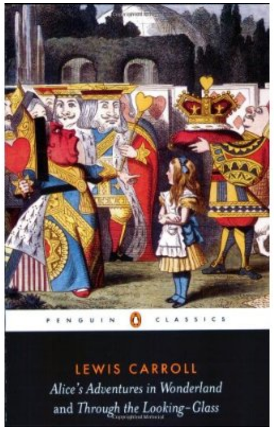
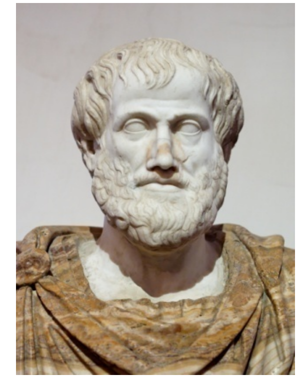


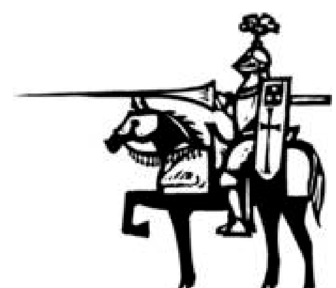


COMP 1002

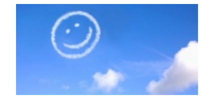
Intro to Logic for Computer Scientists

Lecture 15

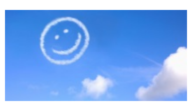
B 5 2 J



Puzzle: better than nothing

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

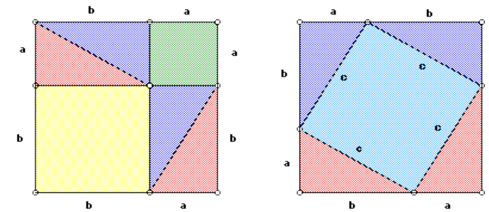
- Therefore, a burger is better than eternal bliss.

 $\leq$ $\leq$ 

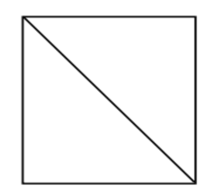
Is there anything wrong with this argument?

The premise: "Nothing is better than eternal bliss" is not true.

Types of proofs

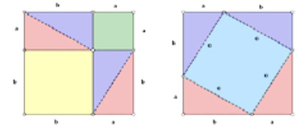


- Direct proof of $\forall x\, F(x)$
  - Show that $F(x)$ holds for arbitrary x, then use universal generalization.
    - Often, $F(x)$ is of the form $G(x) \to H(x)$
  - Example: A sum of two even numbers is even.
  - Example: Difference of numbers congruent mod d.
- Proof by cases
  - If can write $\forall x\, F(x)$ as $\forall x (G_1(x) \vee G_2(x) \vee \cdots \vee G_k(x)) \to H(x)$, prove $(G_1(x) \to H(x)) \wedge (G_2(x) \to H(x)) \wedge \cdots \wedge (G_k(x) \to H(x))$
  - 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.



Instantiation/generalization

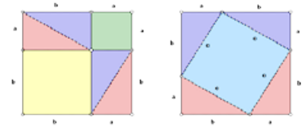
- If $\forall\ x \in S\ \ F(x)$ is true for some formula $F(x)$, when you take any specific element $a \in S$, then $F(a)$ must be true.
  - This is called the **universal instantiation** rule.
    - $\forall x \in \mathbb{N}\ \ (x > -1)$
    - $\therefore\ \ 5 > -1$
- If you prove $F(a)$ without any assumptions about a other than $a \in S$, then $\forall x \in S, F(x)$
  - This is called **universal generalization**.



Direct proof

- Direct proof of $\forall x \in S \;\; F(x)$: show directly that $F(x)$ holds for arbitrary *n* $\in S$, 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.

$\square$ (Done).

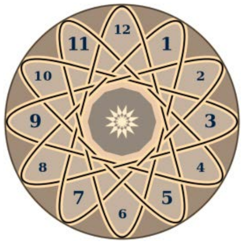


Direct proof

- *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.
  - $\forall x, y \in \mathbb{Z}\ \ Even(x) \land Even(y) \rightarrow Even(x+y)$.
- *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: $\forall x, y \in \mathbb{Z}\ \ Even(x) \land Even(y) \rightarrow Even(x+y)$.
    - 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 $0 \leq r < d$
  - 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.

Calendars vs mod

May 2017

Calendarpedia
Your source for calendars

Wk	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
18	1 Early May Bank Holiday (May Day)	2	3	4	5	6	7
19	8	9	10	11	12	13	14
20	15	16	17	18	19	20	21
21	22	23	24	25	26	27	28
22	29 Spring Bank Holiday	30	31	1	2	3	4

© www.calendarpedia.co.uk
Data provided 'as is' without warranty

October 2017

Calendarpedia
Your source for calendars

Wk	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
39	25	26	27	28	29	30	1
40	2	3	4	5	6	7	8
41	9	10	11	12	13	14	15
42	16	17	18	19	20	21	22
43	23	24	25	26	27	28	29
44	30	31	1	2	3	4	5

© www.calendarpedia.co.uk
Data provided 'as is' without warranty

- Wednesdays are day = 3 (mod 7)

- Wednesdays are day = 4 (mod 7)

Calendars vs mod

- Wednesdays are day = 3 (mod 7)
- Orange stickers are number = 3 (mod 8)

• Example: day of the week.
– Feb 1st and Feb 15th are both on Wednesday: $1 \equiv 15\ (mod\ 7)$
• 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....

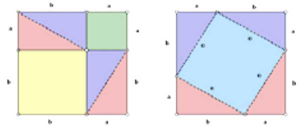
Modular arithmetic in CS

- Example: day of the week.
  - Feb 1st and Feb 15th are both on Wednesday: $1 \equiv 15\ (mod\ 7)$
- 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 credit cards, codes, ISBNs, etc.
    - E.g., look at combination of digits mod 10 to check if a credit card number is valid.
  - Public key crypto, RSA....

Direct proof example

- *Theorem*: for all integers n,m and d, where $d > 0$, if $n \equiv m \pmod d$ then there exists an integer k such that n$= m + kd$
  - $\forall x, y, z \ (z > 0 \land x \equiv y \pmod z) \to \exists u \ \ x = y + uz$
- *Proof*:
  - Let n, m, d be arbitrary integers such that $d > 0$ and $n \equiv m \pmod d$
    - 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 $n \equiv m \pmod d$, $\forall x, y, z \ (z > 0 \land x \equiv y \pmod z) \to \exists u \ \ x = y + uz$
    - By universal generalization.

□ (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 $\forall x \; F(x)$ is true.

□ (Done).

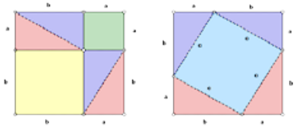
Pigeonhole Principle

- 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.

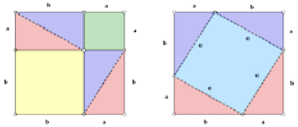
- The Pigeonhole Principle:
  - If there are n pigeons
  - And n-1 pigeonholes
  - Then if every pigeon is in a pigeonhole
  - At least two pigeons sit in the same hole

Proof by contraposition.



- *Theorem (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.
  - $\forall x \in \mathbb{N}\ \big(\forall y \in \{1,..,x+1\}\ \exists z \in \{1,..,x\}\ Sits(y,z)\big) \rightarrow$
    $(\exists u \in \{1,..,x+1\}\ \exists v \in \{1,..,x+1\}\ \exists w \in \{1,..,x\}$
    $(u \neq v \land Sits(u,w) \land Sits(v,w)))$
- *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 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).



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.

□ (Done).

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).
    - A letter numbered x by a letter numbered x-3 mod 26.
    - For example, F would be replaced by C, and A by X

- Suppose he sent the following message.
  - QOBXPROB FK QEB ZXSB
- What does it say?