Sets and Logic

CSC 1300 – Discrete Structures

Villanova University

Major Themes

- Sets
  - Ways of defining sets
  - Subsets, complements, the universal set
  - Venn diagrams
  - Proofs of set equality via double inclusion
- Logic
  - Propositions
  - Truth tables
  - Venn diagrams
  - Quantifiers
  - Proof techniques: direct, indirect, contradiction

Basic terminology

A ***set*** is an unordered collection of distinct objects called ***elements*** or ***members*** of the set.

The cardinality of a finite set S is denoted **|S|**.

The notation **$x \in S$** — means "x is an element of S"

Example: S = {2, 4, 6, 8}, |S| = 4
$2 \in S$ — "2 is an element of S"
$3 \notin S$ — "3 is not an element of S"

A ***multiset*** or a ***bag*** is an unordered collection of objects that are not necessarily distinct.

Describing sets

Two ways to describe a set:

1. by listing elements, e.g., S = {2, 4, 6, 8}

2. by a property, e.g.,
   S = {x | x is an even positive integer}

- The set that has no elements is called the ***empty set***, or ***null set***, and is denoted by ∅, or **{ }.**

- Note that |∅| = 0

Some important sets

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ - the set of ***natural numbers***
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ - the set of ***integers***
- $\mathbb{W} = \{0, 1, 2, 3, \ldots\}$ - the set of ***positive integers***
- $\mathbb{Z}_2 = \{0, 1\}$ - the ***binary digits***
- $\mathbb{R}$ - the set of ***real numbers***
- $\mathbb{Q} = \{x \mid x = p/q$ where $p, q \in \mathbf{Z}, q \neq 0\}$ - the set of ***rational numbers***

Subsets

S is a ***subset*** of T, denoted $S \subseteq T$, iff every element of S is also an element of T.

<u>Examples:</u> $\{a,b\} \subseteq \{a,b,c\}$

$\{a,b, c\} \subseteq \{a,b,c\}$

$S \subseteq S$ (for any S)

$\emptyset \subseteq S$ (for any S)

S is a ***proper subset*** of T, denoted $S \subset T$, iff S is a subset of T but not vice versa.

<u>Examples:</u> $\{a,b\} \subset \{a,b,c\}$ $\{b\} \subset \{a,b,c\}$

what about $\emptyset \subset S$???

Note that $S \subset T$ iff $S \subseteq T \wedge S \neq T$

The Power Set

The ***power set*** of a set S is the set of all subsets of S.
The power set of S is denoted by $P(S)$.

$P(\varnothing) = \{\varnothing\}$

$P(\{a\}) = \{\varnothing, \{a\}\}$

$P(\{a,b\}) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$

$P(\{0, 1, 2\}) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1,2\}, \{0,1,2\}\}$

Note that $|P(S)| = 2^{|S|}$

Set equality

Two sets S and T are ***equal***, denoted $S = T$, iff they have the same elements, i.e., for every x:

if $x \in S$ then $x \in T$

and if $x \in T$ then $x \in S$

In other words:

$S=T$ iff $S \subseteq T$ and $T \subseteq S$

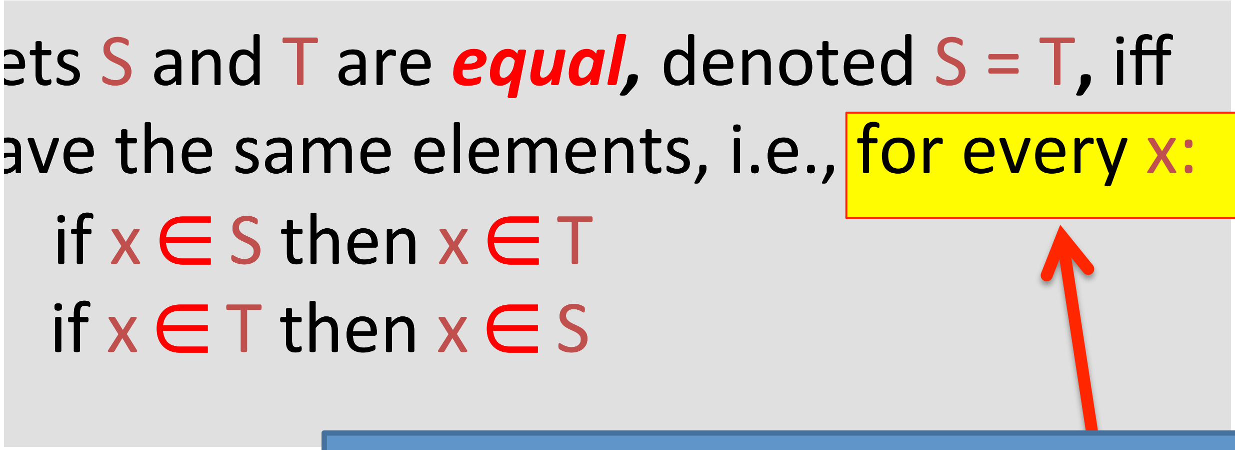
Proof technique: double inclusion

Set equality

Examples:

- {a,b} = {b,a}
- {1, 2, 3} = {x | x is an integer and 0< x < 4}
- {2, 4, 6} = { x | x = 2*y, where y ∈ {1, 2, 3} }

The Universal Set



ets S and T are ***equal***, denoted $S = T$, iff
ave the same elements, i.e., for every x:

if $x \in S$ then $x \in T$

if $x \in T$ then $x \in S$

What does this even mean????

The Universal Set U

We usually think of sets as subsets of a ***universal set*** U.

- Example: {a,b} and {b,d,e} ➔ U = {a,b,c,d,e}

  (or maybe U = {a,b,c,d,e,f,g,…,z} - usually determined by context)

The ***complement*** of S, denoted $\overline{S}$ is the set of elements of U that are not in S.

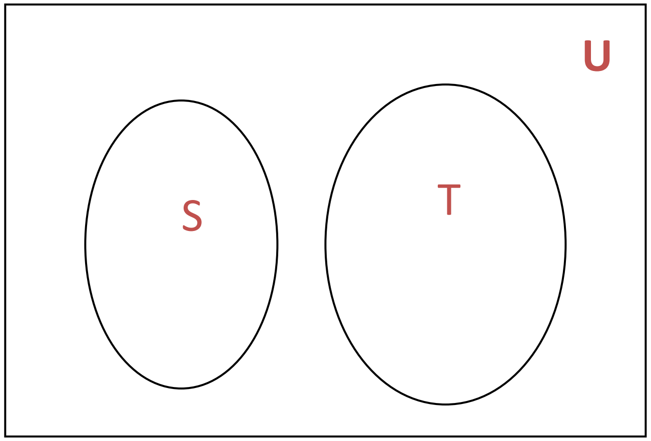
Example: $\overline{\{b,d,e\}} = \{a,c\}$

The ***set difference***, denoted S – T (or S \ T), is the set of elements of S that are NOT also in T.

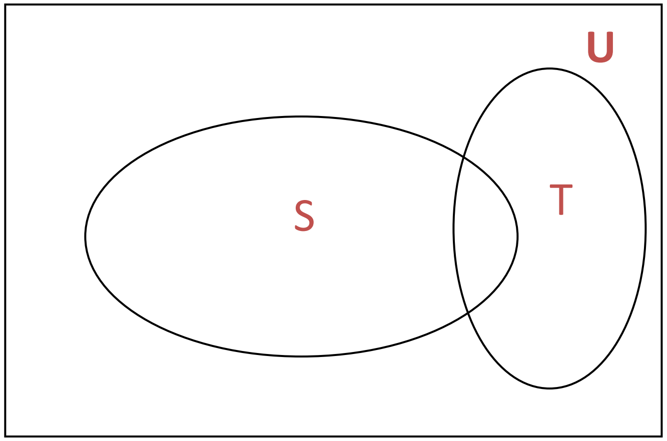
Examples: {a,b,c,d,e} – {b,d,e} = {a,c}   (Note: $\overline{S}$ = U – S)

{b,c} – {a,b} = {c}

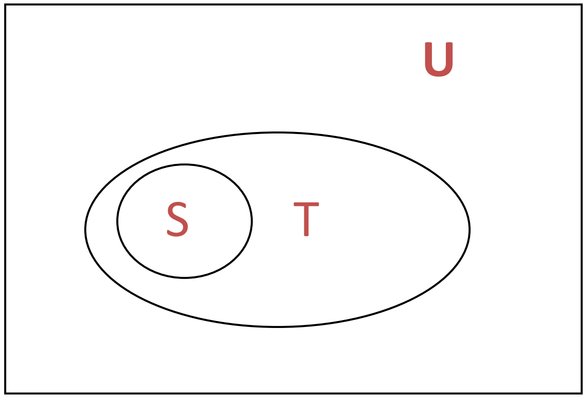
Venn diagrams



disjoint sets S and T



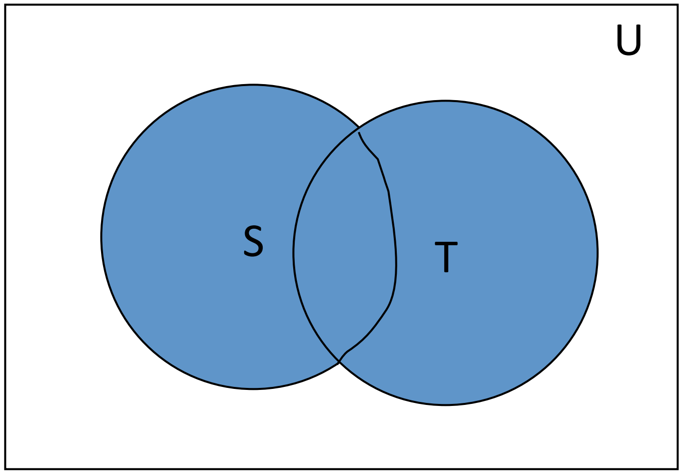
S and T are not disjoint



$S \subseteq T$

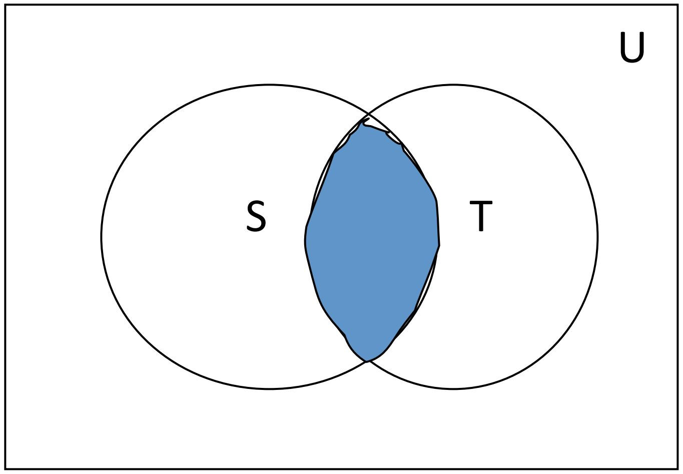
Set Union and Intersection

$S \cup T = \{x \mid x \in S \text{ or } x \in T\}$



$S \cup T$ is shaded

$S \cap T = \{x \mid x \in S \text{ and } x \in T\}$



$S \cap T$ is shaded

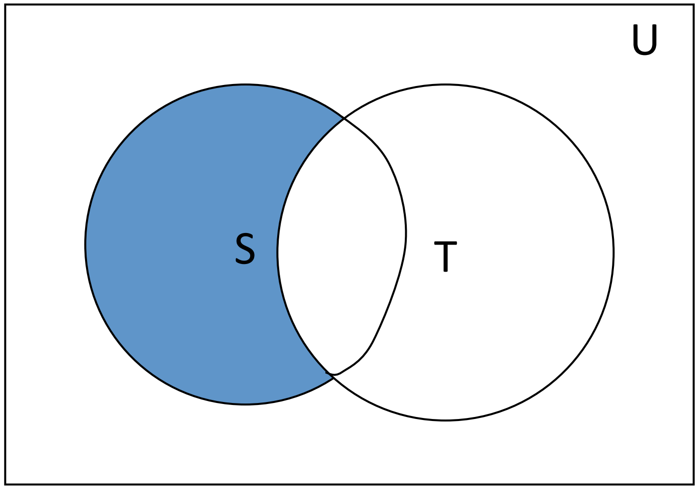
Example: Let $S=\{1,2,3,4\}$ and $T=\{2,3,5\}$. Then

$S \cup T = \{1,2,3,4,5\}$

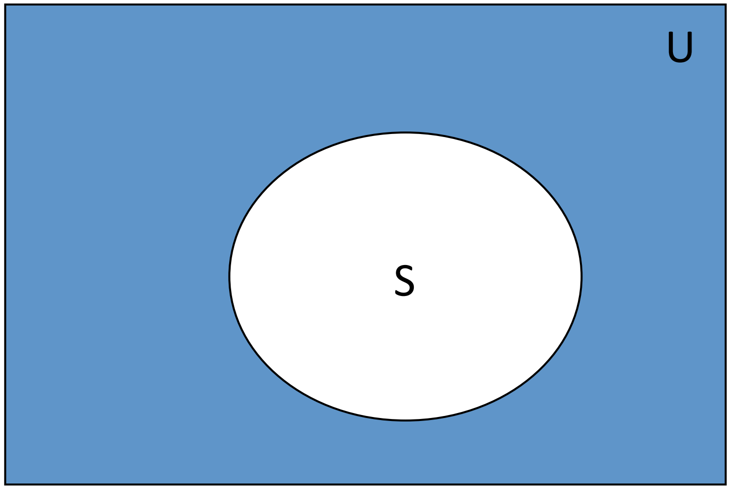
$S \cap T = \{2,3\}$

Set difference and complement

S – T = {x | x∈S and x∉T}



$\overline{\textbf{S}}$ = U - S



Example: Let U = **N**

S = {x | x is an integer greater than 6}

T = {x | x is an even positive integer}

Then S - T = { x | x is an odd integer greater than 6}

$\overline{S}$ = {x | x is an integer less than or equal to 6}

Generalized unions and intersections

$S_1 \cap S_2 \cap \ldots \cap S_n$ denoted by $\bigcap_{i=1}^{n} S_i$

$S_1 \cup S_2 \cup \ldots \cup S_n$ denoted by $\bigcup_{i = 1}^{n} S_i$

Example: Let $S_i = \{ i \}$.

$\bigcap_{i=1}^{n} S_i = \varnothing$ and $\bigcup_{i=1}^{n} S_i = \{1,2,\ldots,n\}$

review

Sets and cardinality

Let $A = \{a, b, c\}$, $B = \{1, 2\}$

cardinality of a set = number of members

$|A| = 3$

$|B| = 2$

$A \cup B = \{a, b, c, 1, 2\}$ $A \cap B = \varnothing$

Sum Principle: If A and B are ***disjoint***

$$|A \cup B| = |A| + |B|$$

Sets and cardinality

Let $A = \{a, b, c, d, e\}$, $B = \{b, d\}$

$|A| = 5$

$|B| = 2$

$A \setminus B = \{a, c, e\}$

Difference Principle: If $A \subseteq B$,

$$|A \setminus B| = |A| - |B|$$

review

Cartesian product

Let A = {a, b, c}, B = {1, 2}

The ***<u>cartesian product</u>*** is the set of ordered pairs (x,y) where x ε A and y ε B:

A x B = { (a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2) }

Product Principle: |A x B| = |A| · |B|

Ordered pairs and n-tuples

ordered pairs (a_1,a_2)

and

ordered n-tuples $(a_1,a_2,\ldots,a_n)$

- represent sequences where the order of elements **does** matter and repetitions are allowed.

The ***Cartesian product*** of the sets $S_1, S_2, \ldots, S_n$, denoted by $\mathbf{S_1 \times S_2 \times \ldots \times S_n}$, is the set of all ordered n-tuples $(s_1,s_2,\ldots,s_n)$ where $s_1 \in S_1$, $s_2 \in S_2$, …, $s_n \in S_n$. In other words,

$$S_1 \times S_2 \times \ldots \times S_n = \{(s_1,s_2,\ldots,s_n) \mid s_1 \in S_1 \text{ and } s_2 \in S_2 \text{ and } \ldots \text{ and } s_n \in S_n\}$$

Set identities

$S \cup \varnothing = S$ $S \cap \mathbf{U} = S$	Identity laws	$S \cup (T \cup R) = (S \cup T) \cup R$ $S \cap (T \cap R) = (S \cap T) \cap R$	Associative laws
$S \cup \mathbf{U} = \mathbf{U}$ $S \cap \varnothing = \varnothing$	Domination laws	$S \cap (T \cup R) = (S \cap T) \cup (S \cap R)$ $S \cup (T \cap R) = (S \cup T) \cap (S \cup R)$	Distributive laws
$S \cup S = S$ $S \cap S = S$	Idempotent laws	$\overline{S \cup T} = \overline{S} \cap \overline{T}$ $\overline{S \cap T} = \overline{S} \cup \overline{T}$	De Morgan's laws
$S \cup T = T \cup S$ $S \cap T = T \cap S$	Commutative laws	$\lvert S \cup T \rvert = \lvert S \rvert + \lvert T \rvert - \lvert S \cap T \rvert$	Inclusion-exclusion
$\overline{(\overline{S})} = S$	Complementation law		

Proving set identities - example

Prove that $\overline{S \cap T} = \overline{S} \cup \overline{T}$ (de Morgan's Law for sets).
Proof: We proceed by showing that each set is a subset of the other, i. e. $\overline{S \cap T} \subseteq \overline{S} \cup \overline{T}$ and $\overline{S} \cup \overline{T} \subseteq \overline{S \cap T}$

1. Suppose $x \in \overline{S \cap T}$. i.e. $x \notin S \cap T$. Then $x \notin S$ or $x \notin T$.

   Hence, $x \in \overline{S}$ or $x \in \overline{T}$. This means that $x \in \overline{S} \cup \overline{T}$.

   Thus, $\overline{S \cap T} \subseteq \overline{S} \cup \overline{T}$.

2. Now suppose $x \in \overline{S} \cup \overline{T}$. Then $x \in \overline{S}$ or $x \in \overline{T}$.

   Hence $x \notin S$ or $x \notin T$, which means that $x \notin S \cap T$.

   Therefore, $x \in \overline{S \cap T}$. Thus, $\overline{S} \cup \overline{T} \subseteq \overline{S \cap T}$.

Major Themes

- Sets
  - Ways of defining sets
  - Subsets, complements, the universal set
  - Venn diagrams
  - Proofs of set equality via double inclusion
- Logic
  - Propositions
  - Truth tables
  - Venn diagrams
  - Quantifiers

Why Logic?

Logic – a science of ***reasoning***

- Basis of mathematical reasoning
  - gives precise meaning to mathematical statements
  - is used to distinguish between valid and invalid mathematical arguments

- Applications in CS:
  - design of hardware
  - programming
  - artificial intelligence
  - databases

Proposition

A ***declarative*** statement that is either **true** or **false**

Are the following propositions?

- 1+2 = 3
- today is my birthday
- New York is the capital of the USA
- 5 - 3 + 2
- x+y > 5
- Are you a student?
- Don’t talk
- Your feet are ugly
- This sentence is false

Compound Propositions and Connectives

Compound propositions are formed from simpler propositions using *connectives*, also called *logical operators*.

The connectives we will study are:

- *negation* or *not* operator denoted $\neg$
- *conjunction* or *and* operator $\wedge$
- *disjunction* or *or* operator $\vee$
- *exclusive or* or *xor* operator $\oplus$
- *implication* $\rightarrow$
- *biconditional* $\leftrightarrow$

Negation

If *p* is a proposition, then the statement

"It is not the case that *p*"

is another proposition, called the *negation* of *p*.
The negation of *p*, denoted by ¬*p* and read "not *p*", is true when *p* is false, and is false when *p* is true.

Example: What is the negation of "Today is Wednesday"?

The truth table for negation:

p	¬*p*
T	
F	

Conjunction

The proposition "*p and q*", denoted by $p \land q$, is called the *conjunction of p and q*.

It is true when both p and q are true, otherwise it is false.

Examples: Today is Wednesday and it is raining.

Today is Wednesday but it is not raining.

The truth table for conjunction:

p	q	$p \land q$
T	T	
T	F	
F	T	
F	F	

Disjunction

The proposition "*p* or *q*", denoted by $p \vee q$, is called the *disjunction* of *p* and *q*.
It is false when both *p* and *q* are false, otherwise it is true.

Example: Today is Sunday or a holiday.

The truth table for disjunction:

p	*q*	$p \vee q$
T	T	
T	F	
F	T	
F	F	

Exclusive OR (XOR)

The proposition *$p \oplus q$* is called the *exclusive or* of *p* and *q*. It is true when exactly one of *p* and *q* is true, otherwise it is false.

Example: This dish comes with soup or salad.

The truth table for exclusive or:

p	*q*	$p \oplus q$
T	T	
T	F	
F	T	
F	F	

Implication

The *implication* or *conditional proposition* $p \rightarrow q$ is the proposition that is false only when p is true and q is false.

p is called the *hypothesis* and q is called the *conclusion*.

The truth table for implication:

p	q	$p \rightarrow q$
T	T	
T	F	
F	T	
F	F	

Readings for $p \rightarrow q$:

- “if *p* then *q*”
- “*p* only if *q*”
- “*q* is necessary for *p*”
- “*p* is sufficient for *q*”
- “*p* implies *q*”
- “*q* if *p*”
- “*q* whenever *p*”

Examples of Implication Wording

If John is in L.A., then he is in California.

To be in California, it is sufficient for John to be in L.A.

To be in LA, it is necessary for John to be in California.

You will get an A if you study hard.
vs.
You will get an A only if you study hard.

More Examples of Implication wording:

If you place your order by 11:59pm December 21st, then we guarantee delivery by Christmas.

Placing your order by 11:59pm December 21st guarantees delivery by Christmas.

We guarantee delivery by Christmas if you place your order by 11:59pm December 21st.

More Examples of Implication wording:

If you place your order by 11:59pm December 21st, then
we guarantee delivery by Christmas.

Placing your order by 11:59pm December 21st
guarantees delivery by Christmas.

We guarantee delivery by Christmas
if you place your order by 11:59pm December 21st.

is this the same too?

We guarantee delivery by Christmas
only if you place your order by 11:59pm December 21st.

Biconditional

The *biconditional* $p \leftrightarrow q$ is the proposition that is true when p and q have the same truth values, and is false otherwise.

The truth table for biconditional:

p	q	$p \leftrightarrow q$
T	T	
T	F	
F	T	
F	F	

Readings for $p \leftrightarrow q$:

- "p if and only if q"
- "p is necessary and sufficient for q"
- "if p, then q, and conversely"

Truth tables for more complex propositions

p q r	$r \lor (q \land \neg p)$
T T T	
T T F	
T F T	
T F F	
F T T	
F T F	
F F T	
F F F	

Tautology

- A (compound) proposition that is always true (irrespective of the values of its components)

p	q	r	$(\neg p \wedge (p \vee q)) \rightarrow q$
T	T	T	
T	T	F	
T	F	T	
T	F	F	
F	T	T	
F	T	F	
F	F	T	
F	F	F	

Logical Equivalence

We say that two propositions are logically equivalent iff they have the same truth table.

p	q	$\neg p \lor q$	$p \to q$
T	T		
T	F		
F	T		
F	F		

- we write: $\neg p \lor q \equiv p \to q$

to indicate that the propositions $\neg p \lor q$ and $p \to q$ are logically equivalent

De Morgan's Laws for Logic

First De Morgan's law for logic:

$$\neg (p \vee q) \equiv (\neg p) \wedge (\neg q)$$

Example: Today is Sunday or a holiday.

Second De Morgan's law for logic:

$$\neg (\mathrm{p} \wedge q) \equiv$$

Example: Today is Sunday and a holiday.

Converse, Inverse and Contrapositive

- $q \rightarrow p$ is called the *converse* of $p \rightarrow q$
- $\neg p \rightarrow \neg q$ is called the *inverse* of $p \rightarrow q$
- $\neg q \rightarrow \neg p$ is called the *contrapositive* of $p \rightarrow q$

p	q	$p \rightarrow q$	$q \rightarrow p$	$\neg p \rightarrow \neg q$	$\neg q \rightarrow \neg p$
T	T				
T	F				
F	T				
F	F				

Which of the above are logically equivalent?

Bit operations

Bit (binary digit)- either 0 or 1.

T is usually represented as 1, and F as 0

0 v 0 = 0 (because F v F = F)
0 v 1 = 1 (because F v T = T)

These operations can also be applied to bit strings (sequences of bits):

001 v 010 = 011 (because 0 v 0 = 0, 0 v 1 = 1 and 1v 0 = 1)

Propositional functions

Interesting statements involve ***variables***.

Definition A ***propositional function*** $P(x)$ is a function whose values are propositions, i.e., it's an assignment to each element x of the function's domain D called the ***domain of discourse*** a proposition (a true or false statement).

Example

Let $P(x)$ denote the statement "x is even".

Domain of discourse?

$P(2)$

$P(3)$

Universal quantifier

Definition: ***universal quantification*** of $P(x)$

“$P(x)$ is true for all values of x in its universe of discourse”

“for all x $P(x)$”

“for every x $P(x)$ ”

$$\forall x\ P(x)$$

universal quantifier

Examples of universal quantification

$\forall x\ (x+0 = x)$

$\forall x\ (x^2 > x)$

$\forall x\ P(x)$ where $P(x)$ denotes the statement "x didn't do the homework"

"everyone is mortal":

Let $M(x)$ denote "x is mortal" and $H(x)$ denote "x is a human"

$\forall x\ M(x)$, if the universe of discourse is the set of all humans

or

$\forall x\ [H(x) \rightarrow M(x)]$, if the universe of discourse is the set of all things and creatures.

Existential quantifier

Definition: ***existential quantification*** of $P(x)$
“there exists an element x in its universe of discourse such that $P(x)$ is true”

“there is an x such that $P(x)$”

“for some x $P(x)$”

$\exists x\ P(x)$

existential quantifier.

Examples of existential quantification

True or false?

$\exists x\ (x+x=x*x)$

$\exists x\ (x=x+1)$

$\exists x\ P(x)$ where $P(x)$ denotes the statement "x did the practice problems"?

Generalized De Morgan Laws of Logic

- $\neg \forall x P(x) \equiv \exists x \neg P(x)$

"Not every student did the practice problems"

$\equiv$

"There is a student who did not do the practice problems"

- $\neg \exists x P(x) \equiv \forall x \neg P(x)$

"There is no white elephant"

$\equiv$

"Every elephant is not white"

Expressions with several quantifiers

Let the universe of discourse be the set of all students (of VU).

Let

C(x) means "x has a computer"

F(x,y) means "x and y are friends"

Translate the following into English:

- $\forall x C(x)$
- $\forall x[C(x) \vee \exists y(F(x,y) \wedge C(y))]$
- $\exists x \neg \exists y\, F(x,y)$

Does the order of the quantifiers matter?

— No, if we have several consecutive quantifiers of the same type:

$\forall x \forall y Q(x,y) \equiv \forall y \forall x Q(x,y)$ $\exists x \exists y Q(x,y) \equiv \exists y \exists x Q(x,y)$

— Yes, if we have different quantifiers:

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

Counterexample: Let $Q(x,y)$ mean "$x+y=0$", and let the universe of discourse be the set of all real numbers. What is the truth value of:

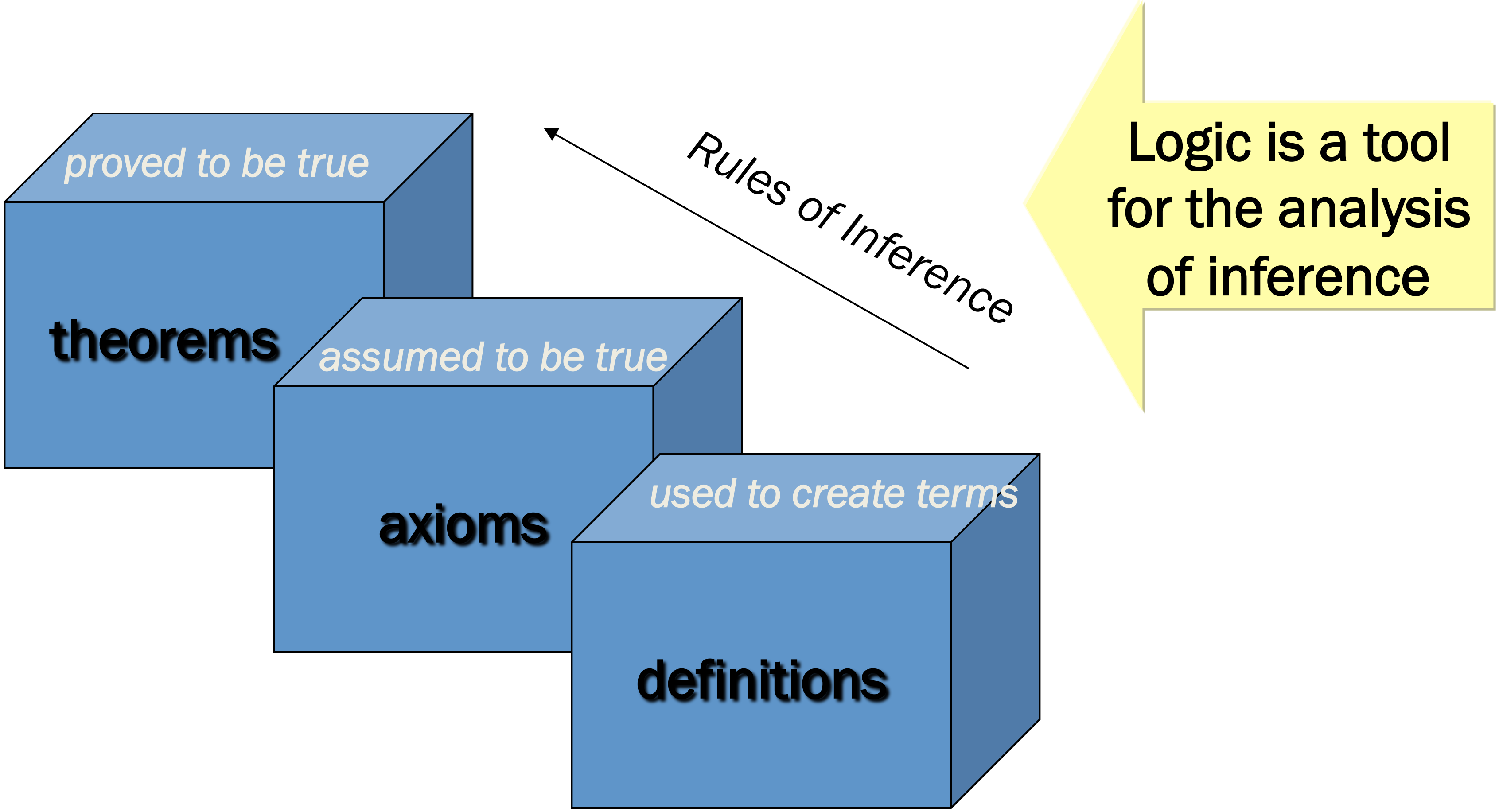
$\forall x \exists y Q(x,y)$?

$\exists y \forall x Q(x,y)$?

Proofs in Computer Science

- Establishing correctness and efficiency of algorithms
- Verification of program correctness
- Establishing that an operating system is secure
- Establishing that certain goals cannot be achieved (such as finding a universal program-correctness checker)
- Making inferences in AI

Mathematical System



Basic Terminology

- ***Axiom (postulate)*** – underlying assumption, does not require a proof
- ***Rules of inference*** – used to draw conclusions from other assertions
- ***Proof*** of a statement ***A*** – a sequence of statements, each of which is:
  - an axiom or
  - follows from one or more earlier statements

  and the last statement in the sequence is ***A***
- ***Informal proof*** *v*s. ***formal*** – uses rules of inference informally and formally, respectively
- ***Theorem*** – a statement that has been proved
- ***Lemma*** – a theorem used in the proof of other theorems
- ***Corollary*** – a theorem that immediately follows from another theorem

Conjecture

… a likely-to-be-true statement that has not yet been proved

- ***Fermat's Last Theorem*** **(17th century)**

Equation $x^n + y^n = z^n$ has no non-zero integer solutions for $n > 2$.
– a conjecture for over 300 years → proved by Andrew Wiles (Princeton, 1994)

- ***Goldbach's Conjecture*** **(18th century)**

Every even integer greater than 4 is the sum of two primes.
– still neither proved nor disproved

- ***P ≠ NP Conjecture*** **(1970s)**

There are problems that cannot be solved by any polynomial-time algorithm (i.e., running time grows slower than exponentially with input size), but whose guessed solutions can be verified by a such an algorithm.
– still neither proved nor disproved

- ***3x + 1 Conjecture*** **(1950s)**

If we repeatedly apply the transformation that sends an even integer x to x/2 and an odd integer to x →3x + 1 we will eventually reach 1. (eg: 13→40→20→10→5→16→8→4→2→1
– still neither proved nor disproved

Types of proofs

- direct
- indirect (by contrapositive)

- by contradiction

- proof of equivalence

- proof by cases
- proof by mathematical induction

Proving $p \rightarrow q$

- Direct Proof

$$p \rightarrow q$$

- Indirect Proof / Contrapositive

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

- Proof by Contradiction

$$p \rightarrow q \equiv (p \wedge \neg q) \rightarrow (r \wedge \neg r)$$

Direct Proof

To prove $p \rightarrow q$**:**

Suppose p ***is true; prove that*** q ***must also be true***

Example:

If n is even, then n^2 is also even

Proof:

Suppose n is even. Thus n = 2k for some k. Thus $n^2 = (2k)(2k) = 2(2k^2)$, which is also even.

Indirect Proof

Prove $p \rightarrow q$ ***by proving contrapositive:*** $\neg q \rightarrow \neg p$

Problem:

If n·m is odd, then an n×m grid cannot be tiled with dominoes.

Proof:

Proceed by proving that if an n×m grid can be tiled with dominoes, then n·m is even. Suppose an n×m grid can be tiled with dominoes. There are a total of n·m squares, so if each domino covers 2 tiles and there is no overlap and the dominoes cover all the squares, then the tiling will use nm/2 squares, which means n·m is even.

Contradiction Proof

Prove s by showing that ¬ s is absurd!

- $\neg s \rightarrow F$

(Reductio ad absurdum)

To prove implication: $p \rightarrow q$ ***show that:***

$(p \wedge \neg q) \rightarrow (r \wedge \neg r)$

Proofs of equivalence

A ***proof of equivalence*** of two assertions (i.e., $p \leftrightarrow q$), often stated by using "if and only if" or "necessary and sufficient," requires two separate parts:

$p \rightarrow q$ and $q \rightarrow p$.

- **Example:** An integer n is odd iff n^2 is odd.

Proofs, examples, and counterexamples: $\forall x\, P(x)$

For universal statements:

- *Checking validity of a theorem for specific examples does NOT constitute a proof* (unless the examples exhaust all the values in the theorem's domain, which is impossible if the latter is infinite).

- *Just a single example suffices to disprove a theorem.* (Such an example is usually called a counterexample).

Proofs, examples, and counterexamples $\exists x\ P(x)$

For existential statements:

- *A single example suffices to prove the theorem (constructive proof).*
- *Alternative, it is possible to show, using contradiction, that it is not possible for such a thing not to exist.*
  - Show that a player in a game has a winning strategy without actually saying what it is!
  - Famous proof: There exist irrational x, y such that x^y is rational

Major Themes

- Sets
  - Ways of defining sets
  - Subsets, complements, the universal set
  - Venn diagrams
  - Proofs of set equality via double inclusion
- Logic
  - Propositions
  - Truth tables
  - Venn diagrams
  - Quantifiers
  - Proof techniques: direct, indirect, contradiction