Fondements de l'Algorithmique Algébrique
Introduction to Algebraic Algorithms

Instructions

This page contains the main instructions.
Page 2 contains the exercises.

Duration: 1h30.

The answers can be written either in English or in French.

All documents and electronic devices are forbidden, except one sheet of paper with your handwritten notes (there can be writing on both recto and verso of this sheet).

Phones must be off or in silent mode, and kept in bags and out of sight. All communication is forbidden, except with the teachers.

The precision, the clarity, and the mathematical rigour of the reasonings, the explanations, and the algorithms, will play an important role in the grading.

In all what follows, $\mathbb{K}$ stands for an arbitrary field, $\mathbb{K}[x]$ stands for the ring of univariate polynomials in x over $\mathbb{K}$, and $\mathbb{K}^{m\times n}$ stands for the space of $m \times n$ matrices over $\mathbb{K}$.

Problem 1 (Knowledge of course material)**.**

1. Is $\mathbb{Z}/7\mathbb{Z}$ a field? Is $\mathbb{Z}/9\mathbb{Z}$ a field? Does there exist a field with 4 elements? Justify your answers.
2. Let $P \in \mathbb{K}[x]$ be an irreducible polynomial. Let A be a nonzero element of the quotient: $A \in \mathbb{K}[x]/\langle P \rangle$. Is A invertible? (If yes, explain why; if no, give a counterexample.) Now, we make the assumption that A is invertible: concisely describe the standard method for computing the inverse of A, and its complexity.
3. Give a concise description of the main steps of an algorithm for computing the evaluations $p(\alpha_1), \ldots, p(\alpha_n)$ of a polynomial $p \in \mathbb{K}[x]$ of degree $< n$ at points $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$. Give a bound on its complexity.
4. Give a complexity bound for the problem of solving a linear system whose matrix is an $n \times n$ Vandermonde matrix. Same question for a quasi-Toeplitz matrix of displacement rank α.
5. In error-correcting codes, what is the goal of "introducing redundancy", and why is it necessary?
6. Recall the Singleton bound for the minimum distance of a linear code. For a code of length $n = 256$ and dimension $k = 156$, what is the maximal number of errors we can hope to correct?

Problem 2 (Matrices: inversion is not easier than multiplication)**.**

1. Let A and B be matrices in $\mathbb{K}^{n \times n}$. We define the matrix
$$C = \begin{bmatrix} I & A & 0 \\ 0 & I & B \\ 0 & 0 & I \end{bmatrix} \in \mathbb{K}^{3n \times 3n},$$
where I is the $n \times n$ identity matrix and 0 is the $n \times n$ zero matrix. What is the inverse of C?
2. Suppose you have an algorithm `Invert(M)` which takes as input a square and invertible matrix M in $\mathbb{K}^{n \times n}$ for some $n > 0$, and returns its inverse M^{-1}. Using the result of the previous question, describe the pseudocode of an algorithm `MatMul(A,B)` which takes as input two matrices A and B in $\mathbb{K}^{n \times n}$ and returns the matrix product $A \cdot B$.
3. Deduce that "*inversion is not easier than multiplication*", that is, more precisely: if there is an algorithm in $O(n^\omega)$ for matrix inversion, then there is an algorithm in $O(n^\omega)$ for matrix multiplication.

Note: the converse is also true, but the proof is a bit more difficult; it is based on blockwise Gaussian elimination / Schur complements. As a result, matrix inversion and matrix multiplication are equivalent in terms of complexity.

Problem 3 (Polynomial division with remainder)**.**

Let $a(x)$ and $b(x)$ be polynomials in $\mathbb{K}[x]$, of respective degrees m and n, with $b \neq 0$. We are interested in the efficient computation of the quotient $q(x)$ and remainder $r(x)$ in the division of $a(x)$ by $b(x)$.

1. Recall the definition of $q(x)$ and $r(x)$. What is the complexity of naive division with remainder?
2. If $m < n$, what is $(q(x), r(x))$? If $m = n$, describe $(q(x), r(x))$ in function of $a(x)$ and $b(x)$ and λ, where $\lambda \in \mathbb{K} \setminus \{0\}$ is the leading coefficient of $b(x)$.
3. Define $\bar{b}(x) = x^n b(1/x)$. For example, describe $\bar{b}(x)$ in the case $b(x) = 5x + 2x^2 + 3x^4$ with $\mathbb{K} = \mathbb{Z}/6\mathbb{Z}$. Coming back to the general case, is $\bar{b}(x)$ in $\mathbb{K}[x]$? Justify your answer.

In what follows, we also define $\bar{a}(x) = x^m a(1/x)$, and we assume $m \geq n$.

3. We can see $\bar{b}(x)$ as a formal power series in $\mathbb{K}[[x]]$. Explain why $\bar{b}(x)$ is invertible as a power series. Give the name of an algorithm, and a corresponding complexity bound, for efficiently computing the truncated expansion of its inverse at a given order k, that is, $\bar{b}(x)^{-1} \bmod x^k$.
4. Deduce a complexity bound for the computation, as a power series, of $\bar{f}(x) = \bar{a}(x)\bar{b}(x)^{-1} \bmod x^{m-n+1}$.
5. Seeing $\bar{f}(x)$ as a polynomial of degree $\leq m-n$, we define $f(x) = x^{m-n}\bar{f}(1/x)$. Prove that the polynomial $a(x) - b(x)f(x)$ has degree less than $n = \deg(b(x))$. *Hint: if you don't manage to solve this question, you can still use the result to continue.*
6. How can one recover the quotient and remainder $(q(x), r(x))$ from $f(x)$ and $a(x) - b(x)f(x)$?
7. Based on your answers to the previous questions, describe an algorithm which takes as input two polynomials $a(x)$ and $b(x)$ in $\mathbb{K}[x]$ with $b \neq 0$, and returns the quotient $q(x)$ and remainder $r(x)$ in the division of $a(x)$ by $b(x)$. Give a complexity bound for this algorithm, and compare to the naive algorithm.