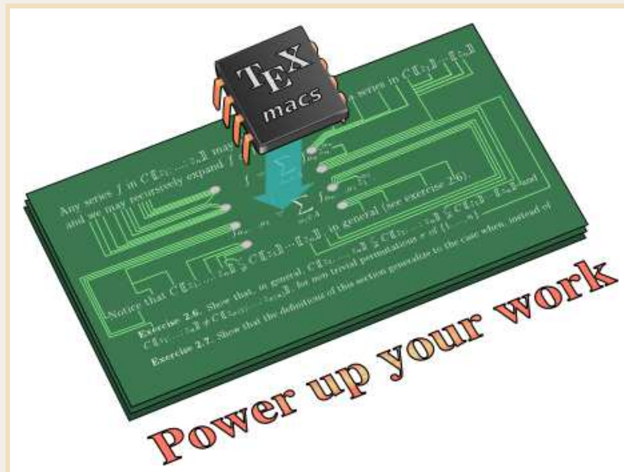
Quasi-optimal multiplication of linear differential operators

Alexandre Benoit, Alin Bostan, Joris van der Hoeven

CNRS, École polytechnique



FOCS, New Brunswick, 2012

http://www.TeXmacs.org

Classical complexity results

Definitions

$\mathbb{K}$: effective field of characteristic zero
$\mathbb{K}[x]_d = \{P \in \mathbb{K}[x] \colon \deg_x P < d\}$
$\mathbb{K}^{r \times r'}$: ring of $r \times r'$ matrices with coefficients in $\mathbb{K}$

Fundamental complexities

- $\mathsf{M}(d) = \mathcal{O}(d \log d \log \log d) = \tilde{\mathcal{O}}(d)$: multiplication in $\mathbb{K}[x]_d$
- $\mathcal{O}(r^\omega)$, $\omega < 2.373$: multiplication in $\mathbb{K}^{r \times r}$

Other operations

- For $\mathbb{K}[x]_d$, division in $\mathcal{O}(\mathsf{M}(d))$, gcd in $\mathcal{O}(\mathsf{M}(d) \log d)$, etc.
- For $\mathbb{K}^{r \times r}$, inversion in $\mathcal{O}(r^\omega)$, etc.

Main problem and applications

Definitions

$\partial = \partial / \partial x$, so that $\partial x = x \partial + 1$ when regarding x as an operator
$\mathbb{K}[x, \partial]_{d,r} = \{L \in \mathbb{K}[x, \partial] \colon \deg_x L < d, \deg_\partial L < r\}$

Main problem

Complexity $\mathsf{SM}(d, r)$ of multiplication in $\mathbb{K}[x, \partial]_{d,r}$?

Applications

Recall: $\mathbb{K}(x)[\partial]$ is a skew polynomial ring

- Exact division, division with remainder, extended division
- Greatest common right divisors, least common left multiples
- Fundamental systems of (truncated) power series solutions
- Smallest annihilator of finite set of (truncated) power series

Main result

Known

[VdH,2002] $\mathsf{SM}(r,r)=\mathcal{O}(r^{\omega})$
[Bostan,Chyzak,LeRoux,2008] $r^{\omega}=\mathcal{O}(\mathsf{SM}(r,r))$

New result

$\mathsf{SM}(d,r)=\tilde{\mathcal{O}}(d\,r\min(d,r)^{\omega-2})$

Generalizations

- Positive characteristic
- Other skew indeterminates $\delta=x\,\partial$, $\sigma: x_c\mapsto x+c$, $Q_q: x\mapsto q\,x$

Outline of the proof

Main ideas

- Evaluation-interpolation strategy:

$$K\,L = \mathrm{Interpolate}(\mathrm{Eval}(K)\,\mathrm{Eval}(L)).$$

- $(d, r) \xleftrightarrow{\text{reflection}} (r, d)$ allows us to assume that $r \geqslant d$

Admitted (Fast Hermite evaluation-interpolation)

Given d, μ, distinct points $\alpha_0, \ldots, \alpha_{d-1}$ and a polynomial $P \in \mathbb{K}[x]_{\mu d}$, we can compute

$$P(\alpha_0), P'(\alpha_0), \ldots, P^{(\mu-1)}(\alpha_0), \ldots\ldots, P(\alpha_{d-1}), P'(\alpha_{d-1}), \ldots, P^{(\mu-1)}(\alpha_{d-1})$$

in time $\mathcal{O}(\mathsf{M}(\mu\,d)\log d) = \tilde{\mathcal{O}}(\mathsf{M}(\mu\,d))$.
Same complexity for inverse operation of interpolation.

Operators $\leftrightsquigarrow$ Matrices

Matrix of an operator

$L \in \mathbb{K}[x,\partial]_{d,r}$, $k \in \mathbb{N}$, $L\colon \mathbb{K}[x]_k \to \mathbb{K}[x]_{k+d}$

$$\Phi_L^{d+r-1,r} = \begin{pmatrix} L(1)_0 & \cdots & L(x^{r-1})_0 \\ \vdots & & \vdots \\ L(1)_{k+d-1} & \cdots & L(x^{r-1})_{k+d-1} \end{pmatrix}$$

"Fourier" multiplication ($K, L \in \mathbb{K}[x,\partial]_{d,r}$)

$$\Phi_{KL}^{2r+2d,2r} = \Phi_K^{2r+2d,2r+d}\,\Phi_L^{2r+d,2r}$$

Complexity ($L \in \mathbb{K}[x,\partial]_{r,r}$)

- We can compute $\Phi_L^{2r,r}$ from L in time $\mathcal{O}(r\,\mathsf{M}(r))$.
- We can recover L from $\Phi_L^{2r,r}$ in time $\mathcal{O}(r\,\mathsf{M}(r))$.

Generalization to the case $r \geqslant d$

Operate on exponential polynomials ($L \in \mathbb{K}[x, \partial]_{d,r}$)

- L also operates on $\mathbb{K}[x, \partial]\, \mathrm{e}^{\alpha x}$ for every $\alpha \in \mathbb{K}$
- More specifically, writing

$$L = \sum_i L_i(x)\, \partial^i$$

  we have:

$$\begin{aligned} L(P\, \mathrm{e}^{\alpha x}) &= L_{\ltimes \alpha}(P) \\ L_{\ltimes \alpha} &= \sum_i L_i(x)\, (\partial + \alpha)^i \end{aligned}$$

Idea

For $p = \lceil r / d \rceil$, choose distinct $\alpha_0, \ldots, \alpha_{p-1}$, and let L operate on

$$\mathbb{V}_k = \mathbb{K}[x]_k\, \mathrm{e}^{\alpha_0 x} \oplus \cdots \oplus \mathbb{K}[x]_k\, \mathrm{e}^{\alpha_{p-1} x}$$

Generalization to the case $r \geqslant d$, continued

Matrix representation (of $L\colon \mathbb{V}_k \to \mathbb{V}_{k+d}$)

$$\Phi_L^{[k+d,k]} = \begin{pmatrix} \Phi_{\ltimes\alpha_0}^{k+d,k} & & \\ & \ddots & \\ & & \Phi_{\ltimes\alpha_{p-1}}^{k+d,k} \end{pmatrix}$$

Complexity ($L \in \mathbb{K}[x,\partial]_{n,r}$, $r \geqslant d$, $p = \lceil r/d \rceil$)

- We may compute $\Phi_L^{[2d,d]}$ as a function of L in time $\mathcal{O}(d\,\mathsf{M}(r)\log r)$.
- We may recover L from $\Phi_L^{[2d,d]}$ in time $\mathcal{O}(d\,\mathsf{M}(r)\log r)$.

Proof

- For $r \geqslant d$, L operates on the same way on $\mathbb{K}[x]_d$ as its truncation

$$L^* = \textstyle\sum_{i<d,j<d} L_{i,j}\,x^i\,\partial^j$$

- $L \leftrightsquigarrow (L^*_{\ltimes\alpha_0}, \ldots, L^*_{\ltimes\alpha_{p-1}})$: Hermite evaluation-interpolation at p points of multiplicity d

Generalization to the case $r \geqslant d$, conclusion

"Fourier" multiplication (of $K, L \in \mathbb{K}[x,\partial]_{d,r}$, $r \geqslant d$)

$$\Phi_{KL}^{[4d+2d,2d]} \;=\; \Phi_K^{[4d,3d]}\,\Phi_L^{[3d,2d]}.$$

Theorem. *Let* $K, L \in \mathbb{K}[x,\partial]_{d,r}$ *with* $r \geqslant d$. *Then* KL *can be computed in time*

$$\mathsf{SM}(n,r) \;=\; \mathcal{O}(d^{\omega-1}\,r + d\,\mathsf{M}(r)\log r).$$

The case when $d > r$

Reflection

$$\begin{aligned} \varphi\colon \mathbb{K}[x,\partial] &\longrightarrow \mathbb{K}[x,\partial] \\ x &\longmapsto \partial \\ \partial &\longmapsto -x \end{aligned}$$

Properties

- φ is a morphism: $\varphi(\partial)\,\varphi(x) - \varphi(x)\,\varphi(\partial) = -x\,\partial + \partial\,x = 1$
- φ is a bijection between $\mathbb{K}[x,\partial]_{n,r}$ and $\mathbb{K}[\partial,x]_{r,n}$
- $\varphi \circ \varphi = -\mathrm{Id}$, so $\varphi^{\mathrm{inv}} = -\varphi$
- Thus, given $K, L \in \mathbb{K}[x,\partial]_{n,r}$ with $d > r$, we may compute $K\,L$ using

$$K\,L \;=\; -\varphi(\varphi(K)\,\varphi(L)).$$

The case when $r > d$, continued

Computing the reflection

Given

$$L = \sum_{i,j} p_{i,j} \, \partial^j \, x^i,$$

compute $q_{i,j}$ with

$$L = \sum_{i,j} q_{i,j} \, x^i \, \partial^j.$$

Theorem. *Given $L \in \mathbb{K}[x, \partial]_{d,r}$, we may compute $\varphi(L)$ in time $\mathcal{O}(\min(d \, \mathsf{M}(r), r \, \mathsf{M}(d)))$.*

Proof: (1) Show that

$$i! \, q_{i,j} = \sum_{k \geqslant 0} \binom{j+k}{k} (i+k)! \, p_{i+k, j+k}$$

(2) Reduce to the computation of $\mathcal{O}(d + r)$ Taylor shifts of length $\min(d, r)$.