SORBONNE UNIVERSITÉ

Fondement de l'algorithmique algébrique - FLAG

Academic year 2022-23

Notes

Instructor : Prof.

written by
Hayato Ishida

Contents

I. Introduction

I.1. Ring and Field

Rough definition : Field is a set F with two operations $(+, \times)$ with "usual" properties (e.g. $a(b+c) = ab+ac$, $a(bc) = (ab)c$ etc...). And every element has an inverse. If one of the elements does not have an inverse, it is a ring.

- So, elements in the field can be inverted except 0.

- Every element $a \in F$ has an opposite for $+$, these act on b s.t. $a + b = 0$. This is true for all rings and fields.

- Therefore, invertibility is about "$\times$"

Remark : Ring $\leftarrow$ Field

Examples

- $\mathbb{R}$ the set of real numbers (field). $\mathbb{Q}$ rational (field). $\mathbb{C}$ complex (field).

- $\mathbb{Z}$ integers is not a field, thus a ring. Why?

This is because 2 is not invertible. For instance, there is no $x \in \mathbb{Z}$ s.t. $2x = 1$.

- $\mathbb{Z}/p\mathbb{Z}$ is a field. In general, $a \in \{1, ..., p-1\}$, there are u, v s.t. $au + pv = 1$, so $au = 1 \, mod \, p$.

- $\mathbb{Z}/4\mathbb{Z}$ is not a field, why? $\rightarrow$ because 2 is not invertible.

I.2. Complexity

In this course, we manipulate algebraic objects. For instance, polynomials (ring), matrices (field) and more. Complexity measure the efficiency of algorithms. Algebraic complexity is counting the number of operations in the base ring and field.

Complexity here does not take into account of ...

- all memory related operations

- the size of the elements in the base ring or field. (e.g. : addition of polynomials of degree $\leq d$ in $\mathbb{Q}[x]$, algebraic complexity is $O(d)$ and ignore the size of the rational coefficients.

*You should be familiar with complexity from MODEL.

I.3. Matrices

For a field $\mathbb{K}$ or denote by $\mathbb{K}^{m \times n}$ the set of $m \times n$ matrices over $\mathbb{K}$.

Recall : Not a ring because .... ??

It is represented as a two dimensional array with rows and columns. $A = (a_{i\,j}) \in \mathbb{K}^{m \times n}$ where $0 \leq i \leq m$ and $0 \leq j \leq n$.

Addition

Complexity is $O(m\,n)$, operations in $\mathbb{K}$.

Multiplication

Multiplication of $A \in \mathbb{K}^{m \times n}$ by $B \in \mathbb{K}^{n \times p}$

- Naive algorithm : $O(m\,n\,p)$

- Strassen's algorithm (recall form MODEL) has complexity $O(n^{log_2(7)})$ where $m = n = p$

- For alternative there is a lot of work on matrix multiplication algorithm. Best performance today is $O(n^{2.37})$ but for the moment it is impractical.

I.4. Polynomials

For a field $\mathbb{K}$ or a ring $\mathbb{R}$, the sets $\mathbb{K}[x]$, $\mathbb{R}[x]$ are those of polynomials in one variable x.

$\mathbb{K}[x] = \{P = P_0 + P_1 x + P_2 x^2 + ... + P_d x^d\}$ in $\mathbb{K}$. (same for $\mathbb{R}$)

They are represented as a one-dimensional array $[P_0, P_1, P_2, ..., P_d]$.

Addition

of two polynomials in $\mathbb{R}[x]$ of degree $\leq d$ has a complexity $O(d)$ operations in $\mathbb{R}$.

Multiplication :

- Naive algorithm : $O(d^2)$ operations in $\mathbb{R}$ - Karatsuba (recall from MODEL) : $O(d^{log_2(3)}) \approx O(d^{1.584})$ operations in $\mathbb{R}$

- For alternative FFT (again, recall from MODEL) : $O(d\,log(d)\,log\,log(d))$