Part 1: Logic and Proof Techniques

Contents [DOCUMENT FINALIZED!]

Course Information

Lecture 1

- Instructor: Michael Buro
  - ATH 337, 492-1763, mburo@cs.ualberta.ca
  - Office hours: Mondays 2-3pm, Wednesdays 1-2pm, and by appointment
- Section web page:

  `http://www.skatgame.net/mburo/courses/272`
- Lecture notes and assignments will be posted on the section web page
- Sources used to create these lecture notes:
  - "Discrete Mathematics and Its Applications" (6th Edition) by K.H. Rosen
  - "A Transition To Advanced Mathematics" (6th Edition) by D. Smith, M. Eggen, R. St. Andre
  - Various web sites and lecture notes

  There is no need to purchase a textbook for this course.

- Course work:
  - 5 assignments : 8% each
  - 1 term test in class (80 min., closed book) : 25%
  - Final (2 hours, closed book) : 35%
- Collaboration policy: Consultation
  - You can talk to anyone,
  - but you must write up the solution on your own,
  - and acknowledge who you talked to. All sources (webpages, books, etc.) used must be cited.
- Grading: approximately curved with reasonable cut-offs. See section page for details.

Expect to invest 4h/week in this course in addition to lectures and seminars.

Important: Do assignments right from the start! Without solving exercises on your own, it will be hard to pass this course.

DON'T CHEAT. Getting caught may end your academic career right there.

Seminars

- start in week 2
- marked assignments are handed back
- assignment solutions are presented
- more problems are discussed
- question and answer sessions

Computing Science Theory Courses

272 Formal Systems and Logic in Computing Science

An introduction to fundamental discrete structures and tools used for the design and analysis of algorithms, including:

- Logic and Proofs
- Sets
- Relations
- Graphs
- Functions
- Program Verification

204 Algorithms I

- Introduction to algorithms
- Analysis: correctness, worst/average/best case behaviour, asymptotical runtime
- Algorithms: sorting and searching, optimization, graph algorithms
- Design techniques: divide-and-conquer, dynamic programming, greedy

304 Algorithms II

- More advanced algorithms, and their design and analysis, complexity, notion of reduction, NP-completeness

474 Formal Languages, Automata and Computability

- More formal approach to models, complexity, and computability
- Computational limitations, problems that computers can't solve

Why Study Mathematics in Computing Science?

Math is the foundation of CS.

CS develops algorithms, i.e. step by step procedures to solve problems, it also is concerned with fundamental limits of computation.

Programs take some input and produce some output that follows some specification. Inputs and outputs are usually mathematical objects composed of integers.

E.g. Input: natural number n, Output: $n \cdot n$.

For a new algorithm we have to prove that the input/output specifications is obeyed, i.e. we need to convince prospective users of the program that it terminates on all valid inputs, and secondly, we need to argue that if the program stops, its output is valid.

In this course we present fundamental mathematical objects and tools that will allow us to specify input/output relations and to prove that algorithms meet their specifications.

Logic and Proofs

Lecture 2

Deductive Reasoning: use logic to draw conclusions based on statements accepted as true.

CS Example: given that a subroutine A is correct, we want to conclude that program B that calls A is also correct. This is the idea of modular programming, in which we establish the correctness of modules first, which we then use as building blocks to create bigger, correct programs.

Topics covered in this part:

- Propositions and connectives
- Predicates and Quantifiers
- Basic proof methods
- Proofs involving quantifiers

Propositions

Natural languages describe real world phenomena

Some sentences are basic, others are built up from simple components to describe more complex thoughts

Some sentences are either true or false, and we call such sentences **propositions**

a. $1 + 1 = 2$

b. Chess is a 2-player game

c. Elephants will become extinct by the year 2525

d. Julius Caesar had two eggs for breakfast on his tenth birthday

Examples of sentences that are not propositions:

e. What did you say?

f. $x^2 = 36$

g. She has your keys

h. This statement is false

Propositions a.-d. are **simple** or **atomic**, they do not have any other propositions as components.

Compound propositions are formed by using logical connectives:

"It is raining AND my shoes are dirty"

"I have no money OR the moon is made of blue cheese"

Definition: Given propositions P and Q,

- the **conjunction** of P and Q, denoted $P \wedge Q$, is the proposition "P and Q"
- the **disjunction** of P and Q, denoted $P \vee Q$, is the proposition "P or Q"
- the **negation** of P, denoted $\neg P$ or $\sim P$, is the proposition "not P." $\neg P$ is true exactly if P is false.

Examples of true compound propositions:

- It is not the case that $\sqrt{2} > 2$
- $2 < 3$ or chickens have lips
- Jupiter is larger than Mars and 1+4=5

Examples of false compound propositions:

- Mozart was born in Salzburg and π is rational
- It is not the case that 10 is divisible by 2
- $2^4 = 15$ or a pound is more than 500g

In general, compound propositions can combine many propositions by logical connectives.

A **propositional form** is a well-formed expression involving finitely many logical connective symbols and letters that represent propositions.

Expressions that are atomic propositions or correctly built using connectives are called well-formed.

The following expressions are well-formed:

$$(P \wedge Q) \vee \neg(\neg R)$$

$$P \vee (Q \wedge R)$$

and these are not:

$$RP \vee Q\neg$$

$$) \wedge PQ($$

Balanced pairs of parentheses are used to avoid ambiguities whenever they appear. We will see a formal definition of well-formed expressions later in the mathematical induction section.

Truth values of compound propositional forms can be obtained by exhibiting all possible combinations of the propositions in a truth table.

Truth tables for $\neg P,\ P \wedge Q,\ P \vee Q$:

P	$\neg P$
F	T
T	F

P	Q	$P \wedge Q$	$P \vee Q$
F	F	F	F
F	T	F	T
T	F	F	T
T	T	T	T

For propositional forms involving 3 propositions we need to list values for $2 \cdot 2 \cdot 2 = 2^3 = 8$ possible combinations. To simplify the evaluation, we first evaluate all subcomponents and then combine the results:

Example: $(P \wedge Q) \vee \neg R$.

P	Q	R	$P \wedge Q$	$\neg R$	$(P \wedge Q) \vee \neg R$
F	F	F	F	T	T
F	F	T	F	F	F
F	T	F	F	T	T
F	T	T	F	F	F
T	F	F	F	T	T
T	F	T	F	F	F
T	T	F	T	T	T
T	T	T	T	F	T

Digression: Logic and Bit Operations

Modern computers represent information using **bits**.

A bit (=binary digit) is a symbol with two possible values, 0 and 1, which are realized as electric potentials (0 Volts vs. 5 Volts say)

Each bit can represent a truth value: 0 for false, and 1 for true.

To speed up computations, data is organized in words of 32 or 64 bits that are accessed in parallel.

In addition to loading and storing data in memory, arithmetic, branches, central processing units (CPUs) have a subset of instructions dealing with bitwise logic operations applied to pairs of bit strings.

Example:

1001010010	bit string A
0100110111	bit string B
0000010010	$A \wedge B$ (bitwise and)
1101110111	$A \vee B$ (bitwise or)
0110101101	$\neg A$ (bitwise not)

Equivalence, Tautology, Contradiction

Writing a proof requires us to connect statements so that the truth of any given statement in the proof follows logically from previous statements in the proof, from known results, or from basic assumptions.

Important is to write a statement equivalent to another:

Definition: Two propositional forms φ ("phi") and ψ ("psi") are **equivalent** if and only if they have the same truth tables when considering all propositions in φ and ψ. We then write $\varphi \equiv \psi$. If they are not equivalent, we write $\varphi \not\equiv \psi$.

Example: P and $\neg(\neg P)$ are equivalent, i.e. $P \equiv \neg(\neg P)$. Here is the evidence:

P	$\neg P$	$\neg(\neg P)$
F	T	F
T	F	T

Columns 1 and 3 are identical.

Another example: "It is not true that Superman is not strong" is equivalent to "Superman is strong".

A more complex example is one of De Morgan's rules:

$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

Truth table check:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
F	F	F	T	T	T	T
F	T	F	T	T	F	T
T	F	F	T	F	T	T
T	T	T	F	F	F	F

Indeed, column 4 and 7 are identical.

In words: "You don't have both P and Q" is the same as saying "You don't have P or you don't have Q"

Note that truth tables need to cover all combinations of all propositions in both propositional forms. E.g. if φ contains P, Q and ψ contains Q, R, the truth table built for establishing the equivalence of φ and ψ lists all choices for P, Q, R.

Often the truth value of propositional forms does not depend on the truth value of its propositions. This warrants a

Definition

- A **tautology** is a propositional form that is **true** for every assignment of truth values to its propositions.
- A **contradiction** is a propositional form that is **false** for every assignment of truth values to its propositions.

The most basic tautology is $P \vee \neg P$, which can easily be checked using a truth table. Likewise, $P \wedge \neg P$ is a contradiction. Here is a more complex tautology: $(P \vee Q) \vee (\neg P \wedge \neg Q)$

P	Q	$P \vee Q$	$\neg P \wedge \neg Q$	$(P \vee Q) \vee (\neg P \wedge \neg Q)$
F	F	F	T	T
F	T	T	F	T
T	F	T	F	T
T	T	T	F	T

The last column is filled with T, so the propositional form is a tautology.

Conditionals

Sentences of the form "If P, then Q" are the most important kind of proposition in mathematics.

Examples:

- If $x = 2$, then $x^2 = 4$
- If $x^2 = 4$, then $x = 2$ or $x = -2$
- If $a < b$ and $c > 0$, then $ac < bc$

In above statements, the second condition holds if the if-condition is true. If it is false, the second condition may or may not hold.

Definition

For propositions P and Q, the **conditional sentence** $P \Rightarrow Q$ is the proposition "If P, then Q." Proposition P is called **hypothesis, premise** or **antecedent** and Q the **conclusion** or **consequence**. $P \Rightarrow Q$ is true if and only if P is false or Q is true, i.e. $\neg P \vee Q$.

Truth table for $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

Lecture 3

Suppose Ann promises to Ben:

"If $1 + 1 = 2$, then I will give you a dollar"

Because $1 + 1 = 2$ is true, we find the truth value of her statement in line 3 or 4:

If Ann pays, the statement is true (line 4).

If she doesn't pay, the statement is false (line 3)

When the hypothesis is false, a promise is always true.

If Ann said "If $1 + 1 = 5$, then I will give you a dollar" she can always keep her promise. According to lines 1 and 2, the sentence is true whether she pays or not.

A conditional sentence may be true even if there is no connection between the hypothesis and the conclusion, because its value only depends on the truth value of the components, not on their interpretation.

Examples

- The sun is green $\Rightarrow$ $1 = 3$ (true)
- Ants have ears $\Rightarrow$ Spiderman can fly (true)
- Bears have ears $\Rightarrow$ Ants have ears (false)

For the proof techniques we will discuss later, the following property of the conditional statement $P \Rightarrow Q$ is key:

If both P and $(P \Rightarrow Q)$ are true, so is Q.

This deduction rule is called **modus ponens** ("mode that affirms") and can be verified by inspecting the truth table for $P \Rightarrow Q$.

Example:

Suppose we know this statement to be true:

$$(2 > 0) \;\Rightarrow\; (3 > 1)$$

and we also know $2 > 0$ is true. Then we know $3 > 1$ is true as well.

Two propositions closely related to $P \Rightarrow Q$ are the following:

Definition

- The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$
- The **contrapositive** $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$

What is their exact relationship to $P \Rightarrow Q$?

Consider the following conditional sentence for fixed values of x:

If $x = 2$, then $x^2 = 4$

which is obviously true. However, what about its converse

If $x^2 = 4$, then $x = 2$?

This sentence is wrong for $x = -2$.

Theorem

a. A conditional sentence and its converse are **not** equivalent

b. A conditional sentence and its contrapositive are equivalent

Proof

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$(\neg Q) \Rightarrow (\neg P)$	$Q \Rightarrow P$
F	F	T	T	T	T	T
F	T	T	T	F	T	F
T	F	F	F	T	F	T
T	T	T	F	F	T	T

a) holds because columns 3 and 7 are different. b) is true because columns 3 and 6 are identical. □

Biconditionals

The last connective we need is the biconditional connective $\Leftrightarrow$. The double arrow reminds one of both $\Leftarrow$ and $\Rightarrow$, and this is no accident:

Definition

For propositions P and Q, the **biconditional sentence** $P \Leftrightarrow Q$ is the proposition "P if and only if Q". $P \Leftrightarrow Q$ is true exactly when P and Q have the same truth values.

The phrase "if and only if" is often abbreviated as "iff"

The truth table for $P \Leftrightarrow Q$ is

P	Q	$P \Leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Example: Consider propositions

P : "You take the flight" and

Q : "You buy a ticket."

Then $P \Leftrightarrow Q$ is the statement:

"You take the flight if and only if you buy a ticket"

This statement is true if P and Q are either both true or both false.

I.e., if you buy a ticket and take the flight, or if you do not buy a ticket and you don't take the flight.

It is false when P and Q have different values

I.e., if you don't buy a ticket, but you take the flight (free trip) or you buy a ticket, but you don't fly (because the airline bumps you).

How do $\Rightarrow$ and $\Leftrightarrow$ relate, exactly?

Theorem: $[P \Leftrightarrow Q]$ and $[(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$ are equivalent.

I.e., if we know that both $P \Rightarrow Q$ and $Q \Rightarrow P$ hold, then we know that $P \Leftrightarrow Q$ is true, and vice versa, if we know that one of $P \Rightarrow Q$ and $Q \Rightarrow P$ does not hold, then $P \Leftrightarrow Q$ is false.

Proof: The truth table entries for both propositional forms are identical:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
F	F	T	T	T	T
F	T	T	F	F	F
T	F	F	T	F	F
T	T	T	T	T	T

□

With the notational convention $(P \Rightarrow Q) \equiv (Q \Leftarrow P)$ above relationship can be easily memorized as

"$\Leftrightarrow$ equals $\Leftarrow$ and $\Rightarrow$"

Observation

Using biconditionals we can characterize equivalence of propositional forms φ and ψ like so:

$$\varphi \equiv \psi \text{ if and only if } \varphi \Leftrightarrow \psi \text{ is a tautology}$$

Both mean that for all truth value assignments of propositions in φ and ψ both forms have the same truth value.

Conditional Statements in Natural Languages

Goal: recognize the structure of a sentence and translate the sentence into symbolic form using logical connectives

Sometimes hard because of ambiguity and language nuances

Example: "You don't win the lottery UNLESS you buy a lottery ticket"

With

A: You don't win the lottery

B: You buy a lottery ticket

this could mean:

$(\neg B) \Rightarrow A$ (preferred meaning of "A unless B": if-not)

but sometimes it is meant like

$(\neg B) \Leftrightarrow A$

which in the lottery case wouldn't make much sense.

$P \Rightarrow Q$ is the translation of the following statements

If P, then Q	P implies Q
P is sufficient for Q	P only if Q
Q, if P	Q whenever P
Q is necessary for P	Q, when P
Q follows from P	Q unless $\neg P$

$P \Leftrightarrow Q$ is the translation of:

P if and only if Q
P if, but only if Q
P is equivalent to Q
P is necessary and sufficient for Q

Example:

$|x| = 2$ is necessary and sufficient for $x^2 = 4$

can be translated into:

$|x| = 2 \;\Leftrightarrow\; x^2 = 4$

Important Equivalences

Here we list some useful equivalences. All of them can be proved by comparing truth table entries.

Let P, Q, R be propositions and T always true and F always false. Then the following equivalences hold:

Law	Equivalence
Identity	$P \wedge T \equiv P$
	$P \vee F \equiv P$
Domination	$P \wedge F \equiv F$
	$P \vee T \equiv T$
Idempotent	$P \wedge P \equiv P$
	$P \vee P \equiv P$
Double negation	$\neg(\neg P) \equiv P$
Commutative	$P \wedge Q \equiv Q \wedge P$
	$P \vee Q \equiv Q \vee P$
Associative	$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
	$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
Distributive	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
De Morgan's	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
Absorption	$P \vee (P \wedge Q) \equiv P$
	$P \wedge (P \vee Q) \equiv P$
Negation	$P \vee \neg P \equiv T$
	$P \wedge \neg P \equiv F$

Observations

The commutative, associative, and distributive laws resemble those you know from arithmetic:

Commutative Law: "You are allowed to switch operands without changing the value"

$$P \wedge Q \equiv Q \wedge P \;, \quad x + y = y + x$$

Associative Law: "Evaluation order does not matter"

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R) \;, \quad (x+y)+z = x+(y+z)$$

Distributive Law: "Factoring-in and out is allowed"

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) \;,$$
$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

De Morgan's Laws: "Negations can be moved inwards by switching $\wedge, \vee$". This can be repeated. In the end, negations are only needed right in front of propositions.

$$\neg(P \wedge (Q \vee R)) \equiv \neg P \vee \neg(Q \vee R) \equiv \neg P \vee (\neg Q \wedge \neg R)$$

Generalisations

The associative laws show that expressions like $P \wedge Q \wedge R$ and $P \vee Q \vee R$ are well-defined, because it doesn't matter what operation we evaluate first. For the truth values it only matters whether all propositions are true in the first case, or all propositions are false in the second. This can be generalized to

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \text{ and } P_1 \vee P_2 \vee \cdots \vee P_n$$

being well-defined for an arbitrary number of propositons n.

De Morgan's laws scale up as well:

$$\neg(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \equiv \neg P_1 \vee \neg P_2 \vee \cdots \vee \neg P_n$$
$$\neg(P_1 \vee P_2 \vee \cdots \vee P_n) \equiv \neg P_1 \wedge \neg P_2 \wedge \cdots \wedge \neg P_n$$

Methods for proving these identities will be given in the section on mathematical induction.

Constructing New Equivalences

Already established equivalences can be used to construct new ones by replacing propositions with equivalent propositions without changing their truth value.

Example 1: We want to show that $\neg(P \Rightarrow Q)$ and $P \wedge \neg Q$ are equivalent.

We could do it by using truth tables, but we now proceed by applying equivalence laws to transform the first into the second propositional form:

$$\begin{aligned} \neg(P \Rightarrow Q) &\equiv \neg(\neg P \vee Q) && \text{definition } \Rightarrow \\ &\equiv \neg(\neg P) \wedge \neg Q && \text{De Morgan law} \\ &\equiv P \wedge \neg Q && \text{double negation} \end{aligned}$$

Example 2: We show that $(P \wedge Q) \Rightarrow (P \vee Q)$ is a tautology by a sequence of equivalences yielding T:

$$\begin{aligned} (P \wedge Q) \Rightarrow (P \vee Q) &\equiv \neg(P \wedge Q) \vee (P \vee Q) && \text{definition } \Rightarrow \\ &\equiv (\neg P \vee \neg Q) \vee (P \vee Q) && \text{De Morgan} \\ &\equiv (\neg P \vee P) \vee (\neg Q \vee Q) && \text{assoc.+com.} \\ &\equiv T \vee T && \text{com.+neg.} \\ &\equiv T && \text{domination} \end{aligned}$$

The truth table method can only be used for small numbers of propositions, because the number of rows grows exponentially. Checking equivalence for 100-proposition forms would require us to verify 2^{100} rows (a number with more than 30 decimal digits) – taking more than 10^{13} years on contemporary hardware!

No other methods are known that could solve the equivalence problem faster in general.

For humans, the equivalence transformation method can work much better than enumerating a large number of truth values.

Predicates

Lecture 4

Unless x has been assigned a value, sentence $x \geq 0$ is not a proposition, because its truth value depends on the value of x

Sentence $x \geq 0$ is an example of an **open sentence** or **predicate**, a sentence containing zero or more variables that becomes a proposition when all variables are assigned specific objects.

Notation: if P is a predicate depending on variables $x_1, \ldots, x_n$ we write $P(x_1, \ldots, x_n)$. In this case, P is called an n-ary predicate — its arity is n.

Examples:

P given as $x+y=z$ is written as $P(x, y, z)$. $P(4, 3, 7)$ is true because $4+3=7$, but $P(1, 2, 4)$ is false. P has arity 3.

Let $Q(x, y)$ be $(x + y > 0)$. Then $Q(1, -1)$ is false and $Q(2, -1)$ is true. Q has arity 2.

Quantifiers

Assigning values to all of a predicate's variables creates a propositional statement which is either true or false.

Another way to create a proposition from a predicate is **quantification**. Quantification expresses the extend to which a predicate is true over a range of objects.

In English, words like *all, some, many, none,* and *few* are used in quantifications.

We will concentrate on two types of quantification:

- **universal quantification** tells us that a predicate is true for every object under consideration, and
- **existential quantification** tells us that for at least one object the predicate is true.

The area of logic dealing with predicates and quantifiers is called **predicate calculus**.

Universal Quantifiers

Many mathematical statements assert that a property is true for all values of a variable in a particular **domain** (or **universe**).

Example: "for all natural numbers x, $x \geq 0$ holds"

Here the domain is $\mathbb{N} = \{0, 1, 2, \ldots\}$, the natural numbers.

The meaning of the universal quantification changes when we change the domain. If we used $\mathbb{Z}$ (the integers) in the example above, the statement is no longer true.

Definition

The universal quantification of $P(x)$ is the statement

"$P(x)$ holds for all values of x in the domain"

which we write as $\forall x\ P(x)$. $\forall$ is called the **universal quantifier**. An object a for which $P(a)$ is false is called a **counterexample** of $\forall x\ P(x)$.

Note: An implicit assumption is that the domain is nonempty. For empty domains $\forall x\ P(x)$ is defined to be true, because no counterexample exists.

Example 1: Consider $P(x) := (x + 1 > x)$. What is the truth value of $\forall x\ P(x)$ in case the domain is $\mathbb{R}$ (the real numbers) ?

Because $x + 1 > x$ is true for every real number x, $\forall x\ P(x)$ is true.

Example 2: Consider $P(x) := x \geq 0$. Then $\forall x\ P(x)$ is true if the domain is $\mathbb{N}$, but it is false for domains $\mathbb{Z}$ and $\mathbb{R}$, because $x = -1$ is a counterexample in these cases.

When all objects in the domain can be listed — say $x_1, x_2, \ldots x_n$ — it follows that universal quantification $\forall x\ P(x)$ has the same truth value as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

(this motivates the other notation that is used for universal quantification: $\bigwedge_x P(x)$)

Example 3:

What is the truth value of $\forall x\ P(x)$, where $P(x)$ is the statement $x^2 < 10$ and the domain is all integers > 0 not exceeding 4?

The domain contains the values $1, 2, 3, 4$. So we can rewrite $\forall x\ P(x)$ as

$$P(1) \wedge P(2) \wedge P(3) \wedge P(4)$$

and check each case separately.

We have the feeling that $P(x)$ does not hold for large values, so we determine $P(4)$ first — it states $4{\cdot}4 < 10$, which is false. So, $x = 4$ is a counterexample and $\forall x\ P(x)$ is false.

Existential Quantifiers

Many mathematical statements assert that there is an object in the domain with a certain property. Such statements are expressed using existential quantification.

Example: There exists a natural number k such that $10 = 2k$.

Here, the domain is $\mathbb{N}$ and $10 = 2{\cdot}5$ shows that for $k = 5$ the predicate holds. Thus, the quantified statement is true.

Definition

The existential quantification of $P(x)$ is the proposition

"$P(x)$ holds for at least one object x in the domain"

which we write as $\exists x\ P(x)$. Here $\exists$ is called the **existential quantifier**. An object a for which $P(a)$ is true is called **witness** for $\exists x\ P(x)$.

Note: If the domain is empty, $\exists x\ P(x)$ is defined to be false, because there can be no witness.

Example 1: Let $P(x)$ denote the statement "$x > 3$". What is the truth value of $\exists x\ P(x)$ for domain $\mathbb{R}$?

4 is a witness because $4 > 3$. Therefore, $\exists x\ P(x)$ is true.

Example 2: Consider $Q(x) :=$ (x = x+1) and domain $\mathbb{N}$. What is the truth value of $\exists x\ Q(x)$?

$x = x+1$ is false for every natural number x. Therefore, there can not exist any witness. Therefore, $\exists x\ Q(x)$ is false.

Similar to the universal quantifier case, if all objects in the domain can be listed, say $x_1, \ldots, x_n$, then $\exists x\ P(x)$ has the same truth value as the disjunction

$$P(x_1) \vee \ldots \vee P(x_n)$$

(this motivates the other notation that is used for existential quantification: $\bigvee_x P(x)$)

Natural Language and Quantified Expressions

To get familiar with the concepts of quantified expressions here we give some examples of translating English phrases.

Example 1: "Some people dislike taxes"
$\exists x$ (x dislikes taxes) [domain people]

Example 2: "All people need oxygen to live"
$\forall x$ (x needs oxygen to live) [domain people]

Example 3: "Automobiles have engines" probably means:
$\forall x$ (x has an engine) [domain automobiles]

Example 4: "Golfers wear knit shirts" probably means:
$\exists x$ (x wears knit shirts) [domain golfers]

Example 5: "All apples have spots" [domain fruit]

Let $A(x) :=$ (x is an apple) and $S(x) :=$ (x has spots)

First attempt: $\forall x\ (A(x) \wedge S(x))$

Doesn't quite work because if this is true it says that all fruit x are apples and have spots.

Second attempt: $\forall x\ (A(x) \Rightarrow S(x))$

This works, because this states that if a fruit is an apple then it has spots.

Example 6: "Some apples have spots" [domain fruit]

First attempt: $\exists x\ (A(x) \Rightarrow S(x))$

Doesn't work, because this doesn't ensure that there actually is an apple. If there were no apple in the fruit domain, the statement would still be true, because $A(x)$ would be false all the time.

Second attempt: $\exists x\ (A(x) \wedge S(x))$

This works, because this states that there is a fruit that is an apple and it has spots.

Logical Equivalence Involving Quantifiers

We would like to make general statements about quantified expressions that do not depend on the actual predicates we use.

Definition

Statements φ and ψ involving predicates and quantifiers are **(logically) equivalent** iff they have the same value no matter which predicates are substituted and which domain is used for the variables. We write $\varphi \equiv \psi$ in this case.

Example 1: The following equivalence holds:

$$\forall x\ [P(x) \wedge Q(x)] \ \equiv\ [\forall x\ P(x)] \wedge [\forall x\ Q(x)]$$

Proof: Suppose P, Q are arbitrary predicates with common domain D. We prove the claim in two parts:

1. prove $\forall x\ [P(x) \wedge Q(x)] \ \Rightarrow\ [\forall x\ P(x)] \wedge [\forall x\ Q(x)]$

and

2. prove $[\forall x\ P(x)] \wedge [\forall x\ Q(x)] \ \Rightarrow\ \forall x\ [P(x) \wedge Q(x)]$

If both parts are true, we know that the truth values of

both sides are identical, and thus the equivalence holds.

ad 1: Suppose $\forall x\ [P(x) \wedge Q(x)]$ is true. This means that for every a in the domain $P(a)$ and $Q(a)$ both hold. This means $[\forall x\ P(x)]$ and $[\forall x\ Q(x)]$ is true.

ad 2: Suppose $[\forall x\ P(x)] \wedge [\forall x\ Q(x)]$ is true. Then for each a in the domain $P(a)$ and $Q(a)$ is true. This means $P(a) \wedge Q(a)$ is true for each a, and thus $\forall x\ [P(x) \wedge Q(x)]$ holds. □

Example 2: Prove or disprove:

$$[\forall x\ (P(x) \vee Q(x))]\ \equiv\ [\forall x\ P(x)] \vee [\forall x\ Q(x)]$$

This statement is wrong. We construct a counterexample: D contains values 0 and 1, and P, Q are defined as follows: $P(0) = F, P(1) = T, Q(0) = T, Q(1) = F$

Then $\forall x\ (P(x) \vee Q(x))$ is true, but both $\forall x\ P(x)$ and $\forall x\ Q(x)$ are false, which shows that the equivalence doesn't hold.

Lecture 5

Negating Quantified Expressions

In mathematics one is often faced with the problem of finding the logical negation of quantified expressions. Consider:

"Every student in this class has graduated from high-school," written as $\forall x\ P(x)$.

What is the negation? $(\neg\forall x\ P(x))$

"It is not the case that ..."

This is equivalent to saying

"There is a student in this class who has not graduated from high-school," which means $\exists x\ \neg P(x)$

So, we conjecture that the following equivalence holds:

$$1.\neg\forall x\ P(x)\ \equiv\ \exists x\ \neg P(x)$$

and similarily

$$2.\neg\exists x\ Q(x)\ \equiv\ \forall x\ \neg Q(x)$$

These are called the **De Morgan laws for quantifiers.**

Examples:

Negation of $\forall x\ (x^2 > x)$?

$\neg\forall x\ (x^2 > x)\ \Leftrightarrow\ \exists x\ \neg(x^2 > x)$ (De Morgan 1)

$\Leftrightarrow \exists x\ (x^2 \leq x)$

Negation of $\exists x\ (x^2 = 2)$?

$\neg\exists x\ (x^2 = 2) \Leftrightarrow \forall x\ (x^2 \neq 2)$ (De Morgan 2)

Proof of De Morgan 1.

To show that $\neg\forall x\ P(x)$ is equivalent to $\exists x\ \neg P(x)$ regardless of the predicates and domains we chose, we fix P and a domain and note:

$[\neg\forall x\ P(x)]$ is true $\Leftrightarrow$ $[\forall x\ P(x)]$ is false

$\Leftrightarrow$ there exists a in the domain with $P(a) = F$

$\Leftrightarrow$ there exists a in the domain with $\neg P(a) = T$

$\Leftrightarrow\ \exists x\ \neg P(x)$ □

Law 2. can be proved similarly.

Nested Quantifiers

Often, we like to model situations with more than one variable.

Example 1 (assuming domain $\mathbb{R}$):

$$\forall x\ [\ \underbrace{\exists y\ \underbrace{(x + y = 0)}_{P(x,y)}\ ]}_{Q(x)}$$

Which means: for each real number x there exists an y such that $x + y = 0$, which is called "additive inverse of x" and written as $y = -x$.

Given x and y, we can evaluate $x + y = 0$. We call this predicate $P(x, y)$. One level up we define $Q(x) := \exists y P(x, y)$, which for a given x is either true or false. In $\exists y(x + y = 0)$, x is called a **free variable** because it is not bound by any quantifier.

y obviously depends on x. We say that y lies in the **scope** of x, which is indicated by the square brackets, or that y is **nested** in the scope of x.

Example 2:

$$\underbrace{\forall x\ \forall y\ \underbrace{(x+y=y+x)}_{P(x,y)}}_{Q(x)}$$

means: operator $+$ is cummutative over $\mathbb{R}$, i.e. operand order doesn't matter.

Example 3:

$$\underbrace{\forall x\ \forall y\ \forall z\ \underbrace{\underbrace{(x+(y+z)=(x+y)+z)}_{R(x,y,z)}}_{P(x,y)}}_{Q(x)}$$

means: operator $+$ is associative over $\mathbb{R}$, i.e. evaluation order doesn't matter

Example 4:

$$\underbrace{\forall x\ \forall y\ \underbrace{[(x>0 \wedge y<0) \Rightarrow (x\cdot y<0)]}_{P(x,y)}}_{Q(x)}$$

means: the product of a positive and a negative real number is negative.

Multiple quantifiers are not always nested:

$$[\forall x\ P(x)]\ \wedge\ [\forall y\ Q(y)]$$

Here, the two quantified expressions are independent of each other because neither lies in the scope of the other. Therefore, x and y are unrelated. In such a case we can even reuse the same variable names without changing the logical meaning:

$$[\forall x\ P(x)]\ \wedge\ [\forall x\ Q(x)]$$

is equivalent to the expression above.

Order of Quantifiers

Does quantifier order matter?

$$\forall x\ \forall y\ P(x,y)\ \equiv\ \forall y\ \forall x\ P(x,y)$$

The order is not important in this case, because both sides are true if and only if $P(x,y)$ is true for all combinations of x and y.

Similarly true:

$$\exists x\ \exists y\ P(x,y)\ \equiv\ \exists y\ \exists x\ P(x,y)$$

But does this equivalence hold in general?

$$\exists x\ \forall y\ Q(x,y)\ \stackrel{?}{\equiv}\ \forall y\ \exists x\ Q(x,y)$$

Consider domain $\mathbb{R}$ and $Q(x,y) := (x+y=0)$. Then the left-hand side says:

"There is a number x such that for every y, $x+y=0$"

This is clearly wrong, because if $x+y=0$ then $x+(y+1)\neq 0$. But the right-hand side is true (the witness is $x=-y$). So, quantifier order may matter when quantifiers alternate ($\exists\forall\exists$...)

Generalized De Morgan Laws

Without proof we state the following generalized version of the De Morgan laws for quantifiers:

$$\neg\forall x_1\ \exists x_2\ \forall x_3 \cdots \forall/\exists x_n\ P(x_1,\ldots,x_n)\ \equiv$$
$$\exists x_1\ \forall x_2\ \exists x_3 \cdots \exists/\forall x_n\ \neg P(x_1,\ldots,x_n)$$

and

$$\neg\exists x_1\ \forall x_2\ \exists x_3 \cdots \forall/\exists x_n\ P(x_1,\ldots,x_n)\ \equiv$$
$$\forall x_1\ \exists x_2\ \forall x_3 \cdots \exists/\forall x_n\ \neg P(x_1,\ldots,x_n)$$

i.e., to negate a nested quantified statement we flip all quantifiers and negate the predicate.

Example:

$$\neg\forall x\ \exists y\ (x+y=0)\ \equiv\ \exists x\ \forall y\ (x+y\neq 0)$$

Observation: These laws in conjunction with the De Morgan laws for compound propositions and double negation allow us to transform quantified expressions into an equivalent form in which negations only appear as singletons immediately in front of predicates:

$$\neg\forall x\ \exists y\ (P(x,y)\wedge\neg Q(x,y)) \equiv \exists x\ \forall y\ (\neg P(x,y)\vee Q(x,y))$$

Rules of Inference

Proofs in mathematics are valid arguments establishing the truth of mathematical statements.

Argument: sequence of statements that end with a conclusion.

Valid Argument: conclusion must follow from the truth of the preceding statements, or **premises**, of the argument.

I.e., arguments are valid iff it is impossible for all premises to be true and the conclusion to be false.

In other words:

An argument form with premises $P_1, \ldots, P_n$ and conclusion Q is valid iff $P_1 \wedge \cdots \wedge P_n \Rightarrow Q$ is a tautology.

To decuce new statements from existing ones, we will use **rules of inference** which are templates for constructing valid arguments.

Valid Arguments

Example:

"If you have a current password, then you can log onto the network"

"You have a current password"

Therefore,

"You can log onto the network"

Is this a valid argument? We must determine if the conclusion must be true if the premises are both true.

Let's look at the arguments propositional form.

Let $P =$ "You have a current password"

and $Q =$ "then you can log onto the network"

Then, the argument has the form

$P \Rightarrow Q$
P
Therefore, Q

written as:

$$\frac{P \Rightarrow Q \qquad P}{Q}$$

If P is true, and $P \Rightarrow Q$ is true, a look at the truth table for $\Rightarrow$ (rows 3 and 4) verifies that Q must also be true:

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

Therefore, $\dfrac{P \qquad P \Rightarrow Q}{Q}$

is a valid argument. It is called the "modus ponens" ("mode that affirms") inference rule which is the single most important rule for carrying out mathematical proofs.

Other important inference rules:

$\dfrac{\neg Q \qquad P \Rightarrow Q}{\neg P}$ "Modus tollens" (Latin: mode that denies)

"I can't log onto the network"

"If you have a current password, then you can log onto the network"

Therefore, "I don't have a current password."

$\dfrac{P \Rightarrow Q \qquad Q \Rightarrow R}{P \Rightarrow R}$ "Hypothetical syllogism"

"If you have a current password, then you can log onto the network"

"If you can log onto the network, then you can remove files"

Therefore, "If you have a current password, then you can remove files"

$P \vee Q$
$\underline{\neg P \quad}$ "Disjunctive syllogism"
Q

"I am rich or I drive a kick scooter to work"

"I am not rich"

Therefore, "I drive a kick scooter to work"

$P \vee Q$
$\underline{\neg P \vee R}$ "Resolution"
$Q \vee R$

Basis for automated theorem proving systems and logic-based programming languages such as Prolog (covered in CMPUT 325 — Non-procedural programming languages)

Theorems and Basic Proof Techniques

Some terminology:

Theorem: (somewhat important) statement that can be shown to be true.

Proposition: less important theorem.

Lemma: (plural: lemmas or lemmata) less important theorem that is helpful in the proof of other results.

Corollary: theorem that can be established directly from another theorem.

Theorems are demonstrated to be true by **proofs**, which are valid arguments.

Statements used in a proof can include **axioms** (statements we assume to be true), premises of the theorem, and previously proven theorems.

All terms used in theorems must be defined.

Rules of inference are used to draw conclusions from assertions, tying together the steps of a proof.

For proving statements of the form $\forall x\ (P(x) \Rightarrow Q(x))$ our goal is to show $P(c) \Rightarrow Q(c)$ is true, where c is an arbitrary object in the domain.

Therefore, we focus on methods that show that conditional statements $P \Rightarrow Q$ are true.

For this, we only need to look at the case where P is true, for which we have to prove that Q is true as well.

Direct Proofs

Direct proofs are formed by implication chains of the form $P_1 \Rightarrow P_2 \Rightarrow \cdots P_n \Rightarrow C$ meaning that if statement P_1 holds then conclusion C also holds.

To show that this argument is valid, we assume that P_1 is true and then proceed by proving that each P_i and C is true as well.

Example:

Claim: The square of every odd natural number is odd.
I.e., $\forall x\ [\text{odd}(x) \Rightarrow \text{odd}(x^2)]$.

Proof: Pick an arbitrary natural number x. By definition we know odd(x) means $\exists k\ (x = 2k + 1)$.
E.g. $17 = 2 \cdot 8 + 1$, so 17 is odd.

Therefore:

odd(x)

$\stackrel{\text{def.}}{\Rightarrow} \exists k\ (x = 2k + 1)$

$\stackrel{\text{square}}{\Rightarrow} \exists k\ (x^2 = (2k + 1)^2) \quad [= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1]$

$\Rightarrow \exists l\ (x^2 = 2 \cdot l + 1)$
(choose $l = 2k^2 + 2k$ with k from the previous line)

$\stackrel{\text{def.}}{\Rightarrow}$ odd(x^2)

Because this argument is valid for arbitrary x, $\forall x\ [\text{odd}(x) \Rightarrow \text{odd}(x^2)]$ is true. □

It is good practice to annotate implications with the reason why they hold, like in the last example (definition, square, etc.)

This simplifies the task of verifying proof steps and helps you to double check your work and us when grading.

Lecture 6

More Complex Direct Proof Templates

Here we consider direct proofs for common statements of the form

$$\varphi \Rightarrow \psi$$

where φ and ψ are compound propositions themselves.

For example:

$(P \wedge Q) \Rightarrow R$

This poses no new difficulty. We even have one more premise to work with compared to $P \Rightarrow R$.

$P \Rightarrow (Q \wedge R)$

This is equivalent to $(P \Rightarrow Q) \wedge (P \Rightarrow R)$.
(If P is false then both statements are true, and if P is true both are equal to $Q \wedge R$). Thus, we can proceed by first showing $P \Rightarrow Q$ and then $P \Rightarrow R$.

$P \Rightarrow (Q \vee R)$

This is equivalent to $(P \wedge \neg Q) \Rightarrow R$ or altnernatively $(P \wedge \neg R) \Rightarrow Q$, because all three are equivalent to

$$\neg P \vee Q \vee R$$

So we have one more premise to work with.

$(P \vee Q) \Rightarrow R$

This is equivalent to $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ (proof exercise). Thus, a proof of above statement can proceed in two steps: 1. $P \Rightarrow R$ and 2. $Q \Rightarrow R$.

Proofs by Exhaustion

Special case: $(P \vee \neg P) \Rightarrow R$, which when true means that R must be true as well. From the previous equivalence we know that

$$[(P \vee \neg P) \Rightarrow R] \equiv [(P \Rightarrow R) \wedge (\neg P \Rightarrow R)]$$

So, if we can show that both $P \Rightarrow R$ and $\neg P \Rightarrow R$ are true, then R is true. This proof is a special case of the more general idea of proving statements by exhaustion, i.e. examining all possible cases.

Example:

Claim: Suppose that n is an odd integer. Then $n = 4j+1$ for some integer j, or $n = 4i-1$ for some integer i.

Proof: Suppose n is odd. Then $n = 2m + 1$ for some integer m. We distinguish two cases: m even and m odd (P and $\neg P$) and show that in both cases the conclusion holds, and thus the claim is valid.

Case 1: If m is even then $m = 2j$ for some integer j, and so $n = 2m + 1 = 2 \cdot 2j + 1 = 4j + 1$.

Case 2: If m is odd then $m = 2k + 1$ for some integer k, and so $n = 2m + 1 = 2 \cdot (2k + 1) + 1 = 4k + 3 = 4(k + 1) - 4 + 3 = 4i - 1$ for $i = k + 1$.

So, in either case the conclusion, which is a disjunction, is true. □

Proof by Contraposition

Attempts at direct proofs often reach dead ends. Here we consider proof methods that do not start with the premises and end with the conclusion, which are called **indirect** proofs.

A useful type of indirect proof is known as **proof by contraposition**, in which we make use of the fact that $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$.

We can therefore start with the negation of the conclusion, and then using axioms and other theorems, we try to show that the premise is false.

Example:

Claim: If $n = a \cdot b$, where a and b are natural numbers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof: Because we can't see an obvious direct proof, we attempt a proof by contraposition. We start with the negation of the conclusion: $(a > \sqrt{n}) \ \wedge \ (b > \sqrt{n})$. Therefore, by multiplying both inequalities we get to $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, which means $a \cdot b \neq n$. This contradicts the premise and the claim is true. $\square$

Proofs by Contradiction

Suppose we want to prove that statement P is true.

If we can find a contradiction Q (e.g. $R \wedge \neg R$) such that $\neg P \Rightarrow Q$, then P is true.

This is called a proof by contradiction.

Example:

Claim: There are infinitely many prime numbers, i.e. natural numbers ≥ 2 that are only divisible by 1 and themselves $(2, 3, 5, 7, 11, 13 \ldots)$

Proof: Assume there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_n$. Let

$$p = p_1 \cdot p_2 \cdots p_n + 1.$$

Then p is bigger than any p_i. Thus, p is not a prime number, because it is not on the list. On the other hand, p is not divisible by any p_i, because the remainder is always 1. Because all non-prime numbers can be decomposed into a product of primes, either p is a prime, or there are prime numbers which p can be decomposed into which are not on the list. In either

case, this leads to a contradiction. Therefore, there are infinitely many prime numbers. $\square$

Proofs of Equivalence

Theorems of the form of biconditional statements

$$P \Leftrightarrow Q$$

can be proved by showing $P \Rightarrow Q$ and $Q \Rightarrow P$ (based on the equivalence we have seen before).

Sometimes, theorems state that several propositions (say $P_1, P_2, \ldots P_n$) are equivalent, i.e.

$$P_1 \Leftrightarrow P_2, \ P_2 \Leftrightarrow P_3, \cdots P_{n-1} \Leftrightarrow P_n,$$

which means that all propositions have the same truth values.

One way of proving this equivalence is to show that

$$P_1 \Rightarrow P_2, \ P_2 \Rightarrow P_3, \ \ldots, \ P_{n-1} \Rightarrow P_n, \ P_n \Rightarrow P_1$$

are all true, which means that all P_i have the same truth value. This is way more economical than proving $n - 1$ equivalences.

Example: (skipped in class, read at home)

Claim: These statements about integer n are equivalent

P_1: n is even

P_2: $n - 1$ is odd

P_3: n^2 is even

Proof: We show $P_1 \Rightarrow P_2, \ P_2 \Rightarrow P_3, \ P_3 \Rightarrow P_1$

$P_1 \Rightarrow P_2$: n even $\Rightarrow \ \ n = 2k$ for some integer k. Therefore $n - 1 = 2k - 1 = 2(k - 1) + 1$ is odd.

$P_2 \Rightarrow P_3$: $n - 1 = 2k + 1$ for some k. Therefore, $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$, which shows that n^2 is even.

$P_3 \Rightarrow P_1$: Proof by contraposition: assume n odd, i.e. $n = 2k + 1$ for some integer k. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd. $\square$

Proofs Involving Quantifiers

The proof methods we described above can be directly applied to expressions of the form

$$\forall x\ P(x) \quad \text{and} \quad \exists x\ P(x)$$

A direct proof of $\forall x\ P(x)$ has the following form:

- Let x be an arbitrary object in the domain.
- ...
- Hence, $P(x)$ is true.
- Because x is arbitrary, $\forall x\ P(x)$ is true

Likewise, a proof of $\forall x\ P(x)$ by contradiction proceeds as follows:

- Suppose $\neg\forall x\ P(x)$
- Then $\exists x\ \neg P(x)$
- Let t be an object such that $\neg P(t)$
- ....
- Therefore, $Q \wedge \neg Q$
- Thus, $\exists x\ \neg P(x)$ is false, and $\forall x\ P(x)$ is true.

For statements of the form $\forall x\ P(x)$ we can either start looking for a direct or indirect proof, or — if we have reason to believe that it doesn't hold, we can try to find a **counterexample** that disproves the statement.

Example: Consider the sequence of prime numbers $2, 3, 5, 7, 11, \ldots = p_1, p_2, p_3, \ldots$ in increasing order. We claim that for each n, $p_1 \cdot p_2 \cdots p_n + 1$ is a prime number (we used that number to prove that the sequence of primes is infinite).

This seems to work in the first couple of cases:

$2 + 1 = 3$

$2 \cdot 3 + 1 = 7$

$2 \cdot 3 \cdot 5 + 1 = 31$

Not finding a direct way of proving the claim, we continue to search for a counterexample and after a few more checks we find one:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

Therefore, the claim is false.

Existence Proofs

A proof of a statement of the form $\exists x\ P(x)$ is called an existence proof.

Often we can find an object a in the domain such that $P(a)$ is true. Such a proof is called **constructive**.

If we prove $\exists x\ P(x)$ in some other way, this proof is called **non-constructive**.

Example of a non-constructive existence proof involving irrational numbers:

Recall: a number is **rational** if it can be expressed as a ratio p/q of integers p, q or equivalently, its decimal representation is either finite, or repeating.

Numbers that are not rational are called **irrational**.

Facts: 1.5 and $1.1111111...$ are rational

$\sqrt{2} = 1.4142...$ is irrational.

Claim: There exist irrational numbers x and y such that x^y is rational, i.e. in domain $\mathbb{R}$

$$\exists x\ \exists y\ (x \text{ irrational} \wedge y \text{ irrational } \wedge x^y \text{ rational})$$

is true.

Proof: Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have found two numbers x, y such that x^y is rational, and we are done.

If $\sqrt{2}^{\sqrt{2}}$ is irrational, let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$.

Then $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$, which is rational.

So, one of the pairs of numbers has the desired property. Even though we don't know which, this proves the claim. □