Unit 4
Proofs

Computer Science 1002
Introduction to Logic for Computer Scientists

1

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?

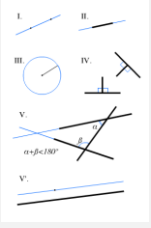
2

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 different numbers there is another number.
    - A theorem for real numbers. False for integers!

3

Axioms of geometry: 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

4

Axioms of propositional logic

- For any logic formulas A, B, C,
  - like in arithmetic (with ∨ as +, ∧ as *)

$A \vee B \equiv B \vee A$ $\quad A \wedge B \equiv B \wedge A$ Commutativity

$(A \vee B) \vee C \equiv A \vee (B \vee C)$ $\quad (A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ Associativity

$(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$

  - And unlike arithmetic $(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$ Distributivity (2)

- Properties of $TRUE$ and $FALSE$

$TRUE \vee A \equiv TRUE.$ $\quad TRUE \wedge A \equiv A$

$FALSE \vee A \equiv A.$ $\quad FALSE \wedge A \equiv FALSE$

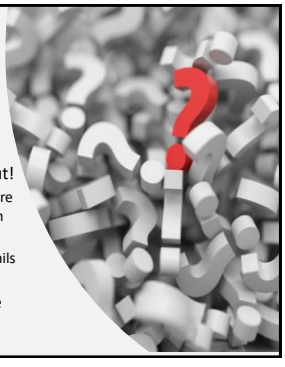
$A \vee \neg A \equiv TRUE$ $\quad A \wedge \neg A \equiv FALSE$

- Double negation: $\neg\neg A \equiv A$
- De Morgan's laws:
  $\neg(A \vee B) \equiv \neg A \wedge \neg B$
  $\neg(A \wedge B) \equiv \neg A \vee \neg B$

5

Proofs in real life

- You will pretty much never see a proof with all the rules and axioms spelled out!
  - If you are reading a proof, if you are not sure why a certain step is valid, work it out from what you know.
  - If you are writing a proof, put enough details to make it clear why each step is valid.
- But here we will start by identifying the logic behind proofs.



6

7

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?

8

Constructive proofs

- To prove an existential statement $\exists x\ F(x)$, find a witness for x and show that it works.
  - This proof is **constructive**, because we constructed an x which makes the formula $Even(x) \wedge Prime(x)$ true.

Rule of Inference

Theorem: $\exists x \in \mathbb{N}\ Even(x) \wedge Prime(x)$
Proof:
Let x=2.
Even(2) is true.
Prime(2) is true.
Therefore, $Even(2) \wedge Prime(2)$ holds.
We found a witness for $\exists x$
Done.

9

Counterexamples

- To disprove a statement, enough to give a counterexample: a scenario where it is false
  - To disprove that $A \rightarrow B \equiv B \rightarrow A$
    - Take $A = true, B = false$,
    - Then $A \rightarrow B$ is false, but $B \rightarrow A$ is true.
    - Hidden universal quantifier: for all truth assignments

All birds can fly

- Disproving a statement is the same as proving its negation.
  - To disprove $\forall x\ F(x)$, give a constructive proof for $\exists x\ \neg F(x)$

10

Counterexamples

- Statement: "For any predicate $P(x,y)$ on any domain S, if $\forall x \in S\ \exists y \in S\ P(x,y)$, then $\exists y \in S\ \forall x \in S\ P(x,y)$"
- Let's disprove it by constructing a counterexample!
  - Let $S = \{0,1\}$ and let interpretation of P on S be:
    - P(0,0), P(1,1) are true, and P(0,1), P(1,0) are false. (So P(x,y) is $x = y$)
  - Then $\forall x\ \exists y\ P(x,y)$ is true, but $\exists y\ \forall x\ P(x,y)$ is false.
    - Because $(P(0,0) \vee P(0,1)) \wedge (P(1,0) \vee P(1,1))$ is true,
    - But $(P(0,0) \wedge P(1,0)) \vee (P(0,1) \wedge P(1,1))$ is false.
  - Our counterexample consists of *domains* for x and y (they don't have to be equal), and an *interpretation* of the predicate $P(x,y)$ over these domains.

11

Proving universal statements

- To prove that something of the form $\forall x\ F(x)$ is true:
  - Make sure it holds in every scenario (method of exhaustion)
    - For all values of A and B, $\neg B \rightarrow \neg A \equiv A \rightarrow B$, by 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.
  - In the next several lectures, we will study how to use axioms and rules of inference to be able to prove such statements.

12

Vacuous puzzle

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

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


13

14

Vacuous puzzle

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

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


15

Vacuous puzzle


- Let $S = \{x \in \mathbb{N} \mid x \text{ is even}\} \cap \{x \in \mathbb{N} \mid x \text{ is odd}\}$
  - But there are no natural numbers that are both even and odd! So S = ∅
- Prove or disprove: $\forall x \in S, \ x \text{ does not divide } x^2$
  - 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 false… But there is nothing 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.**

16

Inference rules with quantifiers

- **Instantiation:** taking a specific instance (value) of a variable
  - Can be just giving this variable a name
  - $Even(2),\ Even(k)$
- **Generalization:** replacing a value with a quantified variable
  - Have $Even(2)$
  - Get $\exists x\ Even(x)$

17

Existential generalization


$F(a)$ is true for some $a \in S$

Therefore, $\exists x \in S\ F(x)$

$Even(2)$

Therefore, $\exists x \in \mathbb{Z},\ Even(x)$

$Loves(Jane, Jim)$

$\therefore \exists x \in PEOPLE\ \ Loves(x, Jim)$

Penguins do not fly

$\therefore \exists x \in BIRDS\ \neg Fly(x)$

$\exists x \in PEOPLE\ \ Loves(x, Jim)$

$\therefore \exists y\ \exists x\ \ Loves(x, y)$

18

Existential instantiation

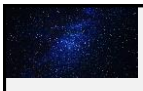
- If $\exists\ x \in S\ \ F(x)$ is true, then you can give that element of S for which $F(x)$ is true a name, as long as that name has not been used elsewhere.
  - "Let n be an even number. Then n=2k for some k".
    - $\forall x \in \mathbb{N}\ \ Even(x) \rightarrow\ \exists\ y \in \mathbb{N}\ \ (x = 2 * y)$
  - Important to have a new name every time the rule is applied!
    - "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"

19

Universal instantiation

- 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.
    - $\forall x \in \mathbb{N}\ \ (x > -1)$
    - $\therefore\ \ 5 > -1$
- In proofs, most often take a to be an arbitrary element of S
  - This just gives that element a name!
  - And allows us to say things like "$a \geq 0$ or $a < 0$", and consider these cases separately.

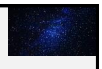
20



Universal generalization

- Let a be an arbitrary element of S
- 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**.
- For an arbitrary $k \in \mathbb{Z}$, $\ Even(k) \vee Odd(k)$
- Therefore, $\forall x \in \mathbb{Z},\ Even(x) \vee Odd(x)$

21



- Theorem:

  For any propositional formulas A,B, $\neg B \rightarrow \neg A \equiv A \rightarrow B$
- Proof: let's use axioms and definitions of logic to prove it.
  - Let A and B be arbitrary propositional formulas — *universal instantiation*
  - $\neg B \rightarrow \neg A \equiv \neg\neg B \vee \neg A$ — *by definition of* $F \rightarrow G$
  - $\equiv B \vee \neg A$ — *by the double negation axiom* $\neg\neg F \equiv F$
  - $\equiv \neg A \vee B$ — *by the axiom* $F \vee G \equiv G \vee F$
  - $\equiv A \rightarrow B$ — *by definition of* $F \rightarrow G$
  - Therefore, for any formulas A, B $\neg B \rightarrow \neg A \equiv A \rightarrow B$ — *by universal generalization*

22

23

Rules of inference in predicate logic

- Combine universal and existential instantiations and generalizations with the rules of inference from propositional logic.
  - Modus ponens and friends,
  - Resolution and friends, etc..

24

Universal Modus Ponens

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

$\forall x\ Man(x) \rightarrow Mortal(x)$
$Man(Socrates) \rightarrow Mortal(Socrates)$
Man(Socrates)

$\therefore Mortal(Socrates)$

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

- $(\forall x)\ Cat(x) \rightarrow like\_fish(x)$
- $like\_fish(Molly)$

$\therefore$ Cat(Molly) X

25

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 integers are either odd or even
- 2 is an integer
- Therefore, 2 is either odd or even.

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

26

Other inference rules

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

$p \rightarrow q$	• $\forall x\ P(x) \rightarrow Q(x)$	For any x, if $x > 3$, then $x > 2$
$q \rightarrow r$	• $\forall x\ Q(x) \rightarrow R(x)$	For any x, if $x > 2$, then $x \neq 1$
$\therefore p \rightarrow r$	$\therefore \forall x\ P(x) \rightarrow R(x)$	$\therefore$ For any x, if $x > 3$, then $x \neq 1$

- (This particular rule is called “transitivity”)

27

28

Types of proofs

- We are not studying these proofs for the sake of proving these theorems.
  - We are using them as examples of underlying proof types.
  - When reading proofs, note where universal and existential instantiation/ generalization are used.
  - And what logic is used to derive each step.

29

Proof example

- Theorem:
  For any propositional formulas A,B, $\neg B \rightarrow \neg A \equiv A \rightarrow B$
- Proof:
  - Let A and B be arbitrary propositional formulas *universal instantiation*
  - $\neg B \rightarrow \neg A \equiv \neg\neg B \vee \neg A$ *by definition of* $F \rightarrow G$
  - $\equiv B \vee \neg A$ *by the double negation axiom* $\neg\neg F \equiv F$
  - $\equiv \neg A \vee B$ *by the axiom* $F \vee G \equiv G \vee F$
  - $\equiv A \rightarrow B$ *by definition of* $F \rightarrow G$

  - And, therefore, for any formulas A, B , $\neg B \rightarrow \neg A \equiv A \rightarrow B$ *universal generalization*

30

Direct proof

- **Direct proof** of $\forall x \in S\ F(x)$: show directly that $F(x)$ holds for an arbitrary $n \in S$, then use universal generalization.
  - Universal instantiation: "let n be an arbitrary element of S"
  - Show that $F(n)$ is true from axioms, definitions, previous theorems…
  - Finally use universal generalization to conclude that $\forall x\ F(x)$ is true.

□ (Done).

31

Direct proof

- **Direct proof** of $\forall x \in S\ F(x)$: show directly that $F(x)$ holds for an arbitrary $n \in S$, then use universal generalization.
- When $F(x)$ is of the form $G(x) \rightarrow H(x)$, assume $G(n)$ is true, and from that (and axioms, etc) derive $H(n)$. That proves $G(n) \rightarrow H(n)$
  - Notice: we are skipping a step here! Here it is:
    - Let n be an arbitrary element of S.
    - If $G(n)$ is false, done (since $false \rightarrow H(n)$ is true, so $F(n)$ is true for this n)
    - Otherwise let n be such that $G(n)$ holds
  - But since when $G(n)$ is false $F(x)$ holds for a trivial reason, it is more common to see just "Let n be arbitrary element of S such that $G(n)$ holds."

□ (Done).

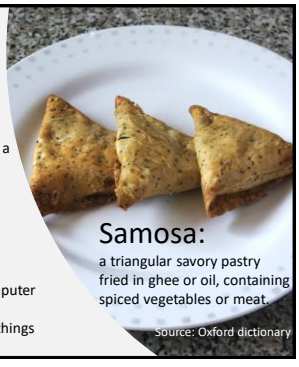
32

Definitions

Informally, a definition is a sentence giving a name to an object with some properties.
- Introducing a shorthand for a formula

- n is **even** if and only if it is divisible by 2
- n is **even** iff $\exists k \in \mathbb{Z}\ n = 2k$

You will see a lot of definitions in your computer science career!
- And will be asked to implement those things



Samosa:

a triangular savory pastry fried in ghee or oil, containing spiced vegetables or meat.

Source: Oxford dictionary

33

Theorem: Sum of two even integers is even.

$\forall x, y \in \mathbb{Z}\ Even(x) \wedge Even(y) \rightarrow Even(x + y).$

- *Proof*:

Definition (of even integers):
An integer n is **even** iff $\exists k \in \mathbb{Z}, n = 2 \cdot k.$

- Suppose m and n are arbitrary even integers.
- Then $\exists k \in \mathbb{Z}, n = 2k$ and $\exists l \in \mathbb{Z}, m = 2l.$
- $m + n = 2k + 2l = 2(k + l)$
- $m + n = 2(k + l)$, so $m + n$ is even
- Since m and n were arbitrary, we have shown $\forall x, y \in \mathbb{Z}, Even(x) \wedge Even(y) \rightarrow Even(x + y).$

□ (Done).

34

Theorem: Sum of two even integers is even.

$\forall x, y \in \mathbb{Z}\ Even(x) \wedge Even(y) \rightarrow Even(x + y).$

- *Proof*:

Definition (of even integers):
An integer n is **even** iff $\exists k \in \mathbb{Z}, n = 2 \cdot k.$

- Suppose m and n are arbitrary even integers. *By 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 existential instantiation, substitution and axioms of theory of integers (algebra).*
- $m + n = 2(k + l)$, so $m + n$ is even *By definition (other direction of iff) and existential generalization*
- Since m and n were arbitrary, we have shown $\forall x, y \in \mathbb{Z}, Even(x) \wedge Even(y) \rightarrow Even(x + y).$ *By universal generalization*

□ (Done).

35

Puzzle: Caesar cipher

- The Roman dictator Julius Caesar encrypted his personal correspondence using the following code.
  - Number letters of the alphabet: A=0, B=1,… Z=25.
  - To encode a message, replace every letter by a letter three positions before that (wrapping around at the beginning of the alphabet).
    - For example, F would be replaced by C, and A by X
- Suppose he sent the following message.
  - QEB QOBXPROB FP RKABO QEB CIXD
- What does it say?

36

37

Puzzle: Caesar cipher

- The Roman dictator Julius Caesar encrypted his personal correspondence using the following code.
  - Number letters of the alphabet: A=0, B=1,… Z=25.
  - To encode a message, replace every letter by a letter three positions before that (wrapping around at the beginning of the alphabet).
    - For example, F would be replaced by C, and A by X
- Suppose he sent the following message.
  - QEB QOBXPROB FP RKABO QEB CIXD
- What does it say?

38

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 $0 \leq r < d$
  - 16 = 3*5+1, 11 = 2*4+3…
- Definition: $n \equiv m \ (mod\ d)$, 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:
    - $10 \equiv 16 \ (\mathrm{mod}\ 3)$, is true, but $16\ mod\ 3 = 10$ is false $(16\ mod\ 3 = 1)$
  - Operator div, "n div d" is sometimes used to compute q.
    - In Python, integer division (or //) does it.

39

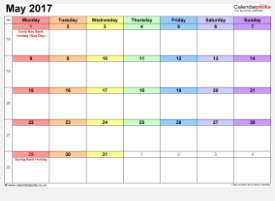
Calendars as modular arithmetic

- Wednesdays are day = 3 (mod 7)

- Wednesdays are day = 4 (mod 7)

40

Calendars vs mod



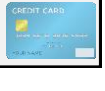
- Wednesdays are day = 3 (mod 7)

- Orange stickers are number = 3 (mod 8)

41

Modular arithmetic in computer science

- Example: day of the week.
  - Feb 1st and Feb 15th are both on Wednesday: $1 \equiv 15\ (mod\ 7)$
- Hash: distribute random data evenly among memory locations
  - Often take h(k) = k mod p for some prime p.
- Cryptography:
  - Parity checks in credit cards, codes, ISBNs, etc.
    - Look at combination of digits mod 10 to check if a credit card number is valid.
    - Google Luhn formula for details.
  - Public key crypto, RSA….



42

- *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 existential instantiation of 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).

43

44

Direct proof

- To prove $\forall x \in S \ F(x)$: show directly that $F(x)$ holds for an arbitrary $n \in S$, then use universal generalization.
  - Universal instantiation: for arbitrary $n \in S$
  - Show $F(n)$ using axioms, definitions, etc…
  - Universal generalization.
- If $F(x)$ is of the form $G(x) \rightarrow H(x)$
  - Universal instantiation + assume $G(n)$ is true.
    - If $G(n)$ is false, $G(n) \rightarrow H(n)$ true no matter what $H(n)$ is: vacuous proof
  - Derive $H(n)$ from $G(n)$ using axioms, definitions, etc.
  - Universal generalization.

□ (Done).

45

Tricks to make proofs easier

- Idea: to prove $\forall x \in S \ F(x)$, replace $F(x)$ with an equivalent formula that is easier to prove.
- **Proof by contraposition**:
  - to prove $\forall x \in S \ G(x) \rightarrow H(x)$, prove $\forall x \in S \ \neg H(x) \rightarrow \neg G(x)$
- **Proof by contradiction**:
  - No matter what $F(x)$ is, $F(x) \equiv TRUE \rightarrow F(x) \equiv \neg F(x) \rightarrow FALSE$
  - So to prove $\forall x \in S \ F(x)$, prove $\forall x \in S \ \neg F(x) \rightarrow FALSE$

46

Tricks to make proofs easier

- **Proof by cases**:
  - When $F(x)$ is of the form $\big(G_1(x) \vee G_2(x)\big) \rightarrow H(x)$, prove $\forall x \ F(x)$ by proving $\forall x \in S \ \big(G_1(x) \rightarrow H(x)\big) \wedge \big(G_2(x) \rightarrow H(x)\big)$
  - Since $F(x) \equiv TRUE \rightarrow F(x)$, can choose formulas $G_1(x), G_2(x)$ so that $\forall x \in S \ (G_1(x) \vee G_2(x))$ is true,
    - Then prove $\forall x \in S \ \big(G_1(x) \rightarrow F(x)\big) \wedge \big(G_2(x) \rightarrow F(x)\big)$ instead of proving $\forall x \in S \ F(x)$ directly.
  - These generalize to as many cases (as many $G_i(x)$ in this OR) as you need.

47

48

Proof by contraposition

- To prove $\forall x \in S \ (G(x) \rightarrow H(x))$, prove its contrapositive $\forall x \in S \ (\neg H(x) \rightarrow \neg G(x))$
  - Universal instantiation: "let n be an arbitrary element of S"
  - 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 $\forall x \ F(x)$ is true.

□ (Done).

49

- *Theorem*: If a square of an integer is even, that integer is even.
  - $\forall x \in \mathbb{Z} \ Even(x^2) \rightarrow Even(x)$.

Lemma: Every integer is odd iff it is not even.

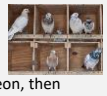
Definition: An integer n is **odd** iff $\exists k \in \mathbb{Z}, n = 2 \cdot k + 1$.

- *Proof*:
  - We will show that for all x the contrapositive of $F(x)$ holds: $\forall x \in \mathbb{Z} \ \neg Even(x) \rightarrow \neg Even(x^2)$.
  - By the lemma, this is equivalent to $\forall x \in \mathbb{Z} \ Odd(x) \rightarrow Odd(x^2)$
  - 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 $\forall x \in \mathbb{Z} \ Odd(x) \rightarrow Odd(x^2)$
  - By the lemma, this is equivalent to $\forall x \in \mathbb{Z} \ \neg Even(x) \rightarrow \neg Even(x^2)$
  - Since the formula under $\forall x$ is a contrapositive of the original $F(x)$, done.

□ (Done).

50

- *Theorem (PigeonHolePrinciple)*: 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.



- *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 most $1 * n = n$ pigeons sitting in holes.
  - Then there is $(n+1) - n = 1$ pigeon that is 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.

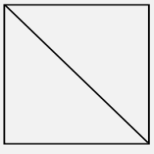
□ (Done).

51

52

Square root of 2

- What is the length of a diagonal of a square with side 1?
  - By Pythagoras' theorem, $1^2 + 1^2 = 2$, so it would have to be $\sqrt{2}$.
- Is it at least possible to represent $\sqrt{2}$ as a ratio of two integers?...
  - Pythagoras and others tried…



53

Rational and irrational numbers

- The numbers that are representable as a ratio of two integers are **rational** numbers. Set of all rational numbers is $\mathbb{Q}$.
- Numbers that are not rational are **irrational**.
- Rational and irrational numbers together form the set of all real numbers.
  - Any sequence of digits, potentially infinite after a decimal point, is a real number. Any point on a line.
- Irrationality of $\sqrt{2}$ is a classic proof by contradiction.

Pythagoras figured out that the diagonal of a square is not comparable to the sides, but did not think of it as a number.
- More like something weird.

Irrational numbers started being treated as numbers in 9th century in the Middle East.
- Starting with a Persian mathematician and astronomer Abu-Abdullah Muhammad ibn Îsa Mâhânî (Al-Mahani).

54

Proof by contradiction

- 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).

55

Definition of rational

- We need a slightly more precise definition of rational numbers for our proof that $\sqrt{2}$ is irrational.
- *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**.
    - Any fraction can be simplified until the numerator and denominator are relatively prime, so it is not a restriction
  - A real number which is not rational is called **irrational**.

56

- *Definition* (of rational and irrational numbers):
  - A real number r is **rational** iff

$$\exists m, n \in \mathbb{Z}, n \neq 0 \wedge \gcd(m,n) = 1 \ \wedge \ r = \frac{m}{n}.$$

- *Definition* (of greatest common divisor):
  - A positive integer d is the greatest common divisor of integers m and n if n is divisible by d, and m is divisible by d, and for any c if both n and m are divisible by c then $d \geq c$.

$$d > 0 \wedge \exists k_1\ \exists k_2\ \ n = k_1 d \wedge\ \ m = k_2 d$$
$$\wedge \forall c\ \ (\exists l_1\ \exists l_2\ \ n = l_1 c \wedge\ \ m = l_2 c\ ) \rightarrow c \leq d$$

- *Theorem*: Square root of 2 is irrational.

57

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 $\sqrt{2} = \frac{m}{n}$. *(definition and existential instantiation)*
  - *By algebra*, squaring both sides we get $2 = \frac{m^2}{n^2}$.
  - Thus m^2 is even (*by definition),* and by the theorem we just proved, then m is even. So $m = 2k$ for some k. *(definition and existential instantiation)*
  - $2n^2 = 4\,k^2$, 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.

58

59

Proof by cases

- If $\forall x \in S\ F(x)$ is $\forall x(G_1(x) \vee G_2(x)) \rightarrow H(x)$, prove $\forall x\ \big(G_1(x) \rightarrow H(x)\big) \wedge (G_2(x) \rightarrow H(x))$.
  - Use the tautology $(p_1 \vee p_2) \wedge (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \rightarrow q$
- Proof structure:
  - Universal instantiation: "let n be an arbitrary element of S"
  - Case 1: Prove $G_1(n) \rightarrow H(n)$
  - Case 2: Prove $G_2(n) \rightarrow H(n)$
  - Therefore, $(G_1(n) \vee G_2(n)) \rightarrow H(n)$,
  - Now use universal generalization to conclude that $\forall x\ F(x)$ is true.
- This generalizes for any number of cases ≥ 2.

60

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 and existential instantiation).
    - 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 and existential generalization).
    - So in this case, n+(n+1) is odd.
  - Case 2: n is odd.
    - So n=2k+1 for some k (by definition and existential instantiation).
    - 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 and existential generalization). 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).

- *Definition* (of odd integers):
  An integer n is **odd** iff $\exists k \in \mathbb{Z}, n = 2 \cdot k + 1$.

61

Theorem: An absolute value of a product of real numbers is equal to the product of their absolute values. $\forall x, y \in \mathbb{R}\ |xy| = |x| \cdot |y|$

- Let's try to understand this definition:

Definition (of absolute value):
An absolute value of a real number r, denoted $|r|$, is equal to r if $r \geq 0$, and to $-r$ otherwise (that is, for $r < 0$).

□ (Done).

62

Theorem: An absolute value of a product of real numbers is equal to the product of their absolute values. $\forall x, y \in \mathbb{R}\ |xy| = |x| \cdot |y|$

- *Proof*:
  - Let x and y be arbitrary real numbers.
  - Case 1: Both $x \geq 0$ and $y \geq 0$
  - Case 2: $x \geq 0$ and $y < 0$
  - Case 3: $x < 0$ and $y \geq 0$
  - Case 4: Both $x < 0$ and $y < 0$
  - By universal generalization, $\forall x, y \in \mathbb{R}\ |xy| = |x| \cdot |y|$

Definition (of absolute value):
An absolute value of a real number r, denoted $|r|$, is equal to r if $r \geq 0$, and to $-r$ otherwise (that is, for $r < 0$).

□ (Done).

63

Theorem: An absolute value of a product of real numbers is equal to the product of their absolute values. $\forall x, y \in \mathbb{R}\ |xy| = |x| \cdot |y|$

- *Proof*:
  - Let x and y be arbitrary real numbers.
  - Case 1: Both $x \geq 0$ and $y \geq 0$
    - By definition of the absolute value, $|x| = x$ and $|y| = y$.
    - So $|x| \cdot |y| = xy = |xy|$, since $xy \geq 0$.
  - Case 2: $x \geq 0$ and $y < 0$
    - Then $|x| = x$, $|y| = -y$. So $|x| \cdot |y| = -xy$.
    - Since $xy \leq 0$, $|xy| = -xy$ too. So $|x| \cdot |y| = -xy = |xy|$
  - Case 3: $x < 0$ and $y \geq 0$
    - Same as Case 2, interchanging x and y
  - Case 4: Both $x < 0$ and $y < 0$
    - Since product of negative numbers is positive, $|xy| = xy$.
    - On the other hand, $|x| \cdot |y| = (-x) \cdot (-y) = xy$. So $|x| \cdot |y| = xy = |xy|$
  - By universal generalization, $\forall x, y \in \mathbb{R}\ |xy| = |x| \cdot |y|$

Definition (of absolute value):
An absolute value of a real number r, denoted $|r|$, is equal to r if $r \geq 0$, and to $-r$ otherwise (that is, for $r < 0$).

□ (Done).

64

Without loss of generality

- *Proof*:
  - .....
  - Case 2: $x \geq 0$ and $y < 0$
    - Then $|x| = x$, $|y| = -y$. So $|x| \cdot |y| = -xy$.
    - Since $xy < 0$, $|xy| = -xy$ too. So $|x| \cdot |y| = -xy = |xy|$
  - Case 3: $x < 0$ and $y \geq 0$
    - Same as Case 2, interchanging x and y
  - .....

We did not need a separate proof for Case 3, since it was essentially identical to case 2, with roles of x and y exchanged.

There, we could use the phrase "**without loss of generality**" (abbreviated "**wlog**"), and combine cases 2 and 3: "Case 2: one of the numbers is nonnegative and the other negative. Without loss of generality, let x be nonnegative, y negative. "

This can be used when one case follows from another in very few simple steps, or the proof is the same.

65

66

Summary: proof techniques

- Proving an existential statement $\exists x \in S\ F(x)$:
  - If possible, give a constructive proof by constructing a witness
    - When does not work, can try to prove that $\forall x\ \neg F(x) \rightarrow FALSE$
- Proving a universal statement $\forall x \in S\ F(x)$:
  - Start with universal instantiation: take an arbitrary $n \in S$
  - Use definitions, axioms, etc to prove $F(n)$
    - If $F(n)$ is $G(n) \rightarrow H(n)$, assume $G(n)$ and derive $H(n)$
    - Use existential instantiation/generalization for $\exists x$ in definitions
  - Replacing $F(x)$ with an equivalent formula that's easier to prove
    - Before or after the universal instantiation.
    - Common tricks: proof by contraposition, by contradiction, by cases.
  - Finish with universal generalization.
- *We will see a few other methods, in particular, proof by induction.*

67

Proofs for other types of statements

- "The following are equivalent" $\forall x \in S\ G(x) \leftrightarrow H(x)$
  - prove $\forall x \in S\ \big(G(x) \rightarrow H(x)\big) \wedge \big(H(x) \rightarrow G(x)\big)$
  - When more than two formulas, can prove a chain of implications:
    - To show that $F(n), G(n), H(n), \ldots$ are equivalent, prove $\big(F(n) \rightarrow G(n)\big) \wedge \big(G(n) \rightarrow H(n)\big) \wedge \big(H(n) \rightarrow F(n)\big)$, in whichever order is most convenient.
- "There is a unique x" … $\exists x\ F(x) \wedge \forall y \neq x\ \neg F(x)$
  - Sometimes written $\exists! x\ F(x)$
  - Note a shorthand: $\forall y \neq x\ \neg F(x)$ means $\forall y\ (y \neq x \rightarrow \neg F(x))$

68

Language of proofs: Theorems, lemmas, claims…

- **Theorem:** usually a major result, often requiring a long proof.
  - Though technically any statement true in a theory is a **theorem** .
- **Lemma**: a technical statement used in a proof of a theorem
  - Some lemmas are more famous than theorems they were designed to prove!
- **Claim/fact/observation**: An easily provable statement used in subsequent proofs.
  - Often stated without a proof.
- **Corollary**: A statement that easily follows from a theorem/lemma or their proofs.
- **Conjecture**: A statement that has not been proven, usually believed to be true
  - Example: Goldbach's conjecture states that every even integer > 2 is a sum of two primes.

69

Proofs are an art!

- As with art, to learn to do proofs look at examples
  - See if an existing proof can be modified to prove what you need.
    - Can a proof that $\sqrt{2}$ is irrational be changed into a proof that $\sqrt{3}$ is irrational?
- Often, the same statement can be proven many different ways.
  - There are no precise rules for when to use which trick – try whichever one you like, and if you cannot get it to work, try another.
  - Often choose whichever way the proof is most beautiful.
- And as with any art – the more you practice, the better you become!

70