Quantifiers, Proofs and Sets

CS 2800: Discrete Structures, Spring 2015

Sid Chaudhuri

Negating Quantified Statements

- It is **not** the case that **every** x **has** property $F(x)$ $\Leftrightarrow$ there is **some** x **without** property $F(x)$

$$\neg(\forall x, F(x)) \Leftrightarrow \exists x, \neg F(x)$$

- It is **not** the case that there is **some** x **with** property $F(x)$ $\Leftrightarrow$ **every** x **lacks** property $F(x)$

$$\neg(\exists x, F(x)) \Leftrightarrow \forall x, \neg F(x)$$

- *"Flip leftmost quantifier, move negation one step rightwards"*

Examples

- Negation of $\forall x, \neg F(x)$

$$\neg(\forall x, \neg F(x))$$
$$\Leftrightarrow \exists x, \neg\neg F(x)$$
$$\Leftrightarrow \exists x, F(x)$$

  - Double negative $\Leftrightarrow$ positive:

    "It is not the case that everyone lacks empathy"
    $\Leftrightarrow$ "Someone has empathy"

"Flip leftmost quantifier, move negation one step rightwards"

Examples

- Negation of $\forall x, \forall y, F(x, y)$

$$\neg(\forall x, \forall y, F(x, y))$$

$$\Leftrightarrow \exists x, \neg(\forall y, F(x, y))$$

$$\Leftrightarrow \exists x, \exists y, \neg F(x, y)$$

  – "It is not the case that every two people are friends"
    $\Leftrightarrow$ "Some two people aren't friends"

"Flip leftmost quantifier, move negation one step rightwards"

Negating Quantified Statements

$$\neg(\forall x, F(x)) \Leftrightarrow \exists x, \neg F(x)$$

$$\neg(\exists x, F(x)) \Leftrightarrow \forall x, \neg F(x)$$

"Flip leftmost quantifier, move negation one step rightwards"

Space for boardwork

Common Types of Proofs

- Direct proof
  - Start with something known to be true
  - Repeatedly derive a statement that is implied by the previous one(s), until arriving at the conclusion
  - Application of *modus ponens*: $P, P \Rightarrow Q \models Q$
- *Proof* that if m, n are perfect squares, so is mn:
  - Since m and n are perfect squares, $m = k^2$, $n = l^2$, for some integers k and l
  - Hence $mn = k^2 l^2 = (kl)^2$
  - Since kl is an integer, mn is a perfect square

Common Types of Proofs

- Proof by contradiction
  - Assume the statement to be proved is *false*
  - Show that it implies an absurd or contradictory conclusion
  - Hence the initial statement must be true
  - Application of *modus tollens*: $P \Rightarrow Q, \neg Q \models \neg P$
- *Proof* that there is no greatest integer:
  - Assume that there is in fact a greatest integer n
  - But $n + 1$ is an integer which is greater than n
  - This is a contradiction, so there cannot be a greatest integer

Common Types of Proofs

- Disproof by counterexample
  - Statement *must be* of the form "Every x satisfies $F(x)$"
  - Disprove it by finding some x that does *not* satisfy $F(x)$
  - Application of *quantifier negation*: $\neg(\forall x, F(x)) \Leftrightarrow \exists x, \neg F(x)$
- *Disproof* that for all reals a, b, if $a^2 = b^2$ then $a = b$
  - Let $a = 1$, $b = -1$, which are real numbers
  - Then $a^2 = b^2 = 1$, but $a \neq b$
  - Hence the statement is false

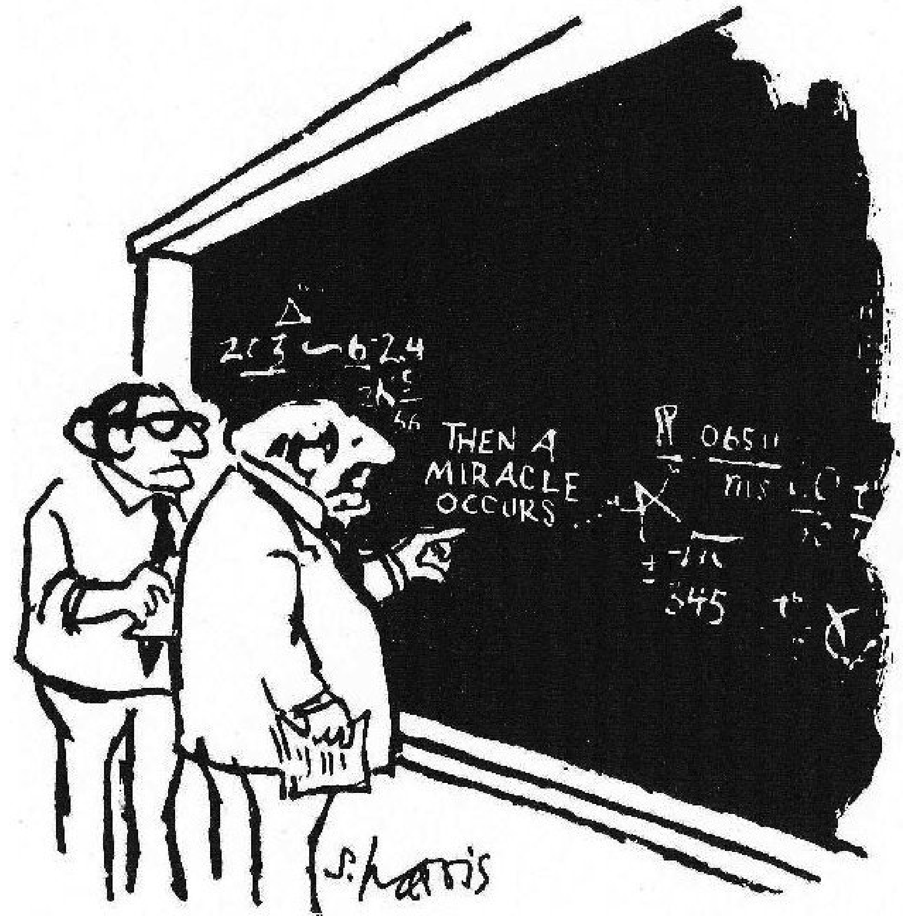
It's not enough to just state the counterexample, you should explain why it is a counterexample as well!

Thought for the Day #1

The different types of proofs are strongly related, indeed they're all variants of the same rule of logical inference. Can you figure out how, for example, disproof by counterexample is nothing but a version of proof by contradiction?

How much detail is enough?

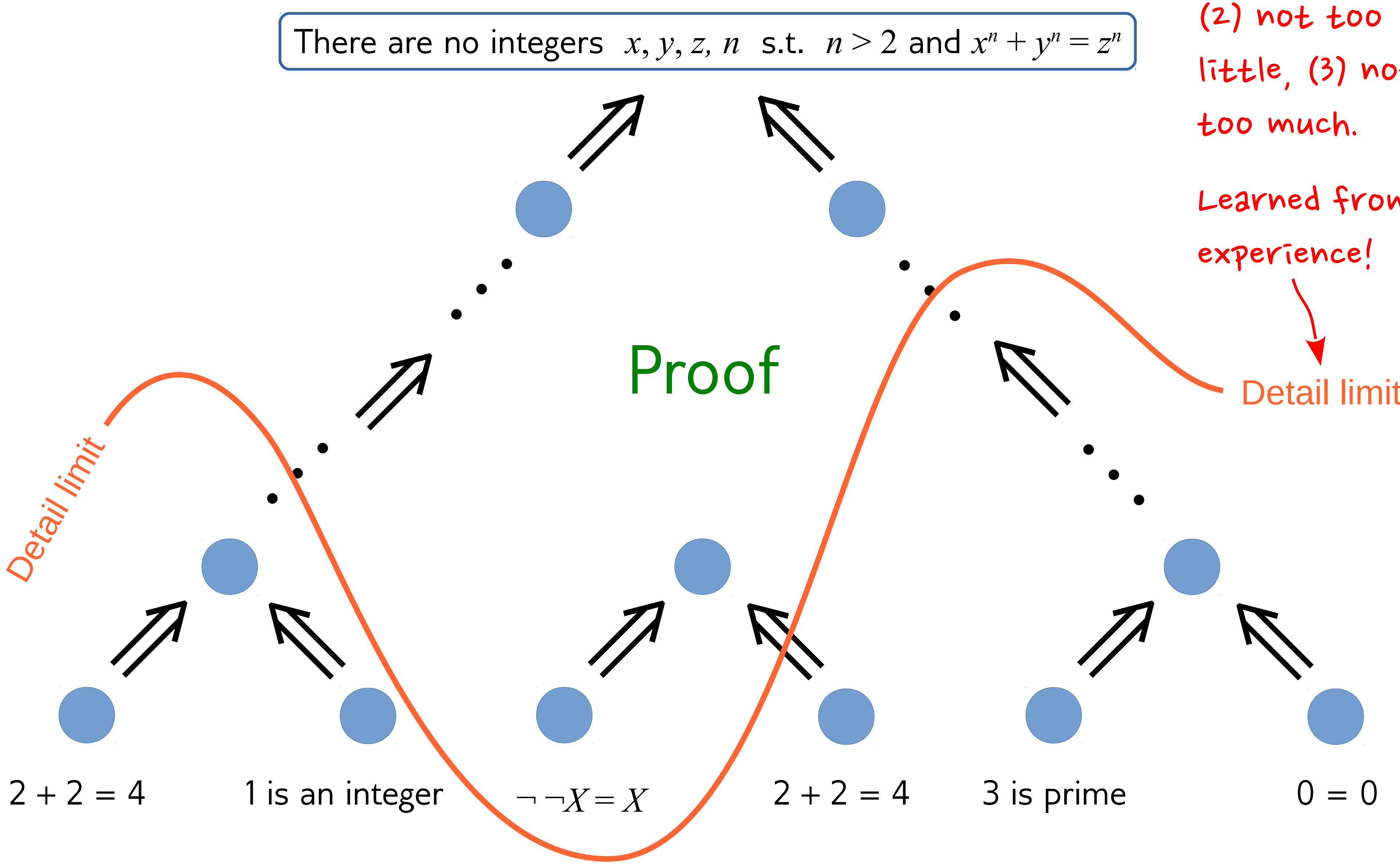
- Know your audience
- Too little detail leaves the reader skeptical that your steps actually check out
- Too much detail overwhelms the reader, who can no longer follow your argument



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Sidney Harris

Hierarchy of Detail



Determined from 3 criteria: (1) audience, (2) not too little, (3) not too much.

Learned from experience!

Set Theory

- Set S: unordered collection of elements

Set Theory

The empty/null set contains zero elements and is denoted { } or $\varnothing$

- Set S: unordered collection of elements

Set Theory

The <u>empty/null set</u> contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. $S = \{$ a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z $\}$

  $V = \{$ a, e, i, o, u $\}$

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. $S = \{$ a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z $\}$

  $V = \{$ a, e, i, o, u $\}$

  or $V = \{\, x \mid x \in S$ and x is a vowel $\}$

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. $S = \{$ a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z $\}$

$V = \{$ a, e, i, o, u $\}$

or $V = \{\ x \mid x \in S$ and x is a vowel $\}$

The set of

Set Theory

The empty/null set contains zero elements and is denoted { } or $\varnothing$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. $S = \{$ a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z $\}$

$V = \{$ a, e, i, o, u $\}$

or $V = \{\, x \mid x \in S$ and x is a vowel $\}$

The set of

all x's

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. $S = \{$ a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z $\}$

$$V = \{ \text{a, e, i, o, u} \}$$

or $V = \{ x \mid x \in S \text{ and } x \text{ is a vowel} \}$

The set of — all x's — **such that**

Set Theory

The empty/null set contains zero elements and is denoted { } or $\varnothing$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. S = { a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z }

V = { a, e, i, o, u }

or $V = \{ x \mid x \in S$ and x is a vowel $\}$

The set of — all x's — such that — **x is an element of S**

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. S = { a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z }

V = { a, e, i, o, u }

or $V = \{ x \mid x \in S$ and x is a vowel $\}$

The set of — all x's — such that — x is an element of S — **and**

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. S = { a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z }

V = { a, e, i, o, u }

or $V = \{ x \mid x \in S$ and x is a vowel $\}$

The set of — all x's — such that — x is an element of S — and — **x is a vowel**

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. S = { a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z }

V = { a, e, i, o, u }

or $V = \{ x \mid x \in S$ and x is a vowel $\}$

or $V = \{ x \in S \mid x$ is a vowel $\}$

Set Theory

The empty/null set contains zero elements and is denoted { } or $\emptyset$

- Set S: unordered collection of elements
- Subset of set S: set of zero, some or all elements of S (we'll give a slightly more formal definition soon)
- E. g. $S = \{$ a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z $\}$

  $V = \{$ a, e, i, o, u $\}$

  or $V = \{ x \mid x \in S$ and x is a vowel $\}$

  or $V = \{ x \in S \mid x$ is a vowel $\}$
- V is a subset of S, or $V \subseteq S$

Building New Sets from Old Ones

- $A \cup B$ (read 'A *union* B') consists of all elements in A or in B (or both!)
- $A \cap B$ (read 'A *intersection* B') consists of all elements in both A and B
- $A \setminus B$ (read 'A *minus* B') consists of all elements in A but not in B
- A' (read 'A *complement*') consists of all elements not in A (that is, $\mathbb{U} \setminus A$, where $\mathbb{U}$ is a suitably chosen "universal set")

Set Relations

- Set A is a subset of set B if and only if every element of A is also present in B (definition)
  - B is a superset of A
- Sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$ (definition)
  - Formally, proving two sets to be equal requires showing containment in *both* directions, but we will often use standard results as shortcuts, e.g. $X \setminus Y = X \cap Y'$ or $X \cap X' = \varnothing$

Exercise: prove these results from the definitions above