Let $\mathbb{K}$ be an effective field of characteristic zero. All complexities are expressed in terms of arithmetic operations in $\mathbb{K}$.

1. Krylov iterates and characteristic polynomial

Let $A \in \mathbb{K}^{n\times n}$. We assume that there exists a vector $v \in \mathbb{K}^{n\times 1}$ such that the matrix

$$P = \begin{bmatrix} v & Av & A^2v & \cdots & A^{n-1}v \end{bmatrix} \in \mathbb{K}^{n\times n}$$

is invertible.

(2.a) Show that there exist coefficients $f_0, \dots, f_{n-1} \in \mathbb{K}$ such that

$$AP = PC, \quad \text{where } C = \begin{bmatrix} 0 & & & f_0 \\ 1 & & & f_1 \\ & \ddots & & \vdots \\ & & 1 & f_{n-1} \end{bmatrix} \in \mathbb{K}^{n\times n}.$$

(2.b) Define $F(x) = x^n - f_{n-1}x^{n-1} - \cdots - f_1 x - f_0 \in \mathbb{K}[x]$. Show that $F(x)$ is the characteristic polynomial of A, that is, $F(x) = \det(xI_n - A)$.

(2.c) Describe an algorithm and the corresponding complexity bound for computing P from A and v. Deduce a complexity bound for computing the characteristic polynomial $F(x)$, given as input A and also the vector v.

2. Composition of a series with arcsine

Given a formal power series $F \in \mathbb{K}[[x]]$ satisfying $F(0) = 0$, we are interested in computing $C(x) := A(F(x))$ for $A(x) := \arcsin(x)$.

(1) Describe a naive general composition algorithm that takes as input two series truncated to order N and returns their composition up to order N, and estimate its complexity.

(2) Describe an algorithm of linear complexity which takes as input $N \in \mathbb{N}$ and computes the first N terms of $A(x)$. *Hint:* recall $A'(x) = (1 - x^2)^{-1/2}$.

(3) Describe an algorithm for calculating $C(x)$ up to order N by employing the naive algorithm of (1). What is its complexity? How much can this be improved by employing Kinoshita and Li's algorithm?

(4) Combine fast algorithms introduced in the course (Newton's scheme/fast computations with series) to compute $C(x)$ in complexity $O(\mathsf{M}(N))$.

3. Polynomial matrix equation $\mathbf{AU} = \mathbf{V}$.

Let $\mathbf{A} \in \mathbb{K}[x]^{m\times m}$ be nonsingular with all entries of degree $\le d_1$, let $\mathbf{V} \in \mathbb{K}[x]^{m\times k}$ with all entries of degree $\le d_2$.

Two typical cases of interest for the equation $\mathbf{AU} = \mathbf{V}$ are $k = 1$ (linear system solving over $\mathbb{K}[x]$), and $k = m$ with $\mathbf{V} = \mathbf{I}_m$ (inversion of $\mathbf{A}$).

(1) Show that $\mathbf{A}^{-1}\mathbf{V}$ can be represented as a fraction with numerator a matrix $\mathbf{U}$ in $\mathbb{K}[x]^{m\times k}$ and denominator a polynomial Δ in $\mathbb{K}[x]$.

(2) Give an upper bound on $\deg(\det(\mathbf{A}))$.

(3) Give upper bounds that you can require on $\deg(\Delta)$ and on the degrees of entries of $\mathbf{U}$ (i.e. there exists a couple $(\mathbf{U}, \Delta)$ for question 1 which satisfies these bounds).

(4) Prove that $\mathbf{A}^{-1} \in \mathbb{K}[x]^{m\times m} \Leftrightarrow \det(\mathbf{A}) \in \mathbb{K} \setminus \{0\}$.

Remark: matrices with determinant in $\mathbb{K} \setminus \{0\}$ are called *unimodular*.

4. Composition of a D-finite series with an algebraic series

(1) Show that if $f \in \mathbb{K}[[x]]$ is D-finite and if $g \in x\mathbb{K}[[x]]$ is algebraic, then $h := f \circ g$ is D-finite.
(2) Given an algorithm that takes as input a linear differential equation with coefficients in $\mathbb{K}[x]$ satisfied by $f(x)$ and a polynomial $P \in \mathbb{K}[x, y]$ such that $P(x, g(x)) = 0$, and that returns as output a linear differential equation with coefficients in $\mathbb{K}[x]$ satisfied by $h(x)$.

5. Differential equations vs differential systems

(1) Suppose that $y \in \mathbb{K}[[x]]$ is a solution of the differential equation

$$a_r(x)y^{(r)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0$$

where $a_0, \ldots, a_r \in \mathbb{K}(x)$ and $a_r \neq 0$. Give an $r \times r$ matrix $A \neq 0$ with entries in $\mathbb{K}(x)$ and a vector $Y \in \mathbb{K}[[x]]^r$ such that the first entry of Y is equal to y and Y satisfies the differential system

$$Y'(x) = A(x)Y(x).$$

(2) Suppose that $Y \in \mathbb{K}[[x]]^r$ satisfies the differential system

$$Y'(x) = A(x)Y(x)$$

where $A \in \mathbb{K}(x)^{r\times r}$. Show that the first entry of $Y(x)$ satisfies a nontrivial differential equation of order at most r with coefficients in $K(x)$ and give an algorithm taking A as input to compute such an equation.

6. Polynomial matrix operations via evaluation-interpolation.

Using the *evaluation-interpolation paradigm*,

(1) Give a multiplication algorithm for matrices in $\mathbb{K}[x]^{m\times m}$.
(2) Give a determinant algorithm.
(3) Give an inversion algorithm (finding the inverse over the fractions $\mathbb{K}(X)$).

Hints: exploit known degree bounds on the output to determine the number of points to use; for inversion, you can assume that you have at your disposal a quasi-linear algorithm for Cauchy interpolation (see the slides for references).

For each of these algorithms,

(1) Give the lower bound it requires on the cardinality of $\mathbb{K}$.
(2) State and prove an upper bound on its complexity.

Further perspective: could your complexity bounds take into account degree measures that refine the matrix degree such as the average row degree?

7. First n terms of a differentially finite series

Let $a_0, \ldots, a_r \in \mathbb{K}[x]$ be polynomials of degree at most d over an effective field $\mathbb{K}$ of characteristic zero. This problem studies the cost of computing the first n terms of a series solution $y(x) = \sum_{k=0}^{\infty} y_k x^k \in \mathbb{K}[[x]]$ to the equation

$$a_r(x)\theta^r(y) + \cdots + a_1(x)\theta(y) + a_0(x)y = 0 \qquad (1)$$

where θ is the operator mapping a series $f \in \mathbb{K}[[x]]$ to $xf'(x)$. We set $L = a_r(x)\theta^r + \cdots + a_1(x)\theta + a_0(x)$, so that (1) rewrites as $L(y) = 0$.

For any series $f \in \mathbb{K}[[x]]$ and integers ℓ, h, we denote $f_{\ell:h}(x) = \sum_{k=\ell}^{h-1} f_k x^k$. We also write $f_{:n}$ for $f_{0:n}$ and $f_{n:}$ for $f_{n:\infty}$.

(1) For $i, k \in \mathbb{N}$, write $\theta^i(x^k)$ as a function of i and k.

(2) Show that $L(y_{:n})$ is a polynomial of the form $\sum_{k=n}^{n+d-1} p_k x^k$.

Let $q(t) = \sum_{i=0}^{r} a_i(0) t^i$. We consider the following problem $T(L, y, n)$: given the operator L, the coefficients y_k for k such that $q(k) = 0$, and an integer n, and compute the truncated solution $y_{:n}$.

(3) For $q(k) \neq 0$, express the coefficient y_k in terms of $L(y_{:k})$ and $q(k)$.

(4) Deduce an algorithm that solves $T(L, y, n)$ in $O(rdn)$ operations. What happens in your algorithm when $q(k) \neq 0$ for all $k \in \mathbb{N}$?

(5) Briefly explain how to solve $T(L, y, n)$ in $O(nd \log(r)^p)$ operations for some $p \in \mathbb{N}$ (for instance, by adapting the previous algorithm).

(6) Show that, given the operator L, integers $m, n \in \mathbb{N}$, and the truncated series solution $y_{:n}$, one can compute $L(y_{n-m:n})_{:n+m}$ in $O(r\mathsf{M}(m))$ operations.

(7)* Describe an algorithm that takes as input L, the coefficients y_k for k such that $q(k) = 0$, two integers $\ell \leqslant h$, and the polynomial $L(y_{\ell:h})_{:h}$, and computes $y_{\ell:h}$ in

$$O(r\mathsf{M}(h - \ell) \log(h - \ell))$$

operations. Deduce that one can solve $T(L, y, n)$ in $O(r\mathsf{M}(n) \log(n))$ operations (uniformly in d, that is, so that the implied constant does not depend on d).

(8) Deduce an algorithm that solves $T(L, y, n)$ in $O(rn \log(d)^p)$ operations for some $p \in \mathbb{N}$.

(9)** Can you solve $T(L, y, n)$ in significantly less than $\min(r, d) n \lambda(\max(r, d))$ operations, where $\lambda(t) = \mathsf{M}(t)/t$?