MATH1005/MATH6005: Discrete Mathematical Models

Adam Piggott

Semester 1, 2021

Section A: The language of mathematics and computer science

Part 2: Sets (continued)

Making new sets from old

Suppose that A and B are subsets of a universe U.

The **union** of A and B, denoted $A \cup B$, is the set

$$\{x \in U \mid (x \in A) \vee (x \in B)\}.$$

The **intersection** of A and B, denoted $A \cap B$, is the set

$$\{x \in U \mid (x \in A) \wedge (x \in B)\}.$$

The **difference** of B minus A, or B **without** A, denoted $B - A$ or $B \setminus A$, is the set

$$\{x \in U \mid (x \in B) \wedge (x \notin A)\}.$$

Making new sets from old

Suppose that A and B are subsets of a universe U.

The **complement** of A (in U), denoted A^c, is the set

$$\{x \in U \mid x \notin A\}$$

The complement of A cannot be understood unless the universe of discourse has been communicated.

The **symmetric difference** of A and B, denoted $A \triangle B$, is the set

$$\{x \in U \mid (x \in A) \oplus (x \in B)\}.$$

Some examples

Suppose that the universe of discourse is the set $\mathbb{Z}$ and let

O be the set of odd integers
E be the set of even integers
P be the set of primes
C be the set of composite numbers.

A **composite number** is a positive integer that can be formed by multiplying two smaller positive integers.

Find simple expressions for: $O \cup E$, $O \cap E$, $E \cap P$, $O \cap P$, $P \cup C$, O^c, P^c, $E \triangle P$, $(O \triangle P) \cap \mathbb{Z}^+$

Some examples

$$\begin{aligned}
O \cup E &= \mathbb{Z} \\
O \cap E &= \emptyset \\
E \cap P &= \{2\} \\
O \cap P &= P \setminus \{2\} \\
P \cup C &= \{2, 3, 4, 5, \ldots, \} \\
&= \{x \in \mathbb{Z} \mid x \geq 2\} \\
O^c &= E \\
P^c &= \{\ldots, -3, -2, -1, 0, 1\} \cup C \\
&= \{z \in \mathbb{Z} \mid z \leq 1\} \cup C \\
E \triangle P &= (E \cup P) \setminus \{2\} \\
(O \triangle P) \cap \mathbb{Z}^+ &= (O \cap C) \cup \{1, 2\}.
\end{aligned}$$

Using logic to prove set identities

Since the set operations $\cup$, $\cap$, $\setminus$, $\subseteq$, ^{c} and $\triangle$ are defined using logical connectives, logical equivalences can be used to proved set theoretic identities (an identity is a relationship that holds not matter which substitutions are made for the variables).

An example

Let A, B and C be subsets of a universe U. Then

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Proof.

$$\begin{aligned}
& x \in A \cap (B \cup C) & \\
\Leftrightarrow & (x \in A) \land (x \in B \cup C) & \text{Defn of } \cup \\
\Leftrightarrow & (x \in A) \land (x \in B \lor x \in C) & \text{Defn of } \cap \\
\Leftrightarrow & ((x \in A) \land (x \in B)) \lor ((x \in A) \land (x \in C)) & \text{Distr.} \\
\Leftrightarrow & (x \in A \cap B) \lor (x \in A \cap C) & \text{Defn of } \cap \\
\Leftrightarrow & x \in (A \cap B) \cup (A \cap C) & \text{Defn of } \cup
\end{aligned}$$

□

Another way to construct a new set from an old set

For any set A, the power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

For example, if $A = \{1, 2, 3\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Q: If A has n elements, how many elements does $\mathcal{P}(A)$ have?

Another way to construct a new set from an old set

For any set A, the power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

For example, if $A = \{1, 2, 3\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Q: If A has n elements, how many elements does $\mathcal{P}(A)$ have?

A: $\mathcal{P}(A)$ has 2^n elements... for reasons we will explain when we discuss counting techniques later in the course.

Cartesian products: Another way to make new sets from old

Order and multiplicity

In sets, there is no sense of the order in which elements appear and there is no idea of how many times an elements appears.

However, in many situations the order in which data appears is important, and the same data sometimes appears multiple times.

We now look at a construction that allows us to represent order and multiplicity.

Ordered n-tuples (see p.11 of our optional text).

Let n be a positive integer and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elements. The **ordered n-tuple** $(x_1, x_2, \ldots, x_n)$ consists of $x_1, x_2, \ldots, x_n$ together with the ordering: first x_1, then x_2, and so forth up to x_n. An ordered 2-tuple is called an **ordered pair**, and an ordered 3-tuple is called an **ordered triple**.

Two ordered n-tuples are **equal** when their elements match up exactly in order. Symbolically:

$$\begin{aligned} &(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \\ \Leftrightarrow &(x_1 = y_1) \wedge (x_2 = y_2) \wedge \cdots \wedge (x_n = y_n). \end{aligned}$$

An ordered m-tuple and an ordered n-tuple cannot be equal if $m \neq n$.

Examples

$(a, b, c) \neq (b, c, a)$ because their first elements differ.

$(a, a, b, c) \neq (a, b, c)$ because one is an ordered 4-tuple and the other is an ordered triple.

The elements in ordered n-tuples do not need to be of the same type. For example, $(\text{cat}, \text{car}, 1, \$)$ is an ordered 4-tuple.

We are, however, usually interested in sets of ordered n-tuples where all of the elements in, say, the i-th position are of the "same type"...

Cartesian product

Given (not necessarily distinct sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1$, $a_2 \in A_2$, $\ldots$, $a_n \in A_n$.

$$\{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

This last expression may be read aloud as:

Cartesian product

Given (not necessarily distinct sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1$, $a_2 \in A_2$, $\ldots$, $a_n \in A_n$.

$$\{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\} .$$

This last expression may be read aloud as: “the set of all ordered n-tuples with elements a_1, a_2, through, a_n such that a_1 comes from A_1, a_2 comes from A_2, through a_n comes from A_n.”

A word about the notation just used

The expression

$$\{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

does not appear to conform to the rules of set-builder notation we laid out in the last lecture because

- the domain part introduces variables but does not specify a domain for each;
- the “predicate” does not appear to be a single predicate.

We can fix the second concern easily by making a rule that in a predicate, each comma is read and understood as “and”. It is usually better to use $\wedge$.

What I have written is an entirely standard way to describe a Cartesian product, even though it seems like a poor use of set-builder notation.

Examples

Let

$$\begin{aligned} A &= \{\text{cat}, \text{dog}, \text{chicken}\} \\ B &= \{\text{yes}, \text{no}\} \\ C &= \{100, 300\} \end{aligned}$$

Then

$$\begin{aligned} A \times B = \{&(\text{cat}, \text{yes}), (\text{cat}, \text{no}), (\text{dog}, \text{yes}), (\text{dog}, \text{no}), \\ &(\text{chicken}, \text{yes}), (\text{chicken}, \text{no})\}. \end{aligned}$$

and

$$C \times C = \{(100, 100), (100, 300), (300, 100), (300, 300)\}\,.$$

How to prove things
Putting our logic to work.

How to prove things I

- To prove a statement of the form $\forall x\ p(x)$, one may follow this plan:
  Let x be a (fixed but arbitrary) element of the predicate domain. Argue that $p(x)$ is true.

- To disprove a statement of the form $\forall x\ p(x)$, one should prove the statement $\exists x\ \neg p(x)$. (This is called providing a **counterexample**)

- To prove a statement of the form $\exists x\ p(x)$, one may identify a particular element of the predicate domain and establish that $p(x)$ is true.

- To disprove a statement of the form $\exists x\ p(x)$, one should prove the statement $\forall x\ \neg p(x)$.

How to prove things II

To prove $\forall x\ p(x) \to q(x)$ you may:

- Let x be an arbitrary element of the domain.
- Suppose that $p(x)$ is true.
- Deduce by valid reasoning that $q(x)$ must be true (using the truth of $p(x)$ along the way).

This is called **arguing directly**.

You may also:

- Let x be an arbitrary element of the domain.
- Suppose that $\neg q(x)$ is true.
- Deduce by valid reasoning that $\neg p(x)$ must be true (using the truth of $\neg q(x)$ along the way).

This is called **arguing via the contrapositive**.

How to prove things III

Some advice:

1. Before starting a proof, clearly identify the logical structure of the statement to be proved.
2. Write down the logical structure of your argument so that the reader knows what is going on.
3. When deciding between a direct argument and an argument via the contrapositive, try whichever direction appears to allow you to make the strongest supposition first.

Example: Show $\{x \in \mathbb{Z} \mid x^2 + 2x - 15 = 0\} = \{-5, 3\}$

Let $A = \{x \in \mathbb{Z} \mid x^2 + 2x - 15 = 0\}$ and $B = \{-5, 3\}$. To show that $A = B$, we must show that $A \subseteq B$ and $B \subseteq A$.

Example: Show $\{x \in \mathbb{Z} \mid x^2 + 2x - 15 = 0\} = \{-5, 3\}$

Let $A = \{x \in \mathbb{Z} \mid x^2 + 2x - 15 = 0\}$ and $B = \{-5, 3\}$. To show that $A = B$, we must show that $A \subseteq B$ and $B \subseteq A$.

First we show that $B \subseteq A$. Let $x \in \mathbb{Z}$. To show that $x \in B \to x \in A$, we argue directly. Suppose that $x \in B$. Then $x = -5$ or $x = 3$. We use a proof by cases.

Example: Show $\{x \in \mathbb{Z} \mid x^2 + 2x - 15 = 0\} = \{-5, 3\}$

Let $A = \{x \in \mathbb{Z} \mid x^2 + 2x - 15 = 0\}$ and $B = \{-5, 3\}$. To show that $A = B$, we must show that $A \subseteq B$ and $B \subseteq A$.

First we show that $B \subseteq A$. Let $x \in \mathbb{Z}$. To show that $x \in B \to x \in A$, we argue directly. Suppose that $x \in B$. Then $x = -5$ or $x = 3$. We use a proof by cases.
Case $x = -5$: Then

$$x^2 + 2x - 15 = (-5)^2 + 2(-5) - 15 = 25 - 10 - 15 = 0.$$

Case $x = 3$: Then

$$x^2 + 2x - 15 = (3)^2 + 2(3) - 15 = 9 + 6 - 15 = 0.$$

In all cases, $x^2 + 2x - 15 = 0$ and hence $x \in A$.

Example continued

Now let $x \in \mathbb{Z}$. To show that $x \in A \to x \in B$, we argue via the contrapositive. Suppose that $x \notin B$. Then $x < -5$ or $-5 < x < 3$ or $x > 3$. We use a proof by cases.

Example continued

Now let $x \in \mathbb{Z}$. To show that $x \in A \to x \in B$, we argue via the contrapositive. Suppose that $x \notin B$. Then $x < -5$ or $-5 < x < 3$ or $x > 3$. We use a proof by cases.

Case $x < -5$: Then $x + 1 < -4$ and $(x + 1)^2 > 16$. Then

$$x^2 + 2x - 15 = x^2 + 2x + 1 - 16 = (x + 1)^2 - 16 > 0.$$

Case $-5 < x < 3$: Then $-4 < x + 1 < 4$ and $(x + 1)^2 < 16$. Then

$$x^2 + 2x - 15 = x^2 + 2x + 1 - 16 = (x + 1)^2 - 16 < 0.$$

Example continued

Case $x > 3$: Then $x + 1 > 4$ and $(x+1)^2 > 16$. Then

$$x^2 + 2x - 15 = x^2 + 2x + 1 - 16 = (x+1)^2 - 16 > 0.$$

In all cases, $x^2 + 2x - 15 \neq 0$ and hence $x \notin A$. $\square$

Example continued

Case $x > 3$: Then $x + 1 > 4$ and $(x + 1)^2 > 16$. Then

$$x^2 + 2x - 15 = x^2 + 2x + 1 - 16 = (x + 1)^2 - 16 > 0.$$

In all cases, $x^2 + 2x - 15 \neq 0$ and hence $x \notin A$. $\square$

The $\square$ at the end used to be read as ‘quod erat demonstrandum” or Q.E.D. for short; now it is more often read as “boom!”.

A counterexample disproves a $\forall$

Prove or disprove the following: The square root of an integer is always an integer.

This has the form of a universally quantified statement over the domain of all real numbers

$$\forall x \ (x \in \mathbb{Z} \rightarrow \sqrt{x} \in \mathbb{Z}).$$

We wish to show that the statement is false, so we wish to prove

$$\exists x \ (x \in \mathbb{Z} \wedge \sqrt{x} \notin \mathbb{Z}).$$

That is, we wish to provide a **counterexample** to the original statement.

Example: What I would write

Prove or disprove the following: The square root of an integer is always an integer.

The statement is false. The number 2 is an integer, but its square root is not. Therefore, 2 is a counterexample. □

Example 6.1.2 on p.378 of our optional text.

Let

$$\begin{aligned} A &= \{m \in \mathbb{Z} \mid \exists r \in \mathbb{Z}\ m = 6r + 12\} \\ B &= \{n \in \mathbb{Z} \mid \exists s \in \mathbb{B}\ n = 3s\} \end{aligned}$$

Prove that $A \subsetneq B$.