Sets, Operations on Sets, and Quantifiers

Discrete Mathematics 27100 Winter 2022

January 19 and January 21

Corresponding sections in Margaret Fleck's "Building Blocks for Theoretical Computer Science": Sections 1.1, 2.10-2.17, 5.1-5.6,5.11
Corresponding sections in Rosen's "Disrete Mathematics and Its Applications": Sections 2.1,2.2
Corresponding material in Professor Kurtz's lecture notes: part of Lecture 2

1 Sets

Set theory is at the foundations of mathematics. We will use sets throughout the course so it is very important to be familiar with them. Using sets, operations on sets, and quantifiers, we can express a wide variety of mathematical statements.

Definition 1.1 (Rough definition of sets)**.** *A set S is an unordered collection of objects. We describe a set S by using $\{$ and $\}$ brackets and putting the objects in S (or a description of these objects) between the brackets. If a set S contains an object x then we write $x \in S$ and say that x is an element of S. If a set S does not contain an object x then we write that $x \notin S$.*

Example 1.2. $S = \{Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday\}$ *is the set of days of the week. Here $Wednesday \in S$ but $Halloween \notin S$.*

Remark 1.3. *Note that for sets, it doesn't matter what order the objects or in or how many times a given object in the set appears as long as it appears at least once. For example, $\{3, 2, 1, 3, 1, 1\}$ is the same set as $\{1, 2, 3\}$. If we want to allow objects to appear multiple times and keep track of how many times they appear, we use multi-sets instead.*

Definition 1.4. *Some very important sets are as follows:*

1. $\emptyset = \{\}$ *is the empty set which contains no objects.*
2. $\mathbb{N} = \{1, 2, 3, \dots\}$ *is the set of natural numbers.*
3. $[n] = \{1, 2, \dots, n\} = \{x \in \mathbb{N} : 1 \leq x \leq n\}$ *is the set of natural numbers between 1 and n.*
4. $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ *is the set of integers.*
5. $\mathbb{Q} = \left\{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}\right\}$ *is the set of rational numbers.*

6. $\mathbb{R}$ *is the set of real numbers.*

7. $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ *is the closed interval between* a *and* b*. Similarly,* $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ *is the open interval between* a *and* b*.*

8. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ *(where* $i = \sqrt{-1}$*) is the set of complex numbers.*

9. *We take* $\mathbb{P} = \{p \in \mathbb{N} : p > 1,$ *the only positive divisors of* p *are* 1 *and* $p\}$ *to be the set of prime numbers.*

Remark 1.5. *Rigorously defining the real numbers takes considerable work. In this course, we don't worry about this and take the real numbers for granted .*

Remark 1.6. *It is not universally agreed that the natural numbers are* $\mathbb{N} = \{1, 2, 3, \ldots\}$*. Some sources (including Margaret's textbook) take* $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$*. However, for this course we take* $\mathbb{N} = \{1, 2, 3, \ldots\}$*. Similarly, it is not universally agreed that* $\mathbb{P}$ *represents the set of prime numbers, but this notation will be very useful for this course.*

1.1 Describing sets

In order to describe a set, we have to describe which elements it contains. Some common ways to do this (which were already used above) are as follows:

1. The most basic way to describe a set is to list the elements it contains. For example, $S = \{1, 2, 3, 5, 6, 10, 15, 30\}$ is the set which contains the elements 1, 2, 3, 5, 6, 10, 15, and 30.

2. If there are too many elements to write down all of them but there is a clear pattern, we can use . . . to say that the pattern continues. For example, $\{3, 6, 9, 12, \ldots\}$ is the set of natural numbers which are multiples of 3 and $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is the set of even integers.

   Note: This method is best combined with an informal description of the elements of the set. This way, the list of the first few elements of the set and the informal description of the elements in the set reinforce each other. For example, writing "let $S = \{0, 1, 4, 9, 16, 25, \ldots\}$ and let $T = \{2, 3, 5, 7, 11, \ldots\}$" would not be so good as the reader may not be sure how the pattern continues but writing "let S = {0,1,4,9,16,25,. . . } be the set of square numbers and let $T = \{2, 3, 5, 7, 11, \ldots\}$ be the set of prime numbers" would be better.

3. A very useful way to describe the elements in a set is by using set builder notation. In set builder notation, we write down the elements in a set as follows. We first write down the elements of the set in terms of parameter(s). We then write a colon : or a vertical bar | followed by the condition(s) which the parameter(s) must satisfy.

   For example, $S = \{2n + 1 : n \in \mathbb{Z}\}$ (which we can also write as $\{2n + 1 | n \in \mathbb{Z}\}$) is the set of objects of the form $2n + 1$ where n is an integer. In other words, S is the set of all odd integers.

Example 1.7. *Some more examples of set builder notation are as follows:*

Q: How would you write down the set of all integers which are the sum of two squares?

Answer: $\{a^2 + b^2 : a, b \in \mathbb{Z}\}$
Q: How would you write down the set of all natural numbers which are the product of two primes?
Answer: $\{pq : p, q \in \mathbb{P}\}$
Q: How would you write down the set of all real roots of the polynomial $p(x) = x^3 - 4x + 3$*?*
Answer: $\{x \in \mathbb{R} : x^3 - 4x + 3 = 0\}$

2 Operations on Sets

Definition 2.1. *The following operations on sets are extremely useful.*

1. *Union: We define the union* $S \cup T$ *of* S *and* T *to be the set* $S \cup T = \{x : x \in S \vee x \in T\}$ *of objects which are in* S *or* T.

2. *Intersection: We define the intersection* $S \cap T$ *of* S *and* T *to be the set* $S \cap T = \{x : x \in S \wedge x \in T\}$ *of objects which are in both* S *and* T.

3. *Set difference: We define the set difference* $S \setminus T$ *to be the set* $S \setminus T = \{x : x \in S \wedge x \notin T\}$ *of objects which are in* S *but are not in* T.

4. *Complement: If we are living inside some universe* U *of objects, we define the complement of* S *to be* $\bar{S} = U \setminus S = \{x \in U : x \notin S\}$

5. *Cartesian Product: We define the Cartesian product* $S \times T$ *of* S *and* T *to be the set* $S \times T = \{(s, t) : s \in S \wedge t \in T\}$ *to be the set of ordered pairs of objects where the first object is in* S *and the second object is in* T.

Example 2.2. *Some examples of these set operations are as follows:*

1. $\{1, 2, 4, 8, 16\} \cup \{1, 4, 9, 16\} = \{1, 2, 4, 8, 9, 16\}$

2. $\{1, 2, 4, 8, 16\} \cap \{1, 4, 9, 16\} = \{1, 4, 16\}$

3. $\{1, 2, 4, 8, 16\} \setminus \{1, 4, 9, 16\} = \{2, 8\}$ *and* $\{1, 4, 9, 16\} \setminus \{1, 2, 4, 8, 16\} = \{9\}$

4. *If our universe* U *is* $\mathbb{Z}$ *and* $S = \{2n : n \in \mathbb{Z}\}$ *is the set of even integers then* $\bar{S} = \{2n + 1 : n \in \mathbb{Z}\}$ *is the set of odd integers.*

5. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ *is the plane.*

6. *If* $S = \{1, 2, 4\}$ *and* $T = \{1, 3\}$ *then* $S \times T = \{(1, 1), (1, 3), (2, 1), (2, 3), (4, 1), (4, 3)\}$

Definition 2.3. *We define the cardinality of a finite set* S *(which we write as* $|S|$*) to be the number of elements contained in* S

Example 2.4. *If* $S = \{1, 3, 6, 10, 15\}$ *then* $|S| = 5$

Remark 2.5. *Cardinality can be defined for infinite sets as well. The cardinality of inifinite sets is a very interesting topic, but we will not cover it in this course.*

3 Universal and Existential Quantifiers

Definition 3.1 (Universal and Existential Quantifiers)**.** *Let $P(x)$ be a statement (called a predicate) which depends on a variable x.*

1. *$\forall x \in S\ (P(x))$ means "for all x, $P(x)$ is true."*
2. *$\exists x \in S\ (P(x))$ means "there exists an x such that $P(x)$ is true."*
3. *$\nexists x \in S\ (P(x))$ means "there does not exist an x such that $P(x)$ is true."*

Example 3.2.
Q: What does the statement $\forall n \in \mathbb{N}\,(\exists p \in \mathbb{P}(p \geq n \wedge p+2 \in \mathbb{P}))$ mean?
Answer: This statement says that for all n, there is a prime p which is at least as large as n such that $p+2$ is also prime. In other words, there are infinitely many pairs of consecutive prime numbers. This is the twin primes conjecture.

Q: The Goldbach conjecture states that every even integer which is at least 4 is the sum of two prime numbers. How would you write the Goldbach conjecture?
Answer: The Goldbach conjecture can be written as $\forall n \in \mathbb{N} \setminus \{1\}\,(\exists p, q \in \mathbb{P}(p+q=2n))$.

3.1 Proving and Disproving Statements with Quantifiers

1. In order to prove a statement of the form $\forall x \in S(P(x))$, we have to take an arbitrary $x \in S$ (we can think of this x as coming from an adversary) and show that $P(x)$ holds. In order to disprove a statement of the form $\forall x \in S(P(x))$, it is sufficient to provide a single $x \in S$ such that $P(x)$ does not hold.
2. In order to prove a statement of the form $\exists x \in S(P(x))$, we have to provide an $x \in S$ such that $P(x)$ holds. In order to disprove a statement of the form $\exists x(P(x))$, we have to show that $\forall x \in S(\neg P(x))$. In other words, we have to take an arbitrary $x \in S$ (we can think of this x as coming from an adversary) and show that $P(x)$ does not hold.
3. $\nexists x \in S(P(x))$ is equivalent to $\forall x \in S(\neg P(x))$. Thus, in order to prove a statement of the form $\nexists x \in S(P(x))$, we have to take an arbitrary $x \in S$ (we can think of this x as coming from an adversary) and show that $P(x)$ does not hold. In order to disprove a statement of the form $\nexists x \in S(P(x))$, it is sufficient to provide a single $x \in S$ such that $P(x)$ holds.

Example 3.3.
Q: Is the statement $\forall n \in \mathbb{N}(n^2-1 \notin \mathbb{P})$ true?
Answer: No. If we take $n=2$ then $n^2-1=3 \in \mathbb{P}$

Q: Is the statement $\forall n \in \mathbb{N}(n \leq 2 \vee n^2-1 \notin \mathbb{P})$ true?
Answer: Yes. Observe that $n^2-1=(n-1)(n+1)$. If $n \in \mathbb{N}$ and $n>2$ then $(n-1)$ and $(n+1)$ are both integers which are greater than 1 so $n^2-1=(n-1)(n+1)$ is not prime.

3.2 Set Equality and Subsets

Now that we have quantifiers, we can define set equality and subsets.

Definition 3.4. *Let S and T be sets.*

1. *Subsets: We say that S is a subset of T (which we write as $S \subseteq T$) if $\forall x \in S(x \in T)$.*
2. *Equality: We say that $S = T$ if $S \subseteq T$ and $T \subseteq S$.*

Example 3.5.

1. *If $S = \{1, 2, 3\}$ and $T = \{3, 1, 2\}$ then $S = T$ because S and T have the same elements.*
2. $\mathbb{P} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Proposition 3.6. *If $S \subseteq T$ and $T \subseteq R$ then $S \subseteq R$*

Proof. We need to show that $\forall x \in S(x \in R)$. To do this, let x be an element in S and take the following steps:

1. Since $x \in S$ and $S \subseteq T$, $x \in T$
2. Since $x \in T$ and $T \subseteq R$, $x \in R$.

Since we took an arbitrary $x \in S$ and showed that $x \in R$, $\forall x \in S(x \in R)$. In other words, $S \subseteq R$, as needed. □

Remark 3.7. *This may remind you of the proof that if $A \to B$ and $B \to C$ then $A \to C$. This is not a coincidence; there is a close connection between set theory and logic. For more details, see the appendix.*

4 Negations with Quantifiers

Recall the rules we've seen so far for negating statements:

1. $\neg\neg P \leftrightarrow P$ (principle of double negation)
2. $\neg(P \vee Q) \leftrightarrow \neg P \wedge \neg Q$ (De Morgan's Law)
3. $\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$ (De Morgan's Law)
4. $\neg(P \to Q) \leftrightarrow P \wedge \neg Q$

There are two more rules for handling $\forall$ and $\exists$ quantifiers.

Proposition 4.1.

1. *The negation of $\forall x(P(x))$ (where $P(x)$ is a statement which depends on x) is $\exists x(\neg P(x))$.*
2. *The negation of $\exists x(P(x))$ is $\forall x(\neg P(x))$*

We also have that the negation of $\nexists x(P(x))$ is $\exists x(P(x))$. Since $\nexists x(P(x))$ is equivalent to $\forall x(\neg P(x))$, this can be seen as an instance of the first rule.

Example 4.2. *Q: What is the negation of the statement $\exists p \in \mathbb{P}(2^p - 1 \notin \mathbb{P})$?*

Answer: The negation of the statement $\exists p \in \mathbb{P}(2^p - 1 \notin \mathbb{P})$ is $\forall p \in \mathbb{P}(2^p - 1 \in \mathbb{P})$

Example 4.3. *Q: What is the negation of the Goldbach conjecture that*
$\forall n \in \mathbb{N} \setminus \{1\} \, (\exists p, q \in \mathbb{P}(p + q = 2n))$*?*

Answer: The negation of the Goldbach conjecture is $\exists n \in \mathbb{N} \setminus \{1\} \, (\forall p, q \in \mathbb{P}(p + q \neq 2n))$. In other words, there exists an integer $n > 1$ such that $2n$ cannot be expressed as the sum of two primes.

Example 4.4. *Q: What is the negation of the twin primes conjecture that*
$\forall n \in \mathbb{N} \, (\exists p \in \mathbb{P}(p \geq n \wedge p + 2 \in \mathbb{P}))$*?*

Answer: The negation of the twin primes conjecture is $\exists n \in \mathbb{N} \, (\forall p \in \mathbb{P}(p < n \vee p + 2 \notin P))$. In other words, there exists an $n \in \mathbb{N}$ such that there is no pair of consecutive primes after n.

A Connection between set theory and logic

There is a close connection between set theory and logic, which is as follows:

Set Theory	Logic
Set S	Proposition S
Object x	Row x in the truth table
$x \in S$	In row x, S is true
$x \notin S$	In row x, S is false
U (the universe the sets are living in)	$TRUE$
$\emptyset$ (which can also be written as $\{\}$)	$FALSE$
$\bar{S}$ (the complement of S)	$\neg S$
$S \cup T$	$S \vee T$
$S \cap T$	$S \wedge T$
$S \setminus T$	$S \wedge \neg T$
$S \subseteq T$	$S \rightarrow T$ is a tautology

Because of this connection, many equalities in set theory correspond to tautologies in propositional logic.

Set theory equality	Propositional logic tautology
$\forall S, S \cup \bar{S} = U$	$S \vee \neg S \leftrightarrow TRUE$
$\forall S, S \cap \bar{S} = \emptyset$	$S \wedge \neg S \leftrightarrow FALSE$
$\forall S, T, \overline{S \cup T} = \bar{S} \cap \bar{T}$ (De Morgan's Law)	$\neg(S \vee T) \leftrightarrow \neg S \wedge \neg T$ (De Morgan's Law)
$\forall S, T, \overline{S \cap T} = \bar{S} \cup \bar{T}$ (De Morgan's Law)	$\neg(S \wedge T) \leftrightarrow \neg S \vee \neg T$ (De Morgan's Law)
$\forall S, T, R, S \cup (T \cap R) = (S \cap T) \cup (S \cap R)$	$S \vee (T \wedge R) \leftrightarrow (S \wedge T) \vee (S \wedge R)$
$\forall S, T, R, S \cap (T \cup R) = (S \cup T) \cap (S \cup R)$	$S \wedge (T \vee R) \leftrightarrow (S \vee T) \wedge (S \vee R)$