\ldots,a_n,b_1,\ldots,b_n$ are pre-chosen (“known”)
The field elements $p_1,\ldots,p_n$ are input

Notice: The polynomial $\bar{f}(X,0)$ is independent of $p_1,\ldots,p_n$ and can be factored into

$$\bar{f}(X,0) = \prod_{i=1}^{r} g_i(X)^{e_i}, \quad g_i(X) \in \mathbb{F}[X] \text{ irreducible}$$

By an ***effective Hilbert Irreducibility Theorem*** one can guarantee that the g_i are distinct images of the factors of f

$$g_i(X) = h_i(X+b_1,\ldots,a_nX+b_n),\ f(x_1,\ldots,x_n) = \prod_{i=1}^{r} h(x_1,\ldots,x_n)^{e_i}$$

$\longrightarrow$ enters randomization

Our Homotopy

For $f(x_1,\ldots,x_n) \in \mathbb{F}[x_1,\ldots,x_n]$ consider

$$\begin{aligned}\bar{f}(X,Y) = f(X+b_1, Y(p_2-a_2(p_1-b_1)-b_2)+a_2X+b_2,\\ \ldots, Y(p_n-a_n(p_1-b_1)-b_n)+a_nX+b_n)\end{aligned}$$

The field elements $a_2,\ldots,a_n,b_1,\ldots,b_n$ are pre-chosen (“known”)
The field elements $p_1,\ldots,p_n$ are input

Notice: The polynomial $\bar{f}(X,0)$ is independent of $p_1,\ldots,p_n$ and can be factored into

$$\bar{f}(X,0) = \prod_{i=1}^{r} g_i(X)^{e_i}, \quad g_i(X) \in \mathbb{F}[X] \text{ irreducible}$$

By ***Hensel Lifting*** we can follow the factorization to

$$\bar{f}(X,Y) = \prod_{i=1}^{r} \bar{h}_i(X,Y)^{e_i}$$

Now

$$\bar{f}(p_1-b_1,1) = f(p_1,\ldots,p_n), \quad \forall i: \bar{h}_i(p_1-b_1,1) = h_i(p_1,\ldots,p_n)$$

Four Corollaries

Corollary 1: (Parallel Factorization)
For $\mathbb{F} = \mathbb{Q}$, we can compute in Monte Carlo $\mathcal{NC}$ all sparse factors of f of fixed degree and with no more than a given number t terms

Corollary 2: (Sparse Rational Interpolation)
Given a degree bound

$$b \geq \max(\deg(f), \deg(g))$$

and a bound t for the maximum number of non-zero terms in both f and g, we can in **Las Vegas** polynomial-time in b and t compute from a black box for f/g the sparse representations of f and g

Corollary 3: (Greatest Common Divisor)
From a black box for

$$f_1(x_1,\dots,x_n),\dots,f_r(x_1,\dots,x_r)\in\mathbb{F}[x_1,\dots,x_n]$$

we can efficiently produce a feasible program with oracle calls that allows to evaluate one and the same associate of

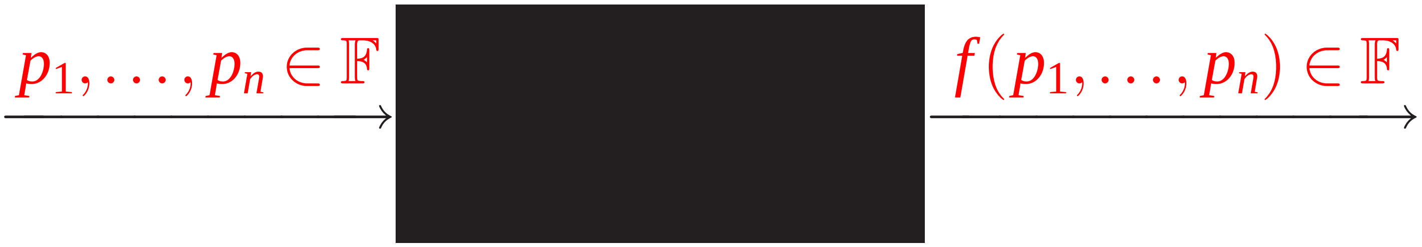
$$\mathrm{GCD}(f_1,\dots,f_r).$$

Corollary 4: (Factors as Straight-Line Programs)
Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be given by a straight-line program of size s, e.g.,

```
$\upsilon_1 \leftarrow c_1 \times x_1;$
$\upsilon_2 \leftarrow y - c_2;$          Comment: $c_1, c_2$ are constants in $\mathbb{F}$
$\upsilon_3 \leftarrow \upsilon_2 \times \upsilon_2;$
$\upsilon_4 \leftarrow \upsilon_3 + \upsilon_1;$
$\upsilon_5 \leftarrow \upsilon_4 \times x_3;$
$\vdots$
$\upsilon_{101} \leftarrow \upsilon_{100} + \upsilon_{51};$
```

The variable υ_{101} holds a polynomial in $\mathbb{F}_q[x_1, \ldots]$ of degree $\leq 2^{101}$. Then one can compute in polynomial-time in $s + \deg(f)$ straight-line programs of **polynomial-size** for all irreducible factors.

Given a black box



$p_1, \dots, p_n \in \mathbb{F} \longrightarrow$ $\longrightarrow f(p_1, \dots, p_n) \in \mathbb{F}$

$f(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$

$\mathbb{F}$ a field

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

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

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

Zippel (1979, 1988), Ben-Or, Tiwari (1988)
Kaltofen, Lakshman (1988)
Grigoriev, Karpinski, Singer (1988)
Mansour (1992)
Kaltofen and Lee (2000)

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
Giesbrecht, Kaltofen, Lee (2002): Chebyshev, Pochhammer, shifted

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

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

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

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));
```

$$\begin{aligned}
&-(2\,d\,c\,a-2\,b\,c\,e+2\,c^2\,a-a^3-d\,a^2+2\,d^2\,c+d^2\,a+b^3+2\,a\,b\,c-2\,c^2\,b\\
&\quad+d^3+2\,a\,b^2-2\,d\,c\,b-2\,c\,b^2-2\,e\,c^2+2\,e\,b^2+2\,f\,c\,b+2\,b\,a\,e\\
&\quad+b^2\,f+c^2\,f+b\,e^2-b\,a^2-f\,d\,b-f\,d\,a-f\,a^2-f\,b\,a+e^2\,a-2\,d\,b^2\\
&\quad+d\,c^2-2\,d\,e\,b-2\,d\,e\,c-d\,b\,a)(2\,d\,c\,a-2\,b\,c\,e-2\,c^2\,a+a^3\\
&\quad-d\,a^2-2\,d^2\,c-d^2\,a+b^3+2\,a\,b\,c-2\,c^2\,b+d^3-2\,a\,b^2+2\,d\,c\,b\\
&\quad+2\,c\,b^2+2\,e\,c^2-2\,e\,b^2-2\,f\,c\,b+2\,b\,a\,e+b^2\,f+c^2\,f+b\,e^2-b\,a^2\\
&\quad-f\,d\,b+f\,d\,a-f\,a^2+f\,b\,a-e^2\,a-2\,d\,b^2+d\,c^2+2\,d\,e\,b-2\,d\,e\,c\\
&\quad+d\,b\,a)
\end{aligned}$$

```
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 $\mathrm{GF}(10^8+7)$ for $N = 10, 11$, and 12 (Pentium 133, Linux 2.0) and $\mathrm{GF}(2^{30}-35)$ 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