CS201

Mathematics for Computer Science I

Lecture 19

Real Numbers and Their Representations

- A real number is typically represented using decimal notation with possibly infinitely many digits after decimal:

$$\pi = 3.1415 \cdots$$

- How does one represent a real number with infinitely many digits using only finite size?
- It is not always possible:
  - Set of all finite representations has size $\aleph_0$ while set of reals has size $\aleph_1$.

Real Numbers and Their Representations

- For many reals a finite representation is possible using algorithms:
  - Specify an algorithm for a real r that on input n, produces nth digit of r after decimal.
- For example, π can be represented by an algorithm that computes nth digit using formulas

$$\pi = 16 \tan^{-1}(\frac{1}{5}) - 4 \tan^{-1}(\frac{1}{239}),$$

and

$$\tan^{-1}(x) = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \frac{1}{7}x^7 + \cdots$$

- The property of such algorithms is that for input n, they produce the nth digit in finite time.

Arithmetic on Reals

- Given two reals numbers r and s in their algorithmic representation, how does one add or multiply them?
- We would like to define an algorithmic representation of their sum and addition.
- Even for sum, it is not clear how to define such an algorithm:
  - To compute nth digit of $r + s$, an algorithm can compute nth and $(n + 1)$st digits of r and s, check if the addition of $(n + 1)$st digits produces a carry, and then add two nth digits with possible carry.
  - This fails if addition of $(n + 1)$st digits equals 9.
  - We may try to compute additional digits after decimal of r and s to decide if there is a carry to nth digit.
  - We will continue failing as long as all pairs of additional digits sum to 9.
  - It may continue for infinitely many digits!

Arithmetic on Reals

- Therefore, it is not clear how to add real numbers in general!
- Situation with multiplication or division is even worst.
- Need to define the real numbers and arithmetic on it in a better way.

Axiomatization of Numbers and Arithmetic

- Axiomatization of mathematics via sets ensured that anomalies are removed.
- Similarly, we need to axiomatize numbers and arithmetic on them to get a proper definition of these for reals.
- We do this over next few slides.

Interdependence of Numbers and Arithmetic

- What are numbers?
  - Symbols are not numbers.
  - It is the properties that define them, that is, arithmetic properties.
- What is arithmetic?
  - Relations on numbers satisfying certain properties.
- Due to this interdependence, we define both simultaneously.

Axioms of Addition

- Let S be a set of elements with relation $A \subset S \times S \times S$ defined.
- Relation A satisfies the following properties:

  Closure For every $a, b \in S$, there is a unique $c \in S$ with $(a, b, c) \in A$.

  Associativity If $(a_1, a_2, b), (b, a_3, c), (a_2, a_3, d), (a_1, d, c') \in A$ then $c = c'$.

  Commutativity If $(a_1, a_2, b) \in A$ then $(a_2, a_1, b) \in A$.

  Identity There is $0 \in S$ such that $(a, 0, a) \in A$ for every a.

  Inverse For every $a \in S$, there exists $b \in S$ such that $(a, b, 0) \in A$.

Axioms of Addition: Restated

- We can view A as a function $A : S \times S \mapsto S$ due to closure property.
- Writing $A(a, b)$ as $a \cdot b$ and e for 0, the axioms can be restated as:

Closure: For every $a, b \in S$, there is a unique $c \in S$ with $a \cdot b = c$.

Associativity: $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$.

Commutativity: $a_1 \cdot a_2 = a_2 \cdot a_1$.

Identity: There is $e \in S$ such that $a \cdot e = a$ for every a.

Inverse: For every $a \in S$, there exists $b \in S$ such that $a \cdot b = e$.

Properties of A

- There is a unique identity.
  - Suppose $a \cdot e' = a$ for all $a \in S$.
  - Then, $e' = e \cdot e' = e$.
- For every $a \in S$, there is a unique $b \in S$ with $a \cdot b = e$.
  - Suppose $a \cdot b = e = a \cdot c$.
  - Then $b = b \cdot e = b \cdot a \cdot c = a \cdot b \cdot c = e \cdot c = c$.

Examples

- Set of integers ($\mathbb{Z}$) with addition
- Set of rationals ($\mathbb{Q}$), reals ($\mathbb{R}$), complex numbers ($\mathbb{C}$) with addition
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with multiplication
- Set of polynomials over $\mathbb{Z}/\mathbb{Q}/\mathbb{R}/\mathbb{C}$ in n variables with addition
- Set of $n \times n$ matrices over $\mathbb{Z}/\mathbb{Q}/\mathbb{R}/\mathbb{C}$ with addition

Definition

Groups

A group $(G, \cdot)$ is a set of elements G with operation $\cdot$ on G satisfying the closure, associativity, identity, and inverse properties.

- Groups with commutativity property are called commutative groups.
- Groups without commutativity property are called non-commutative groups.
- We assume that a group is commutative by default, and specify non-commutative groups.

Example: Non-commutative Groups

- Set of $n \times n$ invertible matrices over $\mathbb{Q}/\mathbb{R}/\mathbb{C}$ with multiplication
- Set of bijections of a set to itself with composition operation:
  - If f and g are bijections, so is $f \circ g$.
  - Identity map is identity and inverse map is inverse.