This Week

• Working with predicates and quantifiers

• Introduction to proofs
Let’s Practice.

Let our domain be the natural numbers greater than 1. Define:

\[ P(a) = \text{“} a \text{ is prime”} \]

\[ Q(a, b) = \text{“} a \text{ divides } b \text{”} \]

Consider the following statement:

*For every \( x \) that is not prime, there is some prime \( y \) that divides it.*

1. Write the statement in predicate logic.

\[ \forall x \in \mathbb{N}_{>1}, (\neg P(x) \rightarrow (\exists y \in \mathbb{N}_{>1}, P(y) \land Q(y, x))) \]

2. Negate your statement from part (a).

\[ \neg \forall x \in \mathbb{N}_{>1}, (\neg P(x) \rightarrow (\exists y \in \mathbb{N}_{>1}, P(y) \land Q(y, x))) \]

bunch of work...

\[ \iff \exists x \in \mathbb{N}_{>1}, (\neg P(x) \land (\forall y \in \mathbb{N}_{>1}, \neg P(y) \lor \neg Q(y, x))) \]

3. Write the English translation of your negated statement. Your statement should sound like English not predicate logic in words.

There is a number that is not prime and has no prime divisors.

Working with Quantifiers

All propositional laws apply to predicates, however, you must be careful when working with quantifiers...

Consider the statement

\[ \forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y \]

Q. Does the order of the \( \forall x \) and \( \exists y \) matter? Are these the same?

\[ \forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y \iff \exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x < y \]

A. No.

Q. What do the following statements say in English and which are actually true?

1. \( \exists x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y \)

   there is a natural number that is smaller than some natural number - true

2. \( \exists y \in \mathbb{N}, \exists x \in \mathbb{N}, x < y \)

   there is a natural number that is bigger than some natural number. true
3. \( \forall x \in \mathbb{N}, \forall y \in \mathbb{N}, x < y \)
   every natural number is smaller than every natural number. false

4. \( \forall y \in \mathbb{N}, \forall x \in \mathbb{N}, x < y \)
   every natural number is bigger than every natural number. false.

5. \( \forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y \)
   every natural number is smaller than some natural number. true

6. \( \exists y \in \mathbb{N}, \forall x \in \mathbb{N}, x < y \)
   there is some natural number that is bigger than all natural numbers. false

7. \( \exists x \in \mathbb{N}, \forall y \in \mathbb{N}, x < y \)
   there is a natural number that is smaller than every natural number. false

8. \( \forall y \in \mathbb{N}, \exists x \in \mathbb{N}, x < y \)
   every natural number is bigger than some natural number. false (zero fails)

Q. Which statements have the same meaning?

A. (1) and (2), (3) and (4),

More Practice.

Let the following predicates be given. The domain is \( \mathbb{C} \), the set of all computer science classes.

\( I(x) = \text{“}x\text{ is interesting.”} \)
\( U(x) = \text{“}x\text{ is useful”} \)
\( H(x, y) = \text{“}x\text{ is at least as hard as } y \text{”} \)
\( M(x, y) = \text{“}x\text{ has more students than } y \text{”} \)

1. Write the following statements in predicate logic:

   (a) All interesting CS classes are useful. \textit{Careful: Is this implication or conjunction (\( \land \))?}

   \[ \forall x \in \mathbb{C}, I(x) \rightarrow U(x) \]

   (b) There are some useful CS classes that are not interesting.

   \[ \exists x \in \mathbb{C}, U(x) \land \neg I(x) \]

   (c) Every interesting CS class has more students than any non-interesting CS class.

   \[ \forall x \in \mathbb{C}, \forall y \in \mathbb{C}, (I(x) \land \neg I(y)) \rightarrow M(x, y) \]

2. Write the following predicate logic statement in everyday English. Do not just give a word-for-word translation; your sentence should make sense.

   \[ \exists x \in \mathbb{C}, (I(x) \land \forall y \in \mathbb{C}, (H(x, y) \rightarrow M(y, x))) \]

   \textit{There are some interesting classes and the harder ones have less students than the easier classes.}
Q. What is $\neg(\forall c \in C, U(c))$?

A. Not every course is useful, or there exists a course that is not useful.

Q. How can we rewrite the $\neg(\forall c \in C, U(c))$ in terms of an $\exists$?

A. $\exists c \in C, \neg U(c)$.

Q. What about $\neg \exists c \in C, I(c)$? What does it mean? how can we rewrite using $\forall$?

A. There does not exist an interesting course, or every course is not interesting. $\forall c \in C, \neg I(c)$.

Write down the equivalence law for Negating Quantifiers:

$$\neg(\exists x \in D, P(x)) \iff \forall x \in D, \neg P(x)$$

$$\neg(\forall x \in D, P(x)) \iff \exists x \in D, \neg P(x)$$

3. Formally negate the statement from Q2). Simplify your negation so that no quantifier lies within the scope of a negation. State which derivation rules you are using.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\neg \exists x \in C, (I(x) \land \forall y \in C, (H(x, y) \rightarrow M(y, x)))$</td>
<td>neg Quantifier</td>
</tr>
<tr>
<td>$\iff \forall x \in C, \neg (I(x) \land \forall y \in C, (H(x, y) \rightarrow M(y, x)))$</td>
<td>DeMorgan</td>
</tr>
<tr>
<td>$\iff \forall x \in C, \neg I(x) \lor \forall y \in C, (H(x, y) \rightarrow M(y, x))$</td>
<td>DeMorgans Law</td>
</tr>
<tr>
<td>$\iff \forall x \in C, \neg I(x) \lor \exists y \in C, (H(x, y) \rightarrow M(y, x))$</td>
<td></td>
</tr>
<tr>
<td>$\iff \forall x \in C, \neg I(x) \lor \exists y \in C, (H(x, y) \land \neg M(y, x))$</td>
<td>DeMorgans Law</td>
</tr>
</tbody>
</table>


Every class is either not interesting or hard and has more students than at least one other class.

1 Direct Proofs and Quantifiers

Let’s try writing a simple direct proof.

Claim. Let $a$ be an arbitrary real number. For all real numbers $x$:

$$x > a > 0 \rightarrow x^2 > a^2$$

Proof Prep.
Let’s think about what this means. The claim is stating that if \( x > a > 0 \) then we can square both sides which is a property of arithmetic we use sometimes.

Q. Does this tell us anything about the implication if \( x < a \) then \( x^2 < a^2 \)? Does this tell us anything about when \( a < 0 \)?

A. NO. Remember implication says if the premise is true, then the conclusion is true and that is it!

Q. Are we talking about one value in the real numbers or about EVERY real number?

A. Since we mean every real number, we need to make sure our proof works for ANY \( x \).

Proof of Claim.

\[
\forall a \in \mathbb{R}, \forall x \in \mathbb{R}, (x > a > 0) \rightarrow (x^2 > a^2)
\]

Let \( a \) be any arbitrary real number. All our steps from now on based on arbitrary \( a \).

Let \( x \) be any arbitrary real number. All our steps from now on based on arbitrary \( x \).

Suppose that \( x > a > 0 \).

Since \( x > 0 \), we can multiply both sides of \( x > a \) by \( x \) to get: \( x^2 > xa \)

Since \( a > 0 \), we can multiply both sides of \( x > a \) by \( a \) to get: \( xa > a^2 \)

Therefore, we can use the transitive property to get:

\[
x^2 > xa > a^2
\]

so we have \( x^2 > a^2 \).

Now we put back our assumptions - our premise implies the conclusion and our statement holds for all \( x \).

Therefore, since we assumed that \( x > a \) and \( a > 0 \),

\[
x > a > 0 \rightarrow x^2 > a^2
\]

Since we assumed that \( x \) is an arbitrary real number, we can say that

\[
\forall x \in \mathbb{R}, x > a > 0 \rightarrow x^2 > a^2.
\]

Since we assumed that \( a \) is an arbitrary real number, we can say that

\[
\forall a \in \mathbb{R}, \forall x \in \mathbb{R}, x > a > 0 \rightarrow x^2 > a^2.
\]

Important Observation 1. Some people might think you can prove this claim simply by saying “square both sides”. Think carefully why this is not valid....

What we are proving is that you can square both sides. You can’t use what you are trying to prove in your proof!!

Observation 2.

Let’s look at the claim again. We have an implication of the form:

\[
\forall a \in D, \forall x \in D, P(x, a) \rightarrow Q(x, a)
\]
with variables $x$ and $a$ where $P(x, a)$ means $x > a > 0$, $Q(x, a)$ means $x^2 > a^2$ and $D$ means $\mathbb{R}$.

For such proofs (even though we have two variables) our proof structure generally follows the form:

**Direct Proof.**
\[
\forall y \in D, P(y) \rightarrow Q(y)
\]
- Let $y$ be arbitrary or any element of the domain.
- Suppose that $P(y)$ is true.
- Use true sentences to derive that $Q(y)$ is true.

Sometimes we translate our claims into predicate logic and sometimes we leave it in written form but still follow the rules of predicate logic.

**Exercise** Prove that there does not exist a largest natural number.

Let’s first try to rewrite this in a way that uses “for all” and “there exists”. Try writing it without using “not” (you can look back at our $L(x, y)$ examples if you are feeling stuck).

\[
\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, x < y.
\]

**Proof.** Fill in the areas to the right of the grey.

Let $x$ be an arbitrary natural number.
Let $y = x + 1$. Now $y \in \mathbb{N}$ and $y$ is a specific value.
Then $y > x$ for any $x \in \mathbb{N}$.
Since there exists $y$, $\exists y \in \mathbb{N}, y > x$
Since $x$ is arbitrary natural number, $\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, y > x$.

2 A Proof Using mod

**Definition.** $a \mod n = b$ means that $a \div n$ has a remainder $b$.

**Definition.** $a \equiv n b$ means that $a \mod n = b \mod n$.

**Theorem. The Division Algorithm.** Let $n$ and $m$ be natural numbers. Then there exist unique integers $q$ (for quotient) and $r$ (for remainder) such that

\[
m = nq + r.
\]
Theorem. For all integers $a$, $b$ and $n$ with $n \geq 1$, $a \equiv_n b$ iff $n$ divides $a - b$.

We will prove this theorem. We split it into two separate proofs. What should they be?

\[ \forall a, b \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 1}, (a \mod n = b \mod n) \rightarrow (n \text{ divides } a - b) \]

Proof of ($\rightarrow$):

If $a \equiv_n b$, then $n$ divides $a - b$.

Let integers $a, b$ and $n \geq 1$ be given and suppose that $a$ and $b$ have the same remainder $r$ on division by $n$. This means that for some integers $q_1$ and $q_2$ we have $a = nq_1 + r$ and $b = n \cdot q_2 + r$. This means that:

\[
\begin{align*}
    a - b &= (n \cdot q_1 + r) - (n \cdot q_2 + r) \\
    &= n(q_1 - q_2)
\end{align*}
\]

Therefore $n$ divides $a - b$.

Proof of ($\leftarrow$):

If $n$ divides $a - b$ then $a \equiv_n b$.

Let $a, b$ and $n \geq 1$ be given, and suppose that $n$ divides $a - b$. By definition, there are integers $q_1, r_1, q_2, r_2$ such that

\[
\begin{align*}
    a &= n \cdot q_1 + r_1, \quad 0 \leq r_1 < n \\
    b &= n \cdot q_2 + r_2, \quad 0 \leq r_2 < n \\
\end{align*}
\]

Let’s look at $(a - b)$:

\[
(a - b) = (n \cdot q_1 + r_1) - (n \cdot q_2 + r_2) = n \cdot (q_1 - q_2) + (r_1 - r_2)
\]

Since $(a-b)$ is divisible by $n$, that means that $r_1 - r_2$ is divisible by $n$. Since $r_1, r_2 < n$ that means $-n < r_1 - r_2 < n$. Which value between $-n$ and $n$ is divisible by $n$? Only 0. So $r_1 - r_2 = 0$ and $r_1 = r_2$ and $a$ and $b$ have the same remainder on division of $n$.

Practice.
Prove that for all real numbers \( x \) and \( y \), if \( x \) and \( y \) are rational then \( xy \) is rational.

Q. What is a rational number?

A. A rational number is one that can be written as a fraction of two integers. We can say this more formally as follows:

\[
x \in \mathbb{R} \iff \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, x = \frac{a}{b} \land b \neq 0
\]

Proof.

Let’s do some rough work first:

- Write \( x \) in terms of integers \( a \) and \( b \), \( b \neq 0 \).
- Write \( y \) in terms of integers \( c \) and \( d \), \( d \neq 0 \).
- Write \( xy \) in terms \( a, b, c \) and \( d \).

Now, let's write the proof:

Let \( x \in \mathbb{R} \) and \( y \in \mathbb{R} \) be arbitrary rational numbers. Then there exist integers \( a, b, c, d \) such that \( x = \frac{a}{b} \land b \neq 0 \) and \( y = \frac{c}{d} \land d \neq 0 \).

Then \( xy = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \) and since \( a, b, c, d \in \mathbb{Z} \), \( ac \in \mathbb{Z} \) and \( bc \in \mathbb{Z} \) and \( bc \neq 0 \) (why?). Therefore, \( xy \) can be written as an integer over an integer and is a rational number.