CS 214
Introduction to Discrete Structures

Chapter 2
Proofs, Induction, and Number Theory

Mikel D. Petty, Ph.D.

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

CMSA
Center for Modeling, Simulation, and Analysis

Chapter sections and objectives

- 2.1 Proof Techniques
  - Prove conjectures using direct proof, proof by contrapositive, and proof by contradiction
- 2.2 Induction
  - Recognize when a proof by induction is appropriate
  - Write proofs by induction using either the first or second principle of induction
- 2.3 More on Proof of Correctness
- 2.4 Number Theory

Not covered in CS 214

Sample problem

The nonprofit organization at which you volunteer has received donations of 792 bars of soap and 400 bottles of shampoo. You want to create packages to distribute to homeless shelters such that each package contains the same number of shampoo bottles and each package contains the same number of bars of soap.

How many packages can you create?

2.1 Proof Techniques

Arguments and theorems

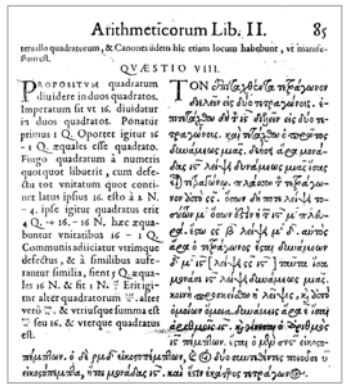
- Formal arguments of Chapter 1
  - Form $P \rightarrow Q$, where P, Q compound wffs
  - Objective: show argument is valid
  - Intrinsically true, based on logical structure
    - Propositional logic; truth of P implied truth of Q
    - Predicate logic; $P \rightarrow Q$ true under all interpretations
- Theorems of Chapter 2
  - Form $P \rightarrow Q$, where P, Q compound wffs
  - Objective: show conclusion is true
  - Contextually true, based on domain knowledge
    - Propositional logic; P true, therefore Q true
    - Predicate logic; P and $P \rightarrow Q$ true under specific interpretation
  - Combine formal logic and domain knowledge
  - Often stated less formally than formal arguments

Inductive and deductive reasoning

- Inductive reasoning
  - Observe instances where $P \rightarrow Q$
  - Assume $P \rightarrow Q$ always true; known as theory
  - Inductive reasoning in science: acceptable
  - Inductive reasoning in math and CS: not acceptable
- Deductive reasoning
  - State $P \rightarrow Q$ as conjecture
  - Prove using logic and domain knowledge; $P \rightarrow Q$ becomes theorem
  - Disprove by showing instance when not true; $P \rightarrow Q$ becomes fallacy
  - Deductive reasoning in science: not possible
  - Deductive reasoning in math and CS: acceptable

Inductive and deductive reasoning in math

- Conjecture: "Fermat's Last Theorem"
  - $x^n + y^n = z^n$ has no integer solutions for $n > 2$, $x, y, z \neq 0$
  - "This margin is too narrow" (1637)
- Inductive reasoning
  - Shown true by hand for $n \leq 14$ (1832)
  - Shown true by computer for $n \leq 4 \cdot 10^6$
  - Conjecture not proven for all n
- Deductive reasoning
  - Multiple incomplete and incorrect proofs
  - Proven true for all n by Wiles (1993)
  - Proof used methods unknown to Fermat


Arithmeticorum Lib. II. 85

QVÆSTIO VIII.

PROPOSITVM quadratum dividere in duos quadratos.


Wiles © C. J. Mozzochi, Princeton NJ

Inductive reasoning and mathematical induction

- Inductive reasoning ≠ mathematical induction
- Inductive reasoning; way to learn about world, develop conjectures, discern patterns
- Mathematical induction; valid proof technique, a type of deductive reasoning
- Confusingly, both AKA “induction”

Proof techniques

- Proof techniques
  - Disproof by counterexample (§ 2.1)
  - Exhaustive proof (§ 2.1)
  - Direct proof (§ 2.1)
  - Proof by contraposition (§ 2.1)
  - Proof by contradiction (§ 2.1)
  - Mathematical induction (§ 2.2)

  } AKA "indirect proof"
- Differences
  - Process of proving theorem
  - Underlying logical structure
- Similarities
  - Prove $P \rightarrow Q$
  - Proofs based on valid argument, domain knowledge

Example disproof by counterexample

Factorial: $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1$

Example: $3! = 3 \cdot 2 \cdot 1 = 6$

Conjecture: For every positive integer n, $n! \leq n^2$

n	$n!$	n^2	$n! \leq n^2$
1	1	1	true
2	2	4	true
3	6	9	true
4	24	16	false

looks good so far …

counterexample

Example 1

Example disproof by counterexample

Conjecture
If a and b are integers and $a^2 = b^2$, then $a = b$.

Counterexample
$1^2 = -1^2$, but $1 \neq -1$.

Example 4.1.4 [Epp, 2011]

Exhaustive proof

- Goal: prove $P \rightarrow Q$
- Method: show conjecture holds for each case, i.e., each object in collection
- Applicable when conjecture $P \rightarrow Q$ is about finite collection of objects
- Exhaustive proof vs. "proof by example"
  - Exhaustive proof covers all possible cases
  - Exhaustive proof is a valid proof method
  - "Proof by example" covers a subset of the cases
  - "Proof by example" is not a valid proof method

Example exhaustive proof

Conjecture: If an integer between 1 and 20 inclusive is divisible by 6, then it is also divisible by 3.

Proof: Show true for each x, $1 \leq x \leq 20$.

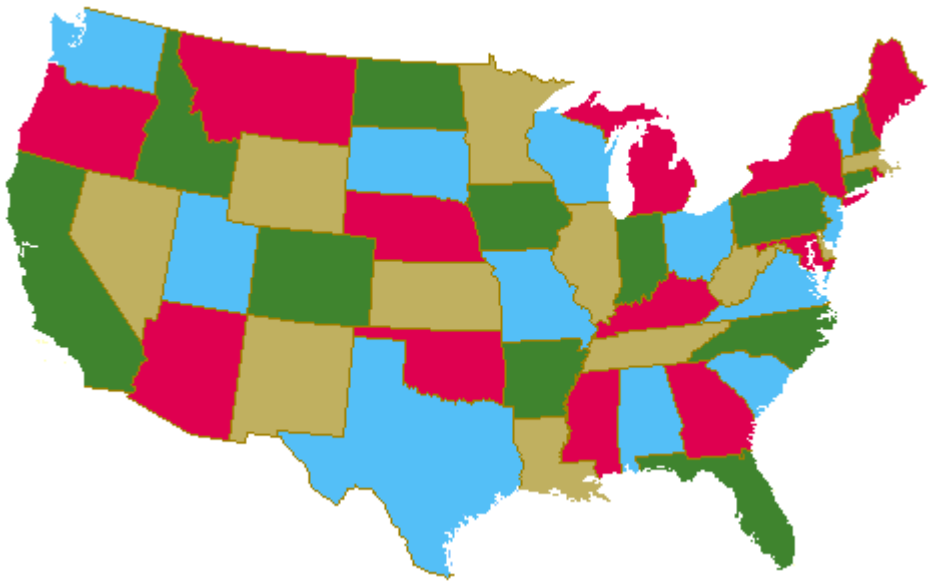
Number	Divisible by 6	Divisible by 3
1	no	
2	no	
3	no	
4	no	
5	no	
6	yes: 6 = 1 x 6	yes: 6 = 2 x 3
7	no	
8	no	
9	no	
10	no	

Number	Divisible by 6	Divisible by 3
11	no	
12	yes: 12 = 2 x 6	yes: 12 = 4 x 3
13	no	
14	no	
15	no	
16	no	
17	no	
18	yes: 18 = 3 x 6	yes: 18 = 6 x 3
19	no	
20	no	

Example 2, Table 2.1

Example exhaustive proof

Problem:	Assign colors to regions of a map so that no two adjacent regions have the same color
Conjecture:	4 colors suffice (1852)
Proof:	Exhaustive analysis of 1,476 cases (1976)



//www.math.gatech.edu/~thomas/FC/fourcolor.html

[Wilson, 2004]

Getting proofs started

- Understand statement of theorem
- Restate in if–then form and assign "names"
- Write first and last lines of proof

Theorem
The product of two even integers is even.
If x and y are even integers, then xy is even.

Proof
Let x and y be even integers.
…
Therefore xy is even. ■

Theorem

Every complete, bipartite graph is connected.

If G is a complete, bipartite graph, then G is connected.

Proof

Let G be a complete, bipartite graph.

…

Therefore G is connected. ■

Example 4.1.8, p. 158, [Epp, 2011]

Direct proof

- Goal: prove $P \rightarrow Q$
- Method: assume hypothesis P is true, deduce conclusion Q is true
- Logical form: prove $P \rightarrow Q$

Example formal direct proof

Theorem

$(\forall x)(\forall y)(x \text{ is even integer} \wedge y \text{ is even integer} \rightarrow \text{product } xy \text{ is even integer})$

Proof

1.	x is even integer $\wedge$ y is even integer	
2.	$(\forall x)[x \text{ is even integer} \rightarrow (\exists k)(k \text{ is integer} \wedge x = 2k)]$	def of even integer
3.	x is even integer $\rightarrow (\exists k)(k \text{ is integer} \wedge x = 2k)]$	1, ui
4.	y is even integer $\rightarrow (\exists k)(k \text{ is integer} \wedge y = 2k)]$	1, ui
5.	x is even integer	4, sim
6.	$(\exists k)(k \text{ is integer} \wedge x = 2k)$	2, 5, mp
7.	m is integer $\wedge$ $x = 2m$	6, ei
8.	y is even integer	4, sim
9.	$(\exists k)(k \text{ is integer} \wedge y = 2k)$	3, 8, mp
10.	n is integer $\wedge$ $y = 2n$	9, ei
11.	$x = 2m$	7, sim
12.	$y = 2n$	10, sim

Example 4

13. $xy = (2m)(2n)$	11, 12, substitution of equals
14. $xy = 2(2mn)$	13, com and ass ?
15. m is integer	7, sim
16. n is integer	10, sim
17. $2mn$ is integer	15, 16, number fact
18. $xy = 2(2mn) \wedge 2mn$ is integer	14, 17, con
19. $(\exists k)(k$ an integer $\wedge\ xy = 2k)$	18, eg
20. $(\forall x)(\exists k)(k$ an integer $\wedge\ x = 2k) \rightarrow x$ is even integer)	def of even integer
21. $(\exists k)(k$ an integer $\wedge\ xy = 2k) \rightarrow xy$ is even integer)	20, ui
22. xy is even integer	19, 21, mp
23. x is even integer $\wedge\ y$ is even integer $\rightarrow xy$ is even integer	temp hyp discharged
24. $(\forall x)(\forall y)(x$ is even integer $\wedge\ y$ is even integer $\rightarrow$ product xy is even integer)	23, ug twice ■

Even more formal version of conjecture:
$(\forall x)(\forall y)(I(x) \wedge E(x) \wedge I(y) \wedge E(y) \rightarrow I(xy) \wedge E(xy))$
where $I(x)$ is x is integer, $E(\mathrm{x})$ is x is even.

Proofs rarely written this formally; possibility of doing so assumed.

Example direct proof

Theorem

The product of two even integers is even.

If two integers are even, then their product is even.

Proof

Let x and y be even integers.

Then $x = 2m$ and $y = 2n$, where m and n are integers. 1

Then $xy = (2m)(2n) = 2(2mn)$, where $2mn$ is an integer. 2

Thus xy has the form $2k$, where $k = 2mn$ is an integer,

and xy is therefore even. ■

Rule 4: In direct proof, assume the hypothesis (antecedent) is true, then use that information to prove the conclusion (consequent).

Example 5

Example direct proof

Notation: $x \mid y$ means x divides y, i.e., y is divisible by x.
$x \mid y$ means $y = xk$ for integer k.

Theorem
If $n \mid m$ and $m \mid p$, then $n \mid p$.

Proof
Let $n \mid m$; then there is integer a such that $m = na$.
Let $m \mid p$; then there is integer b such that $p = mb$.
Substitute for m in $p = mb$ to give $p = mb = (na)b = n(ab)$.
Because $p = n(ab)$, where ab is an integer, then $n \mid p$. ■

Exercise 33

Example direct proof

Theorem
Given any two consecutive integers,
one of them is odd and the other is even.

"Live"

Theorem 4.4.2, p. 158, [Epp, 2011]

Example direct proof

Notation: $x \mid y$ means x divides y, i.e., y is divisible by x.
$x \mid y$ means $y = xk$ for integer k.

Theorem
If $n \mid m$ and $m \mid p$, then $n \mid p$.

Proof
Let $n \mid m$; then there is integer a such that $m = na$.
Let $m \mid p$; then there is integer b such that $p = mb$.
Substitute for m in $p = mb$ to give $p = mb = (na)b = n(ab)$.
Because $p = n(ab)$, where ab is an integer, then $n \mid p$. ■

Exercise 33

Proof by contraposition

- Goal: prove $P \rightarrow Q$
- Method: assume negation of conclusion Q' is true, deduce negation of hypothesis P' is true
- Logical form: prove $Q' \rightarrow P'$
- Valid by tautology: $(Q' \rightarrow P') \Leftrightarrow (P \rightarrow Q)$

P	Q	P'	Q'	$Q' \rightarrow P'$	$P \rightarrow Q$	$(Q' \rightarrow P') \leftrightarrow (P \rightarrow Q)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

tautology

Example proof by contraposition

Theorem
If the square of an integer is odd, then the integer is odd.

Proof (by contraposition)
Original conjecture restated
If n^2 is an odd integer, then n is an odd integer.
Contrapositive
If n is an even integer, then n^2 is an even integer.

Suppose n is even.
Then $n^2 = n \cdot n$ is even by the theorem of Example 5.
Thus if n^2 is an odd integer, then n is an odd integer,
by contraposition. ■

Example 6

Example proof by contraposition

Theorem
If $n + 1$ passwords are issued to n students,
then at least one student received ≥ 2 passwords.

Forming the contrapositive: $P \rightarrow Q$ becomes $Q' \rightarrow P'$
Original antecedent P
"$n + 1$ passwords are issued to n students"
Contrapositive consequent P'
"it is false that $n + 1$ passwords were issued"
Original consequent Q
"at least one student received ≥ 2 passwords" $(\exists x)R(x)$
Contrapositive antecedent Q'
"every student receives < 2 passwords" $(\forall x)R(x)'$

Example 7

Theorem
If $n + 1$ passwords are issued to n students,
then at least one student received ≥ 2 passwords.

Proof (by contraposition)
Contrapositive: If every student receives < 2 passwords,
then it is false that $n + 1$ passwords were issued.

Suppose every student receives < 2 passwords;
then each student receives at most 1 password.
The total number of passwords is at most $n \cdot 1 \neq n + 1$.
Thus the theorem is true by contraposition. ■

Errors in proof by contrapositive

- $P' \rightarrow Q'$ (negate but not reverse) AKA inverse
  - $P \rightarrow Q$ and $P' \rightarrow Q'$ are not equivalent
  - Proving $P' \rightarrow Q'$ does not prove $P \rightarrow Q$
- $Q \rightarrow P$ (reverse but not negate) AKA converse
  - $P \rightarrow Q$ and $Q \rightarrow P$ are not equivalent
  - Proving $Q \rightarrow P$ does not prove $P \rightarrow Q$

Example of converse

Original: If $a > 5$, then $a > 2$. True

Converse: If $a > 2$, then $a > 5$. False

Example 8

If and only if

- Theorems may have form P if and only if Q
  - "if and only if" AKA "iff"
- Parts of "if and only if"
  - "P if Q" means $Q \rightarrow P$
  - "P only if Q" means $P \rightarrow Q$
- To prove P iff Q, prove both $Q \rightarrow P$ and $P \rightarrow Q$
  - Not a separate proof technique
  - If and only if requires two proofs
  - Parts of proof may use same or different techniques

Example if and only if proof

Theorem

Given integers x and y, product xy is odd if and only if x and y are odd integers. ?

Proof

(if) If x and y are odd integers, then xy is odd.

Suppose x and y are odd.

Then $x = 2n + 1$ and $y = 2m + 1$, where m and n are integers.

Then $xy = (2n + 1)(2m + 1) = 4nm + 2m + 2n + 1$

$= 2(2nm + m + n) + 1.$

This has the form $2k + 1$, where $k = (2nm + m + n)$ is an integer, so xy is odd.

Example 9

(only if) If xy is odd, then x and y are odd. ?
Contrapositive: If x is even or y is even, then xy is even.

The antecedent has three cases:
Case 1. x even, y odd: $x = 2m$, $y = 2n + 1$,
Then $xy = (2m)(2n + 1) = 2(2mn + m)$, which is even.
Case 2. x odd, y even: $x = 2m + 1$, $y = 2n$,
Then $xy = (2m + 1)(2n) = 2(2mn + n)$, which is even.
Case 3. x even, y even: $x = 2m + 1$, $y = 2n$,
Then $xy = (2m)(2n) = 2(2mn)$, which is even.
Alternative: xy even by Example 5.

Thus xy odd $\rightarrow$ x and y are odd by contraposition. ■

Proof by contradiction

- Goal: prove $P \rightarrow Q$
- Method: assume negation of conclusion Q', deduce contradiction 0
- Logical form: prove $P \wedge Q' \rightarrow 0$ (contradiction)
- Valid by tautology: $(P \wedge Q' \rightarrow 0) \Leftrightarrow (P \rightarrow Q)$

P	Q	Q'	$P \wedge Q'$	0	$P \wedge Q' \rightarrow 0$	$P \rightarrow Q$	$(P \wedge Q' \rightarrow 0) \leftrightarrow (P \rightarrow Q)$
T	T	F	F	F	T	T	T
T	F	T	T	F	F	F	T
F	T	F	F	F	T	T	T
F	F	T	F	F	T	T	T

Proof by contradiction example

Theorem
If a number added to itself gives itself, then the number is 0.
Restated: If $x + x = x$, then $x = 0$.

Proof (by contradiction)
Assume $x + x = x$ and $x \neq 0$.
Then $2x = x$.
Because $x \neq 0$, divide both sides of $2x = x$ by x to get $2 = 1$, a contradiction.
Thus $x + x = x$ implies $x = 0$. ■

Example 10

Proof by contradiction example

Theorem
The product of two odd integers is not even.
Restated: If x and y are odd integers, then xy is odd.

Proof (by contradiction)
Let $x = 2m + 1$ and $y = 2n + 1$ where m and n are integers,
so $xy = (2m + 1)(2n + 1)$.
Assume by way of contradiction xy is even.
Then $xy = 2k$ for some integer k.
Thus $2k = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1$.
Rearranging, $1 = 2k - 4mn - 2m - 2n$.
Factoring out 2, $1 = 2(k - 2mn - m - n)$,
with $k - 2mn - m - n$ an integer.
This is a contradiction, because 1 is not even. ■

Practice 6

Proof by contradiction example (hard)

Theorem
$\sqrt{2}$ is not rational.
Restated: If $x = \sqrt{2}$, then x can not be written as p/q,
where p and q are integers, $q \neq 0$,
and p and q have no common factors.

Proof (by contradiction)
Assume by way of contradiction $\sqrt{2}$ is rational,
i.e., $\sqrt{2} = p/q$ for integers p and q, $q \neq 0$, with no common factors.
Then $2 = (p/q)^2 = p^2/q^2$ and $2q^2 = p^2$.
Then $2 \mid p^2$ which means $2 \mid p$,
so 2 is a factor of p and 4 is a factor of p^2.
Then $2q^2 = p^2$ can be written $2q^2 = 4x$, so $q^2 = 2x$.
Then $2 \mid q^2$ which means $2|q$.
Now we have 2 is a factor of p and q, which contradicts
the statement that p and q have no common factors. ■

Example 11

Errors in proof by contradiction

- Inadvertent direct proof
  - Goal: prove $P \rightarrow Q$
  - Mistake: assume $P \wedge Q'$, deduce Q (rather than contradiction) without using Q'
  - Incorrectly claim $Q \wedge Q'$ as contradiction
  - Actually direct proof $P \rightarrow Q$
- Inadvertent proof by contrapositive
  - Goal: prove $P \rightarrow Q$
  - Mistake: assume $P \wedge Q'$, deduce P' (rather than contradiction) without using P
  - Incorrectly claim $P \wedge P'$ as contradiction
  - Actually proof of $Q' \rightarrow P'$, proof by contrapositive of $P \rightarrow Q$

Proof technique summary

Goal: prove $P \rightarrow Q$

Proof technique	Approach to prove $P \rightarrow Q$	Remarks
Exhaustive proof	Show $P \rightarrow Q$ for all possible cases	Only useful for a finite number of cases
Direct proof	Assume P, deduce Q	Standard approach, should be considered first
Proof by contraposition	Assume Q', deduce P'	Use if Q′ seems to provide more support to proof than P
Proof by contradiction	Assume P and Q′, deduce a contradiction	Often useful when Q asserts something is not true
If and only if (iff) proof	(only if) Assume P, prove Q (if) Assume Q, prove P	Be careful not to assume too much; either (if) or (only if) false means iff false

Table 2.2

Number theory definitions

- Perfect square: integer n such that $n = k^2$ for integer k.
- Prime number: integer n such that $n > 1$ and n is divisible only by 1 and n.
- Composite number: integer n that is not prime; i.e., $n = ab$ where a and b are integers, $1 < a, b < n$.
- Less than: $x < y$ means that $y - x > 0$.
- Divides: $n \mid m$ means that $m = kn$ for integer k.
- Absolute value: if $x \geq 0$, then $|x| = x$; if $x < 0$, then $|x| = -x$.

Section 2.1 homework assignment

See homework list for specific exercises.

2.2 Induction

Induction analogy: climbing an infinite ladder

- If two things are true …
  - You can reach the first rung
  - From any rung, you can reach the next rung
- … then you can reach every rung

//www.smdc.army.mil/SMDCPhoto_Gallery/Eagle/Jun04/

Induction analogy: knocking over dominoes

- If two things are true …
  - You can knock over the first domino
  - Each domino will knock over the next one
- … then you can knock over all the dominoes

//www.tomgpalmer.com/images/

Induction concept

- Goal
  - Notation $P(n)$ means positive integer n has property P
  - How can it be proven that $(\forall n)P(n)$?
- If two things are true …
  - $P(1)$
  - For any positive integer k, $P(k) \rightarrow P(k+1)$
- … then $P(n)$ holds for every positive integer
- Prove infinitely many statements in two steps

Definition of induction

First principle of mathematical induction

1. $P(1)$
2. $(\forall k)[P(k) \rightarrow P(k+1)]$

$\Big\}$ $\rightarrow P(n)$ for all positive integers n

Equivalently $(P(1) \wedge (\forall k)[P(k) \rightarrow P(k+1)]) \rightarrow (\forall n)P(n)$

Mathematical induction is deductive reasoning.

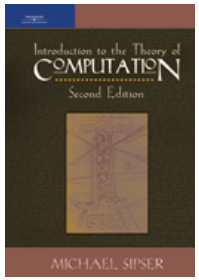
Parts of a proof by induction

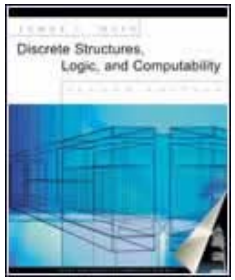
- Basis: Prove $P(1)$ true directly
- Inductive hypothesis: Assume $P(k)$ true
- Inductive step: Prove $P(k+1)$ true
  using assumption that $P(k)$ true

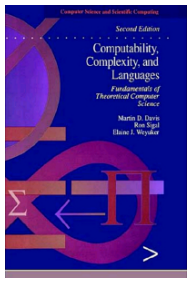
Induction proof steps and step names

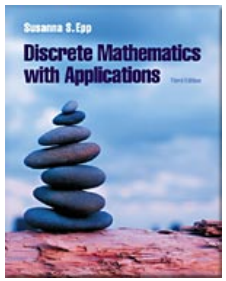
Induction proof step	Name(s) for the step
Show $P(1)$ is true	**Basis step** [Gersting, 2014] [Epp, 2004] [Lewis, 1981] Basis [Hopcroft, 1979] [Sipser, 2006] [Graham, 1989] Inductive base [Grassman, 1996] Basis of induction [Grassman, 1996]
Assume $P(k)$ is true	**Inductive hypothesis** [Gersting, 2014] [Hopcroft, 1979] [Epp, 2004] [Grassman, 1996] Inductive assumption [Gersting, 2014] Induction hypothesis [Sipser] [Lewis, 1981] [Davis, 1994]
Show $P(k) \rightarrow P(k+1)$	**Inductive step** [Gersting, 2014] [Hopcroft, 1979] [Epp, 2004] [Grassman, 1996] Induction step [Sipser, 2006] [Lewis, 1981] Induction [Graham, 1989] Proof under hypothesis [Grassman, 1996]
Discharge (remove) assumption that $P(k)$ is true	Discharge hypothesis [Grassman, 1996]
Generalize from $P(k) \rightarrow P(k+1)$ for arbitrary k to $(\forall k)(P(k) \rightarrow P(k+1))$	Generalize [Grassman, 1996]
Conclude $(\forall n)P(n)$ is true	Conclusion [Grassman, 1996]

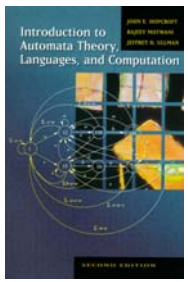
Also “proof by induction” AKA “inductive proof”, “induction proof”.

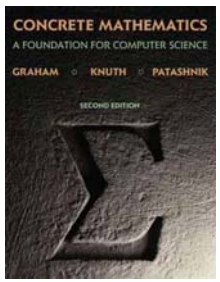


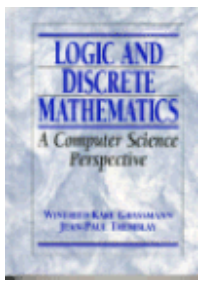


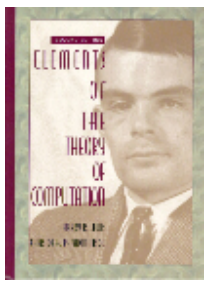












[Davis, 1994] M. D. Davis, R. Sigal, and E. J. Weyuker, *Computability, Complexity, and Languages, Fundamentals of Theoretical Computer Science, Second Edition*, Academic Press, San Diego CA, 1994.

[Epp, 2004] S. S. Epp, *Discrete Mathematics with Applications, Third Edition*, Brooks/Cole, Belmont CA, 2004.

[Gersting, 2014] J. L. Gersting, *Mathematical Structures for Computer Science, A Modern Treatment of Discrete Mathematics, Seventh Edition*, W. H. Freeman, New York NY, 2003.

[Graham, 1989] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics, A Foundation for Computer Science*, Addison-Wesley, Reading MA, 1989.

[Grassman, 1996] W. K. Grassmann and J. Tremblay, *Logic and Discrete Mathematics, A Computer Science Perspective*, Prentice-Hall, Upper Saddle River NJ, 1996.

[Hein, 2002] J. L. Hein, *Discrete Structures, Logic, and Computability, Second Edition*, Jones and Bartlett, Sudbury MA, 2002.

[Hopcroft, 1979] J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, Reading MA, 1979.

[Lewis, 1981] H. R. Lewis and C. H. Papadimitriou, *Elements of the Theory of Computation*, Prentice-Hall, Englewood Cliffs NJ, 1981.

[Sipser, 2006] M. Sipser, *Introduction to the Theory of Computation, Second Edition*, Thomson, Boston MA, 2006.

Example proof by induction

Theorem

$1 + 3 + 5 + \ldots + (2n - 1) = n^2$ for any positive integer n.

Proof

Basis. $1 = 1^2$.

Inductive hypothesis. Assume $1 + 3 + 5 + \ldots + (2k - 1) = k^2$.

Inductive step. Show $1 + 3 + 5 + \ldots + (2(k + 1) - 1) = (k + 1)^2$.

Rewrite left side to show the next to the last term

$1 + 3 + 5 + \ldots + (2k - 1) + (2(k + 1) - 1)$

continued next slide

Example 14

This contains the value assumed for k
as a subexpression; substitute and simplify.

	$1 + 3 + 5 + \ldots + (2(k+1) - 1)$	Left side
$=$	$1 + 3 + 5 + \ldots + (2k - 1) + (2(k+1) - 1)$	Rewrite left side
$=$	$k^2 + (2(k+1) - 1)$	Sub IH
$=$	$k^2 + (2k + 2 - 1)$	Multiply through
$=$	$k^2 + 2k + 1$	Simplify
$=$	$(k+1)^2$	Factor polynomial

Therefore by induction $1 + 3 + 5 + \ldots (2n - 1) = n^2$
for any positive integer n. ■

Rule 5: In a proof by induction, you must find the inductive hypothesis at some point in the inductive step.

Example proof by induction

Theorem

$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ for any integer $n \geq 1$.

Proof

Basis. $2^0 + 2^1 = 3 = 2^{1+1} - 1$.

Inductive hypothesis.

Assume $2^0 + 2^1 + 2^2 + \ldots + 2^k = 2^{k+1} - 1$.

Inductive step.

Show $2^0 + 2^1 + 2^2 + \ldots + 2^{k+1} = 2^{k+1+1} - 1$.

Rewrite left side to show the next to the last term

$2^0 + 2^1 + 2^2 + \ldots + 2^k + 2^{k+1}$

important technique

continued next slide

Example 15

This contains the value assumed for k
as a subexpression; substitute and simplify.

	$2^0 + 2^1 + 2^2 + \ldots + 2^{k+1}$	Left side
$=$	$2^0 + 2^1 + 2^2 + \ldots + 2^k + 2^{k+1}$	Rewrite left side
$=$	$2^{k+1} - 1 + 2^{k+1}$	Sub IH
$=$	$2(2^{k+1}) - 1$	Add like terms
$=$	$2^{k+1+1} - 1$	Law of exponents

Therefore by induction $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$
for any integer $n \geq 1$. ■

Example proof by induction

Theorem

For any positive integer n, $1+2+3+\ldots+n=\frac{n(n+1)}{2}$

Proof

Basis. $1=\frac{1(1+1)}{2}$

Inductive hypothesis. Assume $1+2+3+\ldots+k=\frac{k(k+1)}{2}$

Inductive step. Show $1+2+3+\ldots+(k+1)=\frac{(k+1)[(k+1)+1]}{2}$

continued next slide

Rewrite to show the next to the last term, substitute the value assumed in the IH, and simplify.

$1+2+\ldots+(k+1)$ Left side

$= 1+2+\ldots+k+(k+1)$ Rewrite left side

$= \dfrac{k(k+1)}{2}+(k+1)$ Sub IH

$= (k+1)\left(\dfrac{k}{2}+1\right)$ Factor out $(k+1)$

$= (k+1)\left(\dfrac{k+2}{2}\right)$ Common denominator

$= \dfrac{(k+1)[(k+1)+1]}{2}$ Multiply

Therefore by induction, for any positive integer n

$$1+2+3+\ldots+n = \frac{n(n+1)}{2} \quad \blacksquare$$

Example proof by induction

Theorem

For any positive integer n, $2^n > n$.

Proof

Basis. $2^1 > 1$.

Inductive hypothesis. Assume $2^k > k$.

Inductive step. Show $2^{k+1} > k + 1$.

	2^{k+1}	Left side
$=$	$2^k \cdot 2$	Law of exponents
$>$	$k \cdot 2$	By IH
$=$	$k + k$	Def of multiplication
$\geq$	$k + 1$	k given as "positive integer", thus $k \geq 1$

Thus $2^n > n$ for any positive integer n. ■

Example 16

Example proof by induction

Theorem

For any positive integer $n \geq 4$, $n^2 > 3n$.

Proof

Basis. $4^2 > 3 \cdot 4$, i.e., $16 > 12$.

Inductive hypothesis. Assume $k^2 > 3k$.

Inductive step. Show $(k+1)^2 > 3(k+1)$.

	$(k+1)^2$	Left side
$=$	$k^2 + 2k + 1$	Multiply
$>$	$3k + 2k + 1$	By IH
$\geq$	$3k + 8 + 1$	$k \geq 4$ by basis
$>$	$3k + 3$	$8 + 1 > 3$
$=$	$3(k+1)$	Factor out 3

Thus $n^2 > 3n$ for any positive integer $n \geq 4$. ■

Example 17

Example proof by induction

Theorem
For any positive integer n, $2^{2n} - 1$ is divisible by 3.

Proof
Basis. $2^{2(1)} - 1 = 4 - 1 = 3$ is divisible by 3.

Inductive hypothesis. Assume $2^{2k} - 1$ is divisible by 3.
Therefore $2^{2k} - 1 = 3m$ and $2^{2k} = 3m + 1$ for integer m.

Inductive step.
Show $2^{2(k+1)} - 1$ is divisible by 3.

Example 18

	$2^{2(k+1)} - 1$	Left side
$=$	$2^{2k+2} - 1$	Multiply through exponent
$=$	$2^2 \cdot 2^{2k} - 1$	Law of exponents
$=$	$2^2(3m + 1) - 1$	By IH
$=$	$12m + 4 - 1$	Multiply through
$=$	$12m + 3$	Simplify
$=$	$3(4m + 1)$	$(4m + 1)$ an integer

Thus $2^{2n} - 1$ is divisible by 3 for any positive integer n. ■

Example proof by induction

Theorem

For any real number $r \neq 1$ and any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Proof

Basis. Show $\sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1}$ $\sum_{i=0}^{0} r^i = r^0 = 1, \frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1$

Inductive hypothesis. Assume $\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}$

continued next slide

Example 5.2.3 [Epp, 2011]

Inductive step. Show $\sum_{i=0}^{k+1} r^i = \frac{r^{(k+1)+1} - 1}{r - 1} = \frac{r^{k+2} - 1}{r - 1}$

$\sum_{i=0}^{k+1} r^i$ Left side

$= \sum_{i=0}^{k} r^i + r^{k+1}$ Rewrite left side to show next to last

$= \frac{r^{k+1} - 1}{r - 1} + r^{k+1}$ Sub IH

$= \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r - 1)}{r - 1}$ Multiply by $(r - 1)/(r - 1)$

$= \frac{(r^{k+1} - 1) + r^{k+1}(r - 1)}{r - 1}$ Add fractions

$= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r - 1}$ Multiply through

$= \frac{r^{k+2} - 1}{r - 1}$ ■ Add to cancel terms

Example proof by induction

Programming language denotes multiplication with ( ), e.g., $a{\cdot}b{\cdot}c{\cdot}d{\cdot}e{\cdot}f{\cdot}g$ would be written $((((((a)b)c)d)e)f)g$ or $((a)b)(((c)d)(e)f)g$.

Theorem
Any product of factors in this language can be written with an even number of parentheses.

Proof (by induction on number of factors)
Basis. For a single factor, there are 0 parentheses.

Inductive hypothesis. Assume for k factors there are an even number of parentheses.

Example 19

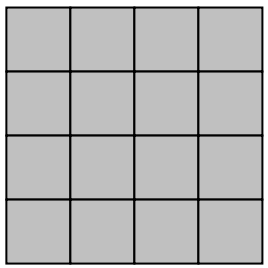
Inductive step. Consider product P of $k + 1$ factors; $P = r \cdot s$, where r has k factors and s is a single factor. By the inductive hypothesis, r has an even number of parentheses.

Write P as $(r)s$, adding 2 parentheses to the even number of parentheses in r, thereby expressing P with an even number of parentheses.

Thus any product of factors can be written with an even number of parentheses. ■

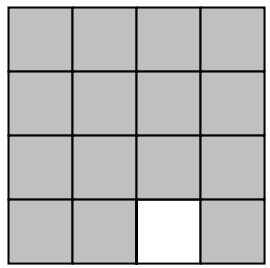
Example proof by induction

Tiling: Cover n x n checkerboard with tiles that conform to the grid, with no missed squares and no overlapping tiles.
Angle iron: L-shaped tile of 3 squares.
Problem: given any n x n checkerboard with one square removed, tile it with angle irons.

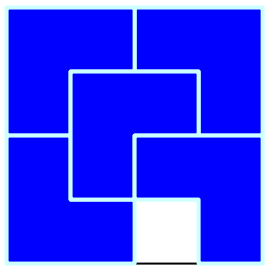


n x n checkerboard
($n = 4$)

angle iron



4 x 4 checkerboard
with 1 square missing



4 x 4 checkerboard
with 1 square missing
tiled with angle irons

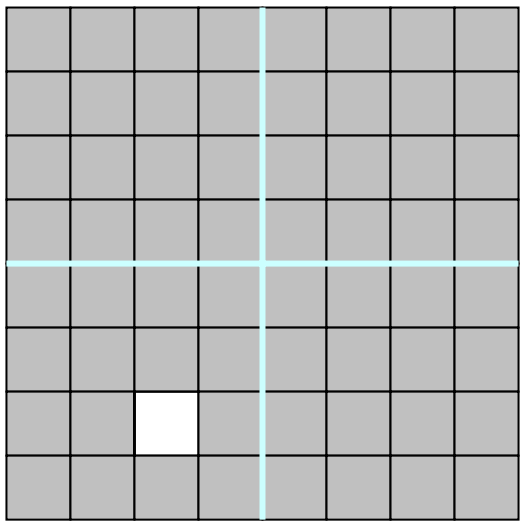
Example 20

Theorem
For any positive n, a 2^n x 2^n checkerboard with 1 square removed can be tiled with angle irons.

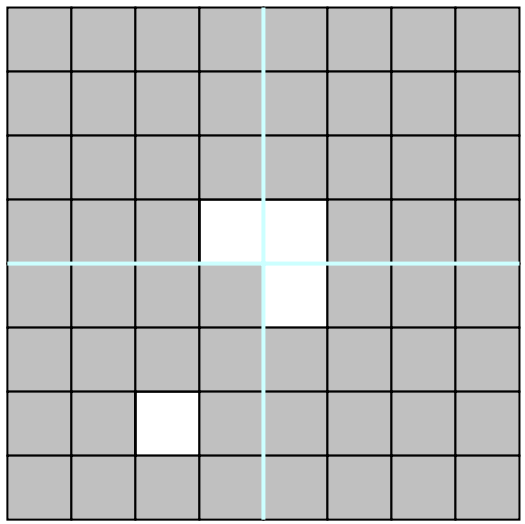
Proof (by induction on size parameter n)
Basis. For $n = 1$, a 2^1 x 2^1 checkerboard, see the figure.

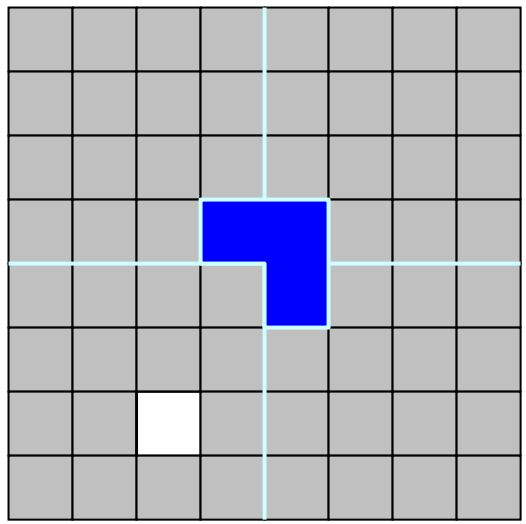
Inductive hypothesis. Assume any 2^k x 2^k checkerboard with 1 square removed can be tiled with angle irons.

Inductive step. Show that any 2^{k+1} x 2^{k+1} checkerboard with 1 square removed can be tiled with angle irons.
Divide the 2^{k+1} x 2^{k+1} checkerboard into quarters;
each will be 2^k x 2^k, and one will be missing a square.
By the inductive hypothesis the 2^k x 2^k quarter missing a square can be tiled with angle irons.



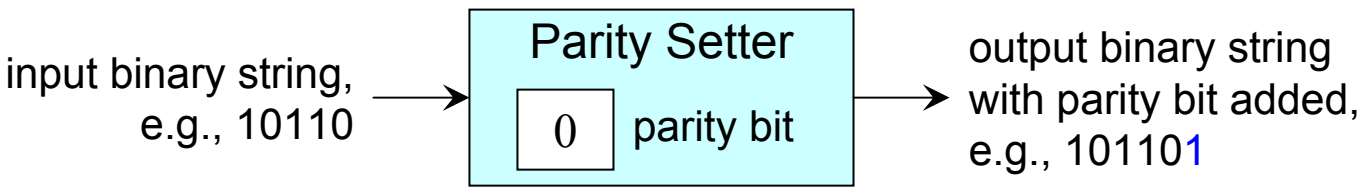
Suppose each of the other three quarters have a specific square removed, as shown in the left figure.
Then by the inductive hypothesis, each of them can be tiled with angle irons, and the three removed squares can be tiled with an angle iron, as shown in the right figure.
Thus the 2^{k+1} x 2^{k+1} checkerboard with 1 square removed can be tiled with angle irons, and so any 2^n x 2^n checkerboard with 1 square removed can so tiled. ■





Example proof by induction

- Parity setter purpose
  - Reads input binary string
  - Writes output binary string with additional bit
  - Additional bit set to ensure even (odd) number of 1s
  - Used for checking data for errors
- Parity setter operation (even parity)
  - Parity bit initially 0
  - Input read one bit at a time, input bit written to output
  - If input bit 0, parity bit not changed
  - If input bit 1, parity bit "flipped": $0 \rightarrow 1$, $1 \rightarrow 0$
  - After last input bit, final parity bit written to output



Exercise 68

Theorem
The number of 1s in the output string
(input string plus final parity bit), is always even.

Proof (by induction on the input length)
Basis. Length $n = 1$. Parity bit initially 0.
Case 1. Input 0, parity bit unchanged, output 00, even.
Case 2. Input 1, parity bit flipped, output 11, even.

Inductive hypothesis. Assume that for input of length k
the output string has an even number of 1s.

Inductive step. Show that for input of length $k + 1$ the output string has an even number of 1s.

Analyze possible cases:

	Case	Parity bit after k bits	Input bit $k + 1$	Parity bit after $k + 1$ bits
all possible cases	1	0	0	0
	2	0	1	1
	3	1	0	1
	4	1	1	0

by definition of parity setter operation

Case 1. No 1s added to or removed from output for bit $k+1$.
Even number of 1s by IH unchanged.

Case 2. Two 1s added to output string for bit $k+1$:
input bit $k+1$ and flipped parity bit $0 \rightarrow 1$.
Even number of 1s by IH plus two more 1s is even.

Case 3. Same as Case 1.

Case 4. One 1 added to output string for bit $k+1$
(input bit $k+1$) and one 1 removed (flipped parity bit $1 \rightarrow 0$).
Even number of 1s by IH plus one minus one is even. ■

Definition of induction, revisited

First principle of mathematical induction

1. $P(1)$
2. $(\forall k)[P(k) \rightarrow P(k+1)]$

$\Big\} \rightarrow P(n)$ for all positive integers n

Second principle of mathematical induction

1. $P(1)$
2. $(\forall k)[P(r)$ true for all r, $1 \le r \le k \rightarrow P(k+1)]$

$\Big\} \rightarrow P(n)$ for all positive integers n

Proving the principles of induction

Principle of well-ordering

Every non-empty collection of positive integers has a smallest member.

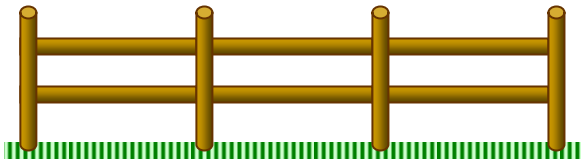
It can be proven that

Second induction → first induction
First induction → well-ordering
Well-ordering → second induction

Example proofs by induction, both principles

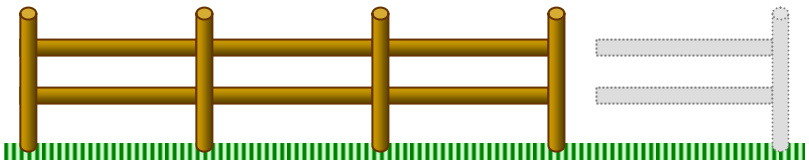
Theorem

A straight fence with n fence posts has $n - 1$ connecting sections for any $n \geq 1$.

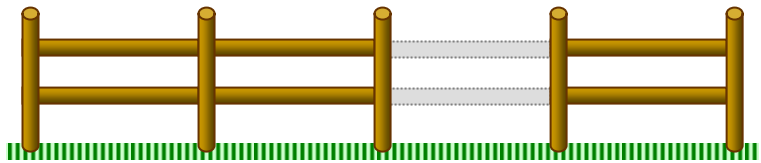


(a) Fence with 4 fence posts, 3 sections

(b) Fence with 1 fence post, 0 sections



(c) Fence with post and section removed



(d) Fence with section removed

Example 21

Proof (by induction on number of posts; first principle)

Basis. A fence with 1 post has 0 sections; see Fig (b).

Inductive hypothesis: Assume that a fence with k posts has $k-1$ sections.

Inductive step. Show that a fence with $k+1$ posts has k sections.
Given a fence with $k+1$ posts, remove last post and section; the remaining fence has k posts and by the inductive hypothesis $k-1$ sections; see Fig (c).
Because 1 section was removed from the original fence, it had $k-1+1=k$ sections.
Thus a fence with n posts has $n-1$ sections. ■

Proof (by induction on number of posts; second principle)

Basis. A fence with 1 post clearly has 0 sections.

Inductive hypothesis: Assume that for all r, $1 \le r \le k$, a fence with r posts has $r - 1$ sections.

Inductive step. Show that a fence with $k + 1$ posts has k sections.
Given a fence with $k + 1$ posts, remove 1 section; Fig (d).
The two parts have r_1 and r_2 posts, $1 \le r_1 \le k$ and $1 \le r_2 \le k$, and $r_1 + r_2 = k + 1$ (no posts were removed).
By the inductive hypothesis the two parts have $r_1 - 1$ and $r_2 - 1$ sections,
thus the original fence had $(r_1 - 1) + (r_2 - 1) + 1 = k$ sections.
Thus a fence with n posts has $n - 1$ sections. ■

Example proof by induction

Integer n is prime iff it is divisible only by 1 and itself.
Integer n is composite iff it can written as the product of two integers other than 1 and n.

Theorem
For every integer $n \geq 2$, n is either prime or a product of primes.

Proof
Basis. 2 is a prime.

Inductive hypothesis. Assume for all r, $2 \leq r \leq k$, r is either prime or the product of primes.

Example 23

Inductive step.
Show $k+1$ is either prime or a product of primes.
If $k+1$ is prime, the proof is complete.
If $k+1$ is not prime (i.e., composite),
it can be written $k+1=ab$ (by definition of composite),
where $1<a<k+1$ and $1<b<k+1$.
Therefore $2\le a\le k$ and $2\le b\le k$.
By inductive hypothesis, a and b are either prime or the product of primes.
Thus $k+1=ab$ is the product of primes.
Therefore n is either prime or a product of primes. ■

Example proof by induction

Theorem
Any postage amount ≥ 8 cents,
can be assembled using only 3 and 5 cent stamps.

Proof
$P(n)$ is the property that n cents of postage can be assembled from 3 and 5 cent stamps.

Basis. $8 = 3 + 5,\ 9 = 3 + 3 + 3,\ 10 = 5 + 5.$

Inductive hypothesis. Assume that for all r, $8 \le r \le k$, r cents can be assembled from 3 and 5 cent stamps.

Example 24

Inductive step. Show $k+1$ can be assembled from 3 and 5.

Consider $k+1 \geq 11$. 1

If $k+1 \geq 11$, then $(k+1)-3 = k-2 \geq 8$. 2

By inductive hypothesis $k-2$ can be written as sum of 3s and 5s. 3

But $(k-2)+3 = k+1$,

so $k+1$ also can be written as sum of 3s and 5s.

Thus n can be assembled as a sum of 3s and 5s. ■

Induction summary

- Parts of a proof by induction
  - Prove $P(1)$ true; "basis step"
  - Assume $P(k)$ true (first principle),
    or assume $P(r)$ true for $1 \leq r \leq k$ (second principle);
    "inductive hypothesis"
  - Prove $P(k+1)$ true using assumption; "inductive step"
  - Conclude that $(\forall n)P(n)$ true
- Induction reminders
  - Prove the basis case (or cases) first
  - Make an assumption (the IH)
  - Find the IH and use it in the IS

- When to use induction
  - Infinite or unknown number of cases
  - Each case can be analyzed in terms of previous cases
  - Examples; objects (previous objects)
    - Integers (lesser integers); Chapter 2
    - Sets (subsets); Chapter 3
    - Graphs (subgraphs); Chapter 5
    - Data structures (data structure before update); Chapter 5
    - Computation steps (earlier computation steps); future classes
- Induction is a computer scientist's essential tool

http://yoda.locutus.be/

Section 2.2 homework assignment

See homework list for specific exercises.

2.3 More on Proof of Correctness

2.4 Number Theory

References

[Gersting, 2014] J. L. Gersting, *Mathematical Structures for Computer Science: Discrete Mathematics and Its Applications*, *Seventh Edition*, W. H. Freeman and Company, New York NY, 2014.

[Davis, 1994] M. D. Davis, R. Sigal, and E. J. Weyuker, *Computability, Complexity, and Languages, Fundamentals of Theoretical Computer Science, Second Edition*, Academic Press, San Diego CA, 1994.

[Epp, 2004] S. S. Epp, *Discrete Mathematics with Applications, Third Edition*, Brooks/Cole, Belmont CA, 2004.

[Epp, 2011] S. S. Epp, *Discrete Mathematics with Applications, Fourth Edition*, Brooks/Cole, Boston MA, 2011.

[Gersting, 2014] J. L. Gersting, *Mathematical Structures for Computer Science, A Modern Treatment of Discrete Mathematics, Seventh Edition*, W. H. Freeman, New York NY, 2003.

[Graham, 1989] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics, A Foundation for Computer Science*, Addison-Wesley, Reading MA, 1989.

[Grassman, 1996] W. K. Grassmann and J. Tremblay, *Logic and Discrete Mathematics, A Computer Science Perspective*, Prentice-Hall, Upper Saddle River NJ, 1996.

[Hein, 2002] J. L. Hein, *Discrete Structures, Logic, and Computability, Second Edition*, Jones and Bartlett, Sudbury MA, 2002.

[Hopcroft, 1979] J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, Reading MA, 1979.

[Lewis, 1981] H. R. Lewis and C. H. Papadimitriou, *Elements of the Theory of Computation*, Prentice-Hall, Englewood Cliffs NJ, 1981.

[Sipser, 2006] M. Sipser, *Introduction to the Theory of Computation, Second Edition*, Thomson, Boston MA, 2006.

[Wilson, 2004] R. Wilson, *Four Colors Suffice*, Princeton University Press, Princeton NJ, 2004.

End

Center for Modeling, Simulation, and Analysis