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

Fundamental complexities

- $M(d) = \mathcal{O}(d \log d \log \log d) = \tilde{\mathcal{O}}(d)$: 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 $\mathcal{O}(M(d))$, gcd in $\mathcal{O}(M(d) \log d)$, etc.
- For $\mathbb{K}^{r \times r}$, inversion in $\mathcal{O}(r^\omega)$, etc.
Main problem and applications

Definitions

\[ \partial = \partial / \partial x, \text{ so that } \partial x = x \partial + 1 \text{ when regarding } x \text{ as an operator} \]

\[ K[x, \partial]_{d,r} = \{ L \in K[x, \partial]: \deg_x L < d, \deg_\partial L < r \} \]

Main problem

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

Applications

Recall: \( K(x)[\partial] \) 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] \( \text{SM}(r, r) = \mathcal{O}(r^\omega) \)

[Bostan, Chyzak, LeRoux, 2008] \( r^\omega = \mathcal{O}(\text{SM}(r, r)) \)

New result

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

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:
  \[ KL = \text{Interpolate}(\text{Eval}(K) \text{ Eval}(L)). \]

- \((d, r) \xrightarrow{\text{reflection}} (r, d)\) allows us to assume that \(r \geq d\)

**Admitted** (Fast Hermite evaluation-interpolation)

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

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

in time \(O(M(\mu d) \log d) = \tilde{O}(M(\mu d))\).

Same complexity for inverse operation of interpolation.
Matrix of an operator

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

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

"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 $\mathcal{O}(r \ M(r))$.
- We can recover $L$ from $\Phi_{L}^{2r,r}$ in time $\mathcal{O}(r \ M(r))$. 
Generalization to the case $r \geq d$

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

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

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

we have:

$$L(P e^{\alpha x}) = L_{\times \alpha}(P)$$

$$L_{\times \alpha} = \sum_i L_i(x) (\partial + \alpha)^i$$

**Idea**

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

$$\mathbb{V}_k = \mathbb{K}[x]_k e^{\alpha_0 x} \oplus \cdots \oplus \mathbb{K}[x]_k e^{\alpha_{p-1} x}$$
Matrix representation (of $L: \mathbb{V}_k \to \mathbb{V}_{k+d}$)

$$
\Phi_L^{[k+d,k]} = \begin{pmatrix}
\Phi_{k+d,k} \\
\Phi_{k+k_0} \\
\vdots \\
\Phi_{k+d,k} \\
\end{pmatrix}
$$

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

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

Proof

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

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

- $L \leftrightarrow (L^*_{\alpha_0}, \ldots, L^*_{\alpha_{p-1}})$: Hermite evaluation-interpolation at $p$ points of multiplicity $d$
Generalization to the case $r \geq d$, conclusion

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

$$
\Phi_{KL}^{[4d+2d,2d]} = \Phi_{K}^{[4d,3d]} \Phi_{L}^{[3d,2d]}.
$$

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

$$
\text{SM}(n, r) = \mathcal{O}(d^{\omega-1} r + dM(r) \log r).
$$
The case when \( d > r \)

Reflection

\[
\varphi: \mathbb{K}[x, \partial] \longrightarrow \mathbb{K}[x, \partial] \\
x \longmapsto \partial \\
\partial \longmapsto -x
\]

Properties

\( \varphi \) is a morphism: \( \varphi(\partial) \varphi(x) - \varphi(x) \varphi(\partial) = -x \partial + \partial x = 1 \)

\( \varphi \) is a bijection between \( \mathbb{K}[x, \partial]_{n,r} \) and \( \mathbb{K}[\partial, x]_{r,n} \)

\( \varphi \circ \varphi = -\text{Id} \), so \( \varphi^{-1} = -\varphi \)

Thus, given \( K, L \in \mathbb{K}[x, \partial]_{n,r} \) with \( d > r \), we may compute \( KL \) using

\[
KL = -\varphi(\varphi(K) \varphi(L)).
\]
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 $\mathcal{O}(\min(dM(r), rM(d)))$.

**Proof:** (1) Show that

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

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