1 Exercise 1 from 25/10

Let $K$ be a field. Show that if $P \in K[x]$ has degree $d$, then the sequence $(P(n))_{n \geq 0}$ is C-recursive, and admits $(x - 1)^{d+1}$ as a characteristic polynomial.

Deduce that $P$ can be evaluated at the $N \gg d$ points $1, 2, \ldots, N$ in $O(N M(d)/d)$ operations in $K$.

2 Exercise 2 from 25/10

Let $P = \sum_{i=0}^{2N} p_i x^i \in \mathbb{Z}[X]$ be the polynomial $P(x) = (1 + x + x^2)^N$.

1. Show that the parity of all coefficients of $P$ can be determined in $O(M(N))$ bit ops.
2. Show that $P$ satisfies a linear differential equation of order 1 with polynomial coefficients.
3. Determine a linear recurrence of order 2 satisfied by the sequence $(p_i)_i$.
4. Give an algorithm that computes $p_N$ in $\tilde{O}(N)$ bit ops.

3 Exercise 1 from 08/11: Matrix equation $A U = V$.

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

Two typical cases of interest for the equation $A U = V$ are $k = 1$ (linear system solving over $K[X]$), and $k = m$ with $V = I_m$ (inversion of $A$).

1. Show that $A^{-1}V$ can be represented as a fraction with numerator a matrix $U \in K[X]^{m \times k}$ and denominator a polynomial $\Delta$ in $K[X]$.
2. Give an upper bound on $\deg \det(A)$.
3. Give upper bounds that you can require on $\deg(\Delta)$ and on the degrees of entries of $U$ (i.e. there exists a couple $(U, \Delta)$ for question 1 which satisfies these bounds).
4. Prove that $A^{-1} \in K[X]^{m \times m} \iff \det(A) \in K \setminus \{0\}$.

Remark: matrices with determinant in $K \setminus \{0\}$ are called unimodular.
4 Exercise 2 from 08/11: Evaluation-interpolation and polynomial matrices.

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?

5 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 $A(X) := \text{arcsin}(X)$.

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 Brent and Kung’s algorithm?
4. Combine fast algorithms introduced in the course (Newton’s scheme/fast computations with series) to compute $C(X)$ in complexity $O(M(N))$.

6 Symmetric functions of roots

Let $N$ be a positive integer and let $P$ and $Q$ be two monic polynomials in $\mathbb{K}[X]$, with degrees at most $N$. The aim of this exercise is to efficiently calculate the sum

$$s(P, Q) = \sum_{\alpha \in \mathbb{P}(\alpha) = 0} Q(\alpha),$$

this sum being taken over all the roots of $P$ in an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, counted with their multiplicities.

1. Express $s(P, Q)$ using a resultant of polynomials in two variables. Deduce that $s(P, Q)$ is an element of $\mathbb{K}$. 

2
2. Propose an algorithm for computing \( s(P,Q) \), based on (1). Estimate its complexity.

3. Show that it is possible to calculate the set of elements

\[
s(P,1), s(P,X), s(P,X^2), \ldots, s(P,X^N)
\]

using \( O(M(N)) \) operations in \( \mathbb{K} \).

4. Deduce that \( s(P,Q) \) can be computed in \( O(M(N)) \) operations in \( \mathbb{K} \).

7 Resultant and modular multiplication

This exercise shows some alternate proofs for the theory of the resultant.

Let \( K \) be a field and, for any integer \( d \), let \( K[X]_{<d} \) be the space of polynomials of degree less than \( d \). Let \( A \) and \( B \) be two monic polynomials of degree \( a \) and \( b \) respectively.

Consider the endomorphism \( F_{A,B} \) of \( K[X]_{<a+b} \) defined by

\[
F_{A,B}(U + X^aV) = BU + AV,
\]

for any \( U \in K[X]_{<a} \) and \( V \in K[X]_{<b} \).

1. Show that \( \det F_{A,B} = \pm \res(A,B) \).

Let \( M_{A,B} \) be the endomorphism of \( K[X]/(A) \) induced by the multiplication by \( B \).

2. Show that \( \det F_{A,B} = \det M_{A,B} \).

Hint: factor \( F_{A,B} \) as \( H \circ G \) where \( G \) is identity on \( K[X]_{<a} \) and \( H \) is identity on \( X^a K[X]_{<b} \).

3. Deduce the multiplicativity of resultant and the Poisson formula.