CS311H: Discrete Mathematics

Sets, Russell's Paradox, and Halting Problem

Instructor: Işıl Dillig

Existence and Uniqueness

- Common math proofs involve showing existence and uniqueness of certain objects
- Existence proofs require showing that an object with the desired property exists
- Uniqueness proofs require showing that there is a unique object with the desired property

Existence Proofs

- One simple way to prove existence is to provide an object that has the desired property
- This sort of proof is called constructive proof
- Example: Prove there exists an integer that is the sum of two perfect squares
- Can also prove existence through other methods (e.g., proof by contradiction or proof by cases)
- Such indirect existence proofs called nonconstructive proofs

Non-Constructive Proof Example

- Prove: "There exist irrational numbers x, y s.t. x^y is rational"
- We'll prove this using a non-constructive proof (by cases), without providing irrational x, y
- Consider $\sqrt{2}^{\sqrt{2}}$. Either (i) it is rational or (ii) it is irrational
- Case 1: We have $x = y = \sqrt{2}$ s.t. x^y is rational
- Case 2: Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, so both are irrational. Then, $\sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$. Thus, x^y is rational

Proving Uniqueness

- Some statements in mathematics assert uniqueness of an object satisfying a certain property
- To prove uniqueness, must first prove existence of an object x that has the property
- Second, we must show that for any other y s.t. $y \neq x$, then y does not have the property
- Alternatively, can show that if y has the desired property that $x = y$

Example of Uniqueness Proof

- Prove: "If a and b are real numbers with $a \neq 0$, then there exists a unique real number r such that $ar + b = 0$"
- Existence: Using a constructive proof, we can see $r = -b/a$ satisfies $ar + b = 0$
- Uniqueness: Suppose there is another number s such that $s \neq r$ and $as + b = 0$. But since $ar + b = as + b$, we have $ar = as$, which implies $r = s$.

Invalid Proof Strategies

- Proof by obviousness: "The proof is so clear it need not be mentioned!"
- Proof by intimidation: "Don't be stupid – of course it's true!"
- Proof by mumbo-jumbo: $\forall \alpha \in \theta \exists \beta \in \alpha \diamond \beta \approx \gamma$
- Proof by intuition: "I have this gut feeling.."
- Proof by resource limits: "Due to lack of space, we omit this part of the proof..."
- Proof by illegibility: "sdjikfhiugyhjlaks??fskl; QED."

Don't use anything like these in CS311!!

Sets and Basic Concepts

- A set is unordered collection of distinct objects
- Example: Positive even numbers less than 10: {2, 4, 6, 8}
- Objects in set S are called members (or elements) of that set
- If x is a member of S, we write $x \in S$
- $\#$ elements in a set is called its cardinality, written $|S|$

Important Sets in Mathematics

- Many sets that play fundamental role in mathematics have infinite cardinality
- Set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- Set of positive integers: $\mathbb{Z}^+ = \{1, 2, \ldots\}$
- Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, ...\}$
- Set of real numbers: $\mathbb{R} = \{\pi, \ldots, -1.999, \ldots, 0, \ldots, 0.000001, \ldots\}$

Set Builder Notation

- Infinite sets are often written using set builder notation

$$S = \{x \mid x \text{ has property } p\}$$

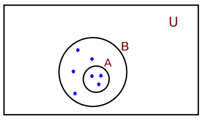
- Example: $S = \{x \mid x \in \mathbb{Z} \ \wedge \ x\%2 = 0\}$
- Which set is S?
- Example: $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z} \ \wedge \ q \in \mathbb{Z} \ \wedge \ q \neq 0\}$
- Which set if $\mathbb{Q}$?

Special Sets

- The universal set, written U, includes all objects under consideration
- The empty set, written $\emptyset$ or $\{\}$, contains no objects
- A set containing exacly one element is called a singleton set
- What special set is $S = \{x \mid p(x) \wedge \neg p(x)\}$ equal to?
- What special set is $S = \{x \mid p(x) \vee \neg p(x)\}$ equal to?

Subsets and Supersets

- A set A is a subset of set B, written $A \subseteq B$, iff every element in A is also an element of B $(\forall x.\ x \in A \Rightarrow x \in B)$



- If $A \subseteq B$, then B is called a superset of A, written $B \supseteq A$
- A set A is a proper subset of set B, written $A \subset B$, iff:

$$(\forall x.\ x \in A \Rightarrow x \in B) \wedge (\exists x.\ x \in B \wedge x \notin A)$$

- Sets A and B are equal, written $A = B$, if $A \subseteq B$ and $B \subseteq A$

Power Set

- The power set of a set S, written $P(S)$, is the set of all subsets of S.
- Example: What is the powerset of $\{a, b, c\}$?
- Fact: If cardinality of S is n, then $|P(S)| = 2^n$
- What is the power set of $\emptyset$?
- What is the power set of $\{\emptyset\}$?

Ordered Tuples

- An important operation on sets is called Cartesian product
- To define Cartesian product, need ordered tuples
- An ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is the ordered collection with a_1 as its first element, a_2 as its second element, $\ldots$, and a_n as its last element.
- Observe: $(1, 2)$ and $(2, 1)$ are not the same!
- Tuple of two elements called pair (3 elements called triple)

Cartesian Product

- The Cartesian product of two sets A and B, written $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

- Example: Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. What is $A \times B$?
- Example: What is $B \times A$?
- Observe: $A \times B \neq B \times A$ in general!
- Observe: If $|A| = n$ and $|B| = m$, $|A \times B|$ is nm.

More on Cartesian Products

- Cartesian product generalizes to more than two sets
- Cartesian product of $A_1 \times A_2 \ldots \times A_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in A_i$
- Example: If $A = \{1, 2\}, B = \{a, b\}, C = \{\star, \circ\}$, what is $A \times B \times C$?

Set Operations

- Set union:

$$A \cup B = \{x \mid x \in A \ \vee x \in B\}$$

- Intersection:

$$A \cap B = \{x \mid x \in A \ \wedge x \in B\}$$

- Difference:

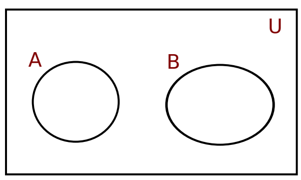
$$A - B = \{x \mid x \in A \ \wedge x \notin B\}$$

- Complement:

$$\overline{A} = \{x \mid x \notin A\}$$

Disjoint Sets

- Two set A and B are called disjoint if $A \cap B = \emptyset$



Exercise

Prove De Morgan's law for sets: $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Naive Set Theory and Russell's Paradox

- Intuitive formulation of sets is called naive set theory – goes back to German mathematician George Cantor (1800's)
- In naive set theory, any definable collection is a set (axiom of unrestricted comprehension)
- In other words, unrestricted comprehension says that $\{x \mid F(x)\}$ is a set, for any formula F
- In 1901, Bertrand Russell showed that Cantor's set theory is inconsistent
- This can be shown using so-called Russell's paradox

Russell's Paradox

- Let R be the set of sets that are not members of themselves:

$$R = \{S \mid S \notin S\}$$

- Two possibilities: Either $R \in R$ or $R \notin R$
- Suppose $R \in R$.
- But by definition of R, R does not have itself as a member, i.e., $R \notin R$
- But this contradicts $R \in R$

Russell's Paradox, cont.

- Now suppose $R \notin R$ (i.e., R not a member of itself)
- But since R is the set of sets that are not members of themselves, R must be a member of R!
- This shows that set R cannot exist, contradicting the axiom of unrestricted comprehension!!
- Since we have a contradiction, one can prove any nonsense using naive set theory!
- Much research on consistent versions of set theory $\Rightarrow$ Zermelo's ZFC, Russell's type theory etc.

Illustration of Russell's Paradox

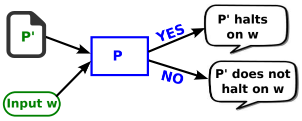
- Russell's paradox and other similar paradoxes inspired artists at the turn of the century, esp. Escher and Magritte
- Belgian painter Rene Magritte made a graphical illustration of Russell's paradox:

Undecidability

- A proof similar to Russell's paradox can be used to show undecidability of the famous Halting problem
- A decision problem is a question of a formal system that has a yes or no answer
- Example: satisfiability/valid in FOL or propositional logic
- A decision problem is undecidable if it is not possible to have algorithm that always terminates and gives correct answer

The Halting Problem

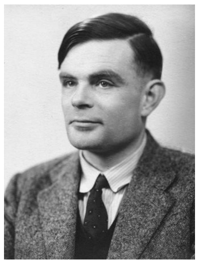
- The famous Halting problem in CS undecidable.
- Halting problem: Given a program P' and an input w, does P' terminate on w?
- What does it mean for this problem to be (un)decidable?



- Important: For this problem to be decidable, P should terminate on all inputs and give correct yes/no answer

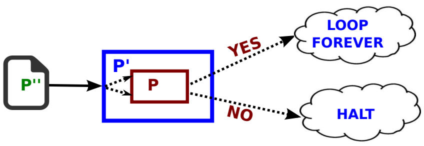
Undecidability of Halting Problem

- Undecidability of Halting Problem proved by Alan Turing in 1936
- Proof is quite similar to Russell's paradox



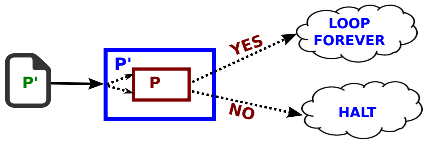
Proof of Undecidability of Halting Problem

- Assume such a program P exists
- Now, construct program P' such that P' halts iff its input does not halt on itself:



Proof of Undecidability, cont.

- Now, consider running P' on itself:



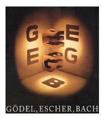
- Two possibilities:
  1. P' halts on itself: P must answer yes $\Rightarrow$ P' loops forever on P', i.e., $\perp$
  2. P' does not halt on P': P must answer no $\Rightarrow$ P' halts on itself, i.e., $\perp$
- Hence, such a program P cannot exist, i.e., Halting problem is undecidable!

Other Famous Undecidable Problems

- Validity in first-order logic: Given an arbitrary first order logic formula F, is F valid? (Hilbert's Entscheidungsproblem)
- Program verification: Given a program P and a non-trivial property Q, does P satisfy property Q? (Rice's theorem)
- Hilbert's 10th problem: Does a diophantine equation $p(x_1, \ldots, x_n) = 0$ have solutions? (i.e., integer solutions)

Provability and Computability

- If paradoxes and computability/provability proofs interest you...
  - Take theory of computation and mathematical logic courses
  - Book recommendation: "Godel, Escher, Bach" by Douglas Hofstadter



Exercise: Barber's paradox

- According to an ancient Sicilian legend, a remote town can only be reached by traveling a dangerous mountain road.
- The barber of this town shaves all those people, and only those people, who do not shave themselves.
- Can such a barber exist?