Lecture 5

Chapter 1. The Foundations

4. Nested Quantifiers
5. Rules of Inference

Nesting of Quantifiers

- Example:

Let the domain of *x* and *y* be people.

Let *L*(*x*,*y*) = "*x* likes *y*" (A statement with 2 free variables – not a proposition)

- Then ∃*y* *L*(*x*,*y*) = "There is someone whom *x* likes." (A statement with 1 free variable *x* – not a proposition)

- Then ∀*x* (∃*y* *L*(*x*,*y*)) =

"Everyone has someone whom they like." (A __with_____ Proposition riables.) 0

Nested Quantifiers

- Nested quantifiers are quantifiers that occur within the scope of other quantifiers.
- The order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.

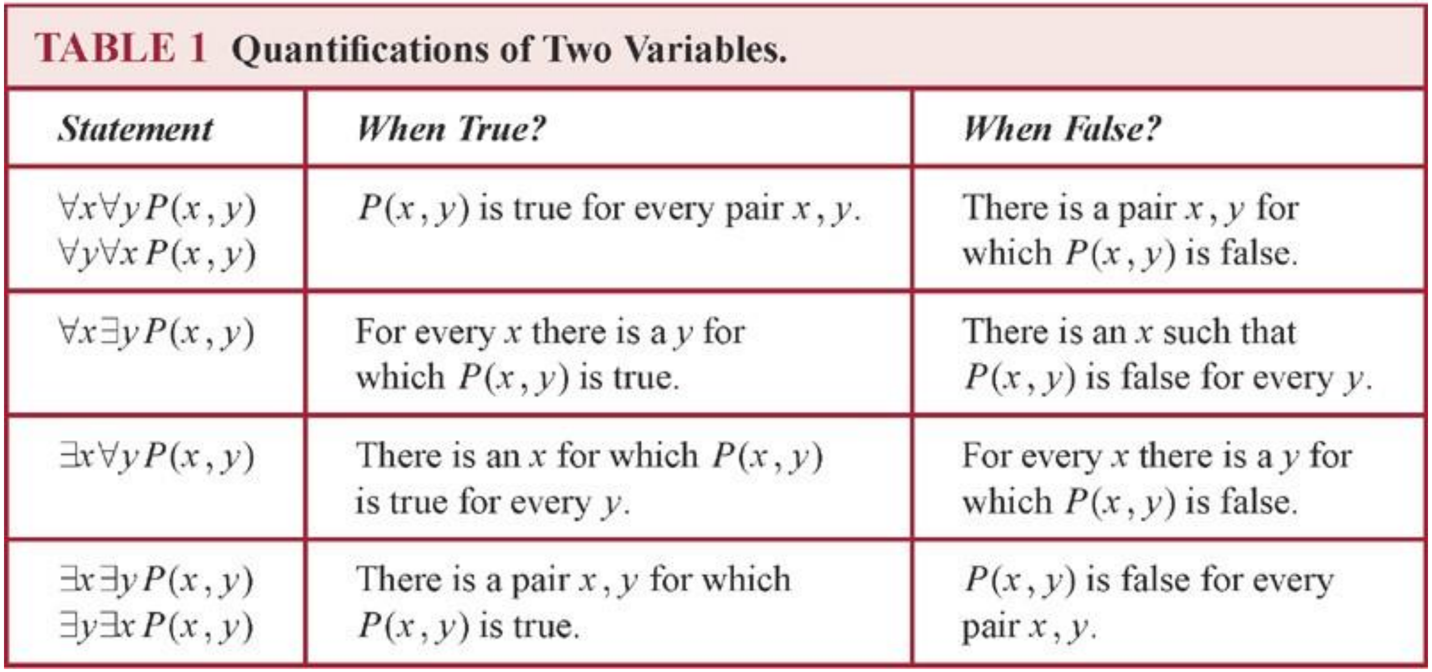


TABLE 1 **Quantifications of Two Variables.**

Statement	*When True?*	*When False?*
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Nested Quantifiers

- Let the domain of x and y is **R**, and $P(x,y)$: $xy = 0$. Find the truth value of the following propositions.
  - $\forall x \, \forall y \, P(x, y)$ (F)
  - $\forall x \, \exists y \, P(x, y)$ (T)
  - $\exists x \, \forall y \, P(x, y)$ (T)
  - $\exists x \, \exists y \, P(x, y)$ (T)

R: set of real numbers

- $\forall x \, \exists y \, P(x,y) \not\equiv \exists y \, \forall x \, P(x,y)$
  - For every x, there exists y such that $x + y = 0$. (T)
  - There exists y such that, for every x, $x + y = 0$. (F)

Nested Quantifiers: Example

- Let the domain = {1, 2, 3}. Find an expression equivalent to $\forall x\, \exists y\, P(x,y)$ where the variables are bound by substitution instead:
- Expand from inside out or outside in.
- Outside in:

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

$\equiv \exists y\, P(1,y) \land \exists y\, P(2,y) \land \exists y\, P(3,y)$

$\equiv [P(1,1) \lor P(1,2) \lor P(1,3)] \land$

$[P(2,1) \lor P(2,2) \lor P(2,3)] \land$

$[P(3,1) \lor P(3,2) \lor P(3,3)]$

Quantifier Exercise

- If $R(x,y)$=“x relies upon y,” express the following in unambiguous English when the domain is all people

$\forall x(\exists y\, R(x,y))$ = Everyone has *someone* to rely on.

$\exists y(\forall x\, R(x,y))$ = There’s a poor overburdened soul whom *everyone* relies upon (including himself)!

$\exists x(\forall y\, R(x,y))$ = There’s some needy person who relies upon *everybody* (including himself).

$\forall y(\exists x\, R(x,y))$ = Everyone has *someone* who relies upon them.

$\forall x(\forall y\, R(x,y))$ = *Everyone* relies upon *everybody*, (including themselves)!

Negating Nested Quantifiers

- Successively apply the rules for negating statements involving a single quantifier

  Example: Express the negation of the statement $\forall x\ \exists y\ (P(x,y) \wedge \exists z\ R(x,y,z))$ so that all negation symbols immediately precede predicates.

  $\neg\forall x\ \exists y\ (P(x,y) \wedge \exists z\ R(x,y,z))$

  $\equiv \exists x\ \neg\exists y\ (P(x,y) \wedge \exists z\ R(x,y,z))$

  $\equiv \exists x\ \forall y\ \neg(P(x,y) \wedge \exists z\ R(x,y,z))$

  $\equiv \exists x\ \forall y\ (\neg P(x,y) \vee \neg\exists z\ R(x,y,z))$

  $\equiv \exists x\ \forall y\ (\neg P(x,y) \vee \forall z\ \neg R(x,y,z))$

Equivalence Laws

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

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

- $\forall x\ \mathbf{(}P(x) \wedge Q(x)\mathbf{)} \equiv \mathbf{(}\forall x\ P(x)\mathbf{)} \wedge \mathbf{(}\forall x\ Q(x)\mathbf{)}$

  $\exists x\ \mathbf{(}P(x) \vee Q(x)\mathbf{)} \equiv \mathbf{(}\exists x\ P(x)\mathbf{)} \vee \mathbf{(}\exists x\ Q(x)\mathbf{)}$

Notational Conventions

- Quantifiers have higher precedence than all logical operators from propositional logic:

$$(\forall x\, P(x)) \wedge Q(x)$$

- Consecutive quantifiers of the same type can be combined:

$\forall x\ \forall y\ \forall z\ P(x,y,z) \equiv \forall x,y,z\ P(x,y,z)$ or even

$$\forall xyz\ P(x,y,z)$$

1.5 Rules of Inference

- ***An argument***: a sequence of statements that end with a conclusion
- Some forms of argument (“valid”) never lead from correct statements to an incorrect conclusion. Some other forms of argument (“fallacies”) can lead from true statements to an incorrect conclusion.
- ***A logical argument*** consists of a list of (possibly compound) propositions called premises/hypotheses and a single proposition called the conclusion.
- ***Logical rules of inference***: methods that depend on logic alone for deriving a new statement from a set of other statements. (Templates for constructing valid arguments.)

Valid Arguments (I)

- Example: A logical argument

If I dance all night, then I get tired. I danced all night.

Therefore I got tired.

- Logical representation of underlying variables:

p: I dance all night. q: I get tired.

- Logical analysis of argument:

$p \rightarrow q$ premise 1

$\underline{p\ \text{ premise 2}}$

$\therefore q$ conclusion

Valid Arguments (II)

- A form of logical argument is ***valid*** if whenever every premise is true, the conclusion is also true. A form of argument that is not valid is called a ***fallacy***.

Inference Rules: General Form

- An *Inference Rule* is
- A pattern establishing that if we know that a set of *premise* statements of certain forms are all true, then we can validly deduce that a certain related *conclusion* statement is true.

$$\begin{array}{l} \textit{premise } 1 \\ \textit{premise } 2 \\ \ldots \\ \hline \therefore \textit{ conclusion} \end{array}$$

"∴" means "therefore"

Inference Rules & Implications

- Each valid logical inference rule corresponds to an implication that is a tautology.

Inference rule

$$\begin{array}{l} \quad \textit{premise 1} \\ \quad \textit{premise 2} \\ \quad \ldots \\ \hline \therefore\ \textit{conclusion} \end{array}$$

- Corresponding tautology:

$$((\textit{premise 1}) \wedge (\textit{premise 2}) \wedge \cdots) \rightarrow \textit{conclusion}$$

Modus Ponens

- $$\begin{array}{l} \quad p \\ \quad p \rightarrow q \\ \hline \therefore\, q \end{array}$$

Rule of ***Modus ponens*** (a.k.a. *law of detachment*)

"the mode of affirming"

- $(p \wedge (p \rightarrow q)) \rightarrow q$ is a tautology

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge (p \rightarrow q)) \rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

- Notice that the first row is the only one where premises are all true

Modus Ponens: Example

If $p \rightarrow q$: “If it snows today then we will go skiing” assumed TRUE

p : “It is snowing today”

Then $\therefore q$: “We will go skiing” is TRUE

If $p \rightarrow q$: “If n is divisible by 3 then n^2 is divisible by 3” assumed TRUE

p : “n is divisible by 3”

Then $\therefore q$: “n^2 is divisible by 3” is TRUE

Modus Tollens

- $$\begin{array}{l} \neg q \\ \underline{p \rightarrow q} \\ \therefore \neg p \end{array}$$ Rule of ***Modus tollens***

"the mode of denying"

- $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ is a tautology

- Example

If $p \rightarrow q$: "If this jewel is really a diamond then it will scratch glass"

$\neg q$: "The jewel doesn't scratch glass"

assumed TRUE

Then $\therefore \neg p$: "The jewel is not a diamond" is TRUE

More Inference Rules

- $$\begin{array}{c} p \\ \hline \therefore p \lor q \end{array}$$

  Rule of ***Addition***

  Tautology: $p \to (p \lor q)$

- $$\begin{array}{c} p \land q \\ \hline \therefore p \end{array}$$

  Rule of ***Simplification***

  Tautology: $(p \land q) \to p$

- $$\begin{array}{c} p \\ q \\ \hline \therefore p \land q \end{array}$$

  Rule of ***Conjunction***

  Tautology: $[(p) \land (q)] \to p \land q$

Examples

- State which rule of inference is the basis of the following arguments:
  - It is below freezing now. Therefore, it is either below freezing or raining now.
  - It is below freezing and raining now. Therefore, it is below freezing now.
- p: It is below freezing now.

q: It is raining now.

  - $p \rightarrow (p \vee q)$ (rule of addition)
  - $(p \wedge q) \rightarrow p$ (rule of simplification)

Hypothetical Syllogism

- $$\boxed{\begin{array}{l} \quad p \rightarrow q \\ \quad q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}}$$

  Rule of ***Hypothetical syllogism***

  Tautology:

  $$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

- Example: State the rule of inference used in the argument:

  p *q*

  “If it rains today, then we will not have a barbecue today. *q* If we do not have a barbecue today, then we will have a barbecue tomorrow.*r* Therefore, if it rains today, then we will have barbecue tomorrow.” *p* *r*

Disjunctive Syllogism

- $$\boxed{\begin{array}{l} \quad p \lor q \\ \quad \neg p \\ \hline \therefore\ q \end{array}}$$

  Rule of ***Disjunctive syllogism***

  Tautology: $[(p \lor q) \land (\neg p)] \to q$

- Example
  - $\underbrace{\text{Ed’s wallet is in his back pocket}}_{p}$ or $\underbrace{\text{it is on his desk}}_{q}$. ($p \lor q$)
  - Ed’s wallet is not in his back pocket. ($\neg p$)
  - Therefore, Ed’s wallet is on his desk. (q)

Lecture 6

Chapter 1. The Foundations

1.5 Rules of Inference

Previously…

- Rules of inference
  - Modus ponens
  - Modus tollens
  - Hypothetical syllogism
  - Disjunctive syllogism
  - Resolution
  - Addition
  - Simplification
  - Conjunction

Table 1 in pp.66

Resolution

- $$\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

  Rule of ***Resolution***

  Tautology:

  $[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$

- When $q = r$:

  $[(p \vee q) \wedge (\neg p \vee q)] \rightarrow q$

- When $r =$ **F**:

  $[(p \vee q) \wedge (\neg p)] \rightarrow q$ (Disjunctive syllogism)

Resolution: Example

$$\boxed{\begin{array}{r} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}}$$

- Example: Use resolution to show that the hypotheses “$\underbrace{\textit{Jasmine is skiing}}_{r}$ *or* $\underbrace{\textit{it is not snowing}}_{\neg p}$” and “$\underbrace{\textit{It is snowing}}_{p}$ *or* $\underbrace{\textit{Bart is playing hockey}}_{q}$” imply that “$\underbrace{\textit{Jasmine is skiing}}_{r}$ *or* $\underbrace{\textit{Bart is playing hockey}}_{q}$”

$$(\boldsymbol{p} \vee \boldsymbol{q}) \wedge (\neg \boldsymbol{p} \vee \boldsymbol{r}) \rightarrow (\boldsymbol{q} \vee \boldsymbol{r})$$

Formal Proofs

- A formal proof of a conclusion *C*, given premises p_1, p_2, …, p_n consists of a sequence of *steps*, each of which applies some inference rule to premises or previously-proven statements to yield a new true statement (the *conclusion*).
- A proof demonstrates that *if* the premises are true, *then* the conclusion is true.

Formal Proof Example

- Suppose we have the following premises:
  “It is not sunny and it is cold.” “We will swim only if it is sunny.”
  “If we do not swim, then we will canoe.”
  “If we canoe, then we will be home by sunset.”

- Given these premises, prove the conclusion **“We will be home by sunset”** using inference rules.

Proof Example *cont.*

- Step 1: Identify the propositions (Let us adopt the following abbreviations)
- *sunny* = **"It is sunny"**; *cold* = **"It is cold"**; *swim* = **"We will swim"**; *canoe* = **"We will canoe"**; *sunset* = **"We will be home by sunset"**.
- Step 2: Identify the argument. (Build the argument form)

$$\begin{array}{l} \neg sunny \wedge cold \\ swim \rightarrow sunny \\ \neg swim \rightarrow canoe \\ canoe \rightarrow sunset \\ \hline \therefore\ sunset \end{array}$$

It is not sunny and it is cold.

We will swim only if it is sunny.

If we do not swim, then we will canoe.

If we canoe, then we will be home by sunset.

We will be home by sunset.

Proof Example *cont.*

- Step 3: Verify the reasoning using the rules of inference

$$\begin{array}{l} \neg sunny \land cold \\ swim \rightarrow sunny \\ \neg swim \rightarrow canoe \\ \underline{canoe \rightarrow sunset} \\ \therefore sunset \end{array}$$

Step	Proved by
1. $\neg sunny \land cold$	Premise #1.
2. $\neg sunny$	Simplification of 1.
3. $swim \rightarrow sunny$	Premise #2.
4. $\neg swim$	Modus tollens on 2 and 3.
5. $\neg swim \rightarrow canoe$	Premise #3.
6. $canoe$	Modus ponens on 4 and 5.
7. $canoe \rightarrow sunset$	Premise #4.
8. $sunset$	Modus ponens on 6 and 7.

Common Fallacies

- A ***fallacy*** is an inference rule or other proof method that is not logically valid.
- A fallacy may yield a false conclusion!
- *Fallacy of affirming the conclusion*:
- "$p \rightarrow q$ is true, and q is true, so p must be true." (No, because **F** → **T** is true.)
- Example
- If David Cameron (DC) is president of the US, then he is at least 40 years old. ($p \rightarrow q$)
- DC is at least 40 years old. (q)
- Therefore, DC is president of the US. (p)

Common Fallacies (*cont’d*)

- *Fallacy of denying the hypothesis*:
- “$p \rightarrow q$ is true, and p is false, so q must be false.” (No, again because **F** → **T** is true.)
- Example
- If a person does arithmetic well then his/her checkbook will balance. ($p \rightarrow q$)
- I cannot do arithmetic well. ($\neg p$)
- Therefore my checkbook does not balance. ($\neg q$)

Inference Rules for Quantifiers

- $$\frac{\forall x\, P(x)}{\therefore P(c)}$$ **Universal instantiation**

  (substitute *any* specific member *c* in the domain)

- $$\frac{P(c)}{\therefore \forall x\, P(x)}$$ (for an arbitrary element *c* of the domain)

  Universal generalization

- $$\frac{\exists x\, P(x)}{\therefore P(c)}$$ **Existential instantiation**

  (substitute an element *c* for which *P*(*c*) is true)

- $$\frac{P(c)}{\therefore \exists x\, P(x)}$$ (for some element *c* in the domain)

  Existential generalization

Example

- Every man has two legs. John Smith is a man. Therefore, John Smith has two legs.
- Proof
- Define the predicates:
- $M(x)$: x is a man
- $L(x)$: x has two legs
- J: John Smith, a member of the universe
- The argument becomes 1. $\forall x\ [M(x) \rightarrow L(x)]$

2. $M(J)$

$\therefore L(J)$

Example *cont.*

$\forall x\,(M(x) \rightarrow L(x))$
$M(J)$
$\therefore L(J)$

- The proof is

1. $\forall x\,[M(x) \rightarrow L(x)]$ *Premise 1*
2. $M(J) \rightarrow L(J)$ *U. I. from (1)*
3. $M(J)$ *Premise 2*
4. $L(J)$ *Modus Ponens from (2) and (3)*

- Note: Using the rules of inference requires lots of practice.
- Try example problems in the textbook.

Another example

- Correct or incorrect: “At least one of the 20 students in the class is intelligent. John is a student of this class. Therefore, John is intelligent.”
- First: Separate premises from conclusion
- *Premises*:

1. At least one of the 20 students in the class is intelligent.
2. John is a student of this class.

- *Conclusion*: John is intelligent.

Answer

- Next, translate the example in logic notation.
- *<u>Premise 1</u>*: At least one of the 20 students in the class is intelligent.

Let the domain = all people

C(*x*) = “*x* is in the class”

I(*x*) = “*x* is intelligent”

Then *Premise 1* says: **$\exists x(C(x) \wedge I(x))$**

- *<u>Premise 2</u>*: John is a student of this class.

Then *Premise 2* says: **C(John)**

- And the *Conclusion* says: ***I*(John)**

$$\boxed{\begin{array}{l} \exists x\,(C(x) \wedge I(x)) \\ C(John) \\ \hline \therefore\ I(John) \end{array}}$$

Answer (*cont'd*)

$$\begin{array}{l} \exists x\,(C(x) \land I(x)) \\ \underline{C(John)\qquad\qquad} \\ \therefore\ I(John) \end{array}$$

- No, the argument is invalid; we can disprove it with a counter-example, as follows:
- Consider a case where there is only one intelligent student A in the class, and A $\neq$ John.
- Then by existential instantiation of the premise **$\exists x\,(C(x) \land I(x))$, $C(\mathrm{A}) \land I(\mathrm{A})$** is true,
- But the conclusion ***I*(John)** is false, since A is the only intelligent student in the class, and John $\neq$ A.
- Therefore, the premises *do not* imply the conclusion.

More Proof Examples

- Is this argument correct or incorrect?
- “All TAs compose easy quizzes.
Mike is a TA.
Therefore, Mike composes easy quizzes.”

- First, separate the premises from conclusion:
  - *Premise 1*: All TAs compose easy quizzes.
- *Premise 2*: Mike is a TA.

- *Conclusion*: Mike composes easy quizzes.

Answer

- Next, re-render the example in logic notation.
  - *Premise 1*: All TAs compose easy quizzes.
    - Let the domain = all people
    - Let $T(x)$ = "x is a TA"
    - Let $E(x)$ = "x composes easy quizzes"
    - Then *Premise 1* says: $\forall x(T(x) \rightarrow E(x))$
  - *Premise 2*: Mike is a TA.
    - Let M = Mike
    - Then *Premise 2* says: $T(\mathrm{M})$
  - And the *Conclusion* says: $E(\mathrm{M})$

$$\boxed{\begin{array}{l} \forall x\,(T(x) \longrightarrow E(x)) \\ T(M) \\ \hline \therefore\ E(M) \end{array}}$$

The Proof in Gory Detail

- The argument is correct, because it can be reduced to a sequence of applications of valid inference rules, as follows:

$$\begin{array}{l} \forall x\,(T(x) \longrightarrow E(x)) \\ \underline{T(M)\qquad\qquad\qquad\qquad} \\ \therefore\ E(M) \end{array}$$

Statement	How obtained
1. $\forall x(T(x) \rightarrow E(x))$	**(Premise #1)**
2. $T(\mathrm{M}) \rightarrow E(\mathrm{M})$	**(Universal Instantiation)**
3. $T(\mathrm{M})$	**(Premise #2)**
4. $E(\mathrm{M})$	**(*Modus Ponens* from**

Another Example

- Prove that the sum of a rational number and an irrational number is always irrational.

- First, you have to understand exactly what the question is asking you to prove:
- “For all real numbers *x*,*y*,

if *x* is rational and *y* is irrational, then *x*+*y* is irrational.”

- $\forall x,y$: Rational(x) $\wedge$ Irrational(y) $\rightarrow$ Irrational($x+y$)

Answer

- Next, think back to the definitions of the terms used in the statement of the theorem:
- ∀ reals r : Rational(r) ↔

∃ Integer(i) ∧ Integer(j *with* ≠ 0): $r = i/j$.

- ∀ reals r : Irrational(r) ↔ ¬Rational(r)

- You almost always need the definitions of the terms in order to prove the theorem!

- Next, let's go through one valid proof:

What you might write

- **Theorem:** $\forall x,y : \text{Rational}(x) \wedge \text{Irrational}(y) \rightarrow \text{Irrational}(x+y)$
- **Proof:** Let x, y be any rational and irrational numbers, respectively. … (universal generalization)
- Now, just from this, what do we know about x and y? Think back to the definition of a rational number:
- … Since x is rational, we know (from the very definition of rational) that there must be some integers i and j such that $x = i/j$. So, let i_x, j_x be such integers …
- Notice that gave them the unique names i_x and j_x so we can refer to them later.

What next?

- What do we know about *y*? Only that *y* is irrational: ¬∃ integers *i*,*j*: *y* = *i*/*j*.
- But, it's difficult to see how to use a direct proof in this case. So let's try to use proof by contradiction.
- So, what are we trying to show?

Just that *x*+*y* is irrational. That is, ¬∃*i*,*j*: (*x* + *y*) = *i*/*j*.

- Now we need to hypothesize the negation of this statement!

More writing…

- Suppose that $x+y$ were not irrational. Then $x + y$ would be rational, so ∃ integers i,j: $x + y = i/j$. So, let i_s and j_s be any such integers where $x + y = i_s / j_s$.
- Now, with all these things named, we can see what happens when we put them together.
- So, we have that $(i_x/j_x) + y = (i_s/j_s)$.
- Notice: We have enough information now to conclude something useful about y, by solving this equation for it!

Finishing the Proof

- Solving that equation for *y*, we have:

$y = (i_s/j_s) - (i_x/j_x)$

$= (i_s j_x - i_x j_s)/(j_s j_x)$

- Now, since the numerator and denominator of this expression are both integers, *y* is rational (by definition of a rational number).
- This contradicts the assumption that *y* is irrational. Therefore, our hypothesis that *x*+*y* is rational must be false, and so the theorem is proved.

Example of a Wrong Answer

- 1 is rational. √2 is irrational. 1+√2 is irrational. Therefore, the sum of a rational number and an irrational number is irrational.

(Attempting a direct proof.)

- Why does this answer deserve no credit?
- We attempted to use an example to prove a universal statement.

This is always invalid!

- Even as an example, it's incomplete, because we never even proved that 1+√2 is irrational!

Proof Terminology

- A ***proof*** is a valid argument that establishes the truth of a mathematical statement
- ***Axiom*** (or ***postulate***): a statement that is assumed to be true
- ***Theorem***
  - A statement that has been proven to be true
- ***Hypothesis***, ***premise***
  - An assumption (often unproven) defining the structures about which we are reasoning

More Proof Terminology

- ***Lemma***
  - A minor theorem used as a stepping-stone to proving a major theorem.
- ***Corollary***
  - A minor theorem proved as an easy consequence of a major theorem.
- ***Conjecture***
  - A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)

Proof Methods

- For proving a statement *p* alone
    - ***Proof by Contradiction*** (indirect proof): Assume $\neg p$, and prove $\neg p \rightarrow \mathbf{F}$.

Proof Methods

- For proving implications $p \rightarrow q$, we have:
  - ***Trivial* proof:** Prove q by itself.
  - ***Direct* proof:** Assume p is true, and prove q.
  - ***Indirect* proof:**
    - ***Proof by Contraposition*** $(\neg q \rightarrow \neg p)$: Assume $\neg q$, and prove $\neg p$.
    - ***Proof by Contradiction***: Assume $p \wedge \neg q$, and show this leads to a contradiction. (i.e. prove $(p \wedge \neg q) \rightarrow$ **F)**
  - ***Vacuous* proof:** Prove $\neg p$ by itself.

Direct Proof Example

- **Definition:** An integer n is called *odd* iff $n=2k+1$ for some integer k; n is *even* iff $n=2k$ for some k.
- **Theorem:** Every integer is either odd or even, but not both.
  - This can be proven from even simpler axioms.
- **Theorem:**

  (For all integers n) If n is odd, then n^2 is odd.

  Proof:

  If n is odd, then $n = 2k + 1$ for some integer k.

  Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

  Therefore n^2 is of the form $2j + 1$ (with j the integer $2k^2 + 2k$), thus n^2 is odd. ■

Indirect Proof Example: Proof by Contraposition

- **Theorem:** (For all integers n)
  If $3n + 2$ is odd, then n is odd.
- **Proof:**

(Contrapositive: If n is even, then $3n + 2$ is even)

Suppose that the conclusion is false, *i.e.*, that n is even.

Then $n = 2k$ for some integer k.

Then $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$. So $3n + 2$ is not odd.

We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n + 2 \text{ is odd})$, thus its contrapositive $(3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. ■

Vacuous Proof Example

- Show $\neg p$ (i.e. p is false) to prove $p \to q$ is true.

- **Theorem:** (For all *n*) If *n* is both odd and even, then $n^2 = n + n$.
- **Proof:**

  The statement "*n* is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. ■

Trivial Proof Example

- Show *q* (i.e. *q* is true) to prove $p \rightarrow q$ is true.

- **Theorem:** (For integers *n*) If *n* is the sum of two prime numbers, then either *n* is odd or *n* is even.
- **Proof:**

  Any integer *n* is either odd or even. So the conclusion of the implication is true regardless of the truth of the hypothesis. Thus the implication is true trivially. ■

Proof by Contradiction

- A method for proving *p*.
  - Assume $\neg p$, and prove both *q* and $\neg q$ for some proposition *q*. (Can be anything!)
  - Thus $\neg p \rightarrow (q \wedge \neg q)$
  - $(q \wedge \neg q)$ is a trivial contradiction, equal to **F**
  - Thus $\neg p \rightarrow$ **F**, which is only true if $\neg p =$ **F**
  - Thus *p* is true

Rational Number

- Definition:

  The real number r is *rational* if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called *irrational*.

Proof by Contradiction Example

- **Theorem:** $\sqrt{2}$ is irrational.
  - **Proof:**
  - Assume that $\sqrt{2}$ is rational. This means there are integers x and y ($y \neq 0$) with no common divisors such that $\sqrt{2} = x/y$.

    Squaring both sides, $2 = x^2/y^2$, so $2y^2 = x^2$. So x^2 is even; thus x is even (see earlier).

    Let $x = 2k$. So $2y^2 = (2k)^2 = 4k^2$. Dividing both sides by 2, $y^2 = 2k^2$. Thus y^2 is even, so y is even.

    But then x and y have a common divisor, namely 2, so we have a contradiction.

    Therefore, $\sqrt{2}$ is irrational. ■

Proof by Contradiction

- Proving implication $p \rightarrow q$ by contradiction
  - Assume $\neg q$, and use the premise p to arrive at a contradiction, i.e. $(\neg q \wedge p) \rightarrow \mathbf{F}$ $(p \rightarrow q \equiv (\neg q \wedge p) \rightarrow \mathbf{F})$
  - How does this relate to the proof by contraposition?
  - ***Proof by Contraposition*** $(\neg q \rightarrow \neg p)$: Assume $\neg q$, and prove $\neg p$.

Proof by Contradiction Example: Implication

- **Theorem:** (For all integers n)

  If $3n + 2$ is odd, then n is odd.

- **Proof:**

  Assume that the conclusion is false, *i.e.*, that n is even, and that $3n + 2$ is odd.

  Then $n = 2k$ for some integer k and $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$.

  This contradicts the assumption "$3n + 2$ is odd".

  This completes the proof by contradiction, proving that if $3n + 2$ is odd, then n is odd. ■

Circular Reasoning

- The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof. Example:
- Prove that an integer *n* is even, if n^2 is even.
- **Attempted proof:**

Assume n^2 is even. Then $n^2 = 2k$ for some integer *k*.

Dividing both sides by *n* gives $n = (2k)/n = 2(k/n)$.

So there is an integer *j* (namely *k*/*n*) such that $n = 2j$. Therefore *n* is even.

- Circular reasoning is used in this proof. Where?

*Begs the question: How do you show that $j = k/n = n/2$ is an integer, without **first** assumig that n is even?*

Lecture 8

Chapter 2. Basic Structures

1. Sets
2. Set Operations

2.1 Sets

- A ***set*** is a new type of structure, representing an ***unordered*** collection (group) of zero or more ***distinct*** (different) objects. The objects are called ***elements*** or ***members*** of the set.
- Notation: $x \in S$
- Set theory deals with operations between, relations among, and statements about sets.
- Sets are ubiquitous in computer software systems.
- (E.g. data types `Set`, `HashSet` in `java.util`)

Basic Notations for Sets

- For sets, we'll use variables *S*, *T*, *U*,…
- We can denote a set *S* in writing by listing all of its elements in curly braces:
  - {*a*,*b*,*c*} is the set whose elements are *a*, *b*, and *c*
- ***Set builder notation***:
  - For any statement *P*(*x*) over any domain,

{*x* | *P*(*x*)} is *the set of all x such that P*(*x*) is true

- Example: {1, 2, 3, 4}

$= \{x \mid x$ is an integer where $x > 0$ and $x < 5\}$

$= \{x \in \mathbf{Z} \mid x > 0$ and $x < 5\}$

Basic Properties of Sets

- Sets are inherently ***unordered***:
  - No matter what objects a, b, and c denote, $\{a, b, c\} = \{a, c, b\} = \{b, a, c\} = \{b, c, a\} = \{c, a, b\} = \{c, b, a\}$.
- All elements are ***distinct*** (unequal); multiple listings make no difference!
  - If $a = b$, then $\{a, b, c\} = \{a, c\} = \{b, c\} = \{a, a, b, a, b, c, c, c, c\}$.
  - This set contains (at most) 2 elements!

Definition of Set Equality

- Two sets are declared to be equal *if and only if* they contain exactly the same elements.
- In particular, it does not matter *how the set is defined or denoted.*
- Example:

The set $\{1, 2, 3, 4\}$

$= \{x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5\}$

$= \{x \mid x \text{ is a positive integer where } x^2 < 20\}$

Infinite Sets

- Conceptually, sets may be *infinite* (*i.e.*, not *finite*, without end, unending).
- Symbols for some special infinite sets:

N = {0, 1, 2,…} the set of **N**atural numbers.

Z = {…, –2, –1, 0, 1, 2,…} the set of **Z**ntegers. **Z**$^+$ = {1, 2, 3,…} the set of positive integers.

Q = {*p*/*q* | *p*,*q* ∈ **Z**, and *q* ≠ 0}

the set of Rational numbers.

R = the set of "**R**eal" numbers.

- "Blackboard Bold" or double-struck font is also often used for these special number sets.

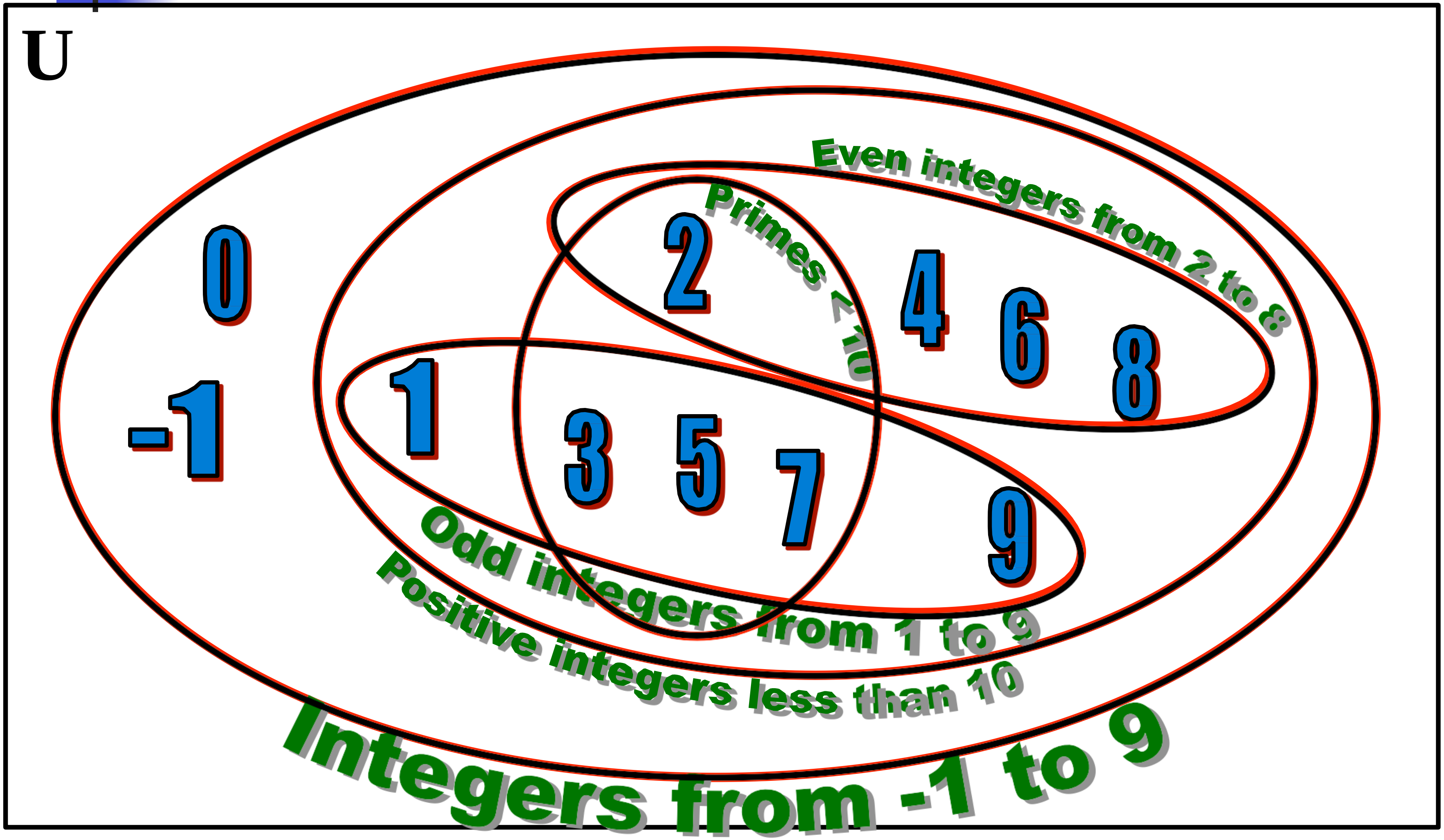
Basic Set Relations

- $x \in S$ ("x is in S") is the proposition that object x is an $\in$*lement* or *member* of set S.
  - *e.g.* $3 \in \mathbf{N}$, $a \in \{x \mid x \text{ is a letter of the alphabet}\}$
  - Can define set equality in terms of $\in$ relation: $\forall S,T{:}\ S = T \leftrightarrow [\forall x\,(x \in S \leftrightarrow x \in T)]$ "Two sets are equal iff they have all the same members."
- $x \notin S \equiv \neg(x \in S)$ "x is not in S"

The Empty Set

- $\varnothing$ (“null”, “the empty set”) is the unique set that contains no elements whatsoever.
- $\varnothing = \{\ \} = \{x \mid \textbf{False}\}$
- No matter the domain of discourse, we have the axiom $\neg\exists x\colon x \in \varnothing$.
- $\{\ \} \neq \{\varnothing\} = \{\ \{\ \}\ \}$
- $\{\varnothing\}$ it isn’t empty because it has $\varnothing$ as a member!

Venn Diagrams



Subset and Superset

- $S \subseteq T$ (“S is a subset of T”) means that every element of S is also an element of T.
- $S \subseteq T \equiv \forall x\,(x \in S \rightarrow x \in T)$
- $\varnothing \subseteq S$, $S \subseteq S$
- $S \subseteq T$ (“S is a superset of T”) means $T \subseteq S$
- Note $(S = T) \equiv (S \subseteq T \land S \subseteq T)$

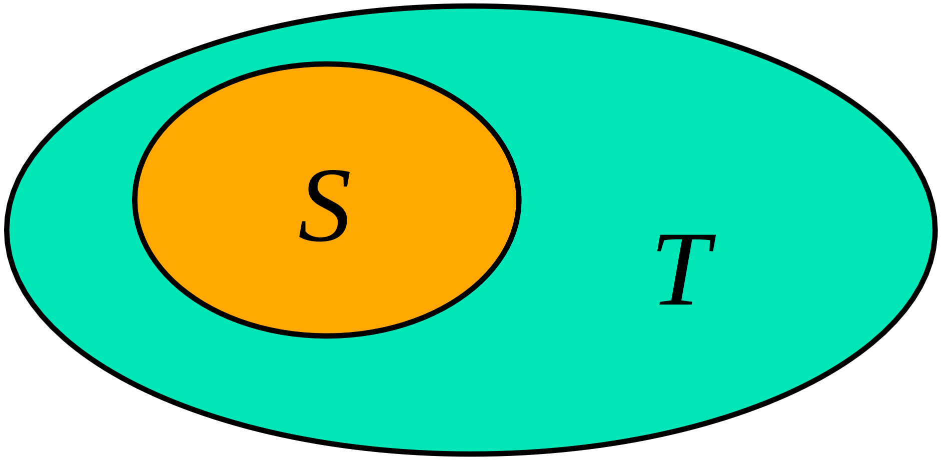
$\equiv \forall x(x \in S \rightarrow x \in T) \land \forall x(x \in T \rightarrow x \in S)$

$\equiv \forall x(x \in S \leftrightarrow x \in T)$

- $S \not\subseteq T$ means $\neg(S \subseteq T)$, *i.e.* $\exists x(x \in S \land x \notin T)$

Proper (Strict) Subsets & Supersets

- $S \subset T$ ("*S* is a proper subset of *T*") means that $S \subseteq T$ but $T \nsubseteq S$. Similar for $S \supset T$.
- Example:
  {1, 2} ⊂ {1, 2, 3}



Venn Diagram of $S \subset T$

Sets Are Objects, Too!

- The objects that are elements of a set may *themselves* be sets.
- Example:

Let $S = \{x \mid x \subseteq \{1, 2, 3\}\}$ then $S = \{ \emptyset,$
$\{1\}, \{2\}, \{3\},$
$\{1, 2\}, \{1, 3\}, \{2, 3\},$
$\{1, 2, 3\} \}$

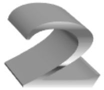
- Note that $1 \neq \{1\} \neq \{\{1\}\}$!!!!

Very Important!

Cardinality and Finiteness

- $|S|$ (read "the *cardinality of S*") is a measure of how many different elements S has.

- *E.g.*, $|\varnothing| = 0$, $|\{1, 2, 3\}| = 3$, $|\{a, b\}| = 2$,



$$|\{\{1, 2, 3\}, \{4, 5\}\}| = \_$$

  - If $|S| \in \mathbf{N}$, then we say S is *finite*. Otherwise, we say S is *infinite*.

- What are some infinite sets we've seen?

N, Z, Q, R

The *Power Set* Operation

- The ***power set*** $P(S)$ of a set S is the set of all subsets of S. $P(S) = \{x \mid x \subseteq S\}$.
- Examples
- $P(\{a, b\}) = \{ \emptyset, \{a\}, \{b\}, \{a, b\} \}$
- $S = \{0, 1, 2\}$

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

- $P(\emptyset) = \{\emptyset\}$
- $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

- Note that for finite S, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S\ (|P(S)| > |S|)$, *e.g.* $|P(\mathbf{N})| > |\mathbf{N}|$.

Ordered *n*-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbf{N}$, an *ordered n-tuple* or a *sequence* or *list of length n* is written $(a_1, a_2, \ldots, a_n)$. Its *first* element is a_1, its second element is a_2, *etc.*
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.

Contrast with sets' {}

- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, *n*-tuples.

Cartesian Products of Sets

- For sets A and B, their ***Cartesian product*** denoted by $\boldsymbol{A \times B}$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in$ B. Hence,

$$A \times B = \{ (a, b) \mid a \in A \wedge b \in B \}.$$

- $E.g.$ $\{a, b\} \times \{1, 2\}$

$$= \{ (a, 1), (a, 2), (b, 1), (b, 2) \}$$

  - Note that for finite A, B, $|A \times B| = |A||B|$.

- Note that the Cartesian product is ***not*** commutative: *i.e.*, $\neg\forall A,B\ (A \times B = B \times A)$.

- Extends to $A_1 \times A_2 \times \ldots \times A_n$

$$= \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$$

The Union Operator

- For sets A and B, their ***union*** $A \cup B$ is the set containing all elements that are either in A, **or** (“$\vee$”) in B (or, of course, in both).

- Formally, $\forall A,B$: $A \cup B = \{x \mid x \in A \vee x \in B\}$.

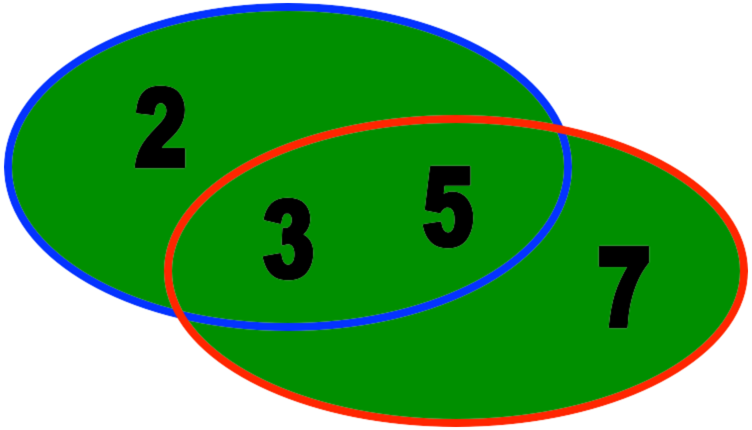
- Note that $A \cup B$ is a **superset** of both A and B (in fact, it is the smallest such superset):
$\forall A,B$: $(A \cup B \subseteq A) \wedge (A \cup B \subseteq B)$

Union Examples

- $\{a, b, c\} \cup \{2, 3\} = \{a, b, c, 2, 3\}$
- $\{2, 3, 5\} \cup \{3, 5, 7\} = \{2, 3, 5, 3, 5, 7\}$

  $= \{2, 3, 5, 7\}$

Required Form



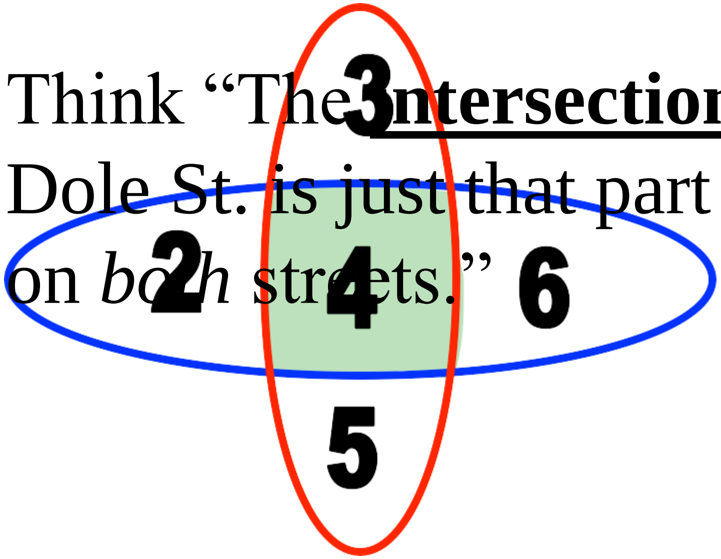
The Intersection Operator

- For sets A and B, their ***intersection*** $A \cap B$ is the set containing all elements that are simultaneously in A **and** ("$\wedge$") in B.
  - Formally, $\forall A,B: A \cap B = \{x \mid x \in A \wedge x \in B\}$.
- Note that $A \cap B$ is a **subset** of both A and B (in fact it is the largest such subset):

$$\forall A,B: (A \cap B \subseteq A) \wedge (A \cap B \subseteq B)$$

Intersection Examples

- $\{a, b, c\} \cap \{2, 3\} = \underline{\ \varnothing\ }$
- $\{2, 4, 6\} \cap \{3, 4, 5\} = \underline{\ \{4\}\ }$



Think "The **Intersection** of University Ave. and Dole St. is just that part of the road surface that lies on *both* streets."

Disjointedness

- Two sets *A*, *B* are called ***disjoint*** (*i.e.*, unjoined) iff their intersection is empty. ($A \cap B = \varnothing$)

- Example: the set of even integers is disjoint with the set of odd integers.

Inclusion-Exclusion Principle

Un

- How many elements are in $A \cup B$?

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

- Example: How many students in the class major in Computer Science or Mathematics?

- Consider set $E = C \cup M$,

$C = \{s \mid s$ is a Computer Science major$\}$

$M = \{s \mid s$ is a Mathematics major$\}$

- Some students are joint majors!

$|E| = |C \cup M| = |C| + |M| - |C \cap M|$

Inclusion-Exclusion Principle

- How many elements are in $A \cup B$?

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

- Example: How many students in the class major in Computer Science or Mathematics?

- Consider set $E = C \cup M$,

$C = \{s \mid s$ is a Computer Science major$\}$

$M = \{s \mid s$ is a Mathematics major$\}$

- Some students are joint majors!

$|E| = |C \cup M| = |C| + |M| - |C \cap M|$

Set Difference

- For sets *A* and *B*, the ***difference of A and B***, written *A* - *B*, is the set of all elements that are in *A* but not *B*.

- Formally:

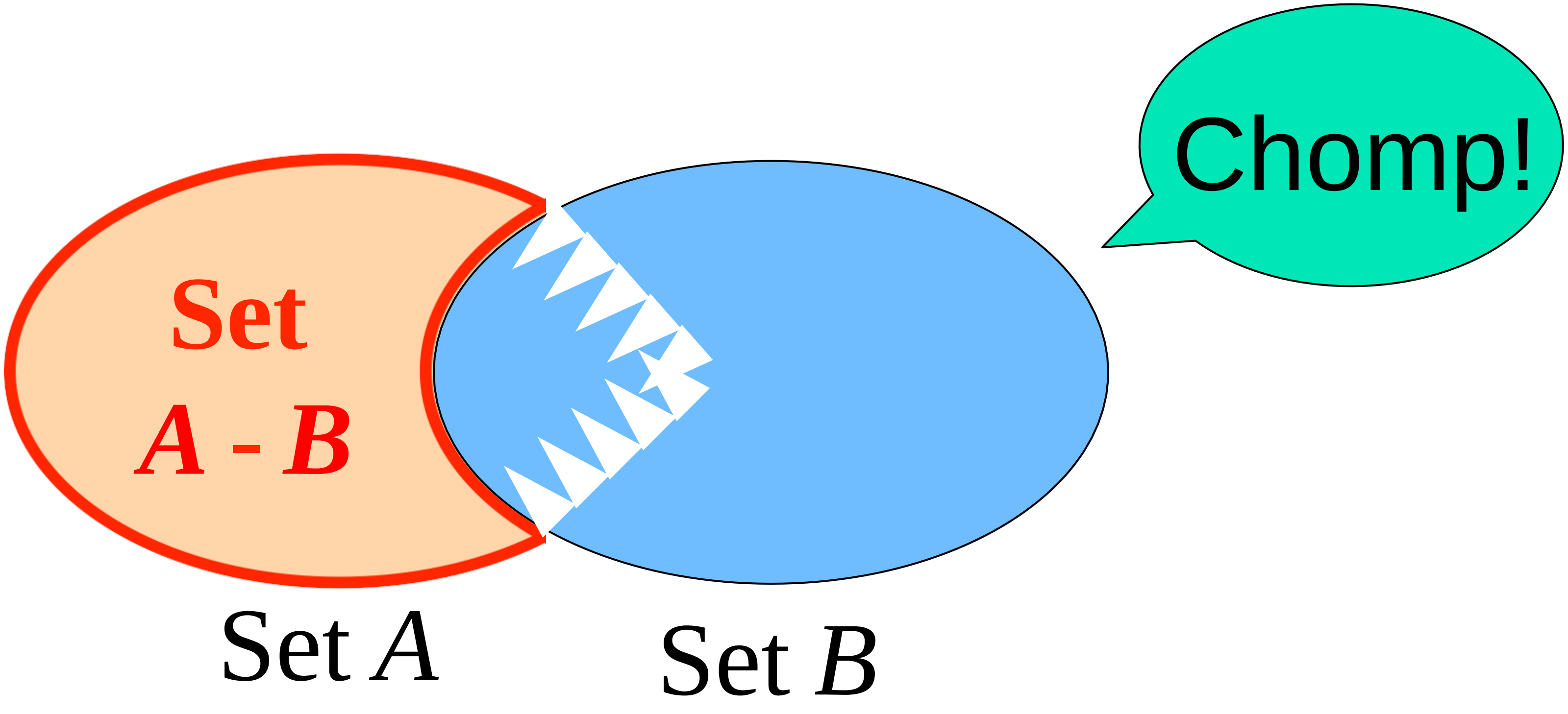
$$A - B = \{x \mid x \in A \wedge x \notin B\}$$
$$= \{x \mid \neg(x \in A \rightarrow x \in B)\}$$

- Also called:

The ***complement of B with respect to A***.

Set Difference: Venn Diagram

- *A* − *B*
is what's left after *B* "takes a bite out of *A*"



Set Difference Examples

- $\{1, \cancel{2}, \cancel{3}, 4, \cancel{5}, 6\} - \{2, 3, 5, 7, 9, 11\} =$

  $\underline{\{1, 4, 6\}}$

- **Z** - **N** = {… , −1, 0, 1, 2, … } - {0, 1, … }

  = {*x* | *x* is an integer but not a natural #}

  = {… , −3, −2, −1}

  = {*x* | *x* is a negative integer}

Set Complements

- The *universe of discourse* (or the *domain*) can itself be considered a set, call it *U*.

- When the context clearly defines *U*, we say that for any set $A \subseteq U$, the ***complement*** of *A*, written as $\overline{A}$, is the complement of *A* with respect to *U*, *i.e.*, it is *U* - *A.*

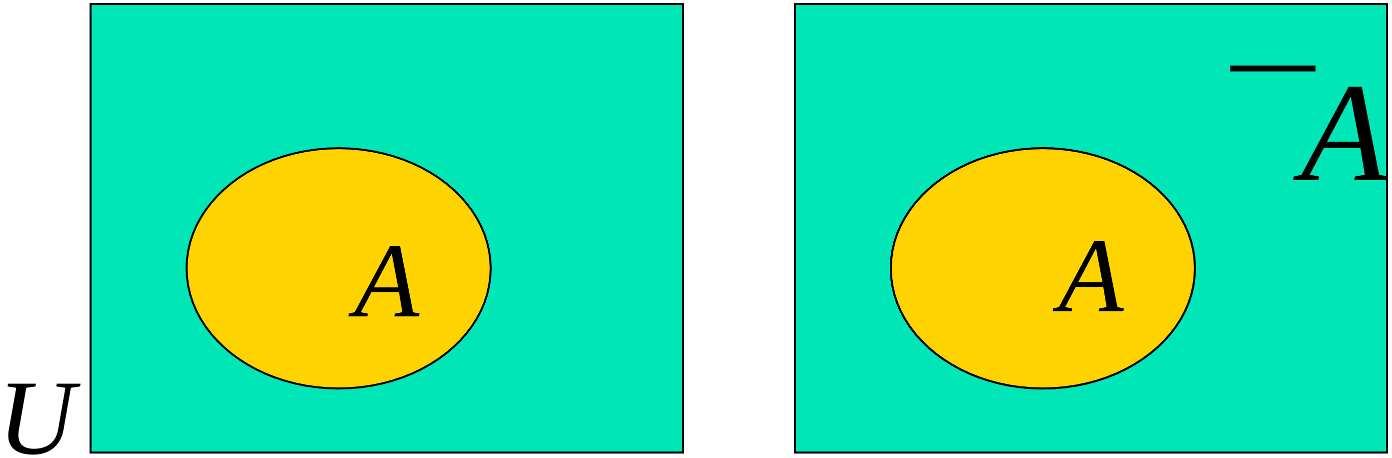
- *E.g.*, If *U* = **N**,

$$\overline{\{3, 5\}} = \{0,1, 2, 4, 6, 7,...\}$$

More on Set Complements

- An equivalent definition, when *U* is obvious:

$$\overline{A} = \{x \mid x \notin A\}$$



Interval Notation

- $a, b \in \mathbf{R}$, and $a < b$ then
  - $(a, b) = \{x \in \mathbf{R} \mid a < x < b\}$
  - $[a, b] = \{x \in \mathbf{R} \mid a \le x \le b\}$
  - $(a, b] = \{x \in \mathbf{R} \mid a < x \le b\}$
  - $(-\infty, b] = \{x \in \mathbf{R} \mid x \le b\}$
  - $[a, \infty) = \{x \in \mathbf{R} \mid a \le x\}$
  - $(a, \infty) = \{x \in \mathbf{R} \mid a < x\}$