Fast modular composition using spiroids

Joris van der Hoeven

Joint work with Grégoire Lecerf

CNRS, École polytechnique, France

Funded by the European Union

European Research Council

Established by the European Commission

PolSys seminar

February 20, 2026

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

$\longrightarrow$ Interesting special moduli: $R = x^n$, $R = R_1 \cdots R_n$

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

$\longrightarrow$ Interesting special moduli: $R = x^n$, $R = R_1 \cdots R_n$

$\longrightarrow$ Kaltofen–Shoup 1997: application to factorization in $\mathbb{F}_q[x]$

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

$\longrightarrow$ Interesting special moduli: $R = x^n$, $R = R_1 \cdots R_n$

$\longrightarrow$ Kaltofen–Shoup 1997: application to factorization in $\mathbb{F}_q[x]$

$\longrightarrow$ Various generalizations, e.g. $P \in \mathbb{A}[u_1, \dots, u_n]$, $Q = (Q_1, \dots, Q_n) \in \mathbb{A}[x]^n$

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

$\longrightarrow$ Interesting special moduli: $R = x^n$, $R = R_1 \cdots R_n$

$\longrightarrow$ Kaltofen–Shoup 1997: application to factorization in $\mathbb{F}_q[x]$

$\longrightarrow$ Various generalizations, e.g. $P \in \mathbb{A}[u_1, \dots, u_n]$, $Q = (Q_1, \dots, Q_n) \in \mathbb{A}[x]^n$

vdH–Lecerf 2021: application to geometric resolution of polynomial systems

The problem

Input: polynomials $P, Q, R \in \mathbb{A}[x]$ with R monic, $\mathbb{A}$: ring

Output: $P \circ Q \operatorname{rem} R$

$\longrightarrow$ Interesting special cases: $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/r\mathbb{Z}, \mathbb{Z}_p, \Bbbk[[z]], \dots\}$

$\longrightarrow$ Interesting special moduli: $R = x^n$, $R = R_1 \cdots R_n$

$\longrightarrow$ Kaltofen–Shoup 1997: application to factorization in $\mathbb{F}_q[x]$

$\longrightarrow$ Various generalizations, e.g. $P \in \mathbb{A}[u_1, \dots, u_n]$, $Q = (Q_1, \dots, Q_n) \in \mathbb{A}[x]^n$

vdH–Lecerf 2021: application to geometric resolution of polynomial systems

$\longrightarrow$ Fundamental: cost of "polynomial evaluation" in algebraic extensions $\mathbb{A}[x]/(R)$

Complexity bounds

General rings $\mathbb{A}$

$\deg P, \deg Q, \deg R \leqslant D$

Complexity bounds

General rings $\mathbb{A}$

$\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$

Complexity bounds

General rings $\mathbb{A}$ $\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$

Complexity bounds

General rings $\mathbb{A}$ $\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$

Complexity bounds

General rings $\mathbb{A}$ $\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Complexity bounds

General rings $\mathbb{A}$

$\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Special rings $\mathbb{A}$

Complexity bounds

General rings $\mathbb{A}$

$\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Special rings $\mathbb{A}$

- Kedlaya–Umans 2008: $D^{1+o(1)}$ if $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$ or $\mathbb{A} = \mathbb{Z}$

Complexity bounds

General rings $\mathbb{A}$ $\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Special rings $\mathbb{A}$

- Kedlaya–Umans 2008: $D^{1+o(1)}$ if $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$ or $\mathbb{A} = \mathbb{Z}$

  refinement vdH–Lecerf 2020: $\mathrm{e}^{\sqrt{(28+o(1))\log D\,\log\log D}}\,\tilde{O}(D \log r)$

Complexity bounds

General rings $\mathbb{A}$

$\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Special rings $\mathbb{A}$

- Kedlaya–Umans 2008: $D^{1+o(1)}$ if $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$ or $\mathbb{A} = \mathbb{Z}$

  refinement vdH–Lecerf 2020: $\mathrm{e}^{\sqrt{(28+o(1))\log D \log\log D}}\,\tilde{O}(D \log r)$
- vdH–Lecerf 2020 (Ritzmann 1986), $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{C}\}$ large precision: $\tilde{O}(D)$

Complexity bounds

General rings $\mathbb{A}$ $\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Special rings $\mathbb{A}$

- Kedlaya–Umans 2008: $D^{1+o(1)}$ if $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$ or $\mathbb{A} = \mathbb{Z}$

  refinement vdH–Lecerf 2020: $\mathrm{e}^{\sqrt{(28+o(1))\log D \log\log D}}\,\tilde{O}(D \log r)$
- vdH–Lecerf 2020 (Ritzmann 1986), $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{C}\}$ large precision: $\tilde{O}(D)$

Special moduli R

Complexity bounds

General rings $\mathbb{A}$ $\deg P, \deg Q, \deg R \leqslant D$

- Horner over $\mathbb{A}[x]/(R)$: $O(D^3)$ or $O(D\,\mathsf{M}(D))$
- Brent–Kung 1978, baby-step-giant-step: $O(D^2 + \sqrt{D}\,\mathsf{M}(D))$
- Kaltofen–Shoup 1997, fast linear algebra: $O(D^{\omega_2/2} + \sqrt{D}\,\mathsf{M}(D))$, $3 \leqslant \omega_2 \leqslant 4$
- Neiger, Salvy, Schost, Villard, 2026: $\tilde{O}(D^{(\omega+3)/4})$, $2 \leqslant \omega \leqslant 3$

Special rings $\mathbb{A}$

- Kedlaya–Umans 2008: $D^{1+o(1)}$ if $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$ or $\mathbb{A} = \mathbb{Z}$

  refinement vdH–Lecerf 2020: $\mathrm{e}^{\sqrt{(28+o(1))\log D \log\log D}}\,\tilde{O}(D \log r)$
- vdH–Lecerf 2020 (Ritzmann 1986), $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{C}\}$ large precision: $\tilde{O}(D)$

Special moduli R

- Kinoshita–Li 2024, $R = x^D$: $\tilde{O}(D)$

Reduction to factorization

$$R = R_1^{k_1} \cdots R_n^{k_n}$$

Reduction to factorization

$$R \;=\; R_1^{k_1} \cdots R_n^{k_n}$$

$\longrightarrow$ Multi-remaindering $\mathbb{A}[x]/(R) \cong \mathbb{A}[x]/(R_1^{k_1}) \oplus \cdots \oplus \mathbb{A}[x]/(R_n^{k_n})$ reduces to the case when $R = R_i^{k_i}$ with R_i irreducible

Reduction to factorization

$$R \;=\; R_1^{k_1} \cdots R_n^{k_n}$$

$\longrightarrow$ Multi-remaindering $\mathbb{A}[x]/(R) \cong \mathbb{A}[x]/(R_1^{k_1}) \oplus \cdots \oplus \mathbb{A}[x]/(R_n^{k_n})$
reduces to the case when $R = R_i^{k_i}$ with R_i irreducible

$\longrightarrow$ Kinoshita–Li 2024, combined with vdH–Lecerf 2017
reduces to the case when R is irreducible

Reduction to factorization

$$R = R_1^{k_1} \cdots R_n^{k_n}$$

$\longrightarrow$ Multi-remaindering $\mathbb{A}[x]/(R) \cong \mathbb{A}[x]/(R_1^{k_1}) \oplus \cdots \oplus \mathbb{A}[x]/(R_n^{k_n})$
reduces to the case when $R = R_i^{k_i}$ with R_i irreducible

$\longrightarrow$ Kinoshita–Li 2024, combined with vdH–Lecerf 2017
reduces to the case when R is irreducible

$\longrightarrow$ Folklore $\tilde{O}(D)$ algorithm when $\mathbb{A} = \mathbb{C}$ at high precision, since R splits

Reduction to factorization

$$R = R_1^{k_1} \cdots R_n^{k_n}$$

$\longrightarrow$ Multi-remaindering $\mathbb{A}[x]/(R) \cong \mathbb{A}[x]/(R_1^{k_1}) \oplus \cdots \oplus \mathbb{A}[x]/(R_n^{k_n})$
reduces to the case when $R = R_i^{k_i}$ with R_i irreducible

$\longrightarrow$ Kinoshita–Li 2024, combined with vdH–Lecerf 2017
reduces to the case when R is irreducible

$\longrightarrow$ Folklore $\tilde{O}(D)$ algorithm when $\mathbb{A} = \mathbb{C}$ at high precision, since R splits

$\longrightarrow$ If $\mathbb{A} = \mathbb{F}_q$ and R irreducible of degree $d_1 d_2$, then R factors over $\mathbb{F}_{q^{d_1}}$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1 < d} \cdots \sum_{i_n < d} P_{i_n d^{n-1} + \cdots + i_1} x^{i_1} (x^d)^{i_2} \cdots (x^{d^{n-1}})^{i_n}$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) = \hat{P}(Q(x), Q(x)^d, \ldots, Q(x)^{d^{n-1}})$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) \operatorname{rem} R = \hat{P}(Q(x), Q(x)^d, \ldots, Q(x)^{d^{n-1}}) \operatorname{rem} R$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) \operatorname{rem} R = \hat{P}(Q(x) \operatorname{rem} R, Q(x)^d \operatorname{rem} R, \ldots, Q(x)^{d^{n-1}} \operatorname{rem} R) \operatorname{rem} R$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) \operatorname{rem} R = \hat{P}\Big(\underbrace{Q(x) \operatorname{rem} R}_{Q_1}, \underbrace{Q(x)^d \operatorname{rem} R}_{Q_2}, \ldots, \underbrace{Q(x)^{d^{n-1}} \operatorname{rem} R}_{Q_n} \Big) \operatorname{rem} R$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) \operatorname{rem} R = \hat{P}\Big(\underbrace{Q(x) \operatorname{rem} R}_{Q_1}, \underbrace{Q(x)^d \operatorname{rem} R}_{Q_2}, \ldots, \underbrace{Q(x)^{d^{n-1}} \operatorname{rem} R}_{Q_n} \Big) \operatorname{rem} R$$

$$\deg \hat{P}(Q_1, Q_2, \ldots, Q_n) < D d n$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) \operatorname{rem} R = \hat{P}\Big(\underbrace{Q(x) \operatorname{rem} R}_{Q_1}, \underbrace{Q(x)^d \operatorname{rem} R}_{Q_2}, \ldots, \underbrace{Q(x)^{d^{n-1}} \operatorname{rem} R}_{Q_n} \Big) \operatorname{rem} R$$

$$\deg \hat{P}(Q_1, Q_2, \ldots, Q_n) < D d n, \qquad n \approx \sqrt{\log_2 D}$$

Reduction to multivariate multi-point evaluation

$$D < d^n$$

$$P(x) = \sum_{i_1<d} \cdots \sum_{i_n<d} P_{i_n d^{n-1}+\cdots+i_1} (\underbrace{x}_{z_1})^{i_1} (\underbrace{x^d}_{z_2})^{i_2} \cdots (\underbrace{x^{d^{n-1}}}_{z_n})^{i_n} = \hat{P}(z_1, z_2, \ldots, z_n)$$

$$P(Q(x)) \operatorname{rem} R = \hat{P}\Big(\underbrace{Q(x) \operatorname{rem} R}_{Q_1}, \underbrace{Q(x)^d \operatorname{rem} R}_{Q_2}, \ldots, \underbrace{Q(x)^{d^{n-1}} \operatorname{rem} R}_{Q_n} \Big) \operatorname{rem} R$$

$$\deg \hat{P}(Q_1, Q_2, \ldots, Q_n) < D d n, \qquad n \approx \sqrt{\log_2 D}$$

$$\hat{P}\Big(\underbrace{Q_1(\alpha_k), Q_2(\alpha_k), \ldots, Q_n(\alpha_k)}_{\xi_k} \Big) \text{ for } k = 1, \ldots, D d n \quad \longrightarrow \quad \hat{R}$$

Multivariate multi-point evaluation

Input: $P \in \mathbb{A}[\boldsymbol{z}] := \mathbb{A}[z_1, \ldots, z_n]$, $\deg_{z_i} < d$, $\qquad \boldsymbol{\xi} := (\boldsymbol{\xi}_k)_{1 \leqslant k \leqslant N} \in (\mathbb{A}^n)^N$

Output: $P(\boldsymbol{\xi}) := (P(\boldsymbol{\xi}_k))_{1 \leqslant k \leqslant N} \in \mathbb{A}^N$

Assume: say $N \geqslant d^n$ (for convenience)

Multivariate multi-point evaluation

Input: $P \in \mathbb{A}[\boldsymbol{z}] := \mathbb{A}[z_1, \ldots, z_n]$, $\deg_{z_i} < d$, $\qquad \boldsymbol{\xi} := (\xi_k)_{1 \leqslant k \leqslant N} \in (\mathbb{A}^n)^N$

Output: $P(\boldsymbol{\xi}) := (P(\xi_k))_{1 \leqslant k \leqslant N} \in \mathbb{A}^N$

Assume: say $N \geqslant d^n$ (for convenience)

Applications

- Modular composition

Multivariate multi-point evaluation

Input: $P \in \mathbb{A}[\boldsymbol{z}] := \mathbb{A}[z_1, \ldots, z_n]$, $\deg_{z_i} < d$, $\qquad \boldsymbol{\xi} := (\xi_k)_{1 \leqslant k \leqslant N} \in (\mathbb{A}^n)^N$

Output: $P(\boldsymbol{\xi}) := (P(\xi_k))_{1 \leqslant k \leqslant N} \in \mathbb{A}^N$

Assume: say $N \geqslant d^n$ (for convenience)

Applications

- Modular composition
- Zero-dimensional polynomial system solving

Multivariate multi-point evaluation

Input: $P \in \mathbb{A}[\boldsymbol{z}] := \mathbb{A}[z_1, \ldots, z_n]$, $\deg_{z_i} < d$, $\qquad \boldsymbol{\xi} := (\xi_k)_{1 \leqslant k \leqslant N} \in (\mathbb{A}^n)^N$

Output: $P(\boldsymbol{\xi}) := (P(\xi_k))_{1 \leqslant k \leqslant N} \in \mathbb{A}^N$

Assume: say $N \geqslant d^n$ (for convenience)

Applications

- Modular composition
- Zero-dimensional polynomial system solving
  - Corresponds to verify correctness of a solution set

Multivariate multi-point evaluation

Input: $P \in \mathbb{A}[\boldsymbol{z}] := \mathbb{A}[z_1, \ldots, z_n]$, $\deg_{z_i} < d$, $\qquad \boldsymbol{\xi} := (\xi_k)_{1 \leqslant k \leqslant N} \in (\mathbb{A}^n)^N$

Output: $P(\boldsymbol{\xi}) := (P(\xi_k))_{1 \leqslant k \leqslant N} \in \mathbb{A}^N$

Assume: say $N \geqslant d^n$ (for convenience)

Applications

- Modular composition
- Zero-dimensional polynomial system solving
  - Corresponds to verify correctness of a solution set
  - Refining approximate solutions using Newton's method

Multivariate multi-point evaluation

Input: $P \in \mathbb{A}[\boldsymbol{z}] := \mathbb{A}[z_1, \ldots, z_n]$, $\deg_{z_i} < d$, $\quad \boldsymbol{\xi} := (\xi_k)_{1 \leqslant k \leqslant N} \in (\mathbb{A}^n)^N$

Output: $P(\boldsymbol{\xi}) := (P(\xi_k))_{1 \leqslant k \leqslant N} \in \mathbb{A}^N$

Assume: say $N \geqslant d^n$ (for convenience)

Applications

- Modular composition
- Zero-dimensional polynomial system solving
  - Corresponds to verify correctness of a solution set
  - Refining approximate solutions using Newton's method
  - vdH–Lecerf 2021: *On the complexity exponent of polynomial system solving*

General rings $\mathbb{A}$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(Nd^n)$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(N d^n)$
- Case $n = 1$: $O(N \mathsf{M}(d) / d) = \tilde{O}(N)$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(N d^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)\,/\,d) = \tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $\quad 3 \leqslant \omega_2 \leqslant 4$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(Nd^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)\,/\,d)=\tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $\quad 3\leqslant\omega_2\leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\quad \frac{4}{3}\leqslant\kappa\leqslant\frac{5}{3}$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(Nd^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)\,/\,d)=\tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $3\leqslant\omega_2\leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\frac{4}{3}\leqslant\kappa\leqslant\frac{5}{3}$
- vdH–Lecerf 2025 (upon Nüsken–Ziegler): $\tilde{O}(Nd^{(n-1)(\omega-1)/2})$, $2\leqslant\omega\leqslant 3$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(Nd^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)/d)=\tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $3\leqslant\omega_2\leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\frac{4}{3}\leqslant\kappa\leqslant\frac{5}{3}$
- vdH–Lecerf 2025 (upon Nüsken–Ziegler): $\tilde{O}(Nd^{(n-1)(\omega-1)/2})$, $2\leqslant\omega\leqslant 3$

Special ring $\mathbb{A}=\mathbb{Z}/r\mathbb{Z}$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(Nd^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)/d) = \tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $3 \leqslant \omega_2 \leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\frac{4}{3} \leqslant \kappa \leqslant \frac{5}{3}$
- vdH–Lecerf 2025 (upon Nüsken–Ziegler): $\tilde{O}(Nd^{(n-1)(\omega-1)/2})$, $2 \leqslant \omega \leqslant 3$

Special ring $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$

- Kedlaya–Umans 2008: $(N \log r)^{1+o(1)}$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(N d^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)/d) = \tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $3 \leqslant \omega_2 \leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\frac{4}{3} \leqslant \kappa \leqslant \frac{5}{3}$
- vdH–Lecerf 2025 (upon Nüsken–Ziegler): $\tilde{O}(N d^{(n-1)(\omega-1)/2})$, $2 \leqslant \omega \leqslant 3$

Special ring $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$

- Kedlaya–Umans 2008: $(N \log r)^{1+o(1)}$
- vdH–Lecerf 2020: $(N + (\varphi \log \varphi)^n)\, \tilde{O}(\mathrm{e}^{o(n)} \varphi^5 \log r)$, $\varphi = nd$

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(N d^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)/d) = \tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $3 \leqslant \omega_2 \leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\frac{4}{3} \leqslant \kappa \leqslant \frac{5}{3}$
- vdH–Lecerf 2025 (upon Nüsken–Ziegler): $\tilde{O}(N d^{(n-1)(\omega-1)/2})$, $2 \leqslant \omega \leqslant 3$

Special ring $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$

- Kedlaya–Umans 2008: $(N \log r)^{1+o(1)}$
- vdH–Lecerf 2020: $(N + (\varphi \log \varphi)^n)\, \tilde{O}(\mathrm{e}^{o(n)} \varphi^5 \log r)$, $\varphi = nd$

Amortized complexity

Complexity bounds

General rings $\mathbb{A}$

- Naive algorithm: $O(N d^n)$
- Case $n=1$: $O(N\,\mathsf{M}(d)/d) = \tilde{O}(N)$
- Case $n=2$, Nüsken–Ziegler 2004: $\tilde{O}(N^{\omega_2/2})$, $3 \leqslant \omega_2 \leqslant 4$
- Case $n=2$, Neiger, Salvy, Schost, Villard, 2023: $\tilde{O}(N^{\kappa})$, $\frac{4}{3} \leqslant \kappa \leqslant \frac{5}{3}$
- vdH–Lecerf 2025 (upon Nüsken–Ziegler): $\tilde{O}(N d^{(n-1)(\omega-1)/2})$, $2 \leqslant \omega \leqslant 3$

Special ring $\mathbb{A} = \mathbb{Z}/r\mathbb{Z}$

- Kedlaya–Umans 2008: $(N \log r)^{1+o(1)}$
- vdH–Lecerf 2020: $(N + (\varphi \log \varphi)^n)\, \tilde{O}(\mathrm{e}^{o(n)}\, \varphi^5 \log r)$, $\varphi = n d$

Amortized complexity

- $n = O(1)$, fixed points ξ, vdH–Lecerf 2023: $\tilde{O}(N)$

New approach for modular composition

Idea: reduce to the computation of $P \circ (Q_1, \ldots, Q_n) \in \mathbb{Z}/r\mathbb{Z}[x]$,

but, instead of doing evaluations at a general point set in $(\mathbb{Z}/r\mathbb{Z})^n$,

lift back to $\mathbb{Z}$ (and then $\mathbb{C}$) such as to approximately use a special point set

New approach for modular composition

Idea: reduce to the computation of $P \circ (Q_1, \ldots, Q_n) \in \mathbb{Z}/r\mathbb{Z}[x]$,
but, instead of doing evaluations at a general point set in $(\mathbb{Z}/r\mathbb{Z})^n$,
lift back to $\mathbb{Z}$ (and then $\mathbb{C}$) such as to approximately use a special point set

Example for $n=2$, $r=10$, $d=4$

$$\begin{aligned} P &= 3z_1^2+5z_2^2+2z_1+7 & & & \check{P} &= 3z_1^2+5z_2^2+2z_1+7 \\ Q_1 &= x^{14}+7x^8+2x^4+6x^2+8 & &\xrightarrow{\text{lift } \mathbb{Z}} & \check{Q}_1 &= x^{14}+7x^8+1002x^4+6x^2+8 \\ Q_2 &= x^{11}+3x^{10}+2x^2+5x+1 & & & \check{Q}_2 &= x^{11}+3x^{10}+2x^2+1005x+1 \end{aligned}$$

New approach for modular composition

Idea: reduce to the computation of $P \circ (Q_1, \ldots, Q_n) \in \mathbb{Z}/r\mathbb{Z}[x]$,
but, instead of doing evaluations at a general point set in $(\mathbb{Z}/r\mathbb{Z})^n$,
lift back to $\mathbb{Z}$ (and then $\mathbb{C}$) such as to approximately use a special point set

Example for $n=2$, $r=10$, $d=4$

$$\begin{aligned} P &= 3z_1^2+5z_2^2+2z_1+7 & & \check{P} = 3z_1^2+5z_2^2+2z_1+7 \\ Q_1 &= x^{14}+7x^8+2x^4+6x^2+8 \xrightarrow{\text{lift } \mathbb{Z}} & & \check{Q}_1 = x^{14}+7x^8+1002x^4+6x^2+8 \\ Q_2 &= x^{11}+3x^{10}+2x^2+5x+1 & & \check{Q}_2 = x^{11}+3x^{10}+2x^2+1005x+1 \end{aligned}$$

$$P(Q_1, Q_2) \operatorname{rem} 10 = \check{P}(\check{Q}_1, \check{Q}_2) \operatorname{rem} 10$$

Example — continued

$$
\begin{aligned}
P &= 3z_1^2+5z_2^2+2z_1+7 & & & \check{P} &= 3z_1^2+5z_2^2+2z_1+7\\
Q_1 &= x^{14}+7x^8+2x^4+6x^2+8 & &\xrightarrow{\text{lift } \mathbb{Z}} & \check{Q}_1 &= x^{14}+7x^8+1002x^4+6x^2+8\\
Q_2 &= x^{11}+3x^{10}+2x^2+5x+1 & & & \check{Q}_2 &= x^{11}+3x^{10}+2x^2+1005x+1
\end{aligned}
$$

$$
P(Q_1, Q_2) \operatorname{rem} 10 = \check{P}(\check{Q}_1, \check{Q}_2) \operatorname{rem} 10
$$

Example — continued

$$
\begin{aligned}
P &= 3z_1^2+5z_2^2+2z_1+7 & \qquad \check{P} &= 3z_1^2+5z_2^2+2z_1+7\\
Q_1 &= x^{14}+7x^8+2x^4+6x^2+8 \xrightarrow{\text{lift } \mathbb{Z}} & \check{Q}_1 &= x^{14}+7x^8+1002x^4+6x^2+8\\
Q_2 &= x^{11}+3x^{10}+2x^2+5x+1 & \check{Q}_2 &= x^{11}+3x^{10}+2x^2+1005x+1
\end{aligned}
$$

$$
\begin{aligned}
P(Q_1,Q_2) \text{ rem } 10 &= \check{P}(\check{Q}_1,\check{Q}_2) \text{ rem } 10\\
&= \check{P}\left(1000\tfrac{\check{Q}_1}{1000}, 1000\tfrac{\check{Q}_2}{1000}\right) \text{ rem } 10
\end{aligned}
$$

Example — continued

$$
\begin{aligned}
P &= 3z_1^2+5z_2^2+2z_1+7 & \check{P} &= 3z_1^2+5z_2^2+2z_1+7\\
Q_1 &= x^{14}+7x^8+2x^4+6x^2+8 \xrightarrow{\text{lift } \mathbb{Z}} & \check{Q}_1 &= x^{14}+7x^8+1002x^4+6x^2+8\\
Q_2 &= x^{11}+3x^{10}+2x^2+5x+1 & \check{Q}_2 &= x^{11}+3x^{10}+2x^2+1005x+1
\end{aligned}
$$

$$
\begin{aligned}
P(Q_1,Q_2) \text{ rem } 10 &= \check{P}(\check{Q}_1,\check{Q}_2) \text{ rem } 10\\
&= \check{P}\left(1000\tfrac{\check{Q}_1}{1000}, 1000\tfrac{\check{Q}_2}{1000}\right) \text{ rem } 10\\
&= \tilde{P}(\tilde{Q}_1,\tilde{Q}_2)
\end{aligned}
$$

Example — continued

$$
\begin{aligned}
P &= 3z_1^2+5z_2^2+2z_1+7 & & & \check{P} &= 3z_1^2+5z_2^2+2z_1+7\\
Q_1 &= x^{14}+7x^8+2x^4+6x^2+8 & \xrightarrow{\text{lift } \mathbb{Z}} & & \check{Q}_1 &= x^{14}+7x^8+1002x^4+6x^2+8\\
Q_2 &= x^{11}+3x^{10}+2x^2+5x+1 & & & \check{Q}_2 &= x^{11}+3x^{10}+2x^2+1005x+1
\end{aligned}
$$

$$
\begin{aligned}
P(Q_1,Q_2) \text{ rem } 10 &= \check{P}(\check{Q}_1,\check{Q}_2) \text{ rem } 10\\
&= \check{P}\left(1000\tfrac{\check{Q}_1}{1000}, 1000\tfrac{\check{Q}_2}{1000}\right) \text{ rem } 10\\
&= \tilde{P}(\tilde{Q}_1,\tilde{Q}_2)
\end{aligned}
$$

$$
\begin{aligned}
\tilde{P} &= 3000000z_1^2+5000000z_2^2+2000z_1+7\\
\tilde{Q}_1 &= 0.001x^{14}+0.007x^8+1.002x^4+0.006x^2+0.008 \approx x^4\\
\tilde{Q}_2 &= 0.001x^{11}+0.003x^{10}+0.002x^2+1.005x+0.001 \approx x
\end{aligned}
$$

Example — continued

$$
\begin{aligned}
\tilde{P} &= 3000000\,z_1^2 + 5000000\,z_2^2 + 2000\,z_1 + 7 \\
\tilde{Q}_1 &= 0.001\,x^{14} + 0.007\,x^8 + 1.002\,x^4 + 0.006\,x^2 + 0.008 \approx x^4 \\
\tilde{Q}_2 &= 0.001\,x^{11} + 0.003\,x^{10} + 0.002\,x^2 + 1.005\,x + 0.001 \approx x \\
\tilde{R} &= \tilde{P}(\tilde{Q}_1, \tilde{Q}_2), \qquad \deg \tilde{R} < 32
\end{aligned}
$$

Example — continued

$$
\begin{aligned}
\tilde{P} &= 3000000\,z_1^2 + 5000000\,z_2^2 + 2000\,z_1 + 7 \\
\tilde{Q}_1 &= 0.001\,x^{14} + 0.007\,x^8 + 1.002\,x^4 + 0.006\,x^2 + 0.008 \approx x^4 \\
\tilde{Q}_2 &= 0.001\,x^{11} + 0.003\,x^{10} + 0.002\,x^2 + 1.005\,x + 0.001 \approx x \\
\tilde{R} &= \tilde{P}(\tilde{Q}_1, \tilde{Q}_2), \qquad \deg \tilde{R} < 32
\end{aligned}
$$

$$
(\tilde{R}(1), \tilde{R}(\omega), \ldots, \tilde{R}(\omega^{31})) \xrightarrow{\text{DFT}^{-1}} \tilde{R}, \qquad \omega = \mathrm{e}^{2\pi\mathrm{i}/32}
$$

Example — continued

$$\begin{aligned}
\tilde{P} &= 3000000\,z_1^2 + 5000000\,z_2^2 + 2000\,z_1 + 7 \\
\tilde{Q}_1 &= 0.001\,x^{14} + 0.007\,x^8 + 1.002\,x^4 + 0.006\,x^2 + 0.008 \approx x^4 \\
\tilde{Q}_2 &= 0.001\,x^{11} + 0.003\,x^{10} + 0.002\,x^2 + 1.005\,x + 0.001 \approx x \\
\tilde{R} &= \tilde{P}(\tilde{Q}_1, \tilde{Q}_2), \qquad \deg \tilde{R} < 32
\end{aligned}$$

$$(\tilde{R}(1), \tilde{R}(\omega), \ldots, \tilde{R}(\omega^{31})) \xrightarrow{\text{DFT}^{-1}} \tilde{R}, \qquad \omega = \mathrm{e}^{2\pi \mathrm{i}/32}$$

$$\tilde{R}(\omega^k) = \tilde{P}(\xi_k), \qquad \xi_k = (\tilde{Q}_1(\omega^k), \tilde{Q}_2(\omega^k)) \approx (\omega^k, \omega^{4k}) =: \omega_k$$

Example — continued

$$\begin{aligned}
\tilde{P} &= 3000000\,z_1^2 + 5000000\,z_2^2 + 2000\,z_1 + 7 \\
\tilde{Q}_1 &= 0.001\,x^{14} + 0.007\,x^8 + 1.002\,x^4 + 0.006\,x^2 + 0.008 \approx x^4 \\
\tilde{Q}_2 &= 0.001\,x^{11} + 0.003\,x^{10} + 0.002\,x^2 + 1.005\,x + 0.001 \approx x \\
\tilde{R} &= \tilde{P}(\tilde{Q}_1, \tilde{Q}_2), \qquad \deg \tilde{R} < 32
\end{aligned}$$

$$(\tilde{R}(1), \tilde{R}(\omega), \ldots, \tilde{R}(\omega^{31})) \xrightarrow{\text{DFT}^{-1}} \tilde{R}, \qquad \omega = \mathrm{e}^{2\pi \mathrm{i}/32}$$

$$\tilde{R}(\omega^k) = \tilde{P}(\xi_k), \qquad \xi_k = (\tilde{Q}_1(\omega^k), \tilde{Q}_2(\omega^k)) \approx (\omega^k, \omega^{4k}) =: \omega_k$$

Required precision: $\approx n\,d \log(Mr)$, where $1000 = Mr$

$$|\tilde{P}| < 10 \cdot 1000^2, \qquad |\tilde{Q}_1 - x^4| < \frac{10}{1000}, \qquad |\tilde{Q}_2 - x| < \frac{10}{1000}$$

Regular spiroids

$$\delta_1, \ldots, \delta_n \in 2^{\mathbb{N}}, \qquad \Delta := \delta_1 \cdots \delta_n, \qquad \omega = \mathrm{e}^{2\pi \mathrm{i}/\Delta}$$

Regular spiroid: tuple of points $\boldsymbol{\omega} := (\omega_k)_{0 \leqslant k < \Delta} \in (\mathbb{C}^n)^\Delta$ with

$$\omega_k := (\omega^{k\Delta/\delta_1}, \omega^{k\Delta/(\delta_1\delta_2)}, \ldots, \omega^k) \in \mathbb{C}^n$$

Associated ideal: $I_\omega \subseteq \mathbb{C}[\boldsymbol{z}]$ generated by the grevlex Gröbner basis

$$z_1^{\delta_1} - 1,\ z_2^{\delta_2} - z_1,\ z_3^{\delta_3} - z_2,\ \ldots, z_n^{\delta_n} - z_{n-1}$$

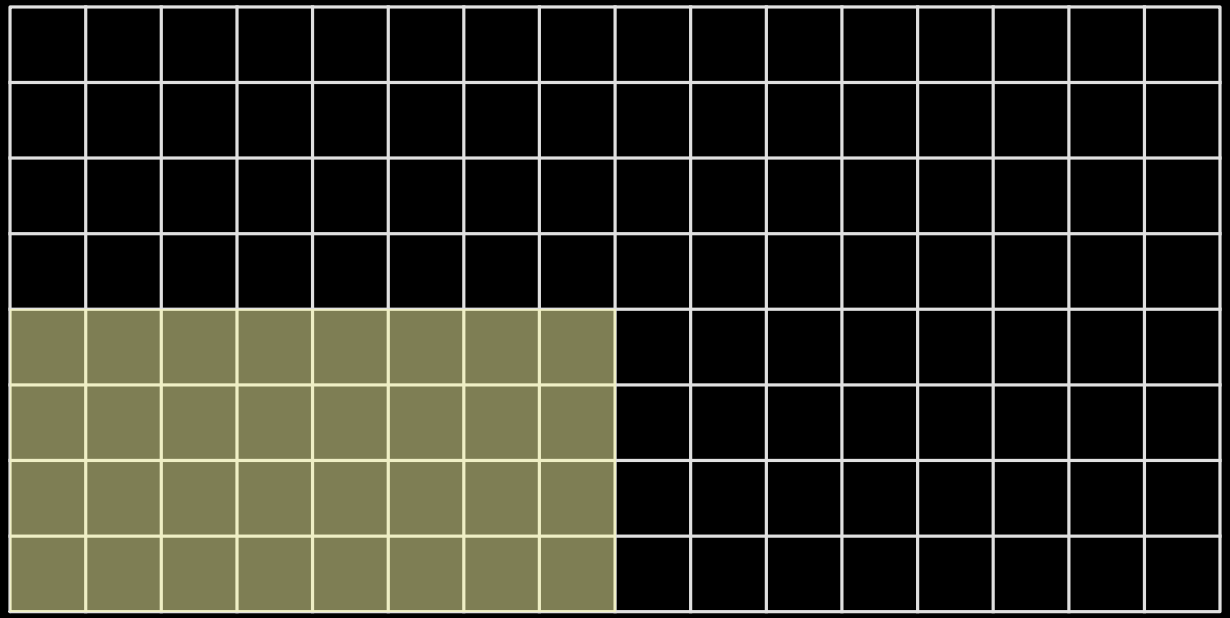
Reduced elements: $\mathbb{C}[\boldsymbol{z}]_{\delta_1,\ldots,\delta_n} := \{P \in \mathbb{C}[\boldsymbol{z}] : \forall k, \deg_{z_k} P < \delta_k\}$

Quotient algebra: $\mathbb{S}_\omega := \mathbb{C}[\boldsymbol{z}] / I_\omega$ with $\dim_{\mathbb{C}} \mathbb{S}_\omega = \Delta$

Regular spiroid arithmetic

Product: $P, Q \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \implies PQ \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$

Reduction: $S \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n} \xrightarrow{2^n\Delta \text{ additions}} \operatorname{red} S \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$



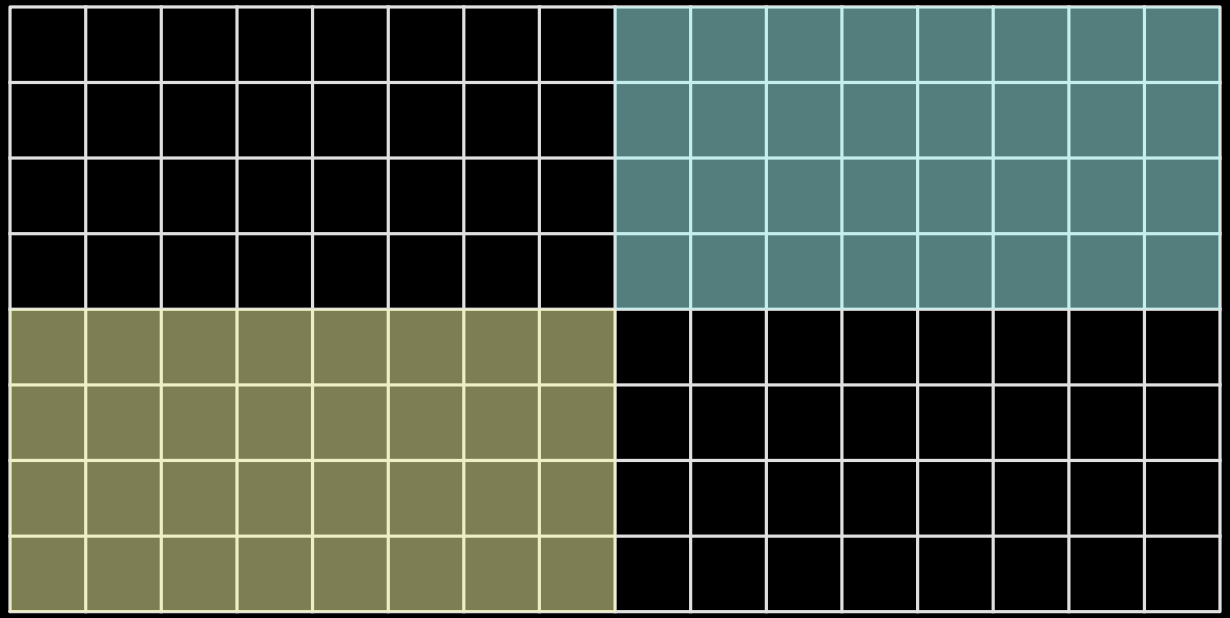
$z_1^8 = 1$

$z_2^4 = z_1$

Regular spiroid arithmetic

Product: $P, Q \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \implies PQ \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$

Reduction: $S \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n} \xrightarrow{2^n\Delta \text{ additions}} \operatorname{red} S \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$



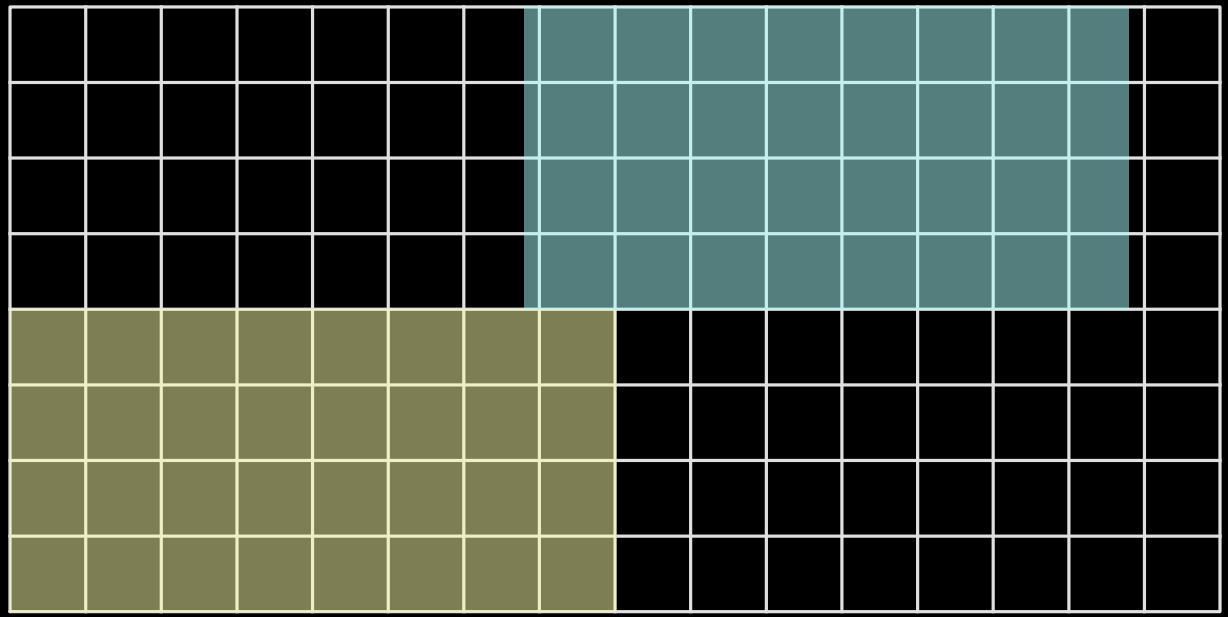
$z_1^8 = 1$

$z_2^4 = z_1$

Regular spiroid arithmetic

Product: $P, Q \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \implies PQ \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$

Reduction: $S \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n} \xrightarrow{2^n\Delta \text{ additions}} \operatorname{red} S \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$



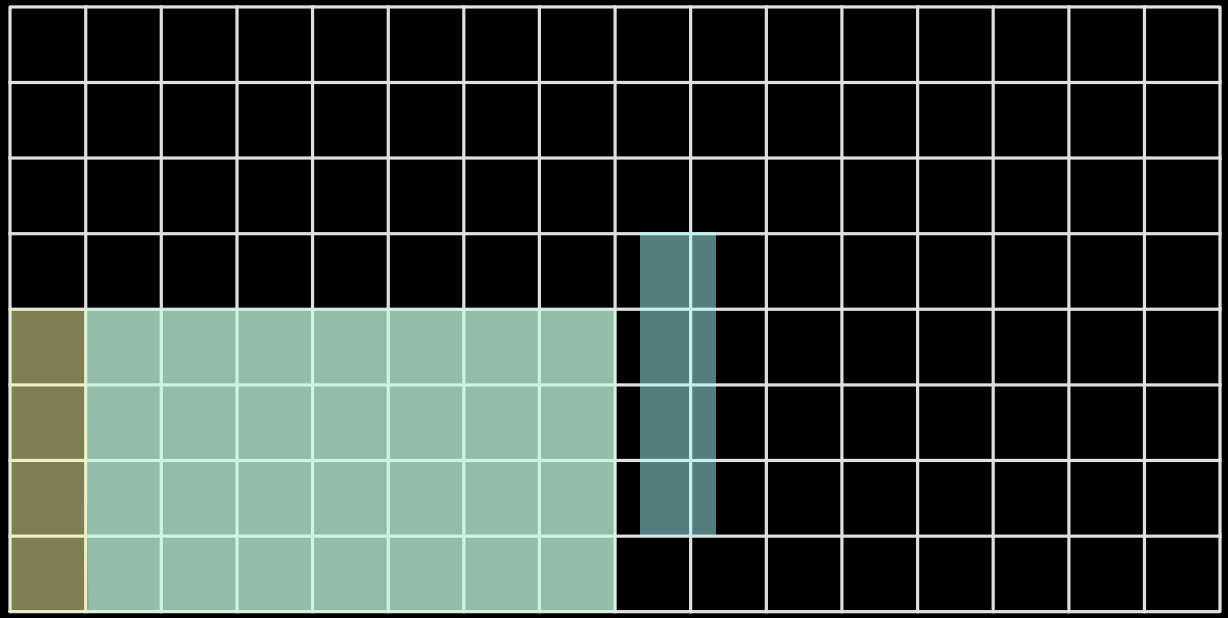
$z_1^8 = 1$

$z_2^4 = z_1$

Regular spiroid arithmetic

Product: $P, Q \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \implies PQ \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$

Reduction: $S \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n} \xrightarrow{2^n\Delta \text{ additions}} \operatorname{red} S \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$



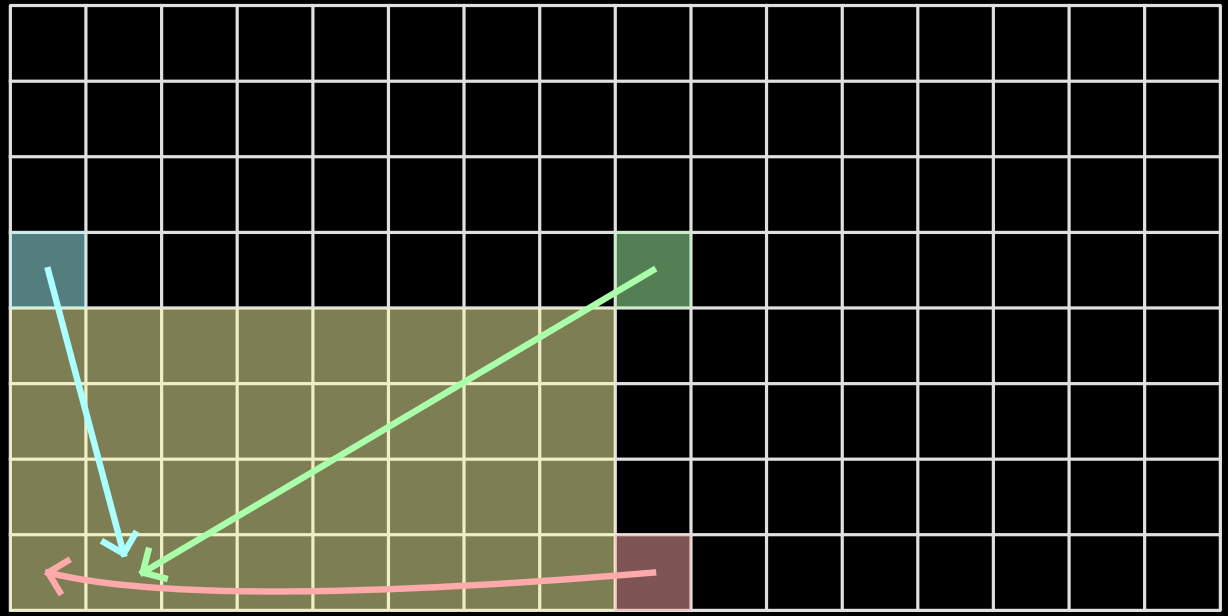
$$z_1^8 = 1$$

$$z_2^4 = z_1$$

Extended reduction for regular spiroids

$\mathbb{E}_n := \{0,1\}^n, \quad \mathbb{E}_n^* := \mathbb{E}_n \setminus \{\mathbf{0}\}.$

$$F_\epsilon := z_1^{\epsilon_1\delta_1} \cdots z_n^{\epsilon_n\delta_n} - z_1^{\epsilon_2} \cdots z_{n-1}^{\epsilon_n} \in I_\omega \qquad \epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbb{E}_n^*$$



$z_1^8 = 1$

$z_2^4 = z_1$

$F_{(0,1)} = z_2^4 - z_1$

$F_{(1,0)} = z_1^8 - 1$

$F_{(1,1)} = z_1^8 z_2^4 - z_1$

Extended reduction for regular spiroids

$\mathbb{E}_n := \{0,1\}^n, \quad \mathbb{E}_n^* := \mathbb{E}_n \setminus \{\mathbf{0}\}.$

$$F_{\mathbf{0}} := 1$$

$$F_\epsilon := z_1^{\epsilon_1\delta_1} \cdots z_n^{\epsilon_n\delta_n} - z_1^{\epsilon_2} \cdots z_{n-1}^{\epsilon_n} \in I_\omega \qquad \epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbb{E}_n^*$$

Extended reduction for regular spiroids

$\mathbb{E}_n := \{0,1\}^n, \quad \mathbb{E}_n^* := \mathbb{E}_n \setminus \{\mathbf{0}\}.$

$$\begin{aligned} F_{\mathbf{0}} &:= 1 \\ F_{\epsilon} &:= z_1^{\epsilon_1\delta_1} \cdots z_n^{\epsilon_n\delta_n} - z_1^{\epsilon_2} \cdots z_{n-1}^{\epsilon_n} \in I_\omega \end{aligned} \qquad \epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbb{E}_n^*$$

Extended reduction of $P \in \mathbb{C}[\boldsymbol{z}]_{2\delta_1,\ldots,2\delta_n}$:

$$P = \sum_{\epsilon \in \mathbb{E}_n} A_\epsilon F_\epsilon, \qquad A_\epsilon \in \mathbb{C}[\boldsymbol{z}]_{\delta_1,\ldots,\delta_n}$$

Extended reduction for regular spiroids

$\mathbb{E}_n := \{0,1\}^n, \quad \mathbb{E}_n^* := \mathbb{E}_n \setminus \{\mathbf{0}\}.$

$$\begin{aligned} F_{\mathbf{0}} &:= 1 \\ F_{\epsilon} &:= z_1^{\epsilon_1\delta_1} \cdots z_n^{\epsilon_n\delta_n} - z_1^{\epsilon_2} \cdots z_{n-1}^{\epsilon_n} \in I_\omega \end{aligned} \qquad \epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbb{E}_n^*$$

Extended reduction of $P \in \mathbb{C}[\boldsymbol{z}]_{2\delta_1,\ldots,2\delta_n}$:

$$P = \sum_{\epsilon \in \mathbb{E}_n} A_\epsilon F_\epsilon, \qquad A_\epsilon \in \mathbb{C}[\boldsymbol{z}]_{\delta_1,\ldots,\delta_n}$$

Note: $\operatorname{red} P = A_{\mathbf{0}}$

Extended reduction for regular spiroids

$\mathbb{E}_n := \{0,1\}^n, \quad \mathbb{E}_n^* := \mathbb{E}_n \setminus \{\mathbf{0}\}.$

$$\begin{aligned} F_{\mathbf{0}} &:= 1 \\ F_\epsilon &:= z_1^{\epsilon_1\delta_1} \cdots z_n^{\epsilon_n\delta_n} - z_1^{\epsilon_2} \cdots z_{n-1}^{\epsilon_n} \in I_\omega \end{aligned} \qquad \epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbb{E}_n^*$$

Extended reduction of $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$:

$$P = \sum_{\epsilon \in \mathbb{E}_n} A_\epsilon F_\epsilon, \qquad A_\epsilon \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$$

Note: $\operatorname{red} P = A_{\mathbf{0}}$

Lemma

We can compute an extended reduction at precision p in time $O(2^n \Delta (p+n))$.

General spiroids

Intuitive definition: $\xi \in (\mathbb{C}^n)^\Delta$ sufficiently close to ω

General spiroids

Intuitive definition: $\xi \in (\mathbb{C}^n)^\Delta$ sufficiently close to ω

More precisely:

$$|\xi - \omega| < \frac{1}{2^{2n}\Delta}$$

General spiroids

Intuitive definition: $\xi \in (\mathbb{C}^n)^\Delta$ sufficiently close to ω

More precisely:

$$|\xi - \omega| < \frac{1}{2^{2n}\Delta}$$

In addition: the vanishing ideal $I_\xi \subseteq \mathbb{C}[z]$ is generated by

$$\begin{aligned} G_\epsilon &= F_\epsilon + E_\epsilon \\ E_\epsilon &\in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \\ \|E\| &:= \max_\epsilon |E_\epsilon| < \frac{1}{2^{2n}\Delta} \end{aligned}$$

General spiroids

Intuitive definition: $\xi \in (\mathbb{C}^n)^\Delta$ sufficiently close to ω

More precisely:

$$|\xi - \omega| < \frac{1}{2^{2n}\Delta}$$

In addition: the vanishing ideal $I_\xi \subseteq \mathbb{C}[z]$ is generated by

$$\begin{aligned} G_\epsilon &= F_\epsilon + E_\epsilon \\ E_\epsilon &\in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \\ \|E\| &:= \max_\epsilon |E_\epsilon| < \frac{1}{2^{2n}\Delta} \end{aligned}$$

Lemma

If $|\xi - \omega|$ is sufficiently small, then ξ is a spiroid.

General spiroids

Intuitive definition: $\xi \in (\mathbb{C}^n)^\Delta$ sufficiently close to ω

More precisely:

$$|\xi - \omega| < \frac{1}{2^{2n}\Delta}$$

In addition: the vanishing ideal $I_\xi \subseteq \mathbb{C}[z]$ is generated by

$$\begin{aligned} G_\epsilon &= F_\epsilon + E_\epsilon \\ E_\epsilon &\in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n} \\ \|E\| &:= \max_\epsilon |E_\epsilon| < \frac{1}{2^{2n}\Delta} \end{aligned}$$

Lemma

If $|\xi - \omega|$ is sufficiently small, then ξ is a spiroid.

Assume for now that ξ is a spiroid and that the G_ϵ are known

Extended reduction for general spiroids

Extended reduction of $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ with respect to I_ξ:

$$P = \sum_{\epsilon \in \mathbb{E}_n} A_\epsilon G_\epsilon, \qquad A_\epsilon \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$$

Extended reduction for general spiroids

Extended reduction of $P \in \mathbb{C}[z]_{2\delta_1,\dots,2\delta_n}$ with respect to I_ξ:

$$P = \sum_{\epsilon \in \mathbb{E}_n} A_\epsilon G_\epsilon, \qquad A_\epsilon \in \mathbb{C}[z]_{\delta_1,\dots,\delta_n}$$

Lemma

We can compute an extended reduction at precision p in time $\tilde{O}(4^n \Delta p)$.

Extended reduction for general spiroids

Extended reduction of $P \in \mathbb{C}[z]_{2\delta_1,\dots,2\delta_n}$ with respect to I_ξ:

$$P = \sum_{\epsilon \in \mathbb{E}_n} A_\epsilon G_\epsilon, \qquad A_\epsilon \in \mathbb{C}[z]_{\delta_1,\dots,\delta_n}$$

Lemma

We can compute an extended reduction at precision p in time $\tilde{O}(4^n \Delta p)$.

Proof. Assume approximation $(\tilde{A}_\epsilon)$ of (A_ϵ) and let $\tilde{P} = P - \sum_{\epsilon \in \mathbb{E}_n} \tilde{A}_\epsilon G_\epsilon$.

Reduce $\tilde{P} = \sum_{\epsilon \in \mathbb{E}_n} B_\epsilon F_\epsilon$. Then we have the better approximation $(\tilde{A}_\epsilon + B_\epsilon)$.

For large precisions p, one may use this in a divide and conquer fashion. □

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial
$\delta_1 = 1 \longrightarrow$ reduce dimension
Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ compute $P(\xi) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

$$\xi^{[0]} := (\xi_0, \xi_2, \ldots, \xi_{\Delta-2})$$

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ compute $P(\xi) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

$$\xi^{[0]} := (\xi_0, \xi_2, \ldots, \xi_{\Delta-2})$$

Recursively compute $R(\xi^{[0]})$

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\ldots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

$$\boldsymbol{\xi}^{[0]} := (\xi_0, \xi_2, \ldots, \xi_{\Delta-2}) \qquad \boldsymbol{\xi}^{[1]} := \left(\frac{\xi_1}{\omega_1}, \frac{\xi_3}{\omega_1}, \ldots, \frac{\xi_{\Delta-1}}{\omega_1}\right)$$

Recursively compute $R(\boldsymbol{\xi}^{[0]})$

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\dots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

$$\boldsymbol{\xi}^{[0]} := (\xi_0, \xi_2, \dots, \xi_{\Delta-2}) \qquad \boldsymbol{\xi}^{[1]} := \left(\frac{\xi_1}{\omega_1}, \frac{\xi_3}{\omega_1}, \dots, \frac{\xi_{\Delta-1}}{\omega_1}\right)$$

Recursively compute $R(\boldsymbol{\xi}^{[0]})$

$$\tilde{R} := R(\omega_1 z)$$

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\dots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

$$\boldsymbol{\xi}^{[0]} := (\xi_0, \xi_2, \dots, \xi_{\Delta-2}) \qquad \boldsymbol{\xi}^{[1]} := \left(\frac{\xi_1}{\omega_1}, \frac{\xi_3}{\omega_1}, \dots, \frac{\xi_{\Delta-1}}{\omega_1}\right)$$

Recursively compute $R(\boldsymbol{\xi}^{[0]})$

$$\tilde{R} := R(\omega_1 z)$$

Recursively compute $\tilde{R}(\boldsymbol{\xi}^{[1]})$

Evaluation using divide and conquer strategy

Problem: given $P \in \mathbb{C}[z]_{2\delta_1,\dots,2\delta_n}$ compute $P(\boldsymbol{\xi}) := (P(\xi_k)_{k<\Delta})$.

$\Delta = 1 \longrightarrow$ trivial

$\delta_1 = 1 \longrightarrow$ reduce dimension

Otherwise:

$$R := \operatorname{red}(P, I_\xi)$$

$$\boldsymbol{\xi}^{[0]} := (\xi_0, \xi_2, \dots, \xi_{\Delta-2}) \qquad \boldsymbol{\xi}^{[1]} := \left(\frac{\xi_1}{\omega_1}, \frac{\xi_3}{\omega_1}, \dots, \frac{\xi_{\Delta-1}}{\omega_1}\right)$$

Recursively compute $R(\boldsymbol{\xi}^{[0]})$

$$\tilde{R} := R(\omega_1 z)$$

Recursively compute $\tilde{R}(\boldsymbol{\xi}^{[1]})$

Complexity: $\tilde{O}(4^n \Delta p)$

Interpolation

Input: given $v = (v_k)_{k<\Delta} \in (\mathbb{C}^n)^\Delta$, compute

Output: $P \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$ with $P(\xi) = (P(\xi_k))_{k<\Delta} = v$

Interpolation

Input: given $v = (v_k)_{k<\Delta} \in (\mathbb{C}^n)^\Delta$, compute

Output: $P \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$ with $P(\xi) = (P(\xi_k))_{k<\Delta} = v$

Low precision p

Compute $\tilde{P} \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$ with $\tilde{P}(\omega) = v$ using DFT^{-1}

Evaluate $\eta := \tilde{P}(\xi)$ and set $\tilde{v} := v - \eta$

Recurse for $\tilde{v}$ instead of v until sufficiently precise

Interpolation

Input: given $v = (v_k)_{k<\Delta} \in (\mathbb{C}^n)^\Delta$, compute

Output: $P \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$ with $P(\xi) = (P(\xi_k))_{k<\Delta} = v$

Low precision p

Compute $\tilde{P} \in \mathbb{C}[z]_{\delta_1,\ldots,\delta_n}$ with $\tilde{P}(\omega) = v$ using DFT^{-1}

Evaluate $\eta := \tilde{P}(\xi)$ and set $\tilde{v} := v - \eta$

Recurse for $\tilde{v}$ instead of v until sufficiently precise

High precision p

Divide and conquer strategy.

Interpolation

Input: given $v = (v_k)_{k<\Delta} \in (\mathbb{C}^n)^\Delta$, compute

Output: $P \in \mathbb{C}[z]_{\delta_1,\dots,\delta_n}$ with $P(\xi) = (P(\xi_k))_{k<\Delta} = v$

Low precision p

Compute $\tilde{P} \in \mathbb{C}[z]_{\delta_1,\dots,\delta_n}$ with $\tilde{P}(\omega) = v$ using DFT^{-1}

Evaluate $\eta := \tilde{P}(\xi)$ and set $\tilde{v} := v - \eta$

Recurse for $\tilde{v}$ instead of v until sufficiently precise

High precision p

Divide and conquer strategy.

Complexity: $\tilde{O}(4^n \Delta p)$

Computing evaluation/interpolation trees

Problem: compute tree the $G_{\boldsymbol{\epsilon}}$, as well as recursively for $\boldsymbol{\xi}^{[0]}$, $\boldsymbol{\xi}^{[1]}$, $(\boldsymbol{\xi}^{[0]})^{[0]}$, ...

Computing evaluation/interpolation trees

Problem: compute tree the G_ϵ, as well as recursively for $\boldsymbol{\xi}^{[0]}$, $\boldsymbol{\xi}^{[1]}$, $(\boldsymbol{\xi}^{[0]})^{[0]}$, ...

Assume $\delta_1 > 1$ and recursively done for $\boldsymbol{\xi}^{[0]}$, $\boldsymbol{\xi}^{[1]}$

Computing evaluation/interpolation trees

Problem: compute tree the G_{ϵ}, as well as recursively for $\xi^{[0]}$, $\xi^{[1]}$, $(\xi^{[0]})^{[0]}$, ...

Assume $\delta_1 > 1$ and recursively done for $\xi^{[0]}$, $\xi^{[1]}$

For each $\epsilon \in \mathbb{E}_n^*$ do the following

Computing evaluation/interpolation trees

Problem: compute tree the G_ϵ, as well as recursively for $\xi^{[0]}$, $\xi^{[1]}$, $(\xi^{[0]})^{[0]}$, ...

Assume $\delta_1 > 1$ and recursively done for $\xi^{[0]}$, $\xi^{[1]}$

For each $\epsilon \in \mathbb{E}_n^*$ do the following

- Compute $v := -F_\epsilon(\xi)$

Computing evaluation/interpolation trees

Problem: compute tree the G_ϵ, as well as recursively for $\xi^{[0]}$, $\xi^{[1]}$, $(\xi^{[0]})^{[0]}$, ...

Assume $\delta_1 > 1$ and recursively done for $\xi^{[0]}$, $\xi^{[1]}$

For each $\epsilon \in \mathbb{E}_n^*$ do the following

- Compute $v := -F_\epsilon(\xi)$
- Interpolate to recover E_ϵ with $E_\epsilon(\xi) = v$

Computing evaluation/interpolation trees

Problem: compute tree the G_ϵ, as well as recursively for $\xi^{[0]}$, $\xi^{[1]}$, $(\xi^{[0]})^{[0]}$, ...

Assume $\delta_1 > 1$ and recursively done for $\xi^{[0]}$, $\xi^{[1]}$

For each $\epsilon \in \mathbb{E}_n^*$ do the following

- Compute $v := -F_\epsilon(\xi)$
- Interpolate to recover E_ϵ with $E_\epsilon(\xi) = v$
- We have $G_\epsilon = F_\epsilon + E_\epsilon$

Computing evaluation/interpolation trees

Problem: compute tree the G_ϵ, as well as recursively for $\xi^{[0]}$, $\xi^{[1]}$, $(\xi^{[0]})^{[0]}$, ...

Assume $\delta_1 > 1$ and recursively done for $\xi^{[0]}$, $\xi^{[1]}$

For each $\epsilon \in \mathbb{E}_n^*$ do the following

- Compute $v := -F_\epsilon(\xi)$
- Interpolate to recover E_ϵ with $E_\epsilon(\xi) = v$
- We have $G_\epsilon = F_\epsilon + E_\epsilon$

Complexity: $\tilde{O}(8^n \Delta p)$

Back to modular composition

Theorem

The cost of degree D modular composition over $\mathbb{Z}/r\mathbb{Z}$ is bounded by

$$e^{5\sqrt{\log D}}\,\tilde{O}(D \log r).$$

Back to modular composition

Theorem

The cost of degree D modular composition over $\mathbb{Z}/r\mathbb{Z}$ is bounded by

$$e^{5\sqrt{\log D}}\,\tilde{O}(D \log r).$$

Remark: recall previous best bound $e^{\sqrt{(28+o(1))\log D \log\log D}}\,\tilde{O}(D \log r)$

Back to modular composition

Theorem

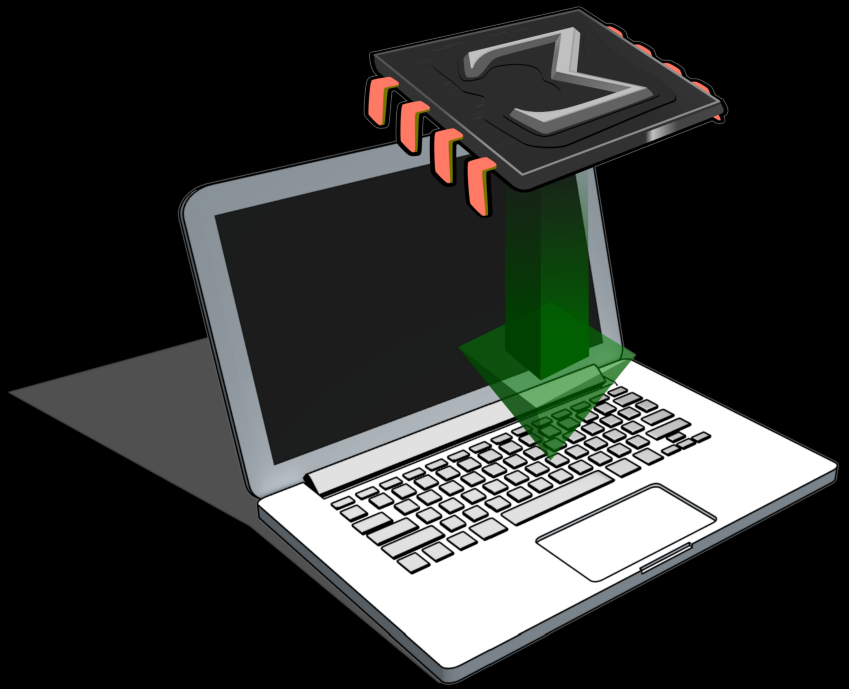
The cost of degree D modular composition over $\mathbb{Z}/r\mathbb{Z}$ is bounded by

$$e^{5\sqrt{\log D}}\,\tilde{O}(D \log r).$$

Remark: recall previous best bound $e^{\sqrt{(28+o(1))\log D \log\log D}}\,\tilde{O}(D \log r)$

Challenge: does there exist a *practical* faster algorithm ?

Thank you !



http://www.TeXmacs.org