Review1. Logic

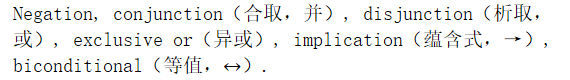
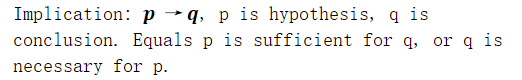
2019年5月27日

18:37

Proof examples

* Proof methods: direct proof, proof by contrapositive, proof by contradiction.
* Euler Circuit: if and only if a connected multigraph with at least 2 vertices has each of its vertex has even degree.

Logic

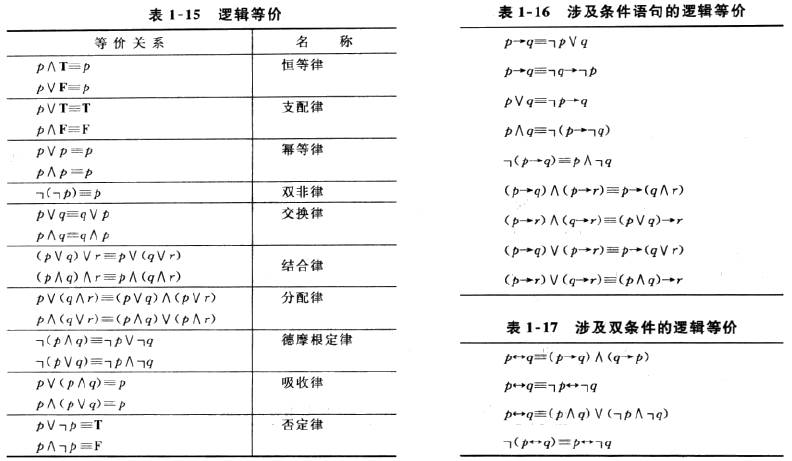
* Proposition logic: declarative statement either true or false.
  + *Also called atomic (elementary) proposition.*
  + *Propositional logic refer to objects and their properties and relations.*
* Logical connectives: connect to form compound propositions（复合命题）.
  + 
    - 
      * Converse, contrapositive, inverse.
    - Biconditional proposition: p iff q.
* Translation: use logic symbol to present language.

Truth table

* Constructing the truth table: 2^n entities for n variables proposition.
* Bit string: sequence of 0 or more bits.

Tautology and contradiction

* Tautology: always true compound proposition.
  + Contradiction: always false compound proposition.
  + Contingency: neither tautology nor contradiction.
* Equivalent: two propositions always have the same truth table.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image003.png



Quantifiers and predicate

* Quantifiers: universal quantifier (all), existential quantifier (at least one).
* Predicate logic: constant, variable, and predicate.
  + Universe (domain), truth set, truth value.
* De Morgan Law for quantifiers:

计算机生成了可选文字:
Negation 
Equivalent 
Statement 

* Nested quantifiers: more than one quantifiers in a predicate logic.
  + Order of quantifiers, negation nested quantifier.

Review2. Mathematical Proofs

2019年5月27日

18:37

Theorems and proofs

* Axiom (postulate): considered to be true.
  + Theorem: proved to be true.
  + Lemma: proved to be true, used to prove other theorems.
* Proof based on logical equivalences.

计算机生成了可选文字:
p 
.•.pvq 
P 
pVq 
-IPVr 
CnqA (p 
[(pVq) 
C(p) —(pAq) 

* Proof methods: direct proof, by contrapositive, by contradiction, by cases, proof of equivalence.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image007.png
    - Trivial proof: prove q is always true.

Review3. Sets and Functions

2019年5月27日

18:37

Sets

* Set: unordered collection of objects (elements, members).
  + *Built with sets: combinations, relations, graphs.*
  + *Axiomatic set theory: avoid Russell's paradox.*
* Venn diagram: visualize sets.
* Proper subset: belongs to but not equal.
  + Two sets are equal if and only if each is a subset of the other.
* Cardinality: number of distinct elements in a finite set.
* Power set: the set of all subsets of set S, denoted by P(S).
* Tuples: ordered n-tuple with n elements and in order.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image008.png
  + Relation A from B: a subset of the Cartesian product.
* Union, intersection, complement, difference.
  + Union of a collection of sets and intersection of a collection of sets.
  + Disjoint: intersection is empty set.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image009.png
* Set identities:

计算机生成了可选文字:
Al-JØ—A 
nntJ=A 
A 1-11,' 
Anø—ø 
AIDA—A 
Ann—A 
AIJB—BIJA 
Ant 
ALJB—AlÄb 
ALIA—U 

* Prove set identities using membership tables.
* Represent sets in computer: bit string to universal set and set in-set-element to 1.

А {2, 5} - д = 01001 
в = {1, 5}-в 10001 

Functions

* Function from A to B: exactly one element of B to each element of A.
  + *A is domain, B is codomain.*
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image012.png
    - *Range of function: set of images of elements of A.*
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image013.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image014.png
  + Bijection: both one-to-one and onto.
* Inverse function: only for bijective function.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image015.png
  + Identity function maps element to itself.
* Floor function, ceiling function.

Sequence

* A function from subset of integers to a set S {an}.

k3 
81 
1x1<1 
n(n4- l) 
2 
6 
4 
1 
1 

* Arithmetic progression (initial term and common difference), geometric progression (initial term and comm ratio).
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image017.png
* Recursively defined sequences: previous elements and initial element.
* Countable set: finite or has the same cardinality as Z+.
  + To prove same cardinality: find a bijective function.

Review4. Complexity of Algorithms

2019年5月27日

18:37

Algorithms

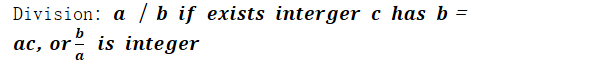
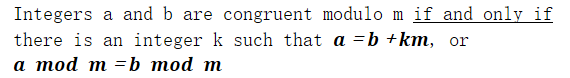
* Algorithm: finite sequence of precise instructions for performing a computation or for solving a problem.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image018.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image019.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image020.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image021.png
  + Big-O is an upper bound while big-Ω is a lower bound.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image022.png
* Compute time complexity: give steps and find time complexity for each step.
  + *Best case, worst case, and average case.*
* NP-Complete problem: any one of NP-Complete problems has an efficient solution then all the them have efficient solutions.
  + Input size: the minimum number of bits needed to encode the input of the problem.
  + Class P: all decision problem solvable in polynomial time.
  + Certificate: corresponding to a yes-input. NP problem can be verified certificate in polynomial time.
  + Problems belongs to NP: composite, D subset sum, SAT problem.
* Boolean formula satisfiable: assign truth values to acquire final result 1.

Review5. Number Theory

2019年5月27日

18:37

Number theory

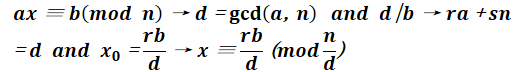
* 
  + Note a is factor of b and b is multiple of a.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image024.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image025.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image026.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image027.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image028.png
  + 
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image030.png
* Arithmetic modulo m:
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image031.png
  + Closure, associativity, identity elements 0 and 1, additive inverses, commutativity, distributivity.

*I'll skip number systems part, as it's basic in previous course.*

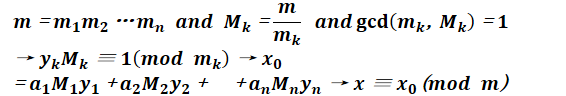
Prime

* Positive integer greater than 1 and divisible only by 1 and itself is prime.
  + *Composite: not prime.*
* Fundamental theorem of arithmetic: every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes.
* GCD (greatest common divisor) and LCM (least common multiple).
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image032.png
  + Find gcd: factorization (can also find lcm), Euclidean algorithm.
    - C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image033.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image034.png
    - C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image035.png
    - C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image036.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image037.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image038.png

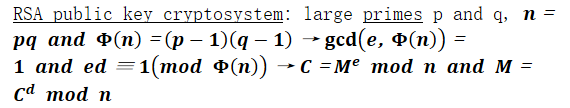
Linear congruence

* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image039.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image040.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image041.png
    - 
* Chinese reminder theorem:

al (mod ml) 
E- a2 (mod ) 
x an (mod mn) 

* 
* Another solution:

2 “ 2(mod6) 
土 ． ÷ 2(mod7) 
二 4 （ mod8 ） 
首 先 求 解 第 一 个 方 程 ， 得 到 丫 二 1 (mod 3), 于 是 令 x ： 3 々 + 1 ， 第 二 个 方 程 就 变 为 
迎 一 1 (mod 7 ） 
解 得 々 三 3 （ m 7 ） · 于 是 ， 再 令 々 = 7 ／ + 3 ， 三 个 万 程 就 可 以 化 为 ： 
42 / 一 16 （ mod8 ） 
解 出 ： / 三 0 (mod4), 即 / = 4 腓 代 入 原 来 的 表 达 式 就 有 ， “ 21 （ 4 囫 + 10 = 84m+ 10 ， 即 解 为 ： 
． “ 10 （ m 。 d84 ） 

* *Modular arithmetic and congruencies: pseudorandom number generators, hash functions, cryptography.*
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image046.png
  + *Cryptography: symmetric cryptography, asymmetric cryptography, RSA cryptography, DLP and EI Gamal cryptography, Diffie-Hellman key exchange protocol, and cryptocurrency.*
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image047.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image048.png
* Cryptography: kryptos (secret) and graphos (writing).
  + 
    - C is encryption and M is decryption.
  + *I'll skip other methods of cryptography and if you are interested, you can join cryptography course next semester.*

Review6. Mathematical Induction

2019年5月27日

18:37

Mathematical induction

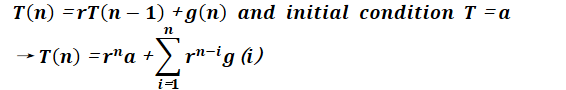
* Start from small examples, then suppose for k case the proposition establishes, finally prove k+1 is also establish.
  + Basic step, inductive hypothesis, and inductive step.
  + Strong principle and weak principle.
* Well-ordering principle: every set of non-negative integers has a smallest element.

Review7. Recursion

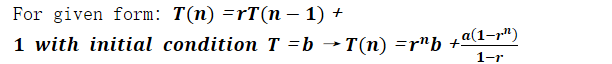
2019年5月27日

18:37

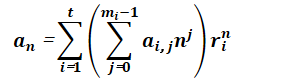
Recursion

* Inductive analysis (prove correctness), towers of Hanoi.
* Recurrences: function defined on the set of n-1 values.
  + Initial condition(s), base case(s).
* Iterating a recurrence: bottom-up, top-down.
  + 

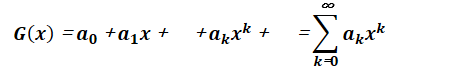
Divide and conquer

* 
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image052.png
  + *Example: binary search.*

Linear recurrence relation

* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image053.png
  + Linear, homogeneous (all terms are multiples of aj's), degree k, constant coefficients.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image054.png
    - C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image055.png
* *You are an adult and you should solve these questions by yourself.*
* Degenerate roots in general: t roots r1,…,rt with multiplicities m1,…,mt
  + 

Generating function

* *Used to characterize sequences.*
* 
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image058.png
* Addition and multiplication of generating function.

(1 + x)” C(n, k)xk 
(1 + ax)n = C(n, k)akxk 
(1 + ELO C(n, k)xrk 

1 — хп41 
1 
ах 
— Lk=oX 
к-=о 
оо rk 

¯ I 3x2 + 
— 1, k)xk 
— 1, k)akxk 

计算机生成了可选文字:
00 
x 
(—1) 

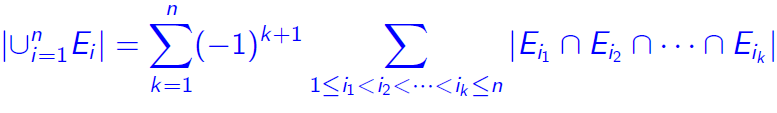
Review8. Counting

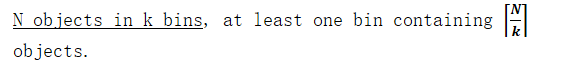
2019年5月27日

18:37

Counting

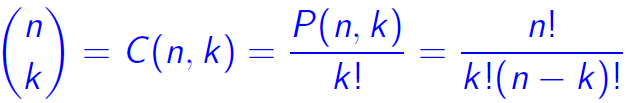
* *Determine the number of these objects.*
  + The product rule and the sum rule or combination.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image063.png

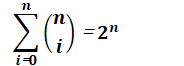
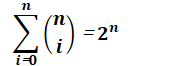


* *Determine the number of onto functions, the appears on tree leaves.*
* Pigeonhole principle: a set of objects stored in a set of bins.
  + If there are k+1 objects and k bins, then there is at least one bin with two or more objects.
  + 
  + Example: bijective functions number, counting triangles, counting pairs.
* The bijection principle: two sets have same size if and only if there is a one-to-one function from one set onto the other.

Binomial coefficient

* K-element permutation of N: a list of k distinct elements chosen from a set N.
* Unorder set formula:



* 
* **Pascal's triangle**: each entry in Pascal's triangle is the sum of two entries directly above it.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image068.png
* Algebraic proof, combinatorial proof, bijective proof, binomial proof.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image069.png
    - 
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image071.png

Review9. Relations

2019年5月27日

18:37

Binary relation

* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image072.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image073.png
  + Use table to represent binary relation.
* Relation: one to many relationships between elements in A and B.
* Number of binary relations:
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image074.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image075.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image076.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image077.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image078.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image079.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image080.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image081.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image082.png
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image083.png
* Combining relations: union, intersection, difference.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image084.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image085.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image086.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image087.png

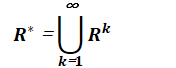
N-ary relation

* *Relation on n sets, these sets are domains of R.*
  + Degree of R is n.
  + R is functional in Ai if contains at most one n-tuple (…, ai, …) for any value ai within domain Ai.
* *Relational database I'll skip due to you already chosen database principle.*
* Represent relations: explicit list, table, function, zero-one matrix, directed graph.

Closure

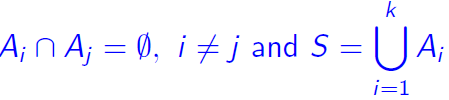
* Reflexive closure: contains R, is reflexive, is minimal.
* Closures: with property P of relation R on set A, and S is minimal.
* Transitive closure: find all pairs of elements that are connected with a directed path.

Connectivity relation

* Consists of all pairs (a, b) there is a path between a and b in R.
  + 
  + The transitive closure of a relation R equals the connectivity relation R\*.

Other relations

* Equivalence relation: reflexive, symmetric, transitive.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image089.png
* Partition of a set S:



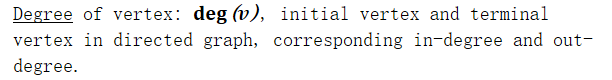
* Partial order (poset): reflexive, antisymmetric, transitive.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image091.png
* Total order (chain): every two elements in poset are comparable.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image092.png
* Hasse diagram: representation of partial ordering.
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image093.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image094.png
  + C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image095.png
    - Least upper bound and greatest lower bound.
* Well-ordered set: a poset is total ordering and every nonempty subset of S has a least element.
* Lattices: partial ordered set with every pair of elements has both least upper bound and greatest lower bound.

Review10. Graphs

2019年5月27日

18:37

Graph

* Vertices, edges (endpoints, joins, adjacent), incident (connect).
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image096.png
  + Simple graph, multigraph pseudograph: edges number and loop.
  + Complete graph Kn: all vertices incident to edge.
  + Directed graph, undirected graph.
* 
* Cycle, wheel, and n-dimensional hypercube.
* Bipartite graphs: partitioned into two disjoint subsets.
  + Complete bipartite graph, matching, and maximum matching.
* Union, intersection of graph.
* *Representation: adjacency lists, adjacency matrices, incidence matrices.*
* Isomorphism: a and b are adjacent in G1 if and only if f(a) and f(b) are adjacent in G2.
  + Function f is one-to-one and onto.
* Path (circuit, simple), length, connectivity, connected component.
  + Disconnected: cut vertices and cut edges.
* Euler Circuit: the degree of every vertex must be even, or exactly two vertices of odd degree.
* Hamilton path: a simple path passes through all vertices exactly once.
* Shortest path problem, weighted graph.

Planar graph

* Draw in plane without any edges crossing.
* C:\B3790EE5\83EF2E5D-1A08-46F0-B96F-9A20485860B6.files\image098.png
* Degree of region: number of edges on the boundary of this region.
* Elementary subdivision: remove an edge {u, v} and add a new vertex w to {u, w}, {w, v}.