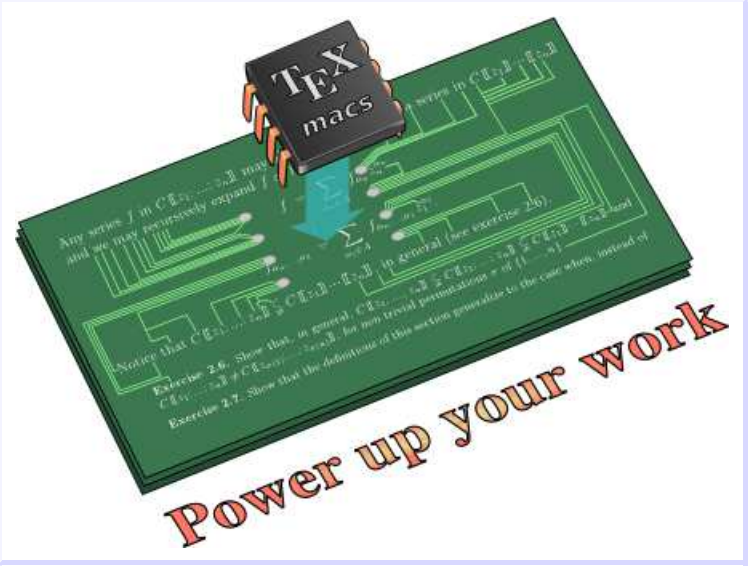
Sparse polynomial interpolation in practice

Joris van der Hoeven, Grégoire Lecerf

CNRS, École polytechnique



Issac, 神戸市, 2014

http://www.TEXMACS.org

Motivation (implementation in upcoming CAAS package, matrices)

```
Caas] M(n) == [ x[i,j] | i in 1 to n || j in 1 to n ];
Caas] M(2)
```

$$\begin{bmatrix} x_{1,1} & x_{2,1} \\ x_{1,2} & x_{2,2} \end{bmatrix}$$

```
Caas] invert M(2)
```

$$\begin{bmatrix} \frac{x_{2,1}\,x_{1,2}}{\left(x_{2,2}-\frac{x_{2,1}\,x_{1,2}}{x_{1,1}}\right)x_{1,1}^2}+\frac{1}{x_{1,1}} & -\left(\frac{x_{2,1}}{\left(x_{2,2}-\frac{x_{2,1}\,x_{1,2}}{x_{1,1}}\right)x_{1,1}}\right) \\ -\left(\frac{x_{1,2}}{\left(x_{2,2}-\frac{x_{2,1}\,x_{1,2}}{x_{1,1}}\right)x_{1,1}}\right) & \frac{1}{x_{2,2}-\frac{x_{2,1}\,x_{1,2}}{x_{1,1}}} \end{bmatrix}$$

```
Caas] simplify (M(12) * invert M(12))
```

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

```
Caas] simplify transpose invert transpose invert M(8)
```

$$\begin{bmatrix} x_{1,1} & x_{2,1} & x_{3,1} & x_{4,1} & x_{5,1} & x_{6,1} & x_{7,1} & x_{8,1} \\ x_{1,2} & x_{2,2} & x_{3,2} & x_{4,2} & x_{5,2} & x_{6,2} & x_{7,2} & x_{8,2} \\ x_{1,3} & x_{2,3} & x_{3,3} & x_{4,3} & x_{5,3} & x_{6,3} & x_{7,3} & x_{8,3} \\ x_{1,4} & x_{2,4} & x_{3,4} & x_{4,4} & x_{5,4} & x_{6,4} & x_{7,4} & x_{8,4} \\ x_{1,5} & x_{2,5} & x_{3,5} & x_{4,5} & x_{5,5} & x_{6,5} & x_{7,5} & x_{8,5} \\ x_{1,6} & x_{2,6} & x_{3,6} & x_{4,6} & x_{5,6} & x_{6,6} & x_{7,6} & x_{8,6} \\ x_{1,7} & x_{2,7} & x_{3,7} & x_{4,7} & x_{5,7} & x_{6,7} & x_{7,7} & x_{8,7} \\ x_{1,8} & x_{2,8} & x_{3,8} & x_{4,8} & x_{5,8} & x_{6,8} & x_{7,8} & x_{8,8} \end{bmatrix}$$

Caas] simplify invert M(2)

$$\begin{bmatrix} \dfrac{x_{2,2}}{x_{2,2}\,x_{1,1} - x_{2,1}\,x_{1,2}} & -\left(\dfrac{x_{2,1}}{x_{2,2}\,x_{1,1} - x_{2,1}\,x_{1,2}}\right) \\ -\left(\dfrac{x_{1,2}}{x_{2,2}\,x_{1,1} - x_{2,1}\,x_{1,2}}\right) & \dfrac{x_{1,1}}{x_{2,2}\,x_{1,1} - x_{2,1}\,x_{1,2}} \end{bmatrix}$$

Caas] simplify invert M(3)

$$\begin{bmatrix} \dfrac{x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,3}}{(x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,3})\,x_{1,1} + (x_{3,2}\,x_{2,1} - x_{3,1}\,x_{2,2})\,x_{1,3} + (x_{3,1}\,x_{2,3} - x_{3,3}\,x_{2,1})\,x_{1,2}} & \dfrac{(x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,} \\ \dfrac{x_{3,2}\,x_{1,3} - x_{3,3}\,x_{1,2}}{(x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,3})\,x_{1,1} + (x_{3,2}\,x_{2,1} - x_{3,1}\,x_{2,2})\,x_{1,3} + (x_{3,1}\,x_{2,3} - x_{3,3}\,x_{2,1})\,x_{1,2}} & \dfrac{(x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,} \\ \dfrac{x_{2,3}\,x_{1,2} - x_{2,2}\,x_{1,3}}{(x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,3})\,x_{1,1} + (x_{3,2}\,x_{2,1} - x_{3,1}\,x_{2,2})\,x_{1,3} + (x_{3,1}\,x_{2,3} - x_{3,3}\,x_{2,1})\,x_{1,2}} & \dfrac{(x_{3,3}\,x_{2,2} - x_{3,2}\,x_{2,} \end{bmatrix}$$

Caas]

Motivation (implementation in upcoming CAAS package, series)

```
Caas] e1 == exp series (0, x + y)
```

$$1 + (x+y)\,z + \frac{1}{2}\,(x+y)^2\,z^2 + \frac{1}{6}\,(x+y)^3\,z^3 + \frac{1}{24}\,(x+y)^4\,z^4 + \frac{1}{120}\,(x+y)^5\,z^5 + \frac{1}{720}\,(x+y)^6\,z^6 + \frac{1}{5040}\,(x+y)^7\,z^7 + \frac{1}{40320}\,(x+y)^8\,z^8 + \frac{1}{362880}\,(x+y)^9\,z^9 + O(z^{10})$$

```
Caas] e2 == exp series (0, x)
```

$$1 + x\,z + \frac{1}{2}\,x^2\,z^2 + \frac{1}{6}\,x^3\,z^3 + \frac{1}{24}\,x^4\,z^4 + \frac{1}{120}\,x^5\,z^5 + \frac{1}{720}\,x^6\,z^6 + \frac{1}{5040}\,x^7\,z^7 + \frac{1}{40320}\,x^8\,z^8 + \frac{1}{362880}\,x^9\,z^9 + O(z^{10})$$

```
Caas] e1 / e2
```

$$1+y\,z+\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)z^2+\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)z^3+\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)z^4+\left(\frac{1}{120}\,(x+y)^5-\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)x-\frac{1}{2}\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x^2-\frac{1}{6}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^3-\frac{1}{24}\,x^4\,y-\frac{1}{120}\,x^5\right)z^5+\left(-\left(\frac{1}{120}\,(x+y)^5-\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)x-\frac{1}{2}\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x^2-\frac{1}{6}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^3-\frac{1}{24}\,x^4\,y-\frac{1}{120}\,x^5\right)x-\frac{1}{2}\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)x^2-\frac{1}{6}\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x^3-\frac{1}{24}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^4+\frac{1}{720}\,(x+y)^6-\frac{1}{120}\,x^5\,y-\frac{1}{720}\,x^6\right)z^6+\left(-\left(-\left(\frac{1}{120}\,(x+y)^5-\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)x-\frac{1}{2}\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x^2-\frac{1}{6}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^3-\frac{1}{24}\,x^4\,y-\frac{1}{120}\,x^5\right)x-\frac{1}{2}\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)x^2-\frac{1}{6}\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x^3-\frac{1}{24}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^4+\frac{1}{720}\,(x+y)^6-\frac{1}{120}\,x^5\,y-\frac{1}{720}\,x^6\right)z^6+\left(-\left(-\left(\frac{1}{120}\,(x+y)^5-\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x-\frac{1}{2}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^2-\frac{1}{6}\,x^3\,y-\frac{1}{24}\,x^4\right)x-\frac{1}{2}\left(\frac{1}{6}\,(x+y)^3-\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x-\frac{1}{2}\,x^2\,y-\frac{1}{6}\,x^3\right)x^2-\frac{1}{6}\left(\frac{1}{2}\,(x+y)^2-\frac{1}{2}\,x^2-x\,y\right)x^3-\frac{1}{24}\,x^4\,y-\frac{1}{120}\,x^5\right)x-\frac{1}{2}\left(\frac{1}{24}\,(x+y)^4-\left(\frac{1}{6}\,(x+
$$

```
Caas] q == simplify (e1 / e2)
```

$$1 + y\,z + \frac{1}{2}\,y^2\,z^2 + \frac{1}{6}\,y^3\,z^3 + \frac{1}{24}\,y^4\,z^4 + \frac{1}{120}\,y^5\,z^5 + \frac{1}{720}\,y^6\,z^6 + \frac{1}{5040}\,y^7\,z^7 + \frac{1}{40320}\,y^8\,z^8 + \frac{1}{362880}\,y^9\,z^9 + O(z^{10})$$

```
Caas] q [15]
```

$$\frac{1}{1307674368000}\,y^{15}$$

```
Caas]
```

The problem

$\mathbb{K}$ field (usually $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$)

Input: an expression P^{expr} in $x_1, ..., x_n$, $+$, $-$, $\times$, $\div$ and constants in $\mathbb{K}$

Output: a sparse polynomial $P = \sum_{i=1}^{t} c_i \, x^{e_i}$ representing P^{expr} resp. P^{fun}

Optionally: a bound on t, or on $d = \deg P$, or on the $d_i = \deg_{x_i} P$

Note: in absence of a bound on t, we are satisfied with probabilistic algorithms

For instance, picking $x := \alpha$ random, we have $P^{\text{fun}}(\alpha) = 0 \Leftrightarrow P = 0$ with high probability

The problem

$\mathbb{K}$ field (usually $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$)

Input: $\begin{cases} \text{an expression } P^{\text{expr}} \text{ in } x_1, \ldots, x_n, +, -, \times, \div \text{ and constants in } \mathbb{K}; \text{ or} \\ \text{a function } P^{\text{fun}} \colon \mathbb{K}^n \to \mathbb{K} \end{cases}$

Output: a sparse polynomial $P = \sum_{i=1}^{t} c_i \, x^{e_i}$ representing P^{expr} resp. P^{fun}

Optionally: a bound on t, or on $d = \deg P$, or on the $d_i = \deg_{x_i} P$

Note: in absence of a bound on t, we are satisfied with probabilistic algorithms

For instance, picking $x := \alpha$ random, we have $P^{\text{fun}}(\alpha) = 0 \Leftrightarrow P = 0$ with high probability

The problem

$\mathbb{K}$ field (usually $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$)

Input: $\begin{cases} \text{an expression } P^{\text{expr}} \text{ in } x_1, \ldots, x_n, +, -, \times, \div \text{ and constants in } \mathbb{K}; \text{ or} \\ \text{a function } P^{\text{fun}} \colon \mathbb{K}^n \to \mathbb{K} \end{cases}$

Output: $\begin{cases} \text{a sparse polynomial } P = \sum_{i=1}^{t} c_i x^{e_i} \text{ representing } P^{\text{expr}} \text{ resp. } P^{\text{fun}}, \\ \text{where } c_i \in \mathbb{K} \setminus \{0\},\ e_i \in \mathbb{N}^n \text{ pairwise distinct; or } \perp \end{cases}$

Optionally: a bound on t, or on $d = \deg P$, or on the $d_i = \deg_{x_i} P$

Note: in absence of a bound on t, we are satisfied with probabilistic algorithms

For instance, picking $x := \alpha$ random, we have $P^{\text{fun}}(\alpha) = 0 \Leftrightarrow P = 0$ with high probability

Interface issue, classical variant

```
Caas] M == [ a, b; c, d ]
```

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

```
Caas] M * invert M
```

$$\begin{bmatrix} \left(\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a^2}+\frac{1}{a}\right)a-\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a} & 0 \\ \left(\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a^2}+\frac{1}{a}\right)c-\frac{c\,d}{\left(d-\frac{b\,c}{a}\right)a} & \frac{d}{d-\frac{b\,c}{a}}-\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a} \end{bmatrix}$$

```
Caas]
```

Interface issue, zero-simplified variant

```
Caas] M == [ force_simplify_zero a, b; c, d ]
```

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

```
Caas] M * invert M
```

$$\begin{bmatrix} \left(\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a^2}+\frac{1}{a}\right)a-\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a} & 0 \\ 0 & \frac{d}{d-\frac{b\,c}{a}}-\frac{b\,c}{\left(d-\frac{b\,c}{a}\right)a} \end{bmatrix}$$

```
Caas]
```

Assume (for known t)

$$P = \sum_{i=1}^{t} c_i \, x^{e_i}.$$

For all $\alpha \in \mathbb{K}^n$ we have

$$f(z) := \sum_{i \geqslant 0} P(\alpha_1^i, \ldots, \alpha_n^i) \, z^i = \sum_{1 \leqslant i \leqslant t} \frac{c_i}{1 - \alpha^{e_i} z}.$$

Choose α such that the α^{e_i} are pairwise distinct

Compute $c_1, \alpha^{e_1}, \ldots, c_t, \alpha^{e_t} \in \mathbb{K}$ from $f_0, \ldots, f_{2t-1}$

- Find $A, B \in \mathbb{K}[z]$ of degrees $< t$ with $f(z) = A(z) / B(z)$ using Padé-Hermite
- Find the roots $\alpha^{e_1}, \ldots, \alpha^{e_t}$ of B
- Solve linear Vandermonde system in order to get the c_i

Recover $e_1, \ldots, e_t$ from $\alpha^{e_1}, \ldots, \alpha^{e_t}$

Without bound for t, try for $t = 1, 2, 4, 8, 16, \ldots$

Prime numbers. [Ben-Or & Tiwari 1988], $\mathbb{K}$ characteristic zero

Take $\alpha_i = \pi_i$ (the i-th prime number)
Roots of integer polynomials can be computed fast
$\alpha^{e_i} \rightsquigarrow e_i$ *via* factoring

Modular arithmetic. [Kaltofen & Lakshman & Wiley 1990], DAGWOOD

Pick a prime p such that $\max_i \alpha^{e_i} < p$ (e.g. $\pi_n^d < p$)
Evaluate P using arithmetic modulo p only
Find roots of polynomials in $\mathbb{F}_p$ using Cantor-Zassenhaus or Moenck (if $p = k\,2^l + 1$)
$\alpha^{e_i} \rightsquigarrow e_i$ *via* factoring

Kronecker approach. [Javadi & Monagan 2010], [Arnold & Roche 2014]

Let $D_i \geqslant \deg_{x_i} P + 1$
Let $p > D_1 \cdots D_n$ and let ω be a primitive element in $\mathbb{F}_p$
Take $\alpha = (1, \omega^{D_1}, \omega^{D_1 D_2}, \ldots, \omega^{D_1 \cdots D_{n-1}})$
Find roots of polynomials in $\mathbb{F}_p$ using Cantor-Zassenhaus or Moenck
$\alpha^{e_i} = \omega^{\Pi \cdot e_i} \rightsquigarrow e_i$ *via* discrete logarithm (fast if $p = k\,2^l + 1$)

Let $Q(x_{m+1},\dots,x_n) = P(\alpha_1,\dots,\alpha_m,x_{m+1},\dots,x_n)$ for random α

Problem: assuming $\operatorname{supp} Q = \{f_1,\dots,f_u\}$ known, efficiently recover $\operatorname{supp} P$

Hope: possible using a much smaller p (fitting in one word)

Coefficient ratios. [Javadi & Monagan, slightly different context], $\pi_1^{e_{i,1}}\cdots\pi_m^{e_{i,m}} < p$

$$\begin{aligned} f(x_1,\dots,x_n) &\rightsquigarrow c_i,\alpha^{e_i} \\ f(\pi_1 x_1,\dots,\pi_m x_m,x_{m+1},\dots,x_n) &\rightsquigarrow \pi_1^{e_{i,1}}\cdots\pi_m^{e_{i,m}} c_i,\alpha^{e_i} \rightsquigarrow e_{i,\leqslant m} := (e_{i,1},\dots,e_{i,m}) \\ \alpha^{e_i - e_{i,\leqslant m}},\operatorname{supp} Q &\rightsquigarrow e_i \end{aligned}$$

Works also for Kronecker approach

Closest point projections. $\alpha = \left(1,\omega^{D_1},\dots,\omega^{D_1\cdots D'_m\cdots D_{n-1}}\right)$, $D'_m > D_m$ random

Consider $\varphi_i \in \{0,\dots,p-2\}$ with $\alpha^{f_i} = \omega^{\varphi_i}$

The φ_i modulo $p-1$ are essentially random with minimal distance $\delta \approx p/u^2$

Assume $D_1\cdots D_m < \delta$

For any $e_i \in \operatorname{supp} P$ and ψ_i with $\alpha^{e_i} = \omega^{\psi_i}$, $\exists!\varphi_{i'}$ with $\psi_i - \varphi_{i'} < \delta$ (modulo $p-1$)

Example: determinant of a matrix

Problem: interpolate generic $k \times k$ determinant

$$P = \begin{vmatrix} x_{1,1} & \cdots & x_{1,k} \\ \vdots & & \vdots \\ x_{k,1} & \cdots & x_{k,k} \end{vmatrix}$$

Interesting parameters, since

$$\begin{aligned} n &= k^2 \\ t &= k! \\ d &= k \\ d_i &= 1 \end{aligned}$$

n	4	5	6	7	8	9	10	11	12
Bound $\log_2 p$ (primes)	23	33	44	55	67	79	91	104	117
Bound $\log_2 p$ (Kronecker)	16	25	36	49	64	81	100	121	144

Implementation in MULTIMIX package

```
Mmx] use "multimix";
```

```
Mmx] n == 4;
```

```
Mmx] M == [ polynomial_dag (1 :> Integer, coordinate ('x[i,j])) |
            i in 1 to n || j in 1 to n ]
```

$$\begin{bmatrix} x_{1,1} & x_{2,1} & x_{3,1} & x_{4,1} \\ x_{1,2} & x_{2,2} & x_{3,2} & x_{4,2} \\ x_{1,3} & x_{2,3} & x_{3,3} & x_{4,3} \\ x_{1,4} & x_{2,4} & x_{3,4} & x_{4,4} \end{bmatrix}$$

```
Mmx] D == det M
```

$$-(x_{1,4}\,x_{4,1} + x_{2,4}\,x_{4,2} + x_{3,4}\,x_{4,3})\,(-x_{1,3}\,x_{3,1} - x_{2,3}\,x_{3,2} - x_{3,3}\,(-x_{2,2} - x_{1,1}) - x_{1,2}\,x_{2,1} + x_{2,2}\,x_{1,1}) - (x_{1,4}\,(x_{1,1}\,x_{4,1} + x_{2,1}\,x_{4,2} + x_{3,1}\,x_{4,3}) + x_{2,4}\,(x_{1,2}\,x_{4,1} + x_{2,2}\,x_{4,2} + x_{3,2}\,x_{4,3}) + x_{3,4}\,(x_{1,3}\,x_{4,1} + x_{2,3}\,x_{4,2} + x_{3,3}\,x_{4,3}))\,(-x_{3,3} - x_{2,2} - x_{1,1}) - x_{1,4}\,(x_{1,1}\,(x_{1,1}\,x_{4,1} + x_{2,1}\,x_{4,2} + x_{3,1}\,x_{4,3}) + x_{2,1}\,(x_{1,2}\,x_{4,1} + x_{2,2}\,x_{4,2} + x_{3,2}\,x_{4,3}) + x_{3,1}\,(x_{1,3}\,x_{4,1} + x_{2,3}\,x_{4,2} + x_{3,3}\,x_{4,3})) - x_{2,4}\,(x_{1,2}\,(x_{1,1}\,x_{4,1} + x_{2,1}\,x_{4,2} + x_{3,1}\,x_{4,3}) + x_{2,2}\,(x_{1,2}\,x_{4,1} + x_{2,2}\,x_{4,2} + x_{3,2}\,x_{4,3}) + x_{3,2}\,(x_{1,3}\,x_{4,1} + x_{2,3}\,x_{4,2} + x_{3,3}\,x_{4,3})) - x_{3,4}\,(x_{1,3}\,(x_{1,1}\,x_{4,1} + x_{2,1}\,x_{4,2} + x_{3,1}\,x_{4,3}) + x_{2,3}\,(x_{1,2}\,x_{4,1} + x_{2,2}\,x_{4,2} + x_{3,2}\,x_{4,3}) + x_{3,3}\,(x_{1,3}\,x_{4,1} + x_{2,3}\,x_{4,2} + x_{3,3}\,x_{4,3})) - x_{4,4}\,(-(x_{1,3}\,x_{3,1} + x_{2,3}\,x_{3,2})\,(-x_{2,2} - x_{1,1}) - x_{1,3}\,(x_{1,1}\,x_{3,1} + x_{2,1}\,x_{3,2}) - x_{2,3}\,(x_{1,2}\,x_{3,1} + x_{2,2}\,x_{3,2}) - x_{3,3}\,(-x_{1,2}\,x_{2,1} + x_{2,2}\,x_{1,1}))$$

```
Mmx] as_mvpolynomial% (D)
```

$$x_{1,1}\,x_{2,2}\,x_{3,3}\,x_{4,4} - x_{1,2}\,x_{2,1}\,x_{3,3}\,x_{4,4} - x_{1,1}\,x_{2,3}\,x_{3,2}\,x_{4,4} + x_{1,3}\,x_{2,1}\,x_{3,2}\,x_{4,4} + x_{1,2}\,x_{2,3}\,x_{3,1}\,x_{4,4} - x_{1,3}\,x_{2,2}\,x_{3,1}\,x_{4,4} - x_{1,1}\,x_{2,2}\,x_{3,4}\,x_{4,3} + x_{1,2}\,x_{2,1}\,x_{3,4}\,x_{4,3} + x_{1,1}\,x_{2,4}\,x_{3,2}\,x_{4,3} - x_{1,4}\,x_{2,1}\,x_{3,2}\,x_{4,3} - x_{1,2}\,x_{2,4}\,x_{3,1}\,x_{4,3} + x_{1,4}\,x_{2,2}\,x_{3,1}\,x_{4,3} + x_{1,1}\,x_{2,3}\,x_{3,4}\,x_{4,2} - x_{1,3}\,x_{2,1}\,x_{3,4}\,x_{4,2} - x_{1,1}\,x_{2,4}\,x_{3,3}\,x_{4,2} + x_{1,4}\,x_{2,1}\,x_{3,3}\,x_{4,2} + x_{1,3}\,x_{2,4}\,x_{3,1}\,x_{4,2} - x_{1,4}\,x_{2,3}\,x_{3,1}\,x_{4,2} - x_{1,2}\,x_{2,3}\,x_{3,4}\,x_{4,1} + x_{1,3}\,x_{2,2}\,x_{3,4}\,x_{4,1} + x_{1,2}\,x_{2,4}\,x_{3,3}\,x_{4,1} - x_{1,4}\,x_{2,2}\,x_{3,3}\,x_{4,1} - x_{1,3}\,x_{2,4}\,x_{3,2}\,x_{4,1} + x_{1,4}\,x_{2,3}\,x_{3,2}\,x_{4,1}$$

```
Mmx]
```

```
template<int n> integer
det_modulo (const vector<integer>& v /* n x n matrix coefficients */,
            const integer& p);
```

```
template<int n> void
print_generic_determinant () {
  function_2<integer, const vector<integer>&, const integer&>
    f (&det_modulo<n>);
  sparse_polynomial<integer> pol =
    pr_as_sparse_polynomial (f, n*n, n /* degree bound */);
  mmout << pol << lf;
}
```

n	5	6	7	8
Kronecker substitution	110 ms	915 ms	9.8 s	162 s

Table 1. Timings for interpolating the determinant polynomial of a $n \times n$ matrix.