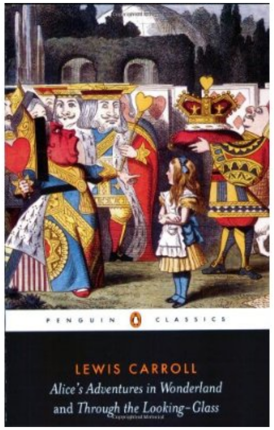
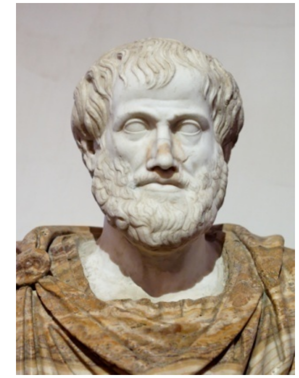


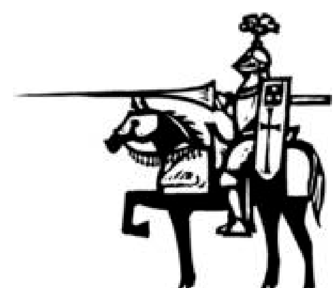


COMP 1002

Intro to Logic for Computer Scientists

Lecture 14

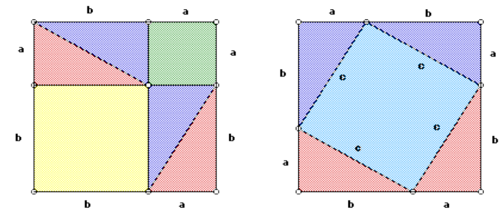
B 5 2 J



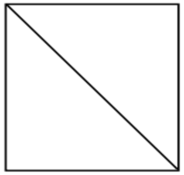
Admin stuff

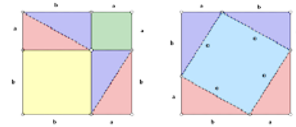
- Assignments schedule? Split a2 and a3 in two (A2,3,4,5) , 5% each. A2 due Feb 17th.
- Midterm date? March 2nd.
- No office hour on Feb 9th

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 $G(x) \rightarrow H(x)$
  - 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 $\forall x (G_1(x) \vee G_2(x) \vee \cdots \vee G_k(x)) \rightarrow H(x)$, prove $(G_1(x) \rightarrow H(x)) \wedge (G_2(x) \rightarrow H(x)) \wedge \cdots \wedge (G_k(x) \rightarrow H(x))$
  - 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.

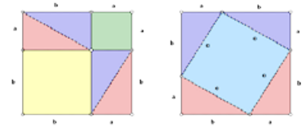




Direct proof

- Direct proof of $\forall x \in S\ \ F(x)$: 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 $G(x) \to H(x)$, then assume $G(n)$ is true, and from that (and axioms, etc) derive H(n)
    - That proves $G(n) \to H(n)$
  - Now use universal generalization to conclude that $\forall x\ F(x)$ is true.

□ (Done).

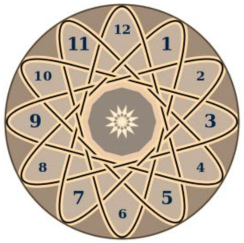


Direct proof

- *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.

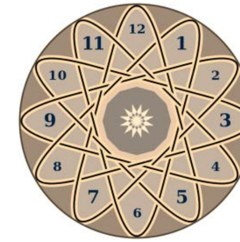
□ (Done).

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:
    - $10 \equiv 16\ (\text{mod } 3)$, 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

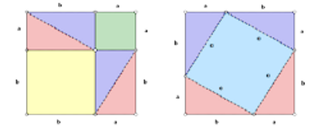


- Example: day of the week.
  - Feb 1st and Feb 15th are both on Wednesday: $1 \equiv 15 \ (mod\ 7)$
- Hash functions: distribute random data evenly among d memory locations
  - Often take h(k) = k mod p for some prime p. If $k \equiv \ell \ (mod\ p)$, get a collision.
- Cryptography:
  - Parity checks in codes, ISBNs, etc.
  - Public key crypto, RSA….

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.

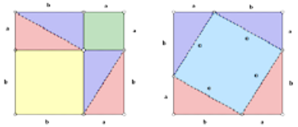
□ (Done).



Proof by cases

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

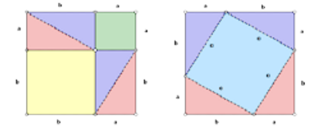
□ (Done).



Proof by cases.

- *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 $\forall x \in \mathbb{Z}\ Odd(x + (x + 1))$.

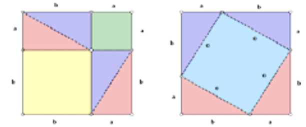
□ (Done).



Proof by cases

- *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 $\forall x, y \in \mathbb{R}\ \ |x + y| \leq |x| + |y|$.

□ (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).

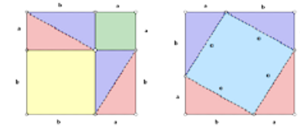
Pigeonhole Principle

- 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.

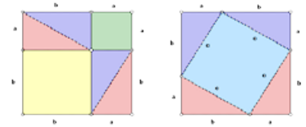
- The Pigeonhole Principle:
  - If there are n pigeons
  - And n-1 pigeonholes
  - Then if every pigeon is in a pigeonhole
  - At least two pigeons sit in the same hole

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.
  - $\forall x \in \mathbb{N} \; \big(\forall\, y \leq x \,\exists\, z < x \;\; Sits(y,z)\big) \rightarrow$
    $\exists\, u \leq x \,\exists\, v \leq x \,\exists w < x \;\; (u \neq v \wedge Sits(u,w) \wedge Sits(v,w))$
- *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.

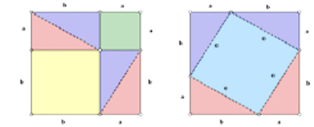
□ (Done).



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.

□ (Done).

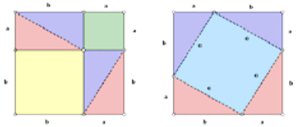


Proof by contradiction

– To prove $\forall x \; F(x)$, prove $\forall x \neg F(x) \rightarrow FALSE$

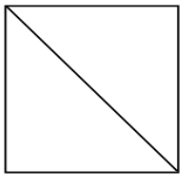
- Universal instantiation: “let n be an arbitrary element of the domain S of $\forall x$ ”
- Suppose that $\neg F(n)$ is true.
- Derive a contradiction.
- Conclude that $F(n)$ is true.
- By universal generalization, $\forall x \, F(x)$ is true.

$\square$ (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).

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?