ACA 2023, Warsaw, (Poland),
July 2023

How a linear recurrence problem inspired a solution in algebraic geometry

Catherine St-Pierre

catherine.st-pierre@uwaterloo.ca
UWaterloo, CA
Inria Saclay, FR

The original problem

(Hyun, Melczer, Schost & S. '19) Finding the n^{th} element of a linear recurrent sequence:

$$a_{i+d} = \sum_{j=0}^{d-1} c_j a_{i+j}$$

Given $a_0, \ldots, a_{d-1}, c_j \in \mathbb{K}$, a field, find a_n.

The original problem

(Hyun, Melczer, Schost & S. '19) Finding the n^{th} element of a linear recurrent sequence:

$$a_{i+d} = \sum_{j=0}^{d-1} c_j a_{i+j} \longleftrightarrow P = x^d - \sum_{j=0}^{d-1} c_j x^j$$

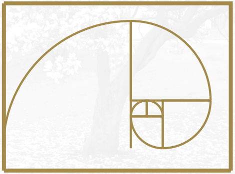
Given $a_0, \ldots, a_{d-1}, c_j \in \mathbb{K}$, a field, find a_n.

e.g. Fibonacci sequence

$$a_{i+2} = a_i + a_{i+1}$$

$$P = x^2 - x - 1$$

$$a_0 = 1, \qquad a_1 = 1$$



The original problem

(Hyun, Melczer, Schost & S. '19) Finding the n^{th} element of a linear recurrent sequence:

$$a_{i+d} = \sum_{j=0}^{d-1} c_j a_{i+j} \longleftrightarrow P = x^d - \sum_{j=0}^{d-1} c_j x^j$$

Given $a_0, \ldots, a_{d-1}, c_j \in \mathbb{K}$, a field, find a_n.

1966
Miller
Spencer Brown
$O(\mathrm{d}^\omega \log(\mathrm{n}))$

$$\begin{bmatrix} a_1 \\ \vdots \\ a_{d+1} \end{bmatrix} = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ c_0 & c_1 & \ldots & c_d \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_d \end{bmatrix}$$

The original problem

(Hyun, Melczer, Schost & S. '19) Finding the n^{th} element of a linear recurrent sequence:

$$a_{i+d} = \sum_{j=0}^{d-1} c_j a_{i+j} \longleftrightarrow P = x^d - \sum_{j=0}^{d-1} c_j x^j$$

Given $a_0, \ldots, a_{d-1}, c_j \in \mathbb{K}$, a field, find a_n.

1966
Miller
Spencer Brown
$O(\mathrm{d}^\omega \log(\mathrm{n}))$

$$\begin{bmatrix} a_n \\ \vdots \\ a_{n+d} \end{bmatrix} = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ c_0 & c_1 & \ldots & c_d \end{bmatrix}^n \begin{bmatrix} a_0 \\ \vdots \\ a_d \end{bmatrix}$$

The original problem

(Hyun, Melczer, Schost & S. '19) Finding the n^{th} element of a linear recurrent sequence:

$$a_{i+d} = \sum_{j=0}^{d-1} c_j a_{i+j} \longleftrightarrow P = x^d - \sum_{j=0}^{d-1} c_j x^j$$

Given $a_0, \ldots, a_{d-1}, c_j \in \mathbb{K}$, a field, find a_n.

- 1966 — Miller, Spencer Brown — $O(\mathrm{d}^\omega \log(\mathrm{n}))$
- 1985 — Fiduccia — $O(\mathrm{M}(\mathrm{d}) \log(\mathrm{n}))$
- 2019
- 2020 — Bostan, Mori — $O(\mathrm{M}(\mathrm{d}) \log(\mathrm{n}))$

Recall Fiduccia's idea

Using the annihilating polynomial of the sequence, define

$$P = x^d - \sum_{i=1}^{d-1} c_i x^i$$

Let

$$l : \mathbb{K}[x]/\langle P \rangle \to \mathbb{K}$$

with $l(x^i) = a_i$ for $i \in [0, d-1]$

$$\implies l(x^n) = a_n$$

Recall Fiduccia's idea

Using the annihilating polynomial of the sequence, define

$$P = x^d - \sum_{i=1}^{d-1} c_i x^i$$

Let

$$l : \mathbb{K}[x]/\langle P \rangle \to \mathbb{K}$$

with $l(x^i) = a_i$ for $i \in [0, d-1]$

$$\Longrightarrow \quad l(x^n) = a_n$$

Recall Fiduccia's idea

Using the annihilating polynomial of the sequence, define

$$P = x^d - \sum_{i=1}^{d-1} c_i x^i$$

Let

$$l : \mathbb{K}[x]/\langle P \rangle \to \mathbb{K}$$

with $l(x^i) = a_i$ for $i \in [0, d-1]$

$$\implies l(x^n) = a_n$$

Recall Fiduccia's algorithm

Thus we find $x^n \mod P$ as $R = r_0 + \cdots + r_{d-1}x^{d-1}$, where

$$a_n = r_0 a_0 + \cdots + r_{d-1} a_{d-1}.$$

Resulting in an overall complexity $O(\mathrm{M(d)\log(n)})$.

The original problem (bivariate)

Given *bivariate* recurrent sequence:

$$\sum_{i,j} a_{i,j} x^i y^j = N(x,y)/Q(x,y),$$

for some $N, Q \in \mathbb{K}[x,y]$ with $Q(0,0) \neq 0$.

- The j-th row $\sum_i a_{i,j} x^i$ has characteristic polynomial P^j, where P is the reverse polynomial of $Q(x,0)$ (Bostan, Caruso, Christol & Dumas '18).

When P is not squarefree

Factorise $P = \prod_i Q_i^{m_i}$ (degree d) with Q_i (degree d_i) squarefree.

When P is not squarefree

Factorise $P = \prod_i Q_i^{m_i}$ (degree d) with Q_i (degree d_i) squarefree.

$$x^n \mod P$$

$$x^n \mod Q_1^{m_1} \qquad \dots \qquad x^n \mod Q_s^{m_s}$$

$$CRT$$

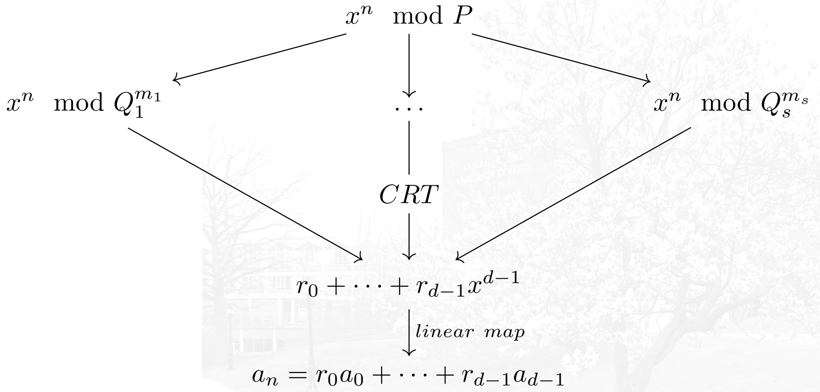
$$r_0 + \cdots + r_{d-1}x^{d-1}$$

$$\downarrow \; linear\ map$$

$$a_n = r_0 a_0 + \cdots + r_{d-1} a_{d-1}$$

When P is not squarefree

Factorise $P = \prod_i Q_i^{m_i}$ (degree d) with Q_i (degree d_i) squarefree.



We want to find the $R_i = x^n \mod Q_i^{m_i}$ efficiently !

Untangling

Theorem (van der Hoeven and Lecerf '17)
Define $\mathbb{F} = \mathbb{K}[\alpha] = \mathbb{K}[y]/Q_i(y)$, separable, then

$$\begin{array}{rccc} \pi_{Q_i,m_i}: & \mathbb{K}[x]/\langle Q_i^{m_i}(x)\rangle & \to & \mathbb{F}[\xi]/\langle \xi^{m_i}\rangle \\ & x & \mapsto & \xi + \alpha \end{array}$$

is a $\mathbb{K}$-algebra isomorphism if $m_i \leq char(\mathbb{K})$.

Untangling

Theorem (van der Hoeven and Lecerf '17)
Define $\mathbb{F} = \mathbb{K}[\alpha] = \mathbb{K}[y]/Q_i(y)$, separable, then

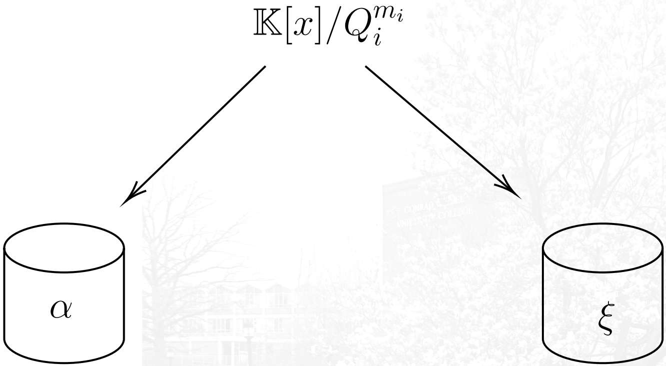
$$\begin{array}{rccc} \pi_{Q_i,m_i}: & \mathbb{K}[x]/\langle Q_i^{m_i}(x)\rangle & \to & \mathbb{F}[\xi]/\langle \xi^{m_i}\rangle \\ & x & \mapsto & \xi + \alpha \end{array}$$

is a $\mathbb{K}$-algebra isomorphism if $m_i \leq char(\mathbb{K})$.

$$\pi_{Q_i,m_i}(f) = \sum_{0 \leq j < m_i} f^{(j)}(\alpha)\xi^j/j!$$

(Taylor expansion)

Untangling



separable extension (roots)

local structure (mutiplicity)

Untangling

Theorem (van der Hoeven and Lecerf '17)
Define $\mathbb{F} = \mathbb{K}[\alpha] = \mathbb{K}[y]/Q_i(y)$, separable, then

$$\begin{array}{rccc} \pi_{Q_i,m_i}: & \mathbb{K}[x]/\langle Q_i^{m_i}(x)\rangle & \to & \mathbb{F}[\xi]/\langle \xi^{m_i}\rangle \\ & x & \mapsto & \xi + \alpha \end{array}$$

is a $\mathbb{K}$-algebra isomorphism if $m_i \leq char(\mathbb{K})$.

e.g. $\mathbb{K} = \mathbb{Q}$, $Q_i = x^2 - x - 1$ and $m_i = 2$

$$\mathbb{Q}[x]/\langle x^4 - 2x^3 - x^2 + 2x + 1\rangle \cong \mathbb{F}[\xi]/\langle \xi^2\rangle$$

where $\mathbb{F} = \mathbb{Q}[y]/Q_i$

Untangling

Theorem (van der Hoeven and Lecerf '17)
Define $\mathbb{F} = \mathbb{K}[\alpha] = \mathbb{K}[y]/Q_i(y)$, separable, then

$$\begin{array}{rccc} \pi_{Q_i,m_i}: & \mathbb{K}[x]/\langle Q_i^{m_i}(x)\rangle & \to & \mathbb{F}[\xi]/\langle \xi^{m_i}\rangle \\ & x & \mapsto & \xi + \alpha \end{array}$$

is a $\mathbb{K}$-algebra isomorphism if $m_i \leq char(\mathbb{K})$.

- $\pi : O(M(d_i m_i)\log(m_i))$
  (van der Hoeven & Lecerf '17)
- $\pi^{-1} : O(M(d_i m_i)\log(m_i) + M(d_i)\log(d_i))$
  (Hyun, Melczer, Schost & S. '19)

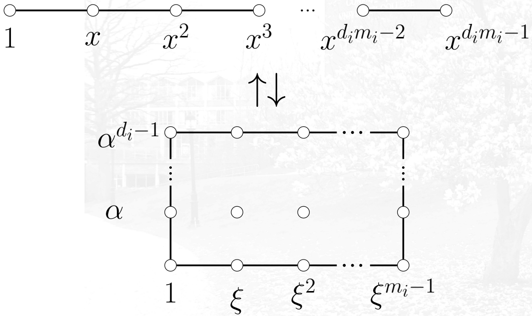
Finding $x^n \mod Q_i^{m_i}$

$$
\begin{aligned}
x^n \bmod Q_i^{m_i} &= \pi_i^{-1}((\xi - \alpha)^n) \text{ with } \mathbb{K}[\alpha][\xi]/\xi^{m_i} = (\mathbb{K}[y]/Q_i(y))[\xi]/\xi^{m_i} \\
&= \pi_i^{-1}\left(\sum_{i=0}^{m_i-1} \binom{n}{i} \xi^i \alpha^{n-i}\right).
\end{aligned}
$$

Finding $x^n \mod Q_i^{m_i}$

$$x^n \bmod Q_i^{m_i} = \pi_i^{-1}((\xi - \alpha)^n) \text{ with } \mathbb{K}[\alpha][\xi]/\xi^{m_i} = (\mathbb{K}[y]/Q_i(y))[\xi]/\xi^{m_i}$$

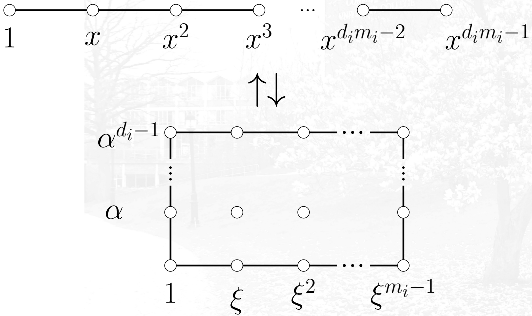
$$= \pi_i^{-1}\left(\sum_{i=0}^{m_i-1} \binom{n}{i} \xi^i \alpha^{n-i}\right).$$



Finding $x^n \mod Q_i^{m_i}$

$$x^n \bmod Q_i^{m_i} = \pi_i^{-1}((\xi - \alpha)^n) \text{ with } \mathbb{K}[\alpha][\xi]/\xi^{m_i} = (\mathbb{K}[y]/Q_i(y))[\xi]/\xi^{m_i}$$

$$= \pi_i^{-1}\left(\sum_{i=0}^{m_i - 1} \binom{n}{i} \xi^i \alpha^{n-i} \right).$$



Overall Complexity

$$
\begin{aligned}
P = \prod_{i \le s} Q_i^{m_i} : \quad & O(M(\sum_i d_i m_i) \log(\sum_i d_i m_i)) \\
\alpha^{n-*} \bmod Q_i : \quad & O(M(d_i)(\log(n) + m_i) \\
\pi^{-1} : \quad & O(M(d_i)(m_i) \log(d_i m_i))
\end{aligned}
$$

total: $O(M(\sum_i d_i) \log(n) + M(d) \log(d))$

Fiducciа: $O(M(\sum_i d_i m_i) \log(n))$

Further applications

- $x^n \mod Q_i^{m_i}$ (+ CTR)
- M^i for M a square matrix (Ranum 1911, Giesbrecht '95);
- $f(g) \mod h^i$ (van der Hoven & Lecerf '17);
- Solving singular points (Lebreton, Mehrabi & Schost '13)

$$F(x_1, x_2, x_3) = G(x_1, x_2, x_3) = 0$$

$$\langle F, G \rangle = \subseteq \mathbb{Q}(x_1)[x_2, x_3]$$

$$V(\langle F, G \rangle) = V(\langle S, Ux_3 - T \rangle)$$

Further applications

- $x^n \mod Q_i^{m_i}$ (+ CTR)
- M^i for M a square matrix (Ranum 1911, Giesbrecht '95);
- $f(g) \mod h^i$ (van der Hoven & Lecerf '17);
- Solving singular points (Lebreton, Mehrabi & Schost '13)

$$F(x_1, x_2, x_3) = G(x_1, x_2, x_3) = 0$$

$$\langle F, G\rangle = \sqrt{\langle F, G\rangle} \subseteq \mathbb{Q}(x_1)[x_2, x_3]$$

$$V(\langle F, G\rangle) = V(\langle S, Ux_3 - T\rangle)$$

Further applications

- $x^n \mod Q_i^{m_i}$ (+ CTR)
- M^i for M a square matrix (Ranum 1911, Giesbrecht '95);
- $f(g) \mod h^i$ (van der Hoven & Lecerf '17);
- Solving singular points (Lebreton, Mehrabi & Schost '13)

$$F(x_1, x_2, x_3) = G(x_1, x_2, x_3) = 0$$

$$\langle F, G \rangle = \cancel{\sqrt{\langle F, G \rangle}} \subseteq \mathbb{Q}(x_1)[x_2, x_3]$$

$$V(\langle F, G \rangle) = V(\langle S, Ux_3 - T \rangle)$$

Connection to algebraic geometry

van der Hoeven and Lecerf pointed out that map

- separates the roots from the multiplicity structure
- preserves the **local structure**

(Appeal) CRT $\rightsquigarrow$ For zero-dimensional ideal $I \subseteq R$, for R a ring, we can use π on all the primary components in other context for R/I.

Connection to algebraic geometry

van der Hoeven and Lecerf pointed out that map

- separates the roots from the multiplicity structure
- preserves the **local structure**

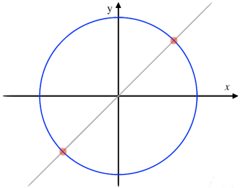
(Appeal) CRT $\rightsquigarrow$ For zero-dimensional ideal $I \subseteq R$, for R a ring, we can use π on all the primary components in other context for R/I.

Motivation

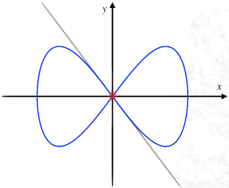
- algebraic geometry
  - *points of the intersections* (maximal ideal in $\mathbb{K}[x,y]/I$)
  - *local structure*: the regular functions at a point p (characterized by $\mathbb{K}[x,y]_p/I_p$)

Applications: local invariants of singular points, algebraic operations on the roots, topology of curves or degree of polynomial maps, analysis of ODEs and PDEs, local isomorphisms ...

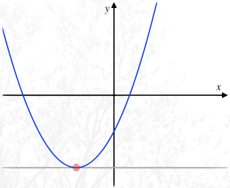
Intersections of plane curves



$$V(\langle x - y, x^2 + y^2 - 1\rangle)$$
$$= \{(-\tfrac{1}{\sqrt{2}}, -\tfrac{1}{\sqrt{2}}), (\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}})\}$$



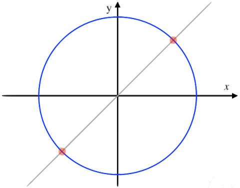
$$V(\langle y^2 + x^4 - x^2, y + x\rangle)$$
$$= \{(0, 0)\}$$



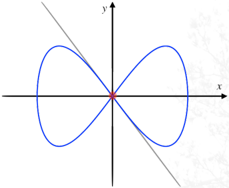
$$V(\langle y - x^2 - 2x + 1, y + 2\rangle)$$
$$= \{(-1, -2)\}$$

Marinari, Möller & Mora '96 presented that the geometric problem can be addressed via Gröbner Bases, border bases and inverse systems.

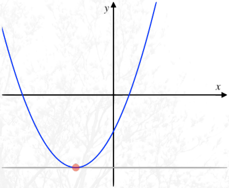
Intersections of plane curves



$$V(\langle x - y, x^2 + y^2 - 1\rangle) = \{(-\tfrac{1}{\sqrt{2}}, -\tfrac{1}{\sqrt{2}}), (\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}})\}$$



$$V(\langle y^2 + x^4 - x^2, y + x\rangle) = \{(0,0)\}$$



$$V(\langle y - x^2 - 2x + 1, y + 2\rangle) = \{(-1,-2)\}$$

Marinari, Möller & Mora '96 presented that the geometric problem can be addressed via Gröbner Bases, border bases and inverse systems.

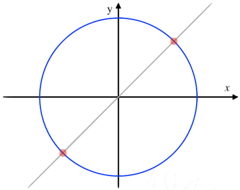
Bivariate setting

Theorem (Hyun, Melczer, Schost & S. '19)
Let $Q \subseteq \mathbb{K}[x,y]$ be a primary ideal. If $\mathbb{L} = \mathbb{K}[x,y]/\sqrt{Q}$ is separable, then there exists a $\mathbb{K}$-algebra isomorphism

$$\pi : \mathbb{K}[x,y]/Q \cong \mathbb{L}[x,y]/J$$

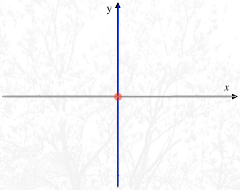
with J $\langle x,y \rangle$-primary.

Example untangling



$$I = \langle x - y, x^2 + y^2 - 1 \rangle$$

$$V(I) = \{(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}), (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})\}$$

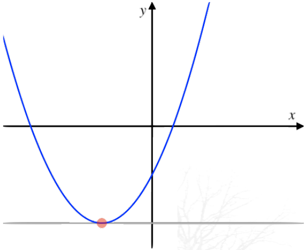


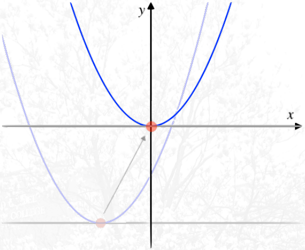
$$J = \langle x, y \rangle$$

$$V(J) = \{(0,0)\}$$

$$\mathbb{Q}[x,y]/I \cong \mathbb{Q}[\frac{1}{\sqrt{2}}][x,y]/J$$

Example untangling





$$I = \langle y - x^2 + 1, y + 2 \rangle \qquad J = \langle y - x^2, y \rangle$$

$$V(I) = \{(-1,-2)\} \qquad V(J) = \{(0,0)\}$$

$$\mathbb{Q}[x,y]/I \cong \mathbb{Q}[x,y]/J$$

Break down π

(Neiger, Rahkooy & Schost '17) Let $\mathbb{F} = \mathbb{Q}$, $T_1 = x^2 + x + 2$, $T_2 = y - x - 1$, and $I = \langle T_1, T_2 \rangle^2$

$$y^2 - 2xy - 2y + x^2 + 2x + 1,$$
$$x^2y + xy + 2y - x^3 - 2x^2 - 3x - 2,$$
$$x^4 + 2x^3 + 5x^2 + 4x + 4.$$

Break down π

(Neiger, Rahkooy & Schost '17) Let $\mathbb{F} = \mathbb{Q}$,
$T_1 = x^2 + x + 2$, $T_2 = y - x - 1$, and $I = \langle T_1, T_2 \rangle^2$

(extension of field) $\mathbb{K} = \mathbb{Q}[\alpha_1, \alpha_2]$, where α_1 to be the residue class of x in $\mathbb{Q}[x]/\langle x_1^2 + x_1 + 2 \rangle$ and $\alpha_2 = \alpha_1 + 1$ (residue class of y)

The $\langle \alpha_1, \alpha_2 \rangle$-primary the extension of I in $\mathbb{K}[\xi_1, \xi_2]$ is

$$\xi_2^2 - 2\xi_2\alpha_1 - 2\xi_2 + \alpha_1 - 1,$$
$$\xi_1\xi_2 - \xi_2\alpha_1 - \xi_1\alpha_1 - \xi_1 - 2,$$
$$\xi_1^2 - 2\xi_1\alpha_1 - \alpha_1 - 2.$$

Break down π

(Neiger, Rahkooy & Schost '17) Let $\mathbb{F} = \mathbb{Q}$, $T_1 = x^2 + x + 2$, $T_2 = y - x - 1$, and $I = \langle T_1, T_2 \rangle^2$

(shift) translating $(\xi_1, \xi_2) \mapsto (\xi_1 + \alpha_1, \xi_2 + \alpha_2)$ the primary becomes

$$\xi_2^2$$
$$\xi_1 \xi_2$$
$$\xi_1^2$$

(extension of field) $+$ **(shift)** $= \pi$

Key features

- Points with the same local structure are bound at the origin under π;
- π preserves the local structure of the points.

Local stucture of intersections of curves

Let $\mathbb{K}$ be a field *similar* to $\mathbb{Q}$.

Theorem (Schost & S. '23) The Gröbner basis of P the $\langle x, y \rangle$-primary component of $I \subseteq \mathbb{K}[x, y]$ in a time (binary operations) softly linear in $(\dim_{\mathbb{K}} \mathbb{K}[x, y]/P)^{\omega}$.

We taylored a Newton iterator that relies on a structural result about the syzygies in such a basis due to Conca & Valla '08, from which arises an explicit map between ideals in a Gröbner cell and points in the associated moduli space.

Gröbner Cell

Definition: Let E be a monomial ideal, then

$$\mathcal{C}(E) = \{I : in(I) = E\}$$

is the Gröbner cell of E.

Theorem:(Conca & Valla '08) there exists an explicit bijection

$$\mathbb{K}^N \xrightarrow{\phi_E} \mathcal{C}(E)$$

$N \in O(\delta)$ where δ is the degree of E

Bijection with the moduli space

The bijection is defined via by a parametric Gröbner basis $\mathcal{G}_E = (g_1, \ldots g_s)$ such that $g_i \in \mathbb{K}[\lambda_1, \ldots, \lambda_N][x, y]$

$$\begin{array}{ccc} \mathbb{K}^N & \xrightarrow{\phi_E} & \mathcal{C}(E) \\ (p_1, \ldots, p_N) & \xrightarrow{\phi_E} & \langle g_i(p_1, \ldots, p_N) | g_i \in \mathcal{G}_E \rangle \end{array}$$

e.g. $E = \langle y^3, xy, x^5 \rangle$

$$\mathcal{G}_E = y^3 - \lambda_2 y^2 x^2 + [...] + (+\lambda_3\lambda_8 - \lambda_5)x^2, \quad yx^3 - \lambda_8 x^4, \quad x^5$$

$$\phi((1,0,0,0,0,0,5,6)) = \langle y^3 + 6yx^2 + 3x^4, yx^3 + x^4, x^5 \rangle$$

Newton iterator

Theorem (Schost & S. '23) Let P the $\langle x, y\rangle$-primary component of $I = \langle \mathcal{F} \rangle \subseteq \mathbb{K}[x, y]$. Let $J \subseteq \mathbb{K}[\lambda_1, \ldots, \lambda_N]$ be the ideal generated by the **coefficients** of $\mathcal{F} \mod \mathcal{G}_{in(P)}$. Then

$$\phi_{in(P)}^{-1}(P) \in V(J) \subset \mathbb{K}^N$$

is smooth.

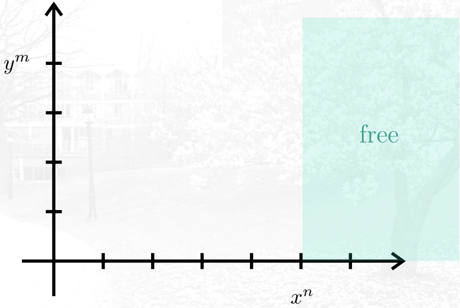
Consequences of π

The positive side of the medal

- Reduce arithmetic (mostly modular with a Gröbner basis);

vs

$\mathbb{K}[x,y]/\langle f_1, \ldots, f_t \rangle$ $\qquad$ $\mathbb{K}[x,y]/\langle y^m + f, \ldots, x^n \rangle$



Consequences of π

The positive side of the medal

- Reduce arithmetic (mostly modular with a Gröbner basis);
- Simplified the isolation of the primary component;

---

e.g. if we are in generic coordinates adding a generator x^i, for i *large enough*, isolate the primary component.

Consequences of π

The positive side of the medal

- Reduce arithmetic (mostly modular with a Gröbner basis);
- Simplified the isolation of the primary component;
- Gain on the complexity (degree ideals);
- Highlights the local structure;
- Fewer parameters required

The other side of the medal

- Base field enlarged.

Thank you for your attention.