Discrete Mathematics

1-2. Basic Proof Methods

Nature & Importance of Proofs

- In mathematics, a *proof* is:
  - a *correct* (well-reasoned, logically valid) and *complete* (clear, detailed) argument that rigorously & undeniably establishes the truth of a mathematical statement.
- Why must the argument be correct & complete?
  - *Correctness* prevents us from fooling ourselves.
  - *Completeness* allows anyone to verify the result.
- In this course (& throughout mathematics), a very high standard for correctness and completeness of proofs is demanded!!

Applications of Proofs

- An exercise in clear communication of logical arguments in any area of study.
- The fundamental activity of mathematics is the discovery and elucidation, through proofs, of interesting new theorems.
- Theorem-proving has applications in program verification, computer security, automated reasoning systems, *etc*.
- Proving a theorem allows us to rely upon on its correctness even in the most critical scenarios.

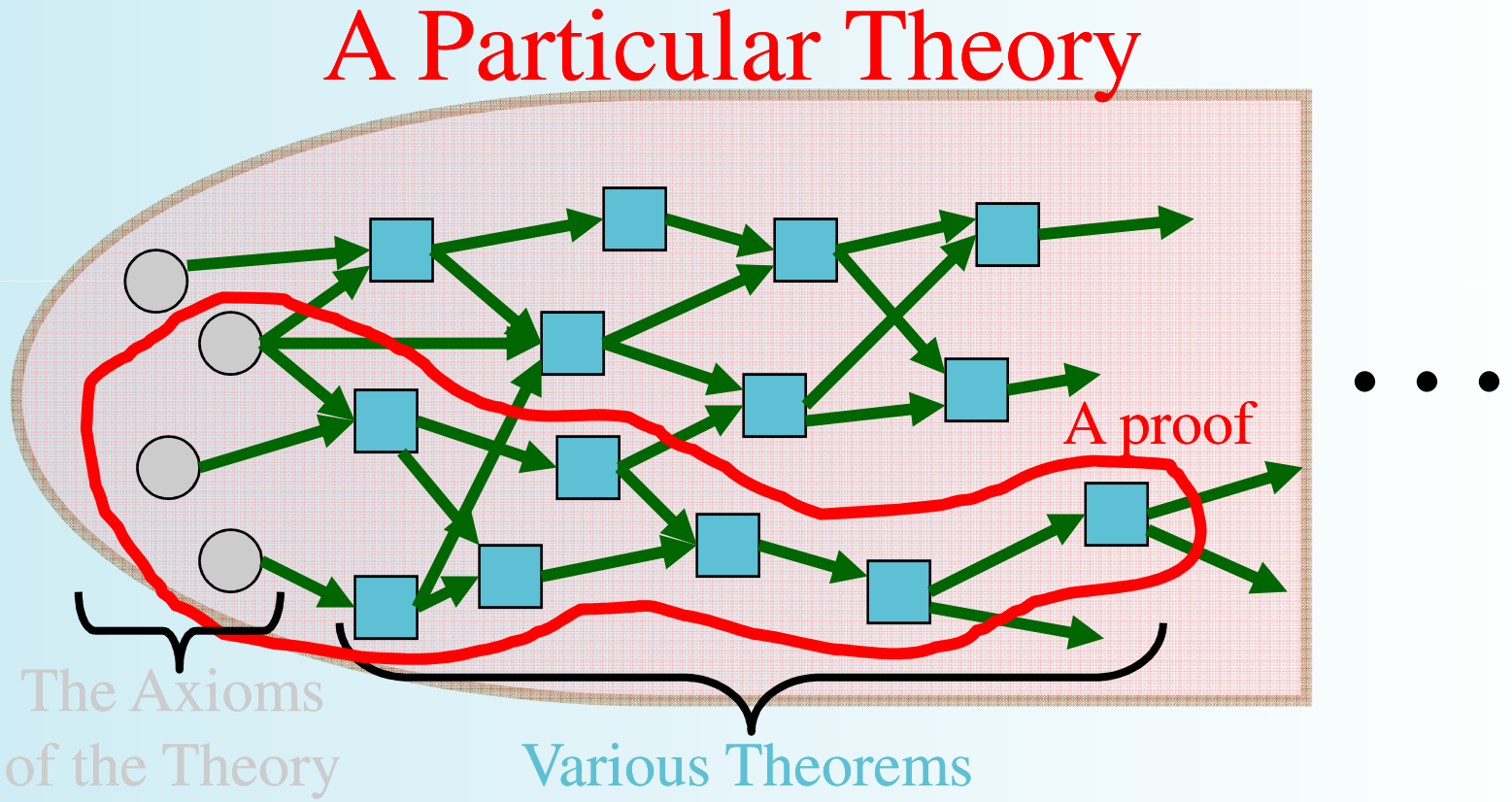
Proof Terminology

- *Theorem*
  - A statement that has been proven to be true.
- *Axioms, postulates, hypotheses, premises*
  - Assumptions (often unproven) defining the structures about which we are reasoning.
- *Rules of inference*
  - Patterns of logically valid deductions from hypotheses to conclusions.

More Proof Terminology

- *Lemma* - A minor theorem used as a stepping-stone to proving a major theorem.
- *Corollary* - A minor theorem proved as an easy consequence of a major theorem.
- *Conjecture* - A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)
- *Theory* – The set of all theorems that can be proven from a given set of axioms.

Graphical Visualization



Inference Rules - General Form

- *Inference Rule*
  - Pattern establishing that if we know that a set of *antecedent* statements of certain forms are all true, then a certain related *consequent* statement is true(valid arguments).
- *antecedent 1*
  antecedent 2 …
  ∴ *consequent*

"∴" means "therefore"

Inference Rules & Implications

- Each logical inference rule corresponds to an implication that is a tautology.
- *antecedent 1*
  antecedent 2 …
  ∴ consequent
  Inference rule
- Corresponding tautology:
  $((ante.\ 1) \wedge (ante.\ 2) \wedge \ldots) \rightarrow consequent$

IMPLICATION

I_1 $P \wedge Q \Rightarrow P$

I_2 $P \wedge Q \Rightarrow Q$

I_3 $P \Rightarrow P \vee Q$

I_4 $Q \Rightarrow P \vee Q$

I_5 $\neg P \Rightarrow P \rightarrow Q$

I_6 $Q \Rightarrow P \rightarrow Q$

I_7 $\neg(P \rightarrow Q) \Rightarrow P$

I_8 $\neg(P \rightarrow Q) \Rightarrow \neg Q$

I_9 $P, Q \Rightarrow P \wedge Q$

I_{10} $\neg P, P \vee Q \Rightarrow Q$

I_{11} $P, P \rightarrow Q \Rightarrow Q$

I_{12} $\neg Q, P \rightarrow Q \Rightarrow \neg P$

I_{13} $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$

I_{14} $P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$

I_{15} $(\forall x)A(x) \vee (\forall x)B(x) \Rightarrow (\forall x)(A(x) \vee B(x))$

I_{16} $(\exists x)(A(x) \wedge B(x)) \Rightarrow (\exists x)A(x) \wedge (\exists x)B(x)$

EQUIVALENCE

E_1 $\neg\neg P \Leftrightarrow P$
E_2 $P \wedge Q \Leftrightarrow Q \wedge P$
E_3 $P \vee Q \Leftrightarrow Q \vee P$
E_4 $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
E_5 $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
E_6 $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
E_7 $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
E_8 $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
E_9 $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
E_{10} $P \vee P \Leftrightarrow P$
E_{11} $P \wedge P \Leftrightarrow P$
E_{12} $R \vee (P \wedge \neg P) \Leftrightarrow R$
E_{13} $R \wedge (P \vee \neg P) \Leftrightarrow R$
E_{14} $R \vee (P \vee \neg P) \Leftrightarrow T$
E_{15} $R \wedge (P \wedge \neg P) \Leftrightarrow F$
E_{16} $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
E_{17} $\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$
E_{18} $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
E_{19} $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$
E_{20} $\neg(P \leftrightarrow Q) \Leftrightarrow (P \leftrightarrow \neg Q)$
E_{21} $(P \leftrightarrow Q) \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
E_{22} $(P \leftrightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$
E_{23} $(\exists x)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$
E_{24} $(\forall x)(A(x) \wedge B(x)) \Leftrightarrow (\forall x)A(x) \wedge (\forall x)B(x)$
E_{25} $\neg(\exists x)A(x) \Leftrightarrow (\forall x)\neg A(x)$
E_{26} $\neg(\forall x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
E_{27} $(\forall x)(A \vee B(x)) \Leftrightarrow A \vee (\forall x)B(x)$
E_{28} $(\exists x)(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)B(x)$
E_{29} $(\forall x)A(x) \rightarrow B \Leftrightarrow (\exists x)(A(x) \rightarrow B)$
E_{30} $(\exists x)A(x) \rightarrow B \Leftrightarrow (\forall x)(A(x) \rightarrow B)$
E_{31} $A \rightarrow (\forall x)B(x) \Leftrightarrow (\forall x)(A \rightarrow B(x))$
E_{32} $A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$
E_{33} $(\exists x)(A(x) \rightarrow B(x)) \Leftrightarrow (\forall x)A(x) \rightarrow \exists x B(x))$

Formal Proofs

- A formal proof of a conclusion C, given premises p_1, p_2,…,p_n consists of a sequence of *steps*, each of which applies some inference rule to premises or to previously-proven statements (as antecedents) to yield a new true statement (the consequent).
- Inference Rules
  - Rule ***P*** : premise
  - Rule ***T*** : tautology
  - Rule ***CP*** : conditional premise
- A proof demonstrates that *if* the premises are true, *then* the conclusion is true.

Example 1

- Suppose we have the following premises:
  "It is not sunny and it is cold."
  "We will swim only if it is sunny."
  "If we do not swim, then we will canoe."
  "If we canoe, then we will be home early."
- Given these premises, prove the theorem
  "We will be home early" using inference rules.

Example 1 (*cont.*)

- Let us adopt the following abbreviations:
  - *sunny* = **"It is sunny"**; *cold* = **"It is cold"**; *swim* = **"We will swim"**; *canoe* = **"We will canoe"**; *early* = **"We will be home early"**.
- Then, the premises can be written as:
  (1) $\neg sunny \wedge cold$ (2) $swim \rightarrow sunny$
  (3) $\neg swim \rightarrow canoe$ (4) $canoe \rightarrow early$

Example 1 (*cont.*)

Step	Inference Rule
(1) $\neg sunny \wedge cold$	***P***
(2) $\neg sunny$	***T***, (1) and I_1
(3) $swim \rightarrow sunny$	***P***
(4) $\neg swim$	***T***, (2), (3) and I_{12}
(5) $\neg swim \rightarrow canoe$	***P***
(6) $canoe$	***T***, (4), (5) and I_{11}
(7) $canoe \rightarrow early$	***P***
(8) $early$	***T***, (6), (7), and I_{11}

Example 2

- Show that (R→S) can be derived from (P →(Q →S)), (¬R ∨ P), and Q

  (Instead of deriving R →S directly, we shall include R as an additional premise and show S can be derive from there premises.)

Step		Inference Rule
(1)	¬R ∨ P	***P***
(2)	R	***P*** (assumed premise)
(3)	P	***T***, (1), (2) and I_{10}
(4)	P→(Q →S)	***P***
(5)	Q →S	***T***, (3), (4) and I_{11}
(6)	Q	***P***
(7)	S	***T***, (5), (6) and I_{11}
(8)	R → S	***CP***, (2), (7)

Example 3

- Show that $S \vee R$ can be derived from $(P \vee Q)$, $(P \rightarrow R)$ and $(Q \rightarrow S)$

Step		Inference Rule
(1)	$P \vee Q$	***P***
(2)	$\neg P \rightarrow Q$	***T,*** (1) , E_1 and E_{16}
(3)	$Q \rightarrow S$	***P***
(4)	$\neg P \rightarrow S$	***T,*** (2), (3), and I_{13}
(5)	$\neg S \rightarrow P$	***T,*** (4) , E_{18} and E_1
(6)	$P \rightarrow R$	***P***
(7)	$\neg S \rightarrow R$	***T,*** (5), (6), and I_{13}
(8)	$S \vee R$	***T,*** (7), E_{16} and E_1

Inference Rules for Quantifiers

- $\dfrac{\forall x\, P(x)}{\therefore P(o)}$ **Universal instantiation (US)**
  (substitute *any* object o)
- $\dfrac{P(g)}{\therefore \forall x\, P(x)}$ (for g a *general* element of u.d.)
  Universal generalization (UG)
- $\dfrac{\exists x\, P(x)}{\therefore P(c)}$ **Existential instantiation (ES)**
  (substitute a *new constant* c)
- $\dfrac{P(o)}{\therefore \exists x\, P(x)}$ (substitute any extant object o)
  Existential generalization (EG)

Example 4

- Show that $(\forall x)\,(P(x) \rightarrow Q(x)) \wedge (\forall x)\,(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)\,(P(x) \rightarrow R(x))$

Step	Inference Rule
(1) $(\forall x)\,(P(x) \rightarrow Q(x))$	***P***
(2) $P(y) \rightarrow Q(y)$	***US***, (1)
(3) $(\forall x)\,(Q(x) \rightarrow R(x))$	***P***
(4) $Q(y) \rightarrow R(y)$	***US***, (3)
(5) $P(y) \rightarrow R(y)$	***T***, (2), (4) and I_{13}
(6) $(\forall x)\,(P(x) \rightarrow R(x))$	***UG***, (5)

Example 5

- Show that from

(a) $(\exists x)\,(F(x) \wedge S(x)) \rightarrow (\forall y)\,(M(y) \rightarrow W(y))$

(b) $(\exists y)\,(M(y) \wedge \neg W(y))$

the conclusion $(\forall x)\,(F(x) \rightarrow \neg\, S(x))$ follows.

	Step	Inference Rule
(1)	$(\exists y)\,(M(y) \wedge \neg W(y))$	***P***
(2)	$M(z) \wedge \neg W(z)$	***ES***, (1)
(3)	$\neg\,(M(z) \rightarrow W(z))$	***T***, (2) and E_{17}
(4)	$(\exists y) \neg\,(M(y) \rightarrow W(y))$	***EG***, (3)
(5)	$\neg(\forall y)(M(y) \rightarrow W(y))$	***T***, (4) and E_{26}
(6)	$(\exists x)\,(F(x) \wedge S(x)) \rightarrow (\forall y)\,(M(y) \rightarrow W(y))$	***P***
(7)	$\neg(\exists x)\,(F(x) \wedge S(x))$	***T***, (5), (6) and I_{12}
(8)	$(\forall x) \neg(F(x) \wedge S(x))$	***T***, (7) and E_{25}
(9)	$\neg(F(x) \wedge S(x))$	***US***, (8)
(10)	$F(x) \rightarrow \neg\, S(x)$	***T***, (9), E_8 and E_{16}
(11)	$(\forall x)\,(F(x) \rightarrow \neg\, S(x))$	***UG***, (10)

Restriction

- UG applicable variable should not be free in any of the given premises
- UG should not be applied to the free variable resulting from ES making other variable free in a prior step.

$D(u,v)$: u is divided by v.

$D(5,5)$ and $D(10,5)$ are TRUE, then $(\exists u)D(u,5)$ is TRUE.

(1) $(\exists u)D(u,5)$ P

(2) $D(x,5)$ *by ES,* (1)

(3) $(\forall y)D(y,5)$ *by UG,* (2) WRONG!

Proof Methods for Implications

For proving implications $p \rightarrow q$, we have:

- *Direct* proof: Assume p is true, and prove q.
- *Indirect* proof: Assume $\neg q$, and prove $\neg p$.
- *Vacuous* proof: Prove $\neg p$ by itself.
- *Trivial* proof: Prove q by itself.
- Proof by cases:
  Show $p \rightarrow (a \vee b)$, and $(a \rightarrow q)$ and $(b \rightarrow q)$.

Example of Direct Proof

- *Definition:*

  An integer n is called *odd* iff $n=2k+1$ for some integer k;

  n is *even* iff $n=2k$ for some k.

- *Axiom:*

  Every integer is either odd or even.

- *Theorem:*

  (For all numbers n) If n is an odd integer, then n^2 is an odd integer.

- *Proof:*

  If n is odd, then $n = 2k+1$ for some integer k.

  Thus, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

  Therefore n^2 is of the form $2j + 1$ (with j the integer $2k^2 + 2k$), thus n^2 is odd. □

Example of Indirect Proof

- *Theorem:*

  (For all integers n)
  If $3n+2$ is odd, then n is odd.

- *Proof:*

  Suppose that the conclusion is false, *i.e.*, that n is even.
  Then $n=2k$ for some integer k.

  Then $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$.

  Thus $3n+2$ is even, because it equals $2j$ for integer $j = 3k+1$.
  So $3n+2$ is not odd.

  We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n+2 \text{ is odd})$, thus its contra-positive $(3n+2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. □

Example of Vacuous Proof

- *Theorem:*

  (For all n) If n is both odd and even, then $n^2 = n + n$.

- *Proof:*

  The statement "n is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. □

Example of Trivial Proof

- *Theorem:*

  (For integers n) If n is the sum of two prime numbers, then either n is odd or n is even.

- *Proof:*

  Any integer n is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent. Thus the implication is true trivially. □

Proof by Contradiction

- A method for proving p.
- Assume $\neg p$, and prove both q and $\neg q$ for some proposition q.
- Thus $\neg p \rightarrow (q \wedge \neg q)$
- $(q \wedge \neg q)$ is a trivial contradition, equal to **F**
- Thus $\neg p \rightarrow \mathbf{F}$, which is only true if $\neg p = \mathbf{F}$
- Thus p is true.

Proving Existentials

- A proof of a statement of the form $\exists x\, P(x)$ is called an *existence proof*.
- If the proof demonstrates how to actually find or construct a specific element a such that $P(a)$ is true, then it is a *constructive* proof.
- Otherwise, it is *nonconstructive*.

Constructive Existence Proof

- *Theorem:*

  There exists a positive integer n that is the sum of two perfect cubes in two different ways:

  - equal to $j^3 + k^3$ and $l^3 + m^3$ where j, k, l, m are positive integers, and $\{j,k\} \neq \{l,m\}$

- *Proof:*

  Consider $n = 1729$, $j = 9$, $k = 10$, $l = 1$, $m = 12$. Now just check that the equalities hold.

Nonconstructive Existence Proof

- *Theorem:*

  There are infinitely many prime numbers.

- *Proof:*

  Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is *no* largest prime number.

  I.e., show that for any number, there is a larger number that is *also* prime.

  More generally: For *any* number, $\exists$ a larger prime.

  Formally: Show $\forall n \, \exists p \, ((p>n) \wedge (p \text{ is prime}))$.

Nonconstructive Existence Proof (cont.)

Given $n>0$, prove there is a prime $p>n$.

Consider $x = n!+1$. Since $x>1$, we know
$(x \text{ is prime}) \vee (x \text{ is composite})$.

Case 1: x is prime.

Obviously $x>n$, so let $p=x$ and we're done.

Case 2: x has a prime factor p.

But if $p \leq n$, then $x \bmod p = 1$.

So $p>n$, and we're done.

Uniqueness Proofs

- Some theorems assert the existence of a unique element with a particular property.
- To prove a statements of this type, we show following two parts.
  - Existence: element x with a desired property exists
  - Uniqueness: if $y \neq x$, then y does not have the desired property

Example of Uniqueness Proofs

- **Theorem:**
  "Every integer has a unique additive inverse."
- **Proof:** If p is an integer, we find that $p+q=0$ whe $q=-p$ and q is also an integer. Consequently, there exists an integer q such that $p+q=0$. (Existence)

  if r is an integer with $r \neq q$ such that $p+r=0$. then $p+q=p+r$. So We can show $q=r$, which contradicts our assumption $r \neq q$. Consequently, there is a unique integer q such that $p+q=0$. □

Exercise

1. Prove that the square of an even number is an even number using
   (a) A direct proof
   (b) An indirect proof
   (c) A proof by contradiction

2. Prove formally using inference rules that *$R \wedge (P \vee Q)$ logically follows from $(P \vee Q)$, $(Q \rightarrow R)$, $(P \rightarrow M)$, and $\neg M$.*