CS2209A 2017

Applied Logic for Computer Science

Lecture 11, 12

Logic and Proof

Instructor: Yu Zhen Xie

Proofs

- What is a theorem?
  - Lemma, claim, etc
- What is a proof?
  - Where do we start?
  - Where do we stop?
  - What steps do we take?
  - How much detail is needed?

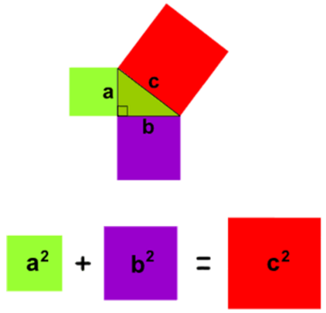
The truth

Theories and theorems

- **Theory:** axioms + everything derived from them using rules of inference
  - Euclidean geometry, set theory, theory of reals, theory of integers, Boolean algebra…
  - In verification: theory of arrays.

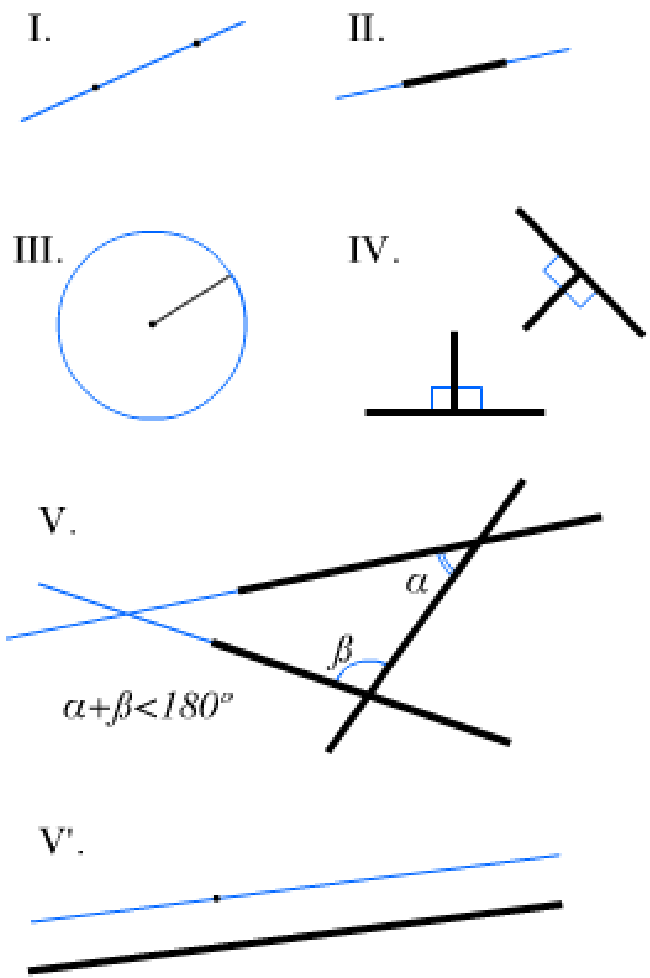
- **Theorem:** a **true statement** in a theory
  - Proved from axioms (usually, from already proven theorems)

- A statement can be a theorem in one theory and false in another!
  - Between any two numbers there is another number.
    - A theorem for real numbers. False for integers!



Pythagorean theorem

Axioms example: Euclid’s postulates

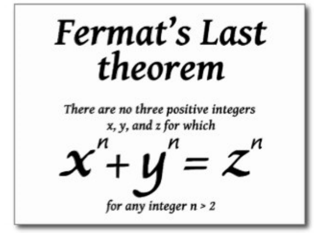


I. Through 2 points a line segment can be drawn
II. A line segment can be extended to a straight line indefinitely
III. Given a line segment, a circle can be drawn with it as a radius and one endpoint as a centre
IV. All right angles are congruent
V. Parallel postulate

Some axioms for propositional logic

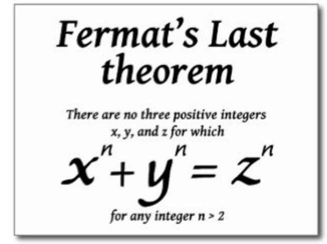
- For any formulas A, B, C:
  - $A \vee \neg A \equiv True$ $\quad A \wedge \neg A \equiv False$
  - $True \vee A \equiv True.$ $\quad True \wedge A \equiv A$
  - $False \vee A \equiv A.$ $\quad False \wedge A \equiv False$
  - $A \vee A \equiv A \wedge A \equiv A$
- Also, like in arithmetic (with ∨ as +, ∧ as *)
  - $A \vee B \equiv B \vee A$, $\quad (A \vee B) \vee C \equiv A \vee (B \vee C)$
  - $\text{Same holds for } \wedge.$
  - Also, $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$
- And unlike arithmetic
  - $(A \wedge B\ ) \vee C \equiv \ (A \vee C) \wedge (B \vee C)$

Counterexamples



- To disprove a statement, enough to give a counterexample: a scenario where it is false
  - To **disprove** that $A \to B \equiv B \to A$
    - Take $A = true, B = false,$
    - Then $A \to B$ is false, but $\mathrm{B} \to A$ is true.
  - To **disprove** that if $\forall x\ \exists y\ P(x,y)$, then $\exists y\ \forall x\ P(x,y)$,
    - Set the domain of x and y to be {0,1}
    - Set P(0,0) and P(1,1) to true, and P(0,1), P(1,0) to false.
    - Then $\forall x\ \exists y\ P(x,y)$ is true, but $\exists y\ \forall x\ P(x,y)$ is false.
      - Because $\big(P(0,0) \lor P(0,1)\big) \land \big(P(1,0) \lor P(1,1)\big)$ is true,
      - But $(P(0,0) \land P(1,0)) \lor (P(0,1) \land P(1,1))$ is false.

Constructive proofs



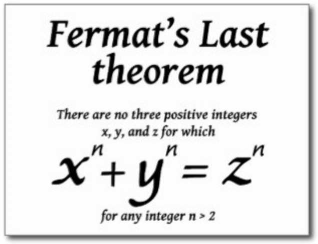
- To prove a statement of the form $\exists x$, sometimes can just find that x
  - $\exists x \in \mathbb{N}\ Even(x) \land Prime(x)$
    - Set x = 2.
    - Even(x) holds.
    - Prime(x) holds.
    - Therefore, $Even(x) \land Prime(x)$ holds.
    - Done.
  - This proof is **constructive**, because we constructed an x which makes the formula $Even(x) \land Prime(x)$ true.

Proof

- To prove that something of the form $\forall x\ F(x)$:
  - Make sure it holds in every scenario (method of exhaustion)
    - For all possible values of A and B, $\neg B \to \neg A$ is equivalent to $A \to B$, by checking the truth table.
  - But there can be too many scenarios!
    - For any integer, there is a larger integer which is a prime.
    - For any two reals, there is a real between them.
  - Instead, use **axioms and rules of inference** to derive it.

    $\neg B \to \neg A \equiv \neg\neg B \vee \neg A \equiv B \vee \neg A \equiv \neg A \vee B \equiv A \to B$
    - So $(\neg B \to \neg A) \leftrightarrow (A \to B)$ is a tautology.
    - And, therefore, $\forall A, B \in \{True, False\}$, $\neg B \to \neg A \equiv A \to B$

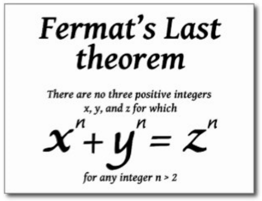
Puzzle



- Let $S = \{x \in \mathbb{N} \mid x \text{ is even}\} \cap \{x \in \mathbb{N} \mid x \text{ is odd}\}$
- Prove or disprove:

$$\forall x \in S, x \text{ does not divide } x^2$$

Puzzle



- Let $S = \{x \in \mathbb{N} \mid x\ is\ even\} \cap \{x \in \mathbb{N} \mid x\ is\ odd\}$

  S = ∅

- Prove or disprove:

  $$\forall x \in S, \qquad x\ does\ not\ divide\ x^2$$

  - Let P(x)= "$x\ does\ not\ divide\ x^2$"
  - To disprove, can give a counterexample
    - Find an element in S such that P(x) is true …
    - But there is no such element in S, because there are no elements in S at all!
  - To prove, enough to check that it holds for all elements of S.
    - There is none, so it does hold for every element in S.
  - Another way: Since S is defined as a subset of natural numbers, can read $\forall x \in S\ P(x)$ as $\forall x \in \mathbb{N}\ \big(x \in S \rightarrow P(x)\big)$.
    - Since "$x \in S$" is always false, $x \in S \rightarrow P(x)$ is true for every $x \in \mathbb{N}$
  - Call a statement $\forall x \in \emptyset\ \ P(x)$ **vacuously true.**

Modus ponens

- The main **rule of inference**, given by the **tautology** $((p \rightarrow q) \wedge p) \rightarrow q$, is called **Modus Ponens** (“method of affirming” in Latin).

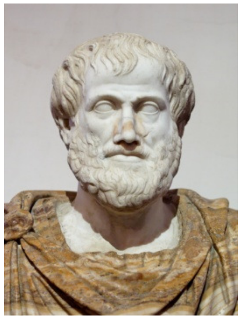
- **If p then q**
- p

$\overline{} \therefore$

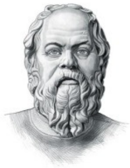
q

p	q	$p \rightarrow q$	$(p \rightarrow q) \wedge p$	$((p \rightarrow q) \wedge p) \rightarrow q$
True	*True*	True	True	True
True	*False*	False	False	True
False	*True*	True	False	True
False	*False*	True	False	True

Universal Modus Ponens

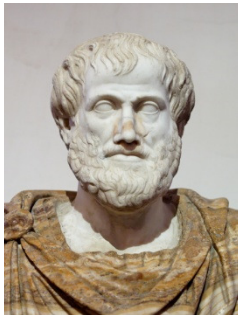


- All men are mortal
- Socrates is a man
- Therefore, Socrates is mortal

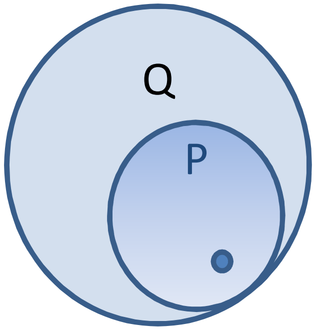


- All cats like fish
- Molly likes fish
- Therefore, Molly is a cat

Universal Modus Ponens



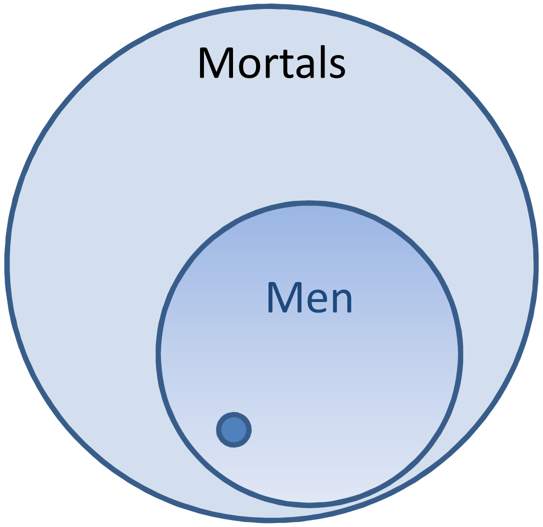
- $\forall x,\ P(x)\ \rightarrow Q(x)$
- $P(a)$
- -------------------------
- $Q(a)$



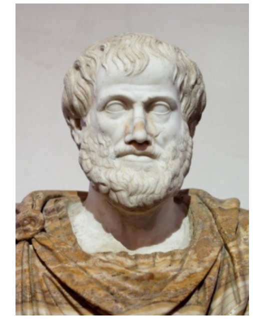
- All men are mortal ($\forall x,\ Man(x) \rightarrow Mortal(x)$)
- Socrates is a man   ($Man(Socrates)$)
- Therefore, Socrates is mortal ($Mortal(Socrates)$)

- All numbers are either odd or even
- 2 is a number
- Therefore, 2 is either odd or even.

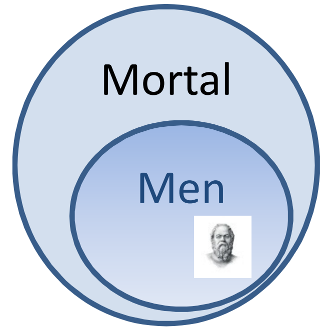
- All trees drop leaves
- Pine does not drop leaves
- Therefore, pine is not a tree



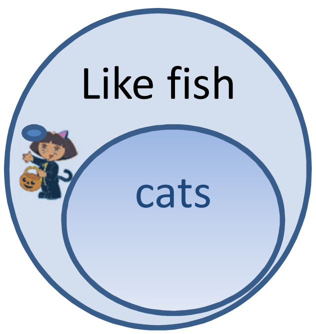
Universal Modus Ponens



- All men are mortal
- Socrates is a man
- Therefore, Socrates is mortal



- All cats like fish
- Molly likes fish
- Therefore, Molly is a cat



Instantiation/generalization

- In general, if $\forall\, x \in S \;\; F(x)$ is true for some formula $F(x)$, if you take any specific element $a \in S$, then $F(a)$ must be true.
  - This is called the **universal instantiation** rule.
    - $\forall x \in \mathbb{N} \;\; (x > -1)$
    - $\therefore \;\; 5 > -1$

- If you prove $F(a)$ without any assumptions about a other than $a \in S$, then $\forall x \in S, F(x)$
  - This is called **universal generalization**.

Instantiation/generalization

- If you can find an element $a \in S$ such that $F(a)$, then $\exists x \in S, F(x)$
  - This is called **existential generalization**.

- Alternatively, if $\exists\ x \in S\ \ F(x)$ is true, then you can give that element of S for which $F(x)$ is true **a name**, as long as that name has not been used elsewhere.
  - This is called the **existential instantiation** rule.
    - $\exists x \in \mathbb{N}\ \ (x - 5 = 0)$
    - $\therefore\ \ k = 0 + 5$

Existential instantiation

- If $\exists\, x \in S\ \ F(x)$ is true, then you can give that element of S for which $F(x)$ is true **a name**, as long as that name has not been used elsewhere.
  - "Let n be an even number. Then n=2k for some k".
    - $\forall x \in \mathbb{N}\ \ Even(x) \rightarrow\ \ \exists\, y \in \mathbb{N}\ \ (x = 2 * y)$
  - Important to have a new name!
    - "Let n and m be two even numbers. Then n=2k and m=2k" is wrong!
    - $\forall x_1, x_2\ \in \mathbb{N}\ \ Even(x_1) \wedge Even(x_2) \rightarrow$
      $$\exists\, y_{1,} y_2 \in \mathbb{N}\ \ (x_1 = 2 * y_1) \wedge (x_2 = 2 * y_2)$$
    - "Let n and m be two even numbers. Then n=2k and m=2ℓ"

Other inference rules

- Combining **universal instantiation** with **tautologies**, get other types of arguments:

$$p \to q$$
$$q \to r$$
$$\underline{\qquad\qquad} \therefore$$
$$p \to r$$

- $\forall x\, P(x) \to Q(x)$
- $\forall x\, Q(x) \to R(x)$

$$\underline{\qquad\qquad\qquad\qquad} \therefore$$
$$\forall x\, P(x) \to R(x)$$

For any x, if $x > 3$, then $x > 2$

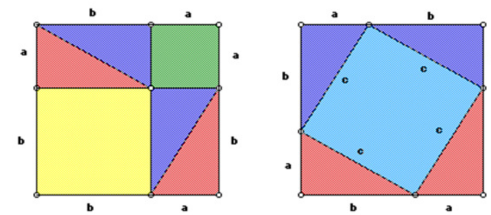
For any x, if $x > 2$, then $x \neq 1$

$\underline{\qquad\qquad\qquad\qquad} \therefore$

For any x, if $x > 3$, then $x \neq 1$

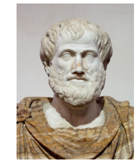
- (This particular rule is called "**transitivity**")

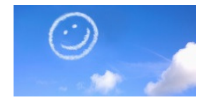
Types of proofs



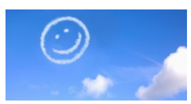
- **Direct proof of $\forall \boldsymbol{x}\ \boldsymbol{F}(\boldsymbol{x})$**
  - Show that $F(x)$ holds for arbitrary x, then use universal generalization.
    - Often, $F(x)$ is of the form $G(x) \rightarrow H(x)$
  - Example: A sum of two even numbers is even.
- **Proof by cases**
  - If can write $\forall x\ F(x)$ as $\forall x (G_1(x) \vee G_2(x) \vee \cdots \vee G_k(x)) \rightarrow H(x)$, prove $\left(G_1(x) \rightarrow H(x)\right) \wedge (G_2(x) \rightarrow H(x)) \wedge \cdots \wedge (G_k(x) \rightarrow H(x))$
  - Example: triangle inequality $(|x+y| \leq |x| + |y|)$
- **Proof by contraposition**
  - To prove $\forall x\ \ G(x) \rightarrow H(x)$, prove $\forall x\ \neg H(x) \rightarrow \neg G(x)$
  - Example: If square of an integer is even, then this integer is even.
- **Proof by contradiction**
  - To prove $\forall x\ F(x)$, prove $\forall x\ \neg F(x) \rightarrow FALSE$
  - Example: $\sqrt{2}$ is not a rational number.
  - Example: There are infinitely many primes.

Puzzle: better than nothing



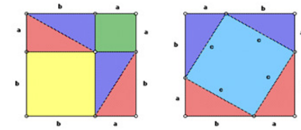
- Nothing is better than eternal bliss 
- A burger is better than nothing 

- Therefore, a burger is better than eternal bliss.

 $\leq$ $\leq$ 

Is there anything wrong with this argument?

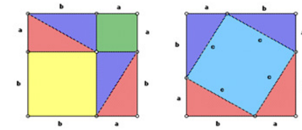
Direct proof



- **Direct proof of $\forall \boldsymbol{x} \in \boldsymbol{S}\ \boldsymbol{F}(\boldsymbol{x})$:** show directly that $F(x)$ holds for arbitrary x, then use universal generalization.
  - Universal instantiation: "let n be an arbitrary element of the domain S of $\forall x$ "
  - Show F(n) from axioms, definitions, previous theorems…
    - When $F(x)$ is of the form $G(x) \rightarrow H(x)$, then assume $G(n)$ is true, and from that (and axioms, etc) derive H(n)
    - That proves $G(n) \rightarrow H(n)$
  - Now use universal generalization to conclude that $\forall x\ F(x)$ is true.

□ (Done).

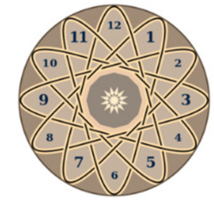
Direct proof



- *Definition* (of even integers):
  - An integer n is **even** iff $\exists k \in \mathbb{Z}, n = 2 \cdot k$.
- *Theorem*: Sum of two even integers is even.
  - $\forall x, y \in \mathbb{Z}\ \ Even(x) \wedge Even(y) \rightarrow Even(x + y)$.
- *Proof*:
  - Suppose m and n are arbitrary even integers.
    - Universal instantiation.
  - Then $\exists k \in \mathbb{Z}, n = 2k$ and $\exists l \in \mathbb{Z}, m = 2l$.
    - By definition: note different variables.
  - $m + n = 2k + 2l = 2(k + l)$
    - By substitution and axioms of theory of integers (algebra).
  - $\mathrm{m} + \mathrm{n} = 2(k + l)$, so $m + n$ is even
    - By definition (other direction of iff).
  - Since m and n were arbitrary, therefore, we have shown what we needed: $\forall x, y \in \mathbb{Z}\ \ Even(x) \wedge Even(y) \rightarrow Even(x + y)$.
    - By universal generalization.

□ (Done).

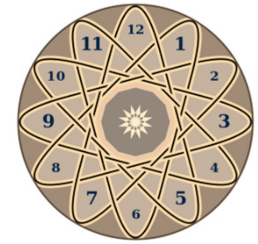
Modular arithmetic



- *Quotient-remainder theorem*: for any integer n and a positive integer *d*, there exist unique integers *q* (**quotient**) and r (**reminder**) such that: $n = dq + r$ and $0 \leq r < q$
  - 16 = 3*5+1, 11 = 2*4+3...

- $n \equiv m \ (mod \ d)$, pronounced "*n* **is congruent to** *m* **mod** *d*", means that n and m have the same remainder when divided by d. That is, $n = dq_1 + r$ and $m = dq_2 + r$, for the same r.
  - In some programming languages, there is an operator mod, so you might see "n mod d", which would return r .
    - In Python, it is n % d.
    - $n \equiv m \ (mod \ d)$ and $m = n \ mod \ d$ are not the same:
    - $10 \equiv 16 \ (\mathrm{mod}\ 3)$, but $10 \ mod \ 3 = 1$
  - Operator div, "n div d" is sometimes used to compute q.
    - In Python, integer division (or /) does it.

Modular arithmetic in CS



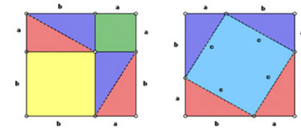
- Example: day of the week.
  - Oct 4th and Oct 11th are both on Wednesday: $4 \equiv 11 \ (mod\ 7)$
- Hash functions: distribute random data evenly among *d* memory locations
  - Often take *h*(*k*) = *k mod p* for some prime *p*. If $k \equiv \ell \ (mod\ p)$, get a collision.
- Cryptography:
  - Parity checks in codes, ISBNs, etc.
  - Public key crypto, RSA ....

Direct proof example

- *Theorem*: for all integers *n, m* and *d*, where $d > 0$, if $n \equiv m \ (mod\ d)$ then there exists an integer k such that n$= m + kd$
  - $\forall x, y, z \ \ (z > 0 \wedge \ x \equiv y \ (mod\ z)) \rightarrow \exists u \ \ x = y + uz$
- *Proof*:
  - Let n, m, d be arbitrary integers such that $d > 0$ and $n \equiv m \ (mod\ d)$
    - Universal instantiation and assuming the premise
  - Then there are integers q_1, q_2, r with $0 \leq r < d$ such that $n = dq_1 + r$ and $m = dq_2 + r$.
    - By the quotient-remainder theorem and definition of congruence.
  - Now, n$-m = (dq_1 + r) - (dq_2 + r) = d(q_1 - q_2)$
    - Substitution and algebra.
  - Set k = $q_1 - q_2$. For this k, $n = m + kd$. Therefore, $\exists u \ \ n = m + ud$
    - By existential generalization
  - Since n, m, d were arbitrary integers with $d > 0$ and $n \equiv m \ (mod\ d)$, $\forall x, y, z \ \ (z > 0 \wedge \ x \equiv y \ (mod\ z)) \rightarrow \exists u \ \ x = y + uz$
    - By universal generalization.

□ (Done).

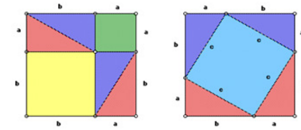
Proof by cases



- Use the tautology $(p_1 \vee p_2) \wedge (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \rightarrow q$
  - Or its variant with cases $p_1 \ldots p_k$
- If $\forall x\, F(x)$ is $\forall x(G_1(x) \vee G_2(x)) \rightarrow H(x)$,
- prove $\big(G_1(x) \rightarrow H(x)\big) \wedge (G_2(x) \rightarrow H(x))$.
- Proof:
  - – Universal instantiation: “let n be an arbitrary element of the domain S of $\forall x$ ”
  - – Case 1: $G_1(n) \rightarrow H(n)$
  - – Case 2: $G_2(n) \rightarrow H(n)$
    - …. (if more cases than 2)
    - Case k: $G_k(n) \rightarrow H(n)$
  - – Therefore, $G_1(n) \vee G_2(n)) \rightarrow H(n)$,
  - – Now use universal generalization to conclude that $\forall x\, F(x)$ is true.

□ (Done).

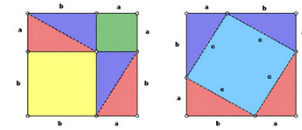
Proof by cases: example 1



- *Definition* (of odd integers):
  - An integer n is **odd** iff $\exists k \in \mathbb{Z}, n = 2 \cdot k + 1$.
- *Theorem*: Sum of an integer with a consecutive integer is odd.
  - $\forall x \in \mathbb{Z}\ Odd(x + (x + 1))$.
- *Proof*:
  - Suppose n is an arbitrary integer.
  - Case 1: n is even.
    - So n=2k for some k (by definition).
    - Its consecutive integer is n+1 = 2k+1.
      Their sum is (n+(n+1))= 2k + (2k+1) = 4k+1. (axioms).
    - Let $l = 2k$. Then $4k + 1 = 2l + 1$ is an odd number (by definition).
      So in this case, n+(n+1) is odd.
  - Case 2: n is odd.
    - So n=2k+1 for some k (by definition).
    - Its consecutive integer is n+1 = 2k+2.
      Their sum is (n+(n+1))= (2k+1) + (2k+2) = 2(2k+1)+1. (axioms).
    - Let $l = 2k + 1$. Then n+(n+1) = 2(2k+1)+1= $2l + 1$,
      which is an odd number (by definition). So in this case, n+(n+1) is also odd.
  - Since in both cases n+(n+1) is odd, it is odd without additional assumptions. Therefore, by universal generalization, get $\forall x \in \mathbb{Z}\ Odd(x + (x + 1))$.

□ (Done).

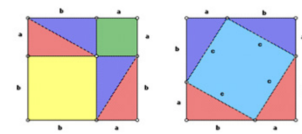
Proof by cases: example 2



- *Definition*: an absolute value of a real number r is a non-negative real number |r| such that if $|r| = r$ if $r \geq 0$, and $|r| = -r$ if $r < 0$
  - Claim 1: $\forall x \in \mathbb{R}, |-x| = |x|$
  - Claim 2: $\forall x \in \mathbb{R}, -|x| \leq x \leq |x|$
- *Theorem*: for any two reals, sum of their absolute values is at least the absolute value of their sum.
  - $\forall x, y \in \mathbb{R}\ \ |x + y| \leq |x| + |y|$
- *Proof*:
  - Let r and s be arbitrary reals. (universal instantiation)
  - Case 1: Let $r + s \geq 0$.
    - Then $|r + s| = r + s$ (definition of $||$)
    - Since $r \leq |r|$ and $s \leq |s|$ (claim 2), r+$s \leq |r| + |s|$ (axioms),
    - so $|r + s| =$ r+$s \leq |r| + |s|$, which is what we need.
  - Case 2: Let $r + s < 0$.
    - Then $|r + s| = -(r + s) = (-r) + (-s)$ (definition of $||$)
    - Since $-r \leq |-r| = |r|$ and $-s \leq |-s| \leq |s|$ (claims 1 and 2),
    - |r+$s| = (-r) + (-s) \leq |r| + |s|$ (axioms), which is what we need.
  - Since in both cases |r+$s| \leq |r| + |s|$, and there are no more cases, |r+$s| \leq |r| + |s|$ without additional assumptions. By universal generalization , can now get $\forall x, y \in \mathbb{R}\ \ |x + y| \leq |x| + |y|$.

$\square$ (Done).

Proof by contraposition



– To prove $\forall x\ \ G(x) \rightarrow H(x)$, prove its contrapositive $\forall x\ \neg H(x) \rightarrow \neg G(x)$

- Universal instantiation: "let n be an arbitrary element of the domain S of $\forall x$ "
- Suppose that $\neg H(n)$ is true.
- Derive that $\neg G(n)$ is true.
- Conclude that $\neg H(n) \rightarrow \neg G(n)$ is true.
- Now use universal generalization to conclude that $\forall x\ \ G(x) \rightarrow H(x)$ is true.

□ (Done).

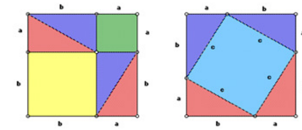
Pigeonhole Principle

- Suppose that nobody in our class carries more than 10 pens.
- There are 70 students in our class.

- Prove that there are at least 2 students in our class who carry the same number of pens.
  - In fact, there are at least 7 who do.

- The Pigeonhole Principle:
  - If there are n pigeons
  - And n-1 pigeonholes
  - Then if every pigeon is in a pigeonhole
  - At least two pigeons sit in the same hole

Proof by contraposition



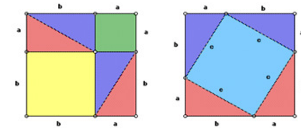
- *Theorem (Pigeon Hole Principle)*: For any n, if there are n+1 pigeons and n holes, then if every pigeon sits in some hole, then there is a hole with at least two pigeons.
  - $\forall x \in \mathbb{N} \; (\forall y \leq x \, \exists z < x \; Sits(y,z)) \rightarrow \exists u \leq x \, \exists v \leq x \, \exists w < x \; (u \neq v \wedge Sits(u,w) \wedge Sits(v,w))$
- *Proof*:
  - Suppose n is an arbitrary integer.
  - We show the **contrapositive**: if every hole has at most one pigeon, then some pigeon is not sitting in any hole.
  - If every hole has at most one pigeon, then there are at $\leq$ 1*n=n pigeons sitting in holes.
  - Then there are $\geq (n+1) - n = 1$ pigeons that are not sitting in a hole, proving the contrapositive.
  - Therefore, if every pigeon sits in a hole, and there are more than n pigeons, then two pigeons sit in the same hole.
  - By universal generalization, done.

□ (Done).

Proof by contraposition

- *Theorem*:
  If a square of an integer is even, that integer is even.
  - $\forall x \in \mathbb{Z}\ \ Even(x^2) \rightarrow Even(x)$.
- *Proof*:
  - We will show a **contrapositive**:
    $\forall x \in \mathbb{Z}\ \neg Even(x) \rightarrow \neg Even(x^2)$.
    That is, square of an odd integer is odd.
  - Let n be an arbitrary odd integer.
    By definition, $n = 2k + 1$ for some integer k.
  - Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$
    $= 2(2k^2 + 2k) + 1,$
  - So $n^2 = 2m + 1$ for m= $2k^2 + 2k$, thus n^2 is odd by definition.
  - By universal generalization,
    get $\forall x \in \mathbb{Z}\ \neg Even(x) \rightarrow \neg Even(x^2)$.
    Since it is a contrapositive of the original statement, done.

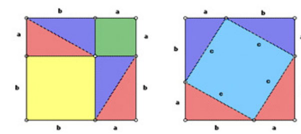
Proof by contradction



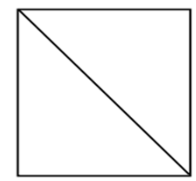
- To prove $\forall x \ \ F(x)$, prove $\forall x \ \neg F(x) \rightarrow FALSE$
  - Universal instantiation: "let *n* be an arbitrary element of the domain S of $\forall x$ "
  - Suppose that $\neg F(n)$ is true.
  - Derive a contradiction.
  - Conclude that $F(n)$ is true.
  - By **universal generalization**, $\forall x \ F(x)$ is true.

□ (Done).

Proof by contradiction



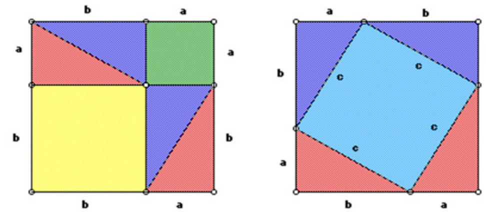
- *Definition* (of rational and irrational numbers):
  - A real number r is **rational** iff $\exists m, n \in \mathbb{Z}, n \neq 0 \wedge \gcd(m,n) = 1 \ \wedge$ $r = \frac{m}{n}$.
    - Reminder: **greatest common divisor gcd(m,n)** is the largest integer which divides both m and n. When d=1, m and n are **relatively prime**.
  - A real number which is not rational is called **irrational**.



- ***Theorem*: Square root of 2 is irrational.**
- *Proof*:
  - Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational. Then there exist relatively prime m, n ∈ $\mathbb{Z}$, $n \neq 0$ such that $\sqrt{2} = \frac{m}{n}$.
  - By algebra, squaring both sides we get $2 = \frac{m^2}{n^2}$.
  - Thus m^2 is even, and by the theorem we just proved, then m is even. So $m = 2k$ for some k.
  - $2n^2 = 4\ k^2$, so $n^2 = 2k^2$, and by the same argument n is even.
  - This contradicts our assumption that m and n are relatively prime. Therefore, such m and n cannot exist, and so $\sqrt{2}$ is not rational.

□ (Done).

Summary: Types of proofs



- **Direct proof of $\forall \boldsymbol{x}\ \boldsymbol{F(x)}$**
  - Show that $F(x)$ holds for arbitrary x, then use universal generalization.
    - Often, $F(x)$ is of the form $G(x) \to H(x)$
  - Example: A sum of two even numbers is even.
- **Proof by cases**
  - If can write $\forall x\ F(x)$ as $\forall x(G_1(x) \vee G_2(x) \vee \cdots \vee G_k(x)) \to H(x)$, prove $\left(G_1(x) \to H(x)\right) \wedge (G_2(x) \to H(x)) \wedge \cdots \wedge (G_k(x) \to H(x))$
  - Example: triangle inequality $(|x+y| \leq |x| + |y|)$
- **Proof by contraposition**
  - To prove $\forall x\ \ G(x) \to H(x)$, prove $\forall x\ \neg H(x) \to \neg G(x)$
  - Example: If square of an integer is even, then this integer is even.
- **Proof by contradiction**
  - To prove $\forall x\ F(x)$, prove $\forall x\ \neg F(x) \to FALSE$
  - Example: $\sqrt{2}$ is not a rational number.
  - Example: There are infinitely many primes.