CSCI 2824 - CU Boulder, 2019 Summer

Lecture 10: Set theory

18 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications,
Rosens's Discrete Mathematics and its Applications,
Bettina and Thomas Richmond's A Discrete Transition to Advanced Mathematics, and Andrew Altomare's notes.

We defined a ton of stuff yesterday. Let's quickly review it. Then, we will do some proofs!

1 Subset relationships

These are some simple ideas that are quick to prove.

Exercise
Prove the inclusion of intersection: that for all sets A and B, we have $A \cap B \subset A$ and $A \cap B \subset B$.

Let A and B be sets. If $x \in A \cap B$ then $x \in A$ and $x \in B$. Thus, we get both statements.

Exercise
Prove the inclusion in union: For all sets A and B we have $A \subset A \cup B$ and $B \subset A \cup B$.

$\forall x \in A$ then $x \in A \cup B$ since $A \cup B$ is the set of all elements in at least A or in B. Similarly, we show $B \subset A \cup B$.

Exercise
Prove the transitive property of subsets. For all sets A, B, and C, if $A \subset B$ and $B \subset C$, then $A \subset C$.

Consider some $x \in A$. Since $A \subset B$, then $x \in B$. Further since $B \subset C$, then $x \subset C$. This applies for all $x \in A$ therefore $A \subset C$.

2 Set Identities

Theorem 2.1. *Let all sets be referred to be subset of the universal set U. Then, the following hold:*

- *Commutativity: For all sets A and B, we have $A \cup B = B \cup A$ and $A \cap B = B \cap A$.*
- *Associativity: For all sets A, B, and C, we have $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.*
- *Distribitivity: For all sets A, B, and C, we have $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*
- *Identity: For all sets A, we have $A \cup \emptyset = A$ and $A \cap U = A$.*
- *Complementarity: For every set A, we have $A \cup A^C = U$ and $A \cap A^C = \emptyset$.*
- *Double complementarity: For every set A, $(A^C)^C = A$.*
- *Idempotency: For every set A, $A \cup A = A$ and $A \cap A = A$.*
- *Universal bound: For every set A, $A \cup U = U$ and $A \cap \emptyset = \emptyset$.*
- *De Morgan's: For all sets A and B: $(A \cup B)^C = A^C \cap B^C$ and $(A \cap B)^C = A^C \cup B^C$.*
- *Absorption: For all sets A and B: $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$.*
- *Complements of U and $\emptyset$: $U^C = \emptyset$ and $\emptyset^C = U$*
- *Set diference: $A \setminus B = A \cap B^C$*

I'm not going to provide all the proofs for these here because many of them are obvious. Let's talk aobut De Morgan's though. We want to prove for all sets A and B that $(A \cup B)^C = A^C \cap B^C$. We can get intuition by using a Venn Diagram.

Exercise
Prove that for all sets A and B that $(A \cup B)^C = A^C \cap B^C$

First, we show that $(A \cup B)^C \subset A^C \cap B^C$. Suppose $x \in (A \cup B)^C$. By the definition of complement then $x \notin A \cup B$. To say this, we mean that "it is false that (x is in A or x is in B)." By De Morgan's for logic this means that "x is not in A and x is not in B" which we can write $x \notin A$ and $x \not inB$. So, $x \in A^C$ and $x \in B^C$. It follows by the definition of intersection that $x \in A^C \cap B^C$. So $(A \cup B)^C \subset A^C \cap B^C$ by definition of subset.

Now, we prove that $A^C \cap B^C \subset (A \cup B)^C$. Suppose $x \in A^C \cap B^C$. By definition of intersection then $x \in A^C$ and $x \in B^C$. This means $x \notin A$ and $x \notin B$. We again use De Morgan's laws of logics to show that "it is false that (x is in A or x is in B)". We can write this as $x \notin A \cup B$ by definition of union. So by definition of complement $x \in (A \cup B)^C$ implying $A^C \cap B^C \subset (A \cup B)^C$ by definition of subset.

Since we have both containments then $(A \cup B)^C = A^C \cap B^C$ by the definition of set equality.

3 In-class exercises

Exercise
Prove: For all sets A, B, and C if $A \subset B$ and $B \subset C^C$, then $A \cap B = \emptyset$.

Suppose A, B, and C are any sets such that $A \subset B$ and $B \subset C^C$. We must show $A \cap C = \emptyset$. Suppose not. That is, suppose $x \in A \cap B$. By definition of intersection then $x \in A$ and $x \in C$. Then since $A \subset B$, $x \subset B$ by definition of subset. Also, since $B \subset C^C$ then $x \in C^C$. It follows by the definition of complement that $x \notin C$. Thus, $x \in C$ and $x \notin C$, a contradiction. So the supposition that there is an element $x \in A \cap C$ is false and thus $A \cap C = \emptyset$.

Exercise
For every integer $n \geq 0$, if a set X ahs n elements then $\mathcal{P}(X)$ has 2^n elements.

There are multiple ways to prove this. We could consider an element $S \in \mathcal{P}(X)$ and note that for every element $x \in X$, we either have $x \in S$ or $x \notin S$. Thus, for every element in S we have two choices. Thus, there are $2^{|S|}$ possible subsets.

We could also prove this inductively: Let S_n be the statement "Any set with n elements has 2^n subsets." Consider the base case S_0. Well a set with 0 elements has $2^0 = 1$ subsets because the emptyset is a subset.

Suppose that S_k is true for a particular but arbitrarily chosen integer $k \geq 0$. We must show that a set with $k+1$ elements has 2^{k+1} subset. Let X be such a set with $k+1$ elements. Since $k+1 \geq 1$, we may pick an element z in X. Observe that any subset of X either contains z or it does not. Furthermore, any subset of X that does not contain z is a subset of $X \setminus \{z\}$. And any subset A of $X \setminus \{z\}$ can be matched up with a subset B, equal to $A \cup \{z\}$, of X that contains z. Consequently, there are as many subsets of X that contains z as do not, and thus there are twice as many subsets of X as there are subsets of $X \setminus \{z\}$. It follows that since $X \setminus \{z\}$ has k elements then it has 2^k subsets. Thus, the number of subset of X is $2 \times 2^k = 2^{k+1}$ as was conjectured.

Exercise
If a set X has infinitely many elements, such as $\mathbb{N}$ or $\mathbb{R}$, then what can we say about the size of $\mathcal{P}(X)$? Is $|X| = |\mathcal{P}(X)|$? Or $|X| \leq |\mathcal{P}(X)|$? Or $|X| < |\mathcal{P}(X)|$? Which seems better? How do we prove it?

It turns out that we want to say $|X| < |\mathcal{P}(X)|$. This is called Cantor's theorem. To formally given an answer to this, we need to wait until tomorrow when we define some properties of functions. We will use functions to measure how big infinite sets are. It's a whole fun time!

4 The Halting Problem

Let's think about a barber named Joe. Joe is a cool guy. It's a really small town so Joe knows everyone. He shaves all the men, and only the men, who do not shave themselves. But... does Joe shave himself?

This is a weird paradox related to Russell's paradox from yesterday. The answer is both yes and no which makes for a weird issue in logic and math. If the barber shaves himself, then he is a member of the class of men who shave themselves. But no member of that class is shaved by the barber, so he can't shave himself. But... if he does not shave himself, then he belongs to the class of men who do not shave themself. But, we know every many who doesn't shave themself is shaved by the barber, so he does shave himself! Oh no! Paradox all over!

I bring this up again because even though it was resolved by a careful definition in set theory, it led to lots of interesting mathematically ideas and questions. Kurt Gödel got interested in these foundational issues in math, and he showed in 1931, that you could not prove, in a mathematically rigorous way, that math was free of contradictions! Oh no! So we can never prove that our math works. It's a scary time. It's led to a lot of interesting realizations and thoughts.

One question that is related and pertinent to us is, "Can you write a computer program that will look at another program taking some specific input data and tell you if that program using that input data will halt in a finite number of sets?" Disconcertingly, the answer is no and is a very famous result that is the foundation of many ideas in computability theory. This idea will come up again and again in your studies as a computer science student. Let's try to prove this theorem. It's a mind bender, so let's go through it together.

Theorem 4.1. *There is no computer algorithm that will accept any algorithm X and a data set D as input and then will output "halts" or "loops forever" to indicate whether or not X terminates in a finite number of steps when X is run with data set D.*

Proof. We will proceed by proof by contradiction. Let's assume there is an algorithm, `CheckHalt`, such that if algorithm X adn a data set D are input then `CheckHalt(X, D)` prints "halts" if X terminates in a finite number of sets when run with data set D and "loops forever" if X does not terminate in a finite number of steps when run with data set D.

The actual program X, the sequence of characters we write down to define X, can be thought of as a form of data itself. So, we can run `CheckHalt(X, X)`. Let's define a new algorithm `Test` as follows: `Test(X)` loops forever if `CheckHalt(X, X)` prints "halts" and stops if `CheckHalt(X, X)` prints "loops forever."

Now, let's be especially pesky and run `Test` with `Test` as input! If `Test(Test)` terminates after a finite number of steps, then the value of `CheckHalt(Test, Test)` is "halts" so `Test(Test)` actually loops forever, a contradiction of it terminating after a finite number of steps.

But, if `Test(Test)` does not terminate after a finite number of steps, then `CheckHalt(Test, Test)` prints "loops forever" so `Test(Test)` actually terminates!

This means in any scenario `Test(Test)` both halts and loops forever, a horrendous contradiction. But `Test` must exist if `CheckHalt exists`. Therefore, supposition is false and `CheckHalt` cannot exist. □

Unfortunately, the axioms in set theory that we use to avoid Russell's paradox don't deal adequately with all the recursive possibilities of computer algorithms. We try to resolve these in research, one such avenue is called hypersets.

4.1 Related concepts

There are many related concepts to the Halting Problem. For example, Gödel's incompleteness theorems in 1931 state:

1. No consistent set of axioms whose theorems can be listed by an effective procedure is capable of proving all truths about arithmetic of natural numbers. We will always have true statements that cannot be proven.

2. A system cannot prove itself consistent.

When we say consistent, it means that we will never produce a contradiction by using logical deduction from the axioms and things we have proven from those axioms. The proofs for these look similar to the proof of the halting problem due to their self-referential manner. This is the outline for the the proof by contradiction of the first theorem:

1. We first show that statements can be represented by natural numbers. We then check the property of the number to establish the truth of the statement.

2. We then construct a self-referential statement that says it itself is unproveable.

3. Finally, we realize that we cannot actually prove or disprove this statement because if we prove it then we have produce a contradiction. If we show it cannot be proven then our system cannot prove all truth about arithmetic of natural numbers.

The proof of the second theorem is similar. We introduce an undecideable statement p that says it cannot be proven. We assume that the system can prove its own consistency. We realize that we cannot prove p. But... that's the same as p so p can be proven in a weird way. It produces a contradiction. These proof sketches overlook many of the details and are just meant to give you the flavor.

There's also the Entscheidungsproblem that states that if we input an arbitrary first-order logic statement we cannot answer yes or no if it is universally valid, i.e. it can be proven from our axioms using the rules of logic. Tarksi's undefinability problem states that "arithmetical truth cannot be defined in arithmetic." The 1930s was a busy time for this type of research.

5 Boolean algebra

Definition: *Boolean algebra*
A Boolean algebra is a set B together with two operations, usually denoted + and $\times$, such that for all a and b both $a + b$ and $a \times b$ are in B and the following axioms are assumed to hold:

- Commutative laws: $\forall a, b \in B\, a + b = b + a$ and $a \times b = b \times a$
- Associative law: $\forall a, b, c \in B\, (a + b) + c = a + (b + c)$ and $(a \times b) \times c = a \times (b \times c)$
- Distributive laws: $\forall a, b, c \in B\, a + (b \times c) = (a + b) \times (a + c)$ and $a \times (b + c) = (a \times b) + (a \times c)$. item Identity laws: There exist distinct elements 0 and 1 in B such that for each a in B we have $a + 0 = a$ and $a \times 1 = a$
- Complement laws: For each a in B, there exists an element in B denoted $\overline{a}$ called the negation or complement of a such that $a + \overline{a} = 1$ and $a \times \overline{a} = 0$.