CS 487/687 Introduction to Symbolic Computation

Keven Qiu
Instructor: Armin Jamshidpey

Chapter 1

Basic Algebraic Domains

1.1 Mathematical Domains

Most algorithms for polynomials, matrices, etc. come from

- Integers
- Rational numbers
- Integers modulo n (n is often a prime or a power of a prime)
- Algebraic extensions ($\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2+\sqrt{3}})$)
- Complex numbers

Definition: Ring

A set with an operation $+$ and an operation $\times$ where

- $a + 0 = 0 + a = a$
- $a + (-a) = 0$
- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- $a(bc) = (ab)c$
- $a(b + c) = ab + ac$

Definition: Commutative Ring

A ring where $ab = ba$.

Definition: Ring with Unit

A ring with a special element 1 such that $a \cdot 1 = 1 \cdot a = a$.

1.2 Integers, Rationals, and Polynomials

Assume that the machine architecture has 64 bits. Therefore, integers are represented exactly in $[0, 2^{64} - 1]$. For larger integers, we can use an array of word-size numbers.

Any integer a can be expressed as

$$a = (-1)^s \sum_{i=0}^{n} a_i B^i$$

where $B = 2^{64}, s \in \{0, 1\}, 0 \leq a_i \leq B - 1$.

If $0 \leq n + 1 < 2^{63}$, then a can be encoded as an array

$$[s \cdot 2^{63} + n + 1, a_0, \ldots, a_n]$$

of 64 bit words.

Polynomials can be represented in dense (arrays) or sparse (linked lists) forms. Multivariate polynomials are typically sparse.

Definition: Field

A ring $\mathbb{F}$ with addition and multiplication such that every nonzero element has a multiplicative inverse.

Some examples of fields include rational numbers $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Z}_p$, $\mathbb{F}_q$ (finite field of size $q = p^k$), $\mathbb{R}$, and $\mathbb{C}$.

Given a base ring R, we can construct a polynomial ring $R[x]$ by adding a new free variable x to R. Elements will have the form $a_0 + a_1 x + \cdots + a_d x^d$, $a_i \in R$. Equality is defined by their coefficients.

Definition: Greatest Common Divisor

The greatest common divisor of $a, b \in R$, denoted $\gcd(a, b)$ is an element $c \in R$ such that c divides both a and b and if r divides both a and b, then r divides c.

gcd's do not always exist as it depends on the ring, and even if it does exist, it is not clear that an algorithm exists.

Definition: Unit

$u \in R$ is a unit if there is $v \in R$ such that $uv = 1$.

Definition: Associates

$a, b \in R$ are associates if $a = ub$ with $u \in R$ a unit.

3 and -3 are associates in $\mathbb{Z}$, 3 and 9 are associates in $\mathbb{Z}_{12}$.

Definition: Irreducible

A non-unit element $a \in R \setminus \{0\}$ is irreducible if $a = bc$ implies one of b, c is a unit.

Definition: Zero Divisor

An element $a \in R \setminus \{0\}$ such that there is a non-zero $b \in R \setminus \{0\}$ such that $a \cdot b = 0$.

Definition: Integral Domain

A ring R having no zero divisor.

Definition: Euclidean Domain

An integral domain R with a Euclidean function $|\cdot| : R \to \mathbb{N} \cup \{-\infty\}$ such that for all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r, |r| < |b|$$

E.g. $\mathbb{Z}$ is a Euclidean domain with Euclidean function absolute value, units are ± 1 and irreducibles are prime integers.

E.g. $\mathbb{F}[x]$ is a Euclidean domain with Euclidean function degree, units are constant polynomials, and irreducibles are polynomials that do not factor.

E.g. $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean function $|a + bi| = a^2 + b^2$, units are $\pm 1, \pm i$.

E.g. $\mathbb{R}[x]$ is not a Euclidean domain when R is not a field, units are constants which are units in R.

Measuring cost in rings:

- $\mathbb{Z}$: The bit complexity of the integer is

$$\log a = \begin{cases} 1 & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor & \text{otherwise} \end{cases}$$

- $\mathbb{Q}$: The complexity of a/b is the total bit complexity of a and b.
- $\mathbb{F}_q$: The complexity is bit complexity $\log q$.
-

1.3 Basic Algebraic Operations with Cost

Addition over $\mathbb{Z}[x]$

Input: two elements $a, b \in \mathbb{Z}[x]$, $\deg(a) = m$, $\deg(b) = n$.
Output: $c = a + b$.
$c_i = a_i + b_i$ for $0 \leq i \leq \max(m, n)$ and the running time is $O(m + n)$.

Multiplication over $\mathbb{Z}[x]$

Input: two elements $a, b \in \mathbb{Z}[x]$.
Output: $a \cdot b$.
$c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Compute all $(m+1)(n+1)$ multiplications of $a_i b_j$ and add them so running time is $O(mn)$.

Addition and Multiplication Over $R = \mathbb{Z}$

Input: two elements $a, b \in \mathbb{Z}$.
Output: $a + b$ and $a \cdot b$.
Use bit representation of a, b. For addition, the running time is $O(\log a + \log b)$. For multiplication, there are $\lceil \log b \rceil$ additions of multiples of a, so running time is $O(\log a \cdot \log b)$.

So over $\mathbb{Z}$ we count bit operations and over $\mathbb{Z}[x]$ we count operations in $\mathbb{Z}$.

Division with Remainder over $\mathbb{Z}[x]$

Input: two elements $a, b \in \mathbb{Z}[x]$, with b nonzero and $LC(b)$ unit in $\mathbb{Z}$.
Output: $q, r \in \mathbb{Z}[x]$ such that $\deg(r) < \deg(b)$ and $a = qb + r$.
Start with $r = a, q = 0$. While $\deg(r) \geq \deg(b)$, do $q = q + x^{\deg(r)-\deg(b)}$ and $r = r - x^{\deg(r)-\deg(b)} \cdot \frac{LC(r)}{LC(b)} \cdot b$. We perform at most $\deg(a) - \deg(b) + 1$ subtractions to r so total time is $(\deg(a) - \deg(b) + 1)(\deg(b) + 1)$.

Division with Remainder over $\mathbb{Z}$

Input: two elements $a, b \in \mathbb{Z}$, with b nonzero.
Output: $q, r \in \mathbb{Z}$ such that $|r| < |b|$ and $a = qb + r$.
Start with $r = a, q = 0$. While $|r| \geq |b|$, do $q = q + 1$ and $r = r - b$. We perform $\lfloor a/b \rfloor$ subtractions to r, total time is $\frac{a \log b}{b}$.