Ve203 Recitation Class

Wang Qian

UM-SJTU Joint Institute

2013-2014 Fall

Personal Info.

Wang Qian
- Office hour: Friday 10 a.m. to 11:40 a.m. at e-reading room
- Recitation class: Wednesday 4 p.m. to 6 p.m. at D206
- e-mail: wangqian1992511@sjtu.edu.cn
- Tel: 18817519155
- Skype: wangqian1992511@gmail.com

When sending an e-mail to me, please begin your subject with "[VE203]", so that I can quickly recognize it. It can also ensure that your mail cannot be filtered, especially for those who use the Tencent Mail. I may not be able to reply your short message at once, but if you have something urgent, please feel free to call me.

Personal Info.

In my recitation class, I will first give you a list of definitions, which are covered in the lecture slides. These are the basic concepts you should know. Then I may add some additional materials. They may be from the textbook, or other references, which I listed in the last slide. After that I will give you about 10 example problems for exercises. For every assignment, I will only talk briefly about it after the due date.

What is discrete math?

"Discrete mathematics is the part of mathematics devoted to the study of discrete objects." [Rosen, 2012]

Example

- To sort a list of elements in a particular order quickly.
- To encrypt messages so that only intended receivers can read them.
- To judge whether one can win a game with probability.
- To find the shortest distance between two cities.
- ...

Contents I

Contents II

Definition Checklist

Definition

- statement(proposition), tautology, contradiction
- nagation, conjunction, disjunction
- truth table, implication, equivalence, contraposition
- logical quantifier, nested quantifier, vacuous truth
- argument, rule of inference

Additional Materials

You should prove these in your assignment. Though these are not covered in the lecture slid, you should still know these useful concepts.

Disjunctive Normal Form

disjunctive normal form: a compound proposition with the form of "disjunction of conjunctions of the variables or their negations".

$A \vee (B \wedge \neg C) \vee (D \wedge E)$ ✓

~~$\neg(A \wedge B)$~~

~~$A \vee (B \wedge (C \vee D))$~~

Conjunctive Normal Form

conjunctive normal form: a compound proposition with the form of "conjunction of disjunctions of the variables or their negations".

Additional Materials

Functionally Complete

functionally complete: a collection of logical operators is called functionally complete if every compound proposition is logically equivalent to a compound proposition involving only these logical operators.

Fuzzy Logic

fuzzy logic: in this kind of logic, a proposition has a truth value between 0 and 1, indicating the varying degree of truth.

Example Problems

Question

Prove that $(x \wedge (x \rightarrow y)) \rightarrow y$ is a tautology.

Example Problems

Answer

$$
\begin{aligned}
&(x \wedge (x \to y)) \to y \\
\Leftrightarrow\ &(x \wedge (\neg x \vee y)) \to y \\
\Leftrightarrow\ &(x \wedge y) \to y \\
\Leftrightarrow\ &\neg(x \wedge y) \vee y \\
\Leftrightarrow\ &(\neg x \vee \neg y) \vee y \\
\Leftrightarrow\ &1
\end{aligned}
$$

Example Problems

Question

Prove that $((x \rightarrow \neg y) \rightarrow z) \Leftrightarrow ((x \wedge y) \vee z)$ is a tautology.

Example Problems

Answer

Let's first learn a new method to prove the tautology with logic function. Suppose we want to prove $A \rightarrow B$, then we have the following two methods:
(1) Solve the logic equation $t(A) = 1$, plug the solution into B to examine $t(B) = 1$. To solve $t(A) = 1$, we can change A to its conjunctive normal form $(A \Leftrightarrow A_1 \wedge ... \wedge A_n)$ and then solve $t(A_i) = 1$, where $i = 1, 2, ..., n$.
(2) Solve the logic equation $t(B) = 0$, plug the solution into A to examine $t(A) = 0$. To solve $t(B) = 0$, we can change B to its disjunctive normal form $(B \Leftrightarrow B_1 \vee ... \vee B_n)$ and then solve $t(B_i) = 0$, where $i = 1, 2, ..., n$.

Example Problems

Answer

Use the second method, we first prove the sufficiency.
Let $(x \wedge y) \vee z = 0$ (since it is already the DNF), then we will get $x \wedge y = 0$ and $z = 0$.
Now, we should derive that $(x \to \neg y) \to z = 0$. Since $z = 0$, we should obtain $x \to \neg y = 1$. This is just means $\neg x \vee \neg y = \neg(x \wedge y) = 1$.
For the necessity, please try it by yourself. You can also use the first method mentioned on the previous slide.

Example Problems

Question

The operators f_1 and f_2 are defined by the truth table below. Prove that $\{f_1, f_2\}$ is a minimized functionally complete set.

x	y	$f_1 x$	$x f_2 y$
0	0	1	1
0	1	1	0
1	0	0	1
1	1	0	1

Example Problems

Answer

We have already known that $\{\neg, \wedge, \vee\}$ is functionally complete, which is what you should prove in your assignment. Since:

$$x \wedge y \Leftrightarrow \neg(x \rightarrow \neg y),\ x \vee y \Leftrightarrow \neg x \rightarrow y$$

we derive that $\{\neg, \rightarrow\}$ is functionally complete. Observe that $f_1 x \Leftrightarrow \neg x$ and $x f_2 y \Leftrightarrow y \rightarrow x$. Therefore, $\{f_1, f_2\}$ is a functionally complete set.
Suppose that $f_1 x \Leftrightarrow x f_2(\ldots y f_2 \ldots)\ldots f_2 z$, then we can obtain a contradiction by assigning all the propositions as true. Therefore, this set is minimized.

Example Problems

Question

Is the following inference correct or wrong? Either mathematical logic is difficult or a minority of students do not like it. If mathematics is easy, then mathematical logic is not difficult. Therefore, if a minority of students like mathematical logic, then mathematics is not easy.

Example Problems

Answer

Let x, y and z be the following propositions:
x: "mathematical logic is difficult"
y: "a minority of students do not like mathematical logic"
z: "mathematics is easy"

(1)	$\neg y$	Premise
(2)	$x \vee y$	Premise
(3)	x	Disjunctive syllogism using (1), (2)
(4)	$z \rightarrow \neg x$	Premise
(5)	$\neg z$	Modus tollens using (3), (4)

Therefore, the inference is correct.

Example Problems

Question

Is the following inference correct or wrong? All rational numbers are real numbers; all irrational numbers are also real numbers; imaginary numbers are not real numbers. Therefore, imaginary numbers are neither rational nor irrational.

Example Problems

Answer

Introduce the quantifiers:
$Q(x)$: "x is rational" $R(x)$: "x is real"
$N(x)$: "x is irrational" $C(x)$: "x is imaginary"

(1)	$\forall x Q(x) \rightarrow R(x)$	Premise
(2)	$\forall x N(x) \rightarrow R(x)$	Premise
(3)	$\forall x C(x) \rightarrow \neg R(x)$	Premise
(4)	$C(x)$	Premise
(5)	$\neg R(x)$	Modus ponens using (3), (4)
(6)	$\neg Q(x)$	Modus tollens using (1), (5)
(7)	$\neg N(x)$	Modus tollens using (2), (5)
(8)	$\neg Q(x) \wedge \neg N(x)$	Conjunction using (6), (7)
(9)	$\forall x C(x) \rightarrow (\neg Q(x) \wedge \neg N(x))$	Universal generalization

Example Problems

Question

Prove the correctness of (2) using (1):
(1) $\forall x(P(x) \wedge Q(x)) \Leftrightarrow \forall x P(x) \wedge \forall x Q(x)$
(2) $\exists x(P(x) \vee Q(x)) \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$

Example Problems

Answer

$$
\begin{aligned}
&\exists x(P(x) \vee Q(x)) \\
\Leftrightarrow\ &\neg\neg\exists x(P(x) \vee Q(x)) \\
\Leftrightarrow\ &\neg\forall x\neg(P(x) \vee Q(x)) \\
\Leftrightarrow\ &\neg\forall x(\neg P(x) \wedge \neg Q(x)) \\
\Leftrightarrow\ &\neg(\forall x\neg P(x) \wedge \forall x\neg Q(x)) \\
\Leftrightarrow\ &\neg\forall x\neg P(x) \vee \neg\forall x\neg Q(x) \\
\Leftrightarrow\ &\exists x P(x) \vee \exists x Q(x)
\end{aligned}
$$

Example Problems

Question

Find the error in the following inference:

$$\forall x(P(x) \to Q(x))$$
$$\Leftrightarrow \forall x(\neg P(x) \vee Q(x))$$
$$\Leftrightarrow \forall x \neg(P(x) \wedge \neg Q(x))$$
$$\Leftrightarrow \neg\exists x(P(x) \wedge \neg Q(x))$$
$$\Leftrightarrow \neg(\exists x P(x) \wedge \exists x \neg Q(x))$$
$$\Leftrightarrow \neg\exists x P(x) \vee \neg\exists x \neg Q(x)$$
$$\Leftrightarrow \neg\exists x P(x) \vee \forall x Q(x)$$
$$\Leftrightarrow \exists x P(x) \to \forall x Q(x)$$

Example Problems

Answer

The reason is that $\exists x(P(x) \wedge Q(x))$ is not always equivalent to $\exists x P(x) \wedge \exists x Q(x)$. We can easily build a counter-example if we let $P(x)$ be the proposition that "x is positive" and $Q(x)$ be the proposition that "x is negative".

Example Problems

Question

Prove that $(\exists x P(x) \to \exists x Q(x)) \to \exists x(P(x) \to Q(x))$ is a tautology.

Example Problems

Answer

$$
\begin{aligned}
&(\exists x P(x) \to \exists x Q(x)) \to \exists x (P(x) \to Q(x)) \\
\Leftrightarrow\ &\neg(\neg\exists x P(x) \vee \exists x Q(x)) \vee \exists x (\neg P(x) \vee Q(x)) \\
\Leftrightarrow\ &(\exists x P(x) \wedge \neg\exists x Q(x)) \vee \exists x \neg P(x) \vee \exists x Q(x) \\
\Leftrightarrow\ &(\exists x P(x) \vee \exists x P(x) \vee \exists x Q(x)) \wedge (\neg\exists x Q(x) \vee \exists x \neg P(x) \vee \exists x Q(x)) \\
\Leftrightarrow\ &(\exists x P(x) \vee \exists x P(x) \vee \exists x Q(x)) \wedge 1 \\
\Leftrightarrow\ &(1 \vee \exists x Q(x)) \wedge 1 \\
\Leftrightarrow\ &1
\end{aligned}
$$

Example Problems

Question

Prove that $\exists x(P(x) \rightarrow Q(x)) \Leftrightarrow (\forall x P(x) \rightarrow \exists x Q(x))$ is a tautology.

Example Problems

Answer

$$\exists x(P(x) \to Q(x))$$
$$\Leftrightarrow \exists x(\neg P(x) \vee Q(x))$$
$$\Leftrightarrow \exists x \neg P(x) \vee \exists x Q(x)$$
$$\Leftrightarrow \neg \forall x P(x) \vee \exists x Q(x)$$
$$\Leftrightarrow \forall x P(x) \to \exists x Q(x)$$

Example Problems

Question

Show that $\exists x \neg R(x)$ if $\exists x \neg P(x)$, $\forall x P(x) \vee Q(x)$, $\forall x \neg Q(x) \vee S(x)$ and $\forall x(R(x) \rightarrow \neg S(x))$.

Example Problems

Answer

(1)	$\exists x \neg P(x)$	Premise
(2)	$\forall x P(x) \vee Q(x)$	Premise
(3)	$\forall x \neg Q(x) \vee S(x)$	Premise
(4)	$\forall x (R(x) \rightarrow \neg S(x))$	Premise
(5)	$\forall x P(x) \vee S(x)$	Resolution using (2), (3)
(6)	$\exists x S(x)$	Disjunctive syllogism using (1), (5)
(7)	$\forall x (S(x) \rightarrow \neg R(x))$	Logical equivalence of (4)

From (6) and (7), we can easily derive the conclusion. Here, I ignore the process of instantiation and generalization but just show you the outline.

Definition Checklist

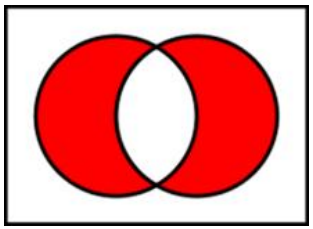
Definition

- set, subset, proper subset
- power set, cardinality
- union, intersection, difference
- ordered pair, Cartesian product
- Russell Antinomy

Additional Materials

Symmetric Difference

symmetric difference: $A \oplus B$ is the set containing those elements in either A or B, but not in both A and B.



Multisets

multisets: unordered collection of elements where an element can occur more than once.

Example Problems

Question

Prove that $A - (B \cap C) = (A - B) \cup (A - C)$
(Similarly $A - (B \cup C) = (A - B) \cap (A - C)$)

Example Problems

Answer

$A - (B \cap C)$
$= A \cap ((B \cap C)^c)$
$= A \cap (B^c \cup C^c)$
$= (A \cap B^c) \cup (A \cap C^c)$
$= (A - B) \cup (A - C)$
You can prove $A - (B \cup C) = (A - B) \cap (A - C)$ by yourself.

Example Problems

Question

Prove that $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

Example Problems

Answer

$$
\begin{aligned}
& A \cap (B \oplus C) \\
&= A \cap ((B \cap C^c) \cup (C \cap B^c)) \\
&= (A \cap B \cap C^c) \cup (A \cap C \cap B^c) \\
&= (A \cap B \cap (A^c \cup C^c)) \cup (A \cap C \cap (A^c \cup B^c)) \\
&= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\
&= (A \cap B) \oplus (A \cap C)
\end{aligned}
$$

Example Problems

Question

Prove that $\wp(A - B) \subseteq (\wp(A) - \wp(B)) \cup \{\emptyset\}$

Example Problems

Answer

For an arbitrary $x \in \wp(A-B)$, if $x = \emptyset$, it is obvious that $x \in (\wp(A)-\wp(B)) \cup \{\emptyset\}$. If $x \neq \emptyset$, then $x \subseteq (A-B)$, which means that $x \subseteq A$ and $x \nsubseteq B$. Therefore, $x \in \wp(A)$ and $x \notin \wp(B)$, which means that $x \in (\wp(A)-\wp(B))$. Hence, $\wp(A-B) \subseteq (\wp(A)-\wp(B)) \cup \{\emptyset\}$ holds true.

Example Problems

Question

Prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$
(Similarly, $(A \cap B) \times C = (A \times C) \cap (B \times C)$)

Example Problems

Answer

Suppose that $\langle x, y\rangle \in A \times (B \cup C)$
$\Leftrightarrow x \in A \wedge y \in (B \cup C)$
$\Leftrightarrow x \in A \wedge (y \in B \vee y \in C)$
$\Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C)$
$\Leftrightarrow \langle x, y\rangle \in A \times B \vee \langle x, y\rangle \in A \times C$
$\Leftrightarrow \langle x, y\rangle \in (A \times B) \cup (A \times C)$
Therefore, $A \times (B \cup C) = (A \times B) \cup (A\times)C$
You can prove $(A \cap B) \times C = (A \times C) \cap (B \times C)$ by yourself.

Example Problems

Question

If $A \cap X = B \cap X = A \cap B$, $A \cup B \cup X = A \cup B$, express X with A and B.

Example Problems

Answer

From the description, we know that $X \supseteq A \cap B$ and $X \subseteq A \cup B$.
Therefore, for all $e \in X$, we can obtain $e \in A \cup B$, which means that $e \in A$ or $e \in B$. That is to say, $e \in A \cap X$ or $e \in B \cap X$. These are both equivalent to $e \in A \cap B$, therefore $X \subseteq A \cap B$.
Hence, $X = A \cap B$

Example Problems

Question

Prove that rational numbers are as many as natural numbers.

Example Problems

Answer

We should find an one-to-one relation between $\mathbb{Q}$ and $\mathbb{N}$, since they are all infinite sets. We first list the rational numbers in the interval (0,1):

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4} \cdots$$

Then insert the reciprocal of each element just behind it and insert 1 at the beginning of the list to represent the rational numbers in the interval $(0,\infty)$:

$$1, \frac{1}{2}, 2, \frac{1}{3}, 3, \frac{2}{3}, \frac{3}{2}, \frac{1}{4}, 4, \frac{3}{4}, \frac{4}{3} \cdots$$

Example Problems

Answer

By now, we can list all the rational numbers by inserting the opposite number of each element just behind it and then inserting 0 at the beginning of the list:

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, \frac{1}{3}, -\frac{1}{3}, 3, -3, \frac{2}{3}, -\frac{2}{3}, \frac{3}{2}, -\frac{3}{2}, \frac{1}{4}, -\frac{1}{4}, 4, -4...$$

Obviously, there is an one-to-one relation between the sequence of natural numbers and the sequence shown above.
Notice that it is not allowed to use $\infty = \infty$ to prove these kinds of problems.

Example Problems

Question

Prove that real numbers are as many as complex numbers.

Example Problems

Answer

This problem is equivalent to prove that the points on a line is as many as the points on the plane.
The same as what we did in the previous problem, we should find an one-to-one relation between the points on the plane and the points on a line. For any point on a plane, such as $(a_1a_2a_3.a_4a_5a_6, b_1b_2b_3.b_4b_5b_6)$, we can build a corresponding point on a line $(a_1b_1a_2b_2a_3b_3.a_4b_4a_5b_5a_6b_6)$. This is the basic strategy.

Example Problems

Question

Let A be the subset of $S = \{1, 2, ..., 1000000\}$ with 101 elements. Prove that there exist $t_1, t_2, ..., t_{100}$ in the set S, such that the union of the any two sets defined as $A_j = \{x + t_j \mid x \in A\}$ (j=1,2,...,100) will be an empty set.

Example Problems

Question

Consider such a set $D = \{x - y \mid x, y \in A\}$. If $A_i \cap A_j \neq \emptyset$, we must obtain $x + t_i = y + t_j$, which means that $t_j - t_i = x - y$. Therefore, we only need to choose 100 integers such that the difference of any two integers is not in the set D. Now, let's choose these 100 integers iteratively.

Suppose that there have already k chosen integers ($k \leqslant 99$). A new integer e should then be chosen so that all the chosen integers are not in $\{e + t \mid t \in D\}$. There are 101*100+1=10101 elements in D, so after k integers are chosen, there are at most $10101k \leqslant 999999$ elements in S cannot be chosen. That is to say, such an e exists.

Example Problems

Question

$M = \{1, 2, ..., 10\}$ has k five-element subsets $A_1, A_2, ..., A_k$. If any two elements in M will appear together in at most two subsets, what is the maximum value of k?

Example Problems

Answer

Note the times for one element i in M to appear in these k subsets as $d(i)$ (i=1,2,...,10). From the description, one ordered pair (i, j) will appear in the subsets twice for a particular j ($j \neq i$). Since there are nine elements different from i, ordered pairs (i, j) will appear eighteen times at most. Since card(A_m)=5 (m=1,2,...,k), for a particular i, there will be four such ordered pairs in one subset. Therefore, $4d(i) \leqslant 18$, which means that $d(i) \leqslant 4$.
From this, we can derive that $5k = d(1)+d(2)+...+d(10) \leqslant 4*10 = 40 \Rightarrow k \leqslant 8$.
It's possible to examine this answer. You can define these subsets by yourself.

Example Problems

Question

The set A is a subset of $\{1, 2, ..., 100\}$. For any two elements in A, $2x \neq y$ always holds true. How many elements are there in A at most?

Example Problems

Answer

Build the subsets: $M_1 = \{51, 52, ..., 100\}$, $M_2 = \{26, 27, ..., 50\}$, $M_3 = \{13, 14, ..., 25\}$, $M_4 = \{7, 8, ..11\}$, $M_5 = \{4, 5, 6\}$, $M_6 = \{2, 3\}$ and $M_7 = \{1\}$. Then, $\text{card}(A)_{max} = \text{card}(M_1 \cup M_3 \cup M_5 \cup M_7) = 67$

Definition Checklist

Definition

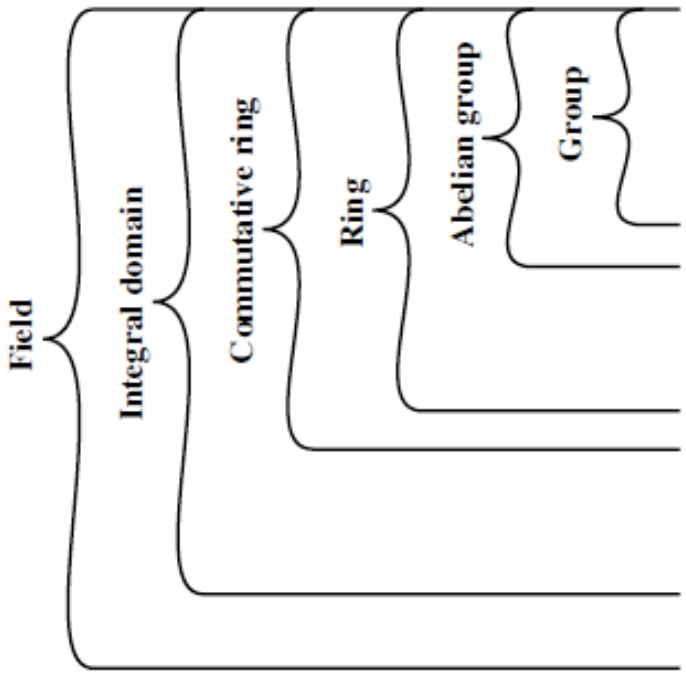
- Peano Axioms, Induction Axiom
- relation, domain, range
- reflexive, symmetric, transitive
- partition, equivalent class

Additional Materials

I will introduce you some basic knowledge about abstract algebra. Remember that we specify the set of integers with Peano Axioms during the lecture. The following axioms can be used (though not still enough) to specify the set of real numbers. These axioms can be viewed as the field axioms for real numbers. I wish that the concepts of groups, rings and fields will not only help you understanding how we specify the set of integers and real numbers, but also provide you with another point of view when you learn the number theory in the near future. The following materials are from [Stallings, 2011].

Additional Materials

The following picture can be regarded as a summary.



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \quad 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Example Problems

Question

Determine whether the following relations are reflexive, symmetric and/or transitive.

(1) $R_1 = \{\langle a, b\rangle \mid a \leqslant b, a, b \in \mathbb{Z}^+\}$

(2) $R_2 = \{\langle a, b\rangle \mid a < b, a, b \in \mathbb{Z}^+\}$

(3) $R_3 = \{\langle a, b\rangle \mid a + b = even, a, b \in \mathbb{Z}^+\}$

(4) $R_4 = \{\langle a, b\rangle \mid gcd(a, b) = 1, a, b \in \mathbb{Z}^+\}$

Example Problems

Answer

(1)reflexive transitive
(2)transitive
(3)reflexive symmetric transitive
(4)symmetric

Example Problems

Question

Let m be an integer larger than 1, $\sim$ be the relation on $\mathbb{Z}$ defined as:

$$\forall a, b \in \mathbb{Z}, a \sim b \Leftrightarrow \frac{a-b}{m} \in \mathbb{Z}$$

Prove that $\sim$ is an equivalent relation.

Example Problems

Answer

(1) $\forall a \in \mathbb{Z}$, since $\frac{a-a}{m} = 0 \in \mathbb{Z}$, we can obtain that $a \sim a$.
That is to say, $\sim$ is reflexive.

(2) $\forall a, b \in \mathbb{Z}$, if $a \sim b$, then $\frac{a-b}{m} \in \mathbb{Z}$.
Since $\frac{b-a}{m} = -\frac{a-b}{m} \in \mathbb{Z}$, we can obtain that $b \sim a$.
That is to say, $\sim$ is symmetric.

(3) $\forall a, b \in \mathbb{Z}$, if $a \sim b$, $b \sim c$, then $\frac{a-b}{m} \in \mathbb{Z}$, $\frac{b-c}{m} \in \mathbb{Z}$.
Since $\frac{a-c}{m} = \frac{a-b}{m} + \frac{b-c}{m} \in \mathbb{Z}$, we can obtain that $a \sim c$.
That is to say, $\sim$ is transitive.
From (1), (2) and (3), $\sim$ is an equivalent relation.

Example Problems

Question

Suppose that R is a symmetric and transitive relation on the set A. If for any element a in A, there exist an element b such that $\langle a, b\rangle$ belongs to R. Prove that R is an equivalent relation.

Example Problems

Answer

Since R is symmetric, then from the description $\langle b, a\rangle \in R$. Since R is transitive, then $\langle a, a\rangle \in R$. Therefore, R is also reflexive. Hence, R is an equivalent relation.

Example Problems

Question

Suppose that R is a reflexive and transitive relation on the set A. T is also a relation on A such that $\langle a, b\rangle$ is in T if and only if both $\langle a, b\rangle$ and $\langle b, a\rangle$ is in R. Prove that T is an equivalent relation.

Example Problems

Answer

According to the definition, $\langle a, a \rangle$ must be in A, since R is reflexive. Moreover, if $\langle a, b \rangle$ is in T, then $\langle b, a \rangle$ is also in T. Since R is transitive, if $\langle a, b \rangle$ and $\langle b, c \rangle$ are in T, then $\langle a, c \rangle$ is also in T. From above, T is an equivalent relation.

Example Problems

Question

Suppose that R is a reflexive relation on the set A. Prove that R is an equivalent relation if and only if when both $\langle a, b\rangle$ and $\langle a, c\rangle$ belongs to R, we will obtain that $\langle b, c\rangle$ belongs to R.

Example Problems

Answer

Since R is reflexive, let c be a, then we find that R is symmetric. Replace $\langle a, c\rangle$ with $\langle c, a\rangle$, then we find that R is also transitive. Therefore, R is an equivalent relation.

Definition Checklist

- mathematical induction, strong induction, structural induction
- well-ordering principle, recursive definition
- string, graph, tree

Additional Materials

There are not too many additional materials in this part. The only thing I want to emphasize is the strategy of inductive loading. Sometimes, you may find it useful to first prove a stronger result. I will show you some examples later.

Example Problems

Question

What's wrong with the following induction to prove that "if we are discussing n horses, then all horses have the same color?"
When $n = 1$, the proposition is obviously true. If the proposition is correct for $n = k$, then when $n = k + 1$: since the first k horses have the same color and the last k horses also have the same color, all the $k+1$ horses have the same color. By mathematical induction, all the horses have the same color.

Example Problems

Answer

From the condition for $n = 1$, we cannot induce the condition for $n = 2$.

Example Problems

Question

What's wrong with the following induction to prove that "all the positive integers are equal"?
To prove this, we only need to prove: for positive integers a and b, if $\max(a,b)=n$, then $a = b$.
For $n = 1$, since a and b are positive integers, we will obtain $a = b = 1$, which means $a = b$. If the proposition is correct for $n = k$, then when $n = k + 1$: since $\max(a,b)=k + 1$, then $\max(a - 1,b - 1)=k$. By mathematical induction, $a = b$ is always true.

Example Problems

Answer

Notice that $a-1$ or $b-1$ may be non-positive.

Example Problems

Question

For an arbitrary $n \in \mathbb{N}^+$, x_1, x_2, ..., x_n are non-negative real numbers. If $x_1 + x_2 + ... + x_n \leqslant \frac{1}{2}$, prove that $(1 - x_1)(1 - x_2)...(1 - x_n) \geqslant \frac{1}{2}$.

Example Problems

Answer

When $n = 1$, the proposition is obviously true. Suppose that the proposition is true for $n = k$, when $n = k+1$, let $x'_k = x_k + x_{k+1}$. Notice that $(1-x_k)(1-x_{k+1}) \geqslant 1-x'_k$. Therefore, from $(1-x_1)(1-x_2)...(1-x'_k) \geqslant \frac{1}{2}$, we can derive that the proposition is also true for $n = k+1$. From the mathematical induction, the proposition is true for an arbitrary $n \in \mathbb{N}^+$.

Example Problems

Question

Label the first prime number 2 as P_1. Label the second prime number 3 as P_2. Similarly, label the n-th prime number as P_n. Prove that $P_n < 2^{2^n}$ for an arbitrary $n \in \mathbb{N}^+$.

Example Problems

Answer

When $n = 1$, the proposition is obviously true. Suppose that the proposition is true for $n \leqslant k$, then we can obtain the relation:

$$P_1P_2...P_k < 2^{2^1+2^2+...+2^k} = 2^{2^{k+1}-2}\ P_1P_2...P_k + 1 < 2^{2^1+2^2+...+2^k} + 1 < 2^{2^{k+1}}$$

Since P_1, P_2, ..., P_k cannot be the factor of the left term:

$$P_{k+1} \leqslant P_1P_2...P_k + 1 < 2^{2^{k+1}}$$

From the strong induction, the proposition is true.
You can also review this question after you learn more about the prime numbers in the near future.

Example Problems

Question

Given a convex polygon with $2n + 1 (n \geqslant 2)$ sides whose adjacent vertices have different colors, prove that this polygon can be divided into several triangles with nonintersecting diagonals, so that the vertices of each diagonal have different colors.

Example Problems

Answer

We move the starting point from $n = 2$ to $n = 1$, for which the proposition is obviously true. Suppose that the proposition is true for $n = k$, then when $n = k+1$, the polygon has $2k+3$ sides. Since $2k+3$ is always an odd number, there must be a vertex v_1, whose adjacent vertices v_2 and v_{2k+3} have different colors. Now, link v_2 and v_{2k+3}, we can obtain a polygon with $2k+2$ sides. For this polygon with $2k+2$ sides:

(1) If the vertices labeled with even numbers have one same color and the vertices labeled with odd numbers have the other same color, then in the original polygon, we can just link v_1 with v_3, v_4, ..., v_{2k+2} to get the triangles.

Example Problems

Answer

(2) If there exists a vertex v_2, whose adjacent vertices v_3 and v_{2k+3} have different colors. Now, link v_3 and v_{2k+3}, we can obtain a polygon with $2k+1$ sides. Under this circumstance, the proposition is true.
By the mathematical induction, the proposition is always true.

Example Problems

Question

Given that $a_0 = 1$, $a_1 = 2$, $a_{n+1} = a_n + \dfrac{a_{n-1}}{1 + a_{n-1}^2}$ for $n \geqslant 1$, prove that $52 < a_{1371} < 65$.

Example Problems

Answer

We will first prove that for $n \geqslant 1$, $a_n = a_{n-1} + \frac{1}{a_{n-1}}$. When $n = 1$, the proposition is obviously true. Suppose that the proposition is also true for $n = k$, it is easy to derive that it holds true also for $n = k + 1$. By mathematical induction, for $n \geqslant 1$, $a_n = a_{n-1} + \frac{1}{a_{n-1}}$.

From this relation, we can derive that for $n \geqslant 1$, $a_n^2 = a_{n-1}^2 + 2 + \frac{1}{a_{n-1}^2}$, which means that $a_{n-1}^2 + 2 \leqslant a_n^2 \leqslant a_{n-1}^2 + 3$

Example Problems

Answer

Then, we should use the strategy of induction loading. Here, we will prove that for $n \geqslant 0$, $\sqrt{2n+1} \leqslant a_n \leqslant \sqrt{3n+2}$. When $n = 0$, the proposition is obviously true. Suppose that the proposition is also true for $n = k$. When $n = k+1$, we find that:

$$a_{k+1} \leqslant \sqrt{a_k^2 + 3} \leqslant \sqrt{3k+2+3} = \sqrt{3(k+1)+2}$$
$$a_{k+1} \geqslant \sqrt{a_{k^2} + 2} \geqslant \sqrt{2k+1+2} = \sqrt{2(k+1)+1}$$

By the mathematical induction, the for $n \geqslant 0$, $\sqrt{2n+1} \leqslant a_n \leqslant \sqrt{3n+2}$. Therefore, $52 < a_{1371} < 65$ is true.

Example Problems

Question

This question is from "The Puzzle TOAD" of Carnegie Mellon University, School of Computer Science.
King Arthur is preparing for a meeting of the round table. The seats at the round table are numbered 1 through n. Each seat has a reading lamp and when Arthur goes into the round table room he finds that someone has switched off some of the reading lamps. Being a king, Arthur cannot simply switch on those lights that are currently off. He has to tell somebody else to do it. So Arthur has to write down a list of numbers of seats and then get a servant to flip the switch on each light that is listed.

Example Problems

Question

The next meeting is to discuss the banishment of Merlin and the meeting can only start when all of the lights are turned on. Using a crystal ball Merlin can see the list of numbers that the king has written and is able to rotate the table before the servant gets there. So for example, if n=100 and the king asks for 3,28,97 to be flipped, then if Merlin rotates the table by 10 places, the servant will in fact flip the switch on lamps that were in positions 93,18,87 and so may flip the switch on a light that is already on. The servant is not allowed to use common-sense. Disobeying the kings instructions can be hazardous to ones health.
Find the value of n when King Arthur has the winning strategy.

Example Problems

Answer

When $n = 2^k$, King Arthur will get the winning strategy. To prove that Merlin will have the winning strategy for $n \neq 2^k$, you can try it by yourself. Let's first discuss two examples.
When $n = 1$, king Arthur will obviously win. When $n = 2$, he can let the servant to flip one of the lamps arbitrarily if the state of the two lamps are different. Since he will then get two lamps with the same state, King Arthur will win during the next round. Now, we just need to illustrate that if King Arthur can win when $n = k$, then he will also win when $n = 2k$.

Example Problems

Answer

Suppose that King Arthur will win when $n = k$ with the strategy S_k, then when $n = 2k$ we call every pair of lamps centrally symmetric as "super-lamps". We define that a super-lamp is on when both lamps belonging to it are in the same state. Then King Arthur is able to "switch on" every super-lamp with S_k. Then, we define that a super-lamp is on when both lamps belonging to it are on. Then King Arthur is able to "switch on" every super-lamp with S_k, again. By mathematical induction, King Arthur will get the winning strategy S_{k+1} for $n = k + 1$.

Definition Checklist

- function, composition, sum, product
- injection, surjection, bijection
- ceiling function, flooring function
- big-o, big-theta, big-omega

Additional Materials

The textbook provides us with a clear summary about showing whether a function is injective or surjective:

Method

For $f : A \to B$:
(1) f is injective $\Leftarrow$ show that $f(x) = f(y)$ for arbitrary $x, y \in A$ with $x \neq y$, then $x = y$
(2) f is not injective $\Leftarrow$ find $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
(3) f is surjective $\Leftarrow$ consider an arbitrary $y \in B$ and find an element $x \in A$ such that $f(x) = y$
(4) f is not surjective $\Leftarrow$ find $y \in B$ such that $f(x) \neq y$ for all $x \in A$

We will use these methods to draw some useful conclusions soon.

Additional Materials

We will practice more about the recursive sequences in the near future. Now let's just focus on the summation of the sequences.Here are some useful formulae:

Formulae

$$a_n = \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1} \qquad a_n = \frac{1}{\sqrt{n+1}+\sqrt{n}} = \sqrt{n+1} - \sqrt{n}$$

$$a_n = n \cdot n! = (n+1)! - n! \qquad a_n = \frac{n}{(n+1)!} = \frac{1}{n!} - \frac{1}{(n+1)!}$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(n+2)}{6} \qquad \sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}, \mid x \mid < 1 \qquad \sum_{k=1}^{\infty} kx^{k-1} = \frac{1}{(1-x)^2}, \mid x \mid < 1$$

Additional Materials

Some students may not be familiar with the asymptotic notation very much. According to [Leiserson et al., 2001], I would like to give you a summary of this part.

Definition

$$\Theta(g(n)) = \{f(n) \mid \exists c_1, c_2, n_0 > 0 \forall n \geqslant n_0 : 0 \leqslant c_1 g(n) \leqslant f(n) \leqslant c_2 g(n)\}$$
$$O(g(n)) = \{f(n) \mid \exists c, n_0 > 0 \forall n \geqslant n_0 : 0 \leqslant f(n) \leqslant cg(n)\}$$
$$\Omega(g(n)) = \{f(n) \mid \exists c, n_0 > 0 \forall n \geqslant n_0 : 0 \leqslant cg(n) \leqslant f(n)\}$$
$$o(g(n)) = \{f(n) \mid \forall c > 0 \exists n_0 > 0 \forall n \geqslant n_0 : 0 \leqslant f(n) \leqslant cg(n)\}$$
$$\omega(g(n)) = \{f(n) \mid \forall c > 0 \exists n_0 > 0 \forall n \geqslant n_0 : 0 \leqslant cg(n) \leqslant f(n)\}$$

We can also draw an analogy between the asymptotic comparison of two functions f and g and the comparison of two real numbers a and b:

Additional Materials

Analogy

$$f(n) = O(g(n)) \approx a \leqslant b$$
$$f(n) = \Omega(g(n)) \approx a \geqslant b$$
$$f(n) = \Theta(g(n)) \approx a = b$$
$$f(n) = o(g(n)) \approx a < b$$
$$f(n) = \omega(g(n)) \approx a > b$$

Now, let's review the concept of the basic relations. We can obtain the following more theorems. You can prove them as exercises if you would like to do this.

Theorem

Reflexivity: $f(n) = O(f(n))$ $f(n) = \Omega(f(n))$ $f(n) = \Theta(f(n))$
Symmetry: $f(n) = \Theta(g(n)) \Leftrightarrow g(n) = \Theta(f(n))$

Additional Materials

Theorem

Transpose symmetry:

$f(n) = O(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$

$f(n) = o(g(n)) \Leftrightarrow g(n) = \omega(f(n))$

Transitivity:

$f(n) = O(g(n)), g(n) = O(h(n)) \Rightarrow f(n) = O(h(n))$

$f(n) = \Omega(g(n)), g(n) = \Omega(h(n)) \Rightarrow f(n) = \Omega(h(n))$

$f(n) = \Theta(g(n)), g(n) = \Theta(h(n)) \Rightarrow f(n) = \Theta(h(n))$

$f(n) = o(g(n)), g(n) = o(h(n)) \Rightarrow f(n) = o(h(n))$

$f(n) = \omega(g(n)), g(n) = \omega(h(n)) \Rightarrow f(n) = \omega(h(n))$

There is a property of trichotomy for the comparison of two real numbers. Your assignment will ask you to discuss whether there is a similar property for the asymptotic comparison of two functions.

Example Problems

Question

Prove (or at least remember) the following conclusions:
(1) If f and g are both surjective, then $g \circ f$ is also surjective.
(2) If f and g are both injective, then $g \circ f$ is also injective.
(3) If f and g are both bijective, then $g \circ f$ is also bijective.
(4) If $g \circ f$ is surjective, then g is surjective.
(5) If $g \circ f$ is injective, then f is injective.
(6) If $g \circ f$ is bijective, then g is surjective and f is injective.
Notice that $f : A \to B$ and $g : B \to C$

Example Problems

Answer

I will prove the first three conclusions for you. For the remaining three terms, please try it by yourself.
(1) Consider a $y \in C$, then we can find $g(t) = y$. For this $t \in B$, we can find $f(x) = t$. Therefore, for a $y \in C$, we can find an $x \in A$ such that $(g \circ f)(x) = y$. Therefore, $g \circ y$ is surjective.
(2) Consider $x, y \in A$ and $x \neq y$, then $f(x) \neq f(y)$. For these $f(x), f(y) \in B$, we can obtain $g(f(x)) \neq g(f(y))$. Therefore, $g \circ f$ is injective.
(3) From (1) and (2), we can draw the conclusion.

Example Problems

Question

Is the following function $f : A \to B$ injective and/or surjective?

(1) $A = B = \mathbb{Z}^+$ $f(x) = x + 1$

(2) $A = B = \mathbb{Z}^+$ $f(x) = x - 1$ for $x > 1$, $f(x) = 1$ for $x = 1$

(3) $A = B = \mathbb{R}^+$ $f(x) = \dfrac{x}{x^2 + 1}$

Example Problems

Answer

(1) Obviously, f is injective. Also, f is not surjective since $1 \notin Ran(f)$
(2) Obviously, f is surjective. Also, f is not injective since $f(1) = f(2)$
(3) Since $f(x) \to 0$ when $x \to 0$ and when $x \to \infty$, also $f(1) = 0.5$ is its maximum, f is not injective. Since $f(x)$ is not $\mathbb{R}^+$, f is not surjective.

Example Problems

Question

There are two sequences, $\{a_n\} = \{3^n\}$ and $\{b_n\} = \{4n + 3\}$. If $d \in \{a_1, a_2, ...\} \cap \{b_1, b_2\}$, then d is called a common term of $\{a_n\}$ and $\{b_n\}$. List all common terms of $\{a_n\}$ and $\{b_n\}$ as shown in the original sequences to form a new sequence $\{d_n\}$. Prove that $\{d_n\} = \{3^{2n+1}\}$

Example Problems

Answer

Suppose that $a_m = b_k$, then $3^m = 4k + 3$. Notice that $3^{m+1} = 4(3k + 2) + 1$, therefore a_{m+1} is not in $\{b_n\}$. Similarly, a_{m+2} is in $\{b_n\}$. That is to say $d_{n+1} = 9d_n$. Since $d_1 = 27$, we conclude that $d_n = 3^{2n+1}$

Example Problems

Question

For the sequence $\{a_n\}$, $S_n = \sum_{k=1}^{n} a_k = 2a_n - 1$. For the sequence $\{b_n\}$, $b_1 = 3$, $b_{n+1} = b_n + a_n$. Find $T_n = \sum_{k=1}^{n} b_k$

Example Problems

Answer

Since $S_1 = a_1$, we have $a_1 = 1$. When $n \geqslant 2$, $a_n = S_n - S_{n-1} = 2a_n - 2a_{n-1}$. Therefore, $a_n = 2a_{n-1}$. Since $b_n = b_1 + (b_2 - b_1) + (b_3 - b_2) + ... + (b_n - b_{n-1})$, we conclude that $b_n = 3 + \frac{1-2^{n-1}}{1-2} = 2^{n-1} + 2$. Therefore, $T_n = 2^n + 2n - 1$

Example Problems

Question

For the sequence $\{a_n\}$, $a_1 = 2$ and $\{\frac{a_n}{n}\}$ is a geometric progression with the common ratio equal to 2. Find $S_n = \sum_{k=1}^{n} a_k$

Example Problems

Answer

It is easy to find that $a_n = n2^n$. Then, $S_n = 2S_n - S_n = (n-1)2^{n+1} + 2$

Example Problems

Question

Find S_{99} for $\{a_n\} = \{\frac{1}{n\sqrt{n+1}+(n+1)\sqrt{n}} + \frac{k+2}{k!+(k+1)!+(k+2)!}\}$

Example Problems

Answer

Notice that $\frac{1}{n\sqrt{n+1}+(n+1)\sqrt{n}} = \frac{\sqrt{n}}{n} - \frac{\sqrt{n+1}}{n+1}$ and $\frac{k+2}{k!+(k+1)!+(k+2)!} = \frac{1}{(k+1)!} - \frac{1}{(k+2)!}$.

So we can obtain $S_{99} = \frac{7}{5} - \frac{1}{101!}$

Example Problems

Question

Given two nonnegative sequences $\{a_n\}$ and $\{b_n\}$, prove that $\{c_n\} = \{max(a_n, b_n)\}$ is $\Theta(a_n + b_n)$

Example Problems

Answer

Since for all $n \in \mathbb{N}^+$, $a_n \geqslant 0$ and $b_n \geqslant 0$, we obtain that $c_n \leqslant a_n + b_n$. Therefore, $\{c_n\} = O(a_n + b_n)$ holds true. We can also obtain that $c_n \geqslant 0.5(a_n + b_n)$. Therefore, $\{c_n\} = \Omega(a_n + b_n)$ holds true. Therefore, $\{c_n\} = \{max(a_n, b_n)\}$ is $\Theta(a_n + b_n)$.

Example Problems

Question

Prove that for arbitrary constant real numbers a and b ($b > 0$), $(n + a)^b = \Theta(n^b)$ holds true.

Example Problems

Answer

Notice that $n+ \mid a \mid \geqslant n + a \geqslant n- \mid a \mid$. Since a is constant, we can find an n_0 such that when $n \geqslant n_0$, $2n \geqslant n+ \mid a \mid \geqslant n + a$. Also, we can find an n_1 such that when $n \geqslant n_1$, $n + a \geqslant n- \mid a \mid \geqslant 0.5n$. Therefore, $(n + a)^b = O(n^b)$ and $(n + a)^b = \Omega(n^b)$, which means that $(n + a)^b = \Theta(n^b)$.

Example Problems

Question

Prove that $\log n!$ is $\Theta(n \log n)$

Example Problems

Answer

$\log n! \leqslant \log n^n = n\log n \Rightarrow \log n! = O(n\log n)$
$2\log n! = \log(n!)^2 = \log\prod_{k=1}^{n}(n-k)(k+1) \geqslant \log n^n \Rightarrow \log n! = \Omega(n\log n)$
Therefore, $\log n!$ is $\Theta(n\log n)$

Example Problems

Question

If we would like to expand the definition of asymptotic notation from one variable to two variables, which of the following definition is valid? Why?

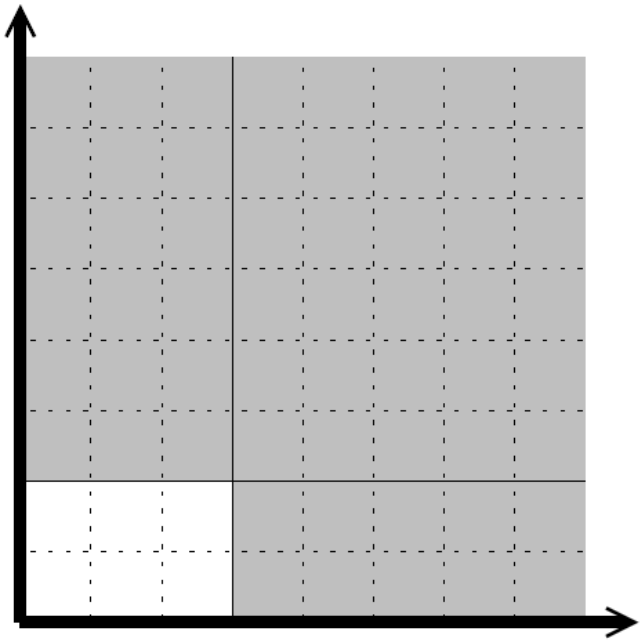
(1) $O(g(n,m)) = \{f(n,m) \mid \exists c, n_0, m_0 > 0 \forall n \geqslant n_0$ **or** $m \geqslant m_0 : 0 \leqslant f(n,m) \leqslant cg(n,m)\}$

(2) $O(g(n,m)) = \{f(n,m) \mid \exists c, n_0, m_0 > 0 \forall n \geqslant n_0$ **and** $m \geqslant m_0 : 0 \leqslant f(n,m) \leqslant cg(n,m)\}$

Example Problems

Answer

Consider the original definition of the big-O notation on a number axis. We find that $n \geqslant n_0$ is represented by the right side of the point $n = n_0$. That is to say, on the rectangular coordinate system, we should determine which definition can represent the shaded part. Therefore, definition (1) is valid.



Definition Checklist

- algorithm, pseudocode, properties
- linear search, binary search
- bubble sort, insertion sort, merge sort
- greedy algorithm, recursive algorithm, iterative algorithm
- program correctness, time complexity, complexity classes

Additional Materials

There is another common sorting algorithm based on comparisons of pairs of elements, called selection sort. Its time complexity is $\Theta(n^2)$. You can prove this by yourself. You can also try to prove the program correctness of this algorithm.

Selection Sort

procedure: *selectionsort*($a_1, a_2, ..., a_n$: real numbers with $n \geqslant 2$)

```
for i := 1 to n − 1 do
    k := i;
    for j := i + 1 to n do
        if a_j < a_k then
            k := j;
    swap(a_i, a_k);
```

Additional Materials

About algorithms, the two important issues are "program correctness" and "time complexity". More difficult time complexity analysis will be covered in the near future. Let's just mainly focus on the part of program correctness. During the lecture, a useful concept, loop invariant, is introduced.

Loop Invariant

Loop invariant is the assertion that should remain true during the whole algorithm. The following three steps are needed when proving the program correctness with loop invariant.

Initialization: it is true prior to the first iteration of the loop

Maintenance: if it is true before an iteration, it remains true before the next iteration

Termination: when the loop terminates, the invariant gives us a useful property that helps show that the algorithm is correct

Also, do not forget to show that the program can actually terminate.

Example Problems

Question

In your assignment, you got an exercise about "binary insertion sort". Will the use of binary search in the insertion sort improve the worst-case complexity of the normal insertion sort? Why?

Example Problems

Answer

No! The reason is that though the worst-case complexity of the searching part is improved to $\Theta(\log n)$, the worst-case complexity of the moving and inserting part is still $\Theta(n)$. So the whole complexity should still be $\Theta(n^2)$.

Example Problems

Question

Design an algorithm with the worst-case complexity of $\Theta(n\log n)$, so that given an integer x and a set S containing n integers, we are able to judge whether there are two integers in S whose sum is equal to x.

Example Problems

Answer

The key point is remembering we are able to sort an array with the worst-case complexity of $\Theta(n\log n)$ and search an element in a sorted array with the worst-case complexity of $\Theta(\log n)$. We can first sort the integers in S. For each element t in S, we should check whether $x - t$ is in this sorted set.

Example Problems

Question

Given an array containing n different integers, design an algorithm with the worst-case complexity of $\Theta(n\log n)$ to calculate the amount of inversions in this array. An inversion means a pair (i, j) such that if $i < j$ then $a_i > a_j$.

Example Problems

Answer

There exists several algorithms using many data structures enable us to find the amount of inversions in an array. But, let's just focus on the method concerning sorting algorithm today.
A straight-forward method may be the bubble sort. (Why? Think it by yourself.) But the worst-case complexity is $\Theta(n^2)$ for this method. Actually, a modification on merge sort can lead us to the answer. Before we achieve the algorithm, we should first have a look at the original merge sort and find what happens in the procedure of **merge**(L_1, L_2: sorted lists) in the lecture.
We found that every elements in L_2 should appear after all the elements in L_1 in the original list. That is to say, if we found that if the smallest elements in these two lists is the first elements in L_2, then we should add the amount of remaining elements in L_1 to the amount of inversions.

Example Problems

Answer

This is the pseudocode for this design.

procedure: *mergesort*(A: list to sort, st: start index, en: end index)

if $st = en$ **then exit**;
$mid := (st + en) \ / \ 2$;
mergesort(A, st, mid);
mergesort$(A, mid + 1, en)$;
$i := 1$; $j := st$; $k := mid + 1$;
while $i \leqslant en - st + 1$ **do**
  if $k = en + 1$ **or** $A_j < A_k$ **and** $j \leqslant mid$ **then**
    $L_i := A_j$; $j := j + 1$; $i := i + 1$;
  else
    $L_i := A_k$; $k := k + 1$; $i := i + 1$; $cnt := cnt + mid + 1 - j$;
$A_{st..en} := L_{1..en-st+1}$;

Example Problems

Question

There is a series of problems called knapsack problems. Most of them are always closely related to dynamic programming, which will be covered in VE281. But one of these problems, called fractional knapsack problem, can be solved with a greedy algorithm. Please design a greedy algorithm for the following fractional knapsack problem:
There exist several kinds of products with different value w_i per unit volume and volume v_i. Tom has a bag with a volume of V. If Tom can take away any amount of any product in his bag, what is the maximized value of the products he takes?

Example Problems

Answer

The strategy is to take the product with the value per volume as high as possible. The pseudocode is shown as following:

procedure: *fracKnap*(*products*)

```
sort(products);
value := 0; load := 0; i := n;
while load < V and i > 0 do
    if V − load > v_i then
        load := load + v_i; value := value + w_i ∗ v_i;
    else
        value := value + w_i ∗ (V − load); load := V;
    i := i + 1;
```

Example Problems

Question

Let's discuss another kind of important problem about the greedy algorithm. It is called "activity selection". Given a set of activities a_i with separate start time s_i and finish time f_i, select the largest possible set of nonoverlapping activities. One greedy algorithm is to choose the activity with the duration time d_i as short as possible. Is it correct?

Example Problems

Answer

No! The following table give us a counter example:

i	s_i	d_i	f_i
1	0	3	3
2	2	2	4
3	3	3	6

According to the algorithm, only the second activity will be chosen. But the best choice is to choose the other two activities.

Example Problems

Question

Let's provide another greedy algorithm for "activity selection". We choose the activity with the finish time as early as possible. Is it correct?

Example Problems

Answer

Yes! Let's first define a set $S_{i,j}$ as following:

$$S_{i,j} = \{a_k \mid f_i \leqslant s_k < f_k \leqslant s_j\}$$

If we also define $f_0 = 0$ and $s_{n+1} = \infty$, then the original activity set is $S_{0,n+1}$. If we list all the activities with the ordering of ascending finish time, then we find that $S_{i,j} = \emptyset$ for $i \geqslant j$. Now, define the amount of activities in the largest possible set of nonoverlapping activities for $S_{i,j}$ as following:

$$C_{i,j} = max\{C_{i,k} + 1 + C_{k,j}\} \text{ for } a_k \in S_{i,j}$$

What we did by now is a process of "dynamic programming". I wish it is clear enough to understand.

Example Problems

Answer

Before we derive the greedy algorithm, let's first prove that for a set $S_{i,j}$, if a_m is the activity with the earliest finish time, then:
(1) $S_{i,m}$ is empty
(2) a_m should be select
To prove (1), we can simply suppose that $S_{i,m}$ is not empty and use proof by contradiction. To prove (2), we still use proof by contradiction. Let a_k be the activity in the largest possible set of nonoverlapping activities for $S_{i,j}$ with the earliest finish time. If $a_k \neq a_m$, it is valid for us to replace a_k with a_m. Now, we can obtain:

$$C_{i,j} = 1 + C_{k,j} \text{ for } a_k \in S_{i,j} \text{ with the earliest finish time}$$

This is just the greedy algorithm in the question description.

Example Problems

Question

Suppose that we have two sets A and B with n positive integers in each set. You can arrange the elements in either set in any order. Now, let's call the i-th element in A as a_i and the i-th element in B as b_i. How to maximize the product $\prod_{i=1}^{n} a_i^{b_i}$ with greedy algorithm?

Example Problems

Answer

We can sort both sets in ascending order. Suppose that $i < j$, then $a_i \leqslant a_j$ and $b_i \leqslant b_j$. Since they are all positive numbers, $a_i^{b_j - b_i} \leqslant a_j^{b_j - b_i}$. Multiply both sides with $(a_i a_j)^{b_i}$ to obtain $a_i^{b_j} a_j^{b_i} \leqslant a_i^{b_i} a_j^{b_j}$

Example Problems

Question

Counting sort is useful when we want sort several discrete elements with a certain range. Suppose we have n elements to sort and each element may be one of k different possible values. Find the time complexity of this algorithm. Specially, what if $k = O(n)$? (Suppose that we want to sort the integers $1 \leqslant a_i \leqslant k$)

procedure: $countingsort(a_{1..n}, k)$

for $i := 1$ **to** k **do** $c_i := 0$
for $i := 1$ **to** n **do** $c_{a_i} := c_{a_i} + 1$;
$p := 1$;
for $i := 1$ **to** k **do**
  for $j := 1$ **to** c_i **do**
    $b_p := i$; $p := p + 1$;
$a_{1..n} := b_{1..n}$;

Example Problems

Answer

It requires k steps in the first loop, n steps in the second loop and n steps in the last statement. There is also one single statement. It can be easily shown that it requires $2n$ steps in the third loop. So, in total, $4n + k + 1$ steps are needed. Therefore, the time complexity is $\Theta(k + n)$. If $k = O(n)$, the time complexity becomes $\Theta(n)$.

Example Problems

Question

Horner's rule can be shown as:

$$P(x) = \sum_{k=0}^{n} = a_0 + x(a_1 + x(a_2 + ... + x(a_{n-1} + xa_n)))$$

Given the coefficients a_0, a_1, ..., a_n and x, we can calculate $P(x)$ with the following pseudocode:

procedure: $horner(a_{0..n}, x)$

$y := 0$; $i := n$;

while $i \geqslant 0$ **do**

$y := a_i + x \cdot y$;

$i := i$ - 1;

Prove the program correctness.

Example Problems

Answer

The loop invariant is that at the beginning of every iteration of this loop:

$$y = \sum_{k=0}^{n-(i+1)} a_{k+i+1} x^k$$

Initialization: At the beginning of this whole loop, $y = 0$ and $i = n$. The loop invariant is true.

Maintenance: Suppose that the loop invariant is true for $i = m$, then for $i = m-1$, we obtain:

$$\begin{aligned} y &= a_m + x \cdot \left(\sum_{k=0}^{n-(i+2)} a_{k+i+2} x^k\right) \\ &= a_m + \sum_{k=0}^{n-(i+2)} a_{k+i+2} x^{k+1} \\ &= a_m + \sum_{k=1}^{n-(i+1)} a_{k+i+1} x^k \\ &= a_{i+1} + \sum_{k=1}^{n-(i+1)} a_{k+i+1} x^k \\ &= \sum_{k=0}^{n-(i+1)} a_{k+i+1} x^k \end{aligned}$$

Example Problems

Answer

Termination: When this whole loop ends, $i = -1$. Since the loop invariant still holds true, we check that this is the result we want.
Since i is always subtracted by one in every iteration, the loop will terminate after $n + 1$ iterations. From what we discussed by now, the program is correct.

Definition Checklist

- division, modular arithmetic, hash function
- pseudorandom number, prime number, pseudoprime
- GCD, LCM, the Euclidean Algorithm
- base conversion, addition, multiplication, modular exponentiation
- linear congruence, Chinese Remainder Theorem
- RSA, Caeser's Cipher

Additional Materials

In the lecture, it said that the greatest common divisor of a and b can be expressed as a linear combination of a and b with integer coefficients. This work can be done by the extended Euclidean Algorithm, whose correctness is left for you to prove in the assignment. The following is the recursive version of this algorithm:

procedure: $extgcd(a, b, x, y, d\text{: } ax + by = d = gcd(a, b))$

  if $b = 0$ then

    $d := a$; $x := 1$; $y := 0$;

  else

    $d := extgcd(b, a \bmod b, x, y)$;

    $t := x$; $x := y$; $y := t - (a \operatorname{div} b)y$

It will also be clear for you to prove and understand this algorithm if you derive the iterative version. This is a very important algorithm in the number theory.

Additional Materials

In the Chinese Remainder Theorem, one step is to find an multiplicative inverse M_k^{-1} to M_k modulo m_k. This can be done by applying the extended Euclidean Algorithm, since $gcd(M_k, m_k) = 1 = M_k x + m_k y$. Then x is the multiplicative inverse M_k^{-1} we want.
Now, I will introduce the Euler ϕ function and some useful theorems.

Definition

Euler *phi* function *phi*(n) is equal to the number of positive integers less than or equal to n that are relatively prime to n.

Theorem

(1) If p is a prime number, then $\phi(p^n) = p^{n-1}(p-1)$
(2) If $gcd(m, n) = 1$*, then* $\phi(mn) = \phi(m)\phi(n)$
(3) If $gcd(m, n) = 1$*, then* $m^{\phi(n)} \equiv 1 \ mod \ n$

Example Problems

Question

Given a hash function H, with n possible outputs and a specific value $H(x)$, if H is applied to k random inputs, what must be the value of k so that the probability that at least one input y satisfies $H(y) = H(x)$ is 0.5?

Example Problems

Answer

For a single value of y, the probability that $H(y) \neq H(x)$ is $1 - \frac{1}{n}$. If we generate k random values of y, the probability that there is at least one match $H(y) = H(x)$ is $1 - (1 - \frac{1}{n})^k$. For a hash function, n is always very large, which means that $\frac{1}{n}$ is very small. Therefore, the probability will be approximated as $\frac{k}{n}$. For a probability of 0.5, we obtain $k = \frac{n}{2}$.

This is just the condition when we are provided with a specific value $H(x)$. If we want an arbitrary hash collision among the k outputs with the probability of 0.5, what must be the value of k? The answer is $k = \sqrt{n}$. This is based on the birthday paradox. You will learn this in VE401.

Example Problems

Question

Stein's Algorithm can also be used to calculate the gcd of two integers:

procedure: $gcd(a, b, d)$

$A_1 := a$; $B_1 := b$; $C_1 := 1$; $n := 1$;

while $A_n \neq B_n$ **do**

if A_n, B_n *are even* **then**

$A_{n+1} := A_n/2$; $B_{n+1} := B_n/2$; $C_{n+1} := 2C_n$;

if A_n, B_n *are odd* **then**

$A_{n+1} := \mid A_n - B_n \mid$; $B_{n+1} := \mathbf{min}(A_n, B_n)$; $C_{n+1} := C_n$;

if A_n *is odd and* B_n *is even* **then**

$A_{n+1} := A_n$; $B_{n+1} := B_n/2$; $C_{n+1} := C_n$;

if A_n *is even and* B_n *is odd* **then**

$A_{n+1} := A_n/2$; $B_{n+1} := B_n$; $C_{n+1} := C_n$;

$d := A_n C_n$;

Example Problems

Question

Show that this algorithm has roughly the same time complexity as the Euclidean Algorithm. For convenience, we suppose that $1 \leqslant a, b \leqslant 2^n$. What is the advantage of Stein's Algorithm over Euclidean Algorithm?

Example Problems

Answer

If at least one of A and B is even, then the product of A and B can be reduced by 2. If both A and B are odd, then A will be even in the next round. That is to say, every two iterations reduces the product of A and B at least by 2. The product starts from 2^{2n}, so there are at most $2n$ pairs of iterations, or at most $4n$ iterations. Therefore, the time complexity is $O(n)$, which is the same as the time complexity of the Euclidean Algorithm.

Euclidean Algorithm requires a "long division" at each step whereas the Stein algorithm only requires division by 2, which is a simple operation in binary arithmetic.

Example Problems

Question

Calculate the multiplicative inverse u^{-1} to $u = 13$ modulo $m = 35$.

Example Problems

Answer

Here, we use the extended Euclidean Algorithm.

a	b	a/b	d	x	y
35	13	2	1	3	-8
13	9	1	1	-2	3
9	4	2	1	1	-2
4	1	4	1	0	1
1	0	-	1	1	0

Therefore, u^{-1} = -8 mod 35 = 27

Also, notice that $\phi(35) = \phi(5)\phi(7) = 24$. Therefore, u^{-1} can also be determined from 13^{23} mod 35. Since 13^2 mod 35 is 29 and 13^4 mod 35 is 1. So we just calculate 13^3 mod 35, which is also 27.

Example Problems

Question

There are n $(3 \leqslant n)$ players $(p_1, p_2, \ldots, p_n)$ playing a game. In the first round, player p_1 has a ball. Then the player with ball should pass it to the k-th player on his/her left hand side. What is the maximized value of k $(1 \leqslant k \leqslant \frac{n}{2})$, so that everyone can get the ball before the ball is passed back to p_1?

Example Problems

Answer

We first translate this description into a mathematical way: given an integer n, find the maximized value of k $(1 \leqslant k \leqslant \frac{n}{2})$, so that $gcd(k, n) = 1$. Now, let's analyze this problem from the view of parity.

(1) If n is odd, then k can be determined by $k = \frac{n-1}{2}$

(2) If n is even and n is a multiple of 4, then $k = \frac{n}{2} - 1$

(3) If n is even but n is not a multiple of 4, then $k = \frac{n}{2} - 2$

Example Problems

Question

Prove that if we can factorize m as $p_1^{k_1}...p_s^{k_s}$, then $\phi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_s})$

Example Problems

Answer

It is easy to get this relation from the two theorems about the Euler ϕ function in the previous slide. You just need to remember this general expression of the Euler ϕ function.

Example Problems

Question

The Fibonacci number sequence is 1, 1, 2, 3, 5, 8, 13 and so on. You can see that except the first two numbers the others are summation of their previous two numbers. A Fibonacci Prime is a Fibonacci number which is relatively prime to all the smaller Fibonacci numbers. First such Fibonacci Prime is 2, the second one is 3, the third one is 5, the fourth one is 13 and so on. Given the index of a Fibonacci number n, design an algorithm with the time complexity of $\Theta(\sqrt{n})$ to judge whether this number is a Fibonacci Prime?

Example Problems

Answer

Let's first consider the remainders produced by dividing each Fibonacci number by a particular Fibonacci number m. Suppose these remainders will form a sequence $\{s_i\}$. Then $s_1 = s_2 = 1$ obviously holds true. Let s_k be the first element with the value of 0 when $s_{k-1} = a$, then $s_{k+1} = s_{k+2} = a$, $s_{k+3} = 2a$, $s_{k+4} = 3a$, $s_{k+5} = 5a$ and the list will go on. That is to say, from $s_{k+i} = F_i a \bmod m = F_i a \bmod F_k$. Therefore, when and only when p is a multiple of k, $s_p = 0$. This means that F_a is a multiple of F_b if a is a multiple of b ($a > b \geqslant 1$). Hence, we can consider the first four terms separately. From the fifth term, we just need to judge whether n is a prime number or not. From what you learnt in VG101, it is possible to design such an algorithm with the time complexity of $\Theta(\sqrt{n})$.

Example Problems

Question

Prove that $gcd(F_n, F_m) = F_{gcd(n,m)}$

Example Problems

Answer

From the previous problem, F_n is a multiple of F_i when n is a multiple of i. Similarly, F_m is a multiple of F_j when m is a multiple of j. Therefore, F_i and F_j may be equal only when i and j can be the multiple of n and m at the same time. Hence, to find the greatest Fibonacci number satisfying this condition, we must let i and j be the greatest common divisor of n and m.

Example Problems

Question

Since the prime numbers are always playing an important role in the cryptography, we might want to find such a nonconstant polynomial $f(n)$ with integer coefficients that $f(n)$ is prime for all $n \in \mathbb{N}^+$. Find such a polynomial or show that it is impossible to do this.

Example Problems

Answer

It is impossible to do this. Suppose that $f(x) = p$ is a prime number. Then $f(x+p) = f(x) + g(p)$, where p can always divide $g(p)$.

Example Problems

Question

Show that in RSA, knowing $\phi(n)$, knowing the factorization of n and obtaining a successful attack are all equivalent sayings.

Example Problems

Answer

If we know, $n = pq$ and $\phi(n) = (p-1)(q-1)$, then we can also get $\phi(n) - n - 1 = -(p+q)$. Therefore, we can form the equation $x^2 + (\phi(n) - n - 1)x + n = 0$ and solve it. The root of this equation is just p and q.
In RSA, if we know the factorization of $n = pq$, then we can easily get $\phi(n) = (p-1)(q-1)$. Then by the Extended Euclid Algorithm, we can get the inverse element of e, which is also d. If we know d, which is the private key, we can break RSA. So knowing either $\phi(n)$ or the factorization of n can lead to breaking RSA. So, they are equivalent in this system.

Example Problems

Question

In RSA, it is required that the difference n between p and q is not very small. Design a successful attack to RSA with the worst-case time complexity of $\Theta(n)$

Example Problems

Answer

The strategy is just to try every possible difference from 0 to n. For any difference k, we have $n = p(p+k) = p^2 + kp$. Therefore, we can just check whether the root p for this equation is an integer or not.
These are just two basic problems about RSA. If you are interested in cryptography, I recommend you to take the course CS381(English) in the School of Electronic, Information and Electrical Engineering during the spring semester.

Definition Checklist

- addition principle, multiplication principle
- pigeonhole principle, generalized pigeonhole principle
- Ramsey Theorem, Ramsey Numbers
- permutation and combination for a set
- permutation and combination for a multiset
- generating permutation and combination
- lexicographic ordering

Additional Materials

I will choose some interesting materials from [Brualdi, 2010] during the two sections about combinational mathematics. This is also the book about combinational mathematics I like most.
In the lecture we learnt the simple pigeonhole principle. We also have a look at the generalized version of this principle. Actually, there is a strong form of pigeonhole principle, from which the generalized pigeonhole principle can be derived. I wish that you could find it useful sometime.

Strong Pigeonhole Principle

Let $q_1, q_2, ..., q_n$ be positive integers. If $q_1 + q_2 + ... + q_n - n + 1$ objects are distributed into n boxes, then either the first box contains at least q_1 objects, or the second box contains at least q_2 objects, ..., or the n-th box contains at least q_n objects.

You can try to prove it by yourself.

Additional Materials

The permutations that we discussed so far are all called linear permutations. If we want to arrange objects in a circle instead of a line, the number of permutations will be smaller.

Circular Permutation

The number of circular r-permutations of a set of n elements is given by

$$\frac{P(n,r)}{r} = \frac{n!}{r(n-r)!}$$

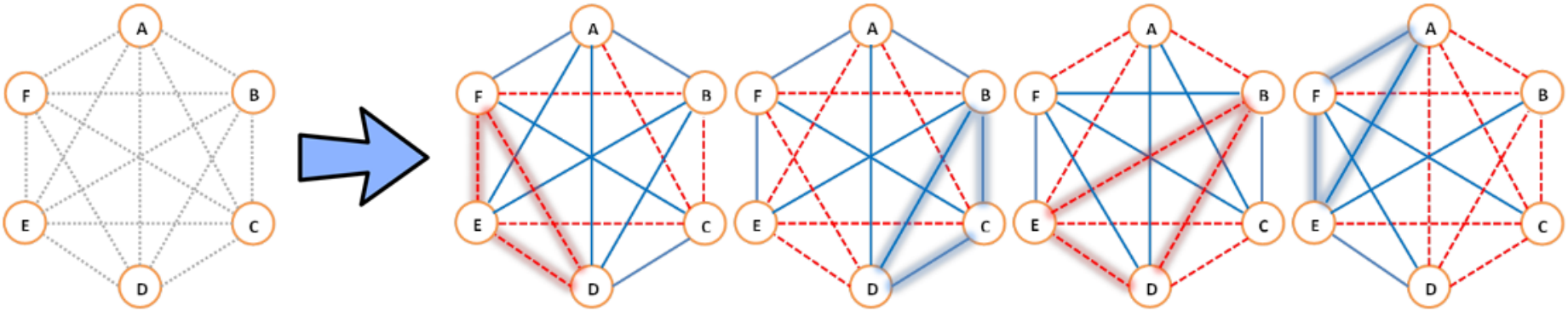
In particular, the number of circular permutations of n elements is $(n-1)!$.

Additional Materials

We can try to illustrate Ramsey Theorem from the view of complete graph. Denote K_n as the complete graph of order n (a set of n objects and all of the pairs of these objects). Then, we can explain the Ramsey Theorem as:

Ramsey Theorem

No matter how the edges of K_6 are colored with red and blue, there is always a red K_3 or a blue K_3.



Example Problems

Question

How many integers between 0 and 10000 have only one digit equal to 5?

Example Problems

Answer

Let S be the set of integers between 0 and 10000 with only one digit equal to 5. By including leading zeros (i.e., think of 6 as 0006, 25 as 0025, 352 as 0352), we can regard each number in S as a four-digit number. Now we partition S into the set S_1', S_2', S_3' and S_4' according to whether the 5 is in the first, second third or fourth position. Each of the four sets in the partition contains $9^3 = 729$ integers, and so the number of integers in S equal to 2916.

You can find that the way how we partition a set is important. If we partition S respect to the number of digits that an integer has and use addition principle as well as multiplication principle several times, then "hehe..."

Example Problems

Question

We have 20 beads with different colors. What is the number of necklaces that can be made from 12 bead?

Example Problems

Answer

From the formula of circular r-permutation, the answer seems to be:

$$\frac{P(20,12)}{12} = \frac{20!}{12 \cdot 8!}$$

But notice that a necklace can be turned over without change the arrange of the beads. So the answer should be:

$$\frac{P(20,12)}{2 \cdot 12} = \frac{20!}{2 \cdot 12 \cdot 8!}$$

Example Problems

Question

How many methods are there to divide n objects into k same boxes with each boxes containing $n_1, n_2, ..., n_k$ objects $(n = n_1 + n_2 + ... + n_k)$.

Example Problems

Answer

If all the boxes are different, then this is a simple problem about permutation for a multiset. However, if all the boxes are the same, then for each way of distributing the objects into k boxes, there are $k!$ ways in which we can now attach the label $1, 2, ..., k$. Therefore, the answer is:

$$\frac{n!}{k!n_1!n_2!...n_k!}$$

Example Problems

Question

What is the number of integral solutions of the equation

$$x_1 + x_2 + x_3 + x_4 = 20$$

in which

$$x_1 \geqslant 3, x_2 \geqslant 1, x_3 \geqslant 0 \text{ and } x_4 \geqslant 5$$

Example Problems

Answer

We introduce the new variables

$$y_1 = x_1 - 3,\ y_2 = x_2 - 1,\ y_3 = x_3,\ y_4 = x_4 - 5$$

and our equation becomes

$$y_1 + y_2 + y_3 + y_4 = 11$$

The lower bounds on the x_i's are satisfied if and only if the y_i's are nonnegative. The number of nonnegative integral solutions of new equation, and hence the number of nonnegative solutions of the original equation is $C(11+4-1, 11) = C(14, 11) = 364$.

Example Problems

Question

Prove that the r-subset $a_1 a_2 ... a_r$ of $\{1, 2, ..., n\}$ occurs in place number

$$C(n, r) - C(n - a_1, r) - C(n - a_2, r - 1) - ... - C(n - a_{r-1}, 2) - C(n - a_r, 1)$$

in the lexicographic order of the r-subsets of $\{1, 2, ..., n\}$.

Example Problems

Answer

There are $C(n-a_1, r)$ r-subsets whose first element is greater than a_1 that come after $a_1a_2...a_r$. There are $C(n-a_2, r-1)$ r-subsets whose first element is a_1 but whose second element is greater than a_2 that come after $a_1a_2...a_r$. ... There are $C(n-a_r)$ r-subsets that begin $a_1...a_{r-1}$ but whose r-th element is greater than a_r that come after $a_1a_2...a_r$. Subtracting the number of r-subsets that come after $a_1a_2...a_r$ from the total number $C(n, r)$ of r-subsets, we find that the place of $a_1a_2...a_r$ is as given.

Example Problems

Question

Prove that of any five points chosen within a square of side length 2, there are two whose distance apart is at most $\sqrt{2}$

Example Problems

Answer

Partition the square into four squares of side length 1. By the pigeonhole principle, at least two of these five points should in one of these four squares. Hence, their distance apart is at most $\sqrt{2}$.

Example Problems

Question

Given m integers $a_1, a_2, ..., a_m$, there exist integers k and l with $0 \leqslant k < l \leqslant m$ such that $a_{k+1} + a_{k+2} + ... + a_l$ is divisible by m.

Example Problems

Answer

To see this, consider the m sums

$$a_1, a_1 + a_2, a_1 + a_2 + a_3, ..., a_1 + a_2 + ... + a_m$$

If any of these sums is divisible by m, then the conclusion holds. Thus, we may suppose that each of these sums has a nonzero remainder when divided by m, and so a remainder equal to one of $1, 2, ..., m - 1$. Since there are m sums and only $m - 1$ remainders, two of the sums have the same remainder when divided by m. Therefore, what we should do now is just to subtract the shorter one of these two sums from the longer one.

Example Problems

Question

A chess master who has 11 weeks to prepare for a tournament decides to play at least one game every day, but, to avoid tiring himself, he decides not to play more than 12 games during any calendar week. Show that there exists a succession of consecutive days during which the chess master will have played exactly 21 games.

Example Problems

Answer

Let a_i be the number of games played from the first day to the i-th day. Then, the sequence of numbers $a_1, a_2, ..., a_{77}$ is exactly increasing. Moreover, $a_1 \geqslant 1$ and $a_{77} \leqslant 132$. Hence, we have

$$1 \leqslant a_1 < a_2 < ... < a_{77} \leqslant 132$$
$$22 \leqslant a_1 + 21 < a_2 + 21 < ... < a_{77} + 21 \leqslant 153$$

Since each of the 154 numbers

$$a_1, a_2, ..., a_{77}, a_1 + 21, a_2 + 21, ..., a_{77} + 21$$

is an integer between 1 and 153. It follows that two of them are equal. Since no two of $a_1, a_2, ..., a_{77}$ are equal, there must be an i and j such that $a_i = a_j + 21$. Therefore, the chess master played a total of 21 games on the days $j+1, j+2, ...i$.

Example Problems

Question

Show that every sequence $a_1, a_2, ..., a_{n^2+1}$ of $n^2 + 1$ different real numbers contains either an increasing or a decreasing subsequence of length $n + 1$.

Example Problems

Answer

We suppose that there is no increasing subsequence of length $n+1$ and show that there must be a decreasing subsequence of length $n+1$. For each $k = 1, 2, ..., n^2+1$, let m_k be the length of the longest increasing subsequence that begins with a_k. Suppose that $1 \leqslant m_k \leqslant n$ for each $k = 1, 2, ..., n^2 + 1$. For the $n^2 + 1$ numbers $m_1, m_2, ..., m_{n^2+1}$ between 1 and n, by the strong pigeonhole principle, $n + 1$ of these numbers are equal.

Let $m_{k_1} = m_{k_2} = ... = m_{k_{n+1}}$, where $1 \leqslant k_1 < k_2 < ... < k_{n+1} \leqslant n^2 + 1$. Suppose that for some $i = 1, 2, ..., n$, $a_{k_i} < a_{k_{i+1}}$. Then since $k_i < k_{i+1}$, we could take a longest increasing subsequence beginning with $a_{k_{i+1}}$ and put a_k in the front, which implies $m_{k_i} > m_{k_{i+1}}$. Therefore, $a_{k_i} > a_{k_{i+1}}$ for all $i = 1, 2, ..., n$. Now, we conclude that $a_{k_1}, a_{k_2}, ..., a_{k_{n+1}}$ is a decreasing sequence.

Example Problems

Question

Prove that $R(m, n) \leqslant R(m-1, n) + R(m, n-1)$ for $m, n \geqslant 3$.

Example Problems

Answer

Let $p = R(m-1, n) + R(m, n-1)$ and suppose that the edges of K_p have been colored red or blue in any way. Consider one of the points x of K_p. Let Re_x be the set of points that are joined to x by a red edge, and let Bl_x be the set of points that are joined to x by a blue edge. Then:

$$| Re_x | + | Bl_x | = p - 1 = R(m-1, n) + R(m, n-1) - 1$$

By the strong pigeonhole principle, we derive that $| Re_x | \geqslant R(m-1, n)$ or $| Bl_x | \geqslant R(m, n-1)$.

Example Problems

Answer

Suppose that $\mid Re_x \mid \geqslant R(m-1,n)$ holds. Let $q = \mid Re_x \mid$ so that $q \geqslant R(m-1,n)$. Then considering K_q on the points of Re_x, we see that either there are $m-1$ points of K_q (and so of K_p) all of whose edges are red or there are n points all of whose edges are blue. If the second possibility holds, we have a blue K_n. If the first possibility holds, add the point x to obtain a red K_m. A similar argument works when $\mid Bl_x \mid \geqslant R(m,n-1)$. We conclude by induction that the Ramsey numbers exist for all integer $m,n \geqslant 3$.

Definition Checklist

- classical probability, conditional probability
- sample space, sample points
- mutually exclusive, independent
- Monte Carlo Algorithm, probabilistic method

Additional Materials

I will first illustrate why the condition $n \geqslant 1.177\sqrt{m}$ must be satisfied, if we want the probability that there is at least one collision in hashing function to be large than 0.5 in the lecture slides. Notice that

$$\begin{aligned} P_n &= 1 - \frac{m \times (m-1) \times (m-2) \times ... \times (m-n+1))}{m^n} \\ &= 1 - [(1 - \frac{1}{m})(1 - \frac{2}{m})...(1 - \frac{n-1}{m})] \end{aligned}$$

Since we always have $(1 - x) \leqslant e^{-x}$ for all $x \geqslant 0$. We obtain

$$\begin{aligned} P_n &= 1 - [e^{-1/m} e^{-2/m} ... e^{-(n-1)/m}] \\ &= 1 - e^{-(n^2-n)/(2m)} \end{aligned}$$

Let $e^{-(n^2-n)/(2m)}$ to be 0.5, we derive that $n = \sqrt{2(ln2)m} \approx 1.177\sqrt{m}$.

Example Problems

Question

There are 8 white balls and 2 red balls in a box. Every time, we will take out a ball randomly and put a white ball back to the box. What is the probability that all the red balls will be taken out exactly during the forth pick?

Example Problems

Answer

$$P = \frac{2}{10} \cdot \frac{9}{10} \cdot \frac{9}{10} \cdot \frac{1}{10} + \frac{8}{10} \cdot \frac{2}{10} \cdot \frac{9}{10} \cdot \frac{1}{10} + \frac{8}{10} \cdot \frac{8}{10} \cdot \frac{2}{10} \cdot \frac{1}{10} = 0.0434$$

Example Problems

Question

It is always a good habit to change your password frequently. Suppose that you have a library containing four different passwords. If you change your password every week with the remaining three password in this library, what is the probability that your password for the seventh week is the same as that of the first week.

Example Problems

Answer

Let P_n be the probability that during the n-th week you use the same password as in the first week. Then we have the recurrence relation that

$$P_{n+1} = \frac{1}{3}(1 - P_n) \Rightarrow (P_{n+1} - \frac{1}{4}) = -\frac{1}{3}(P_n - \frac{1}{4})$$

Since $P_1 = 1$, it is not difficult to derive that

$$P_n = \frac{3}{4}(-\frac{1}{3})^{n-1} + \frac{1}{4}$$

Therefore, P_7 is equal to $\frac{61}{243}$.

Example Problems

Question

Tom and Amy throw the dice in turn. Tom will throw the dice at first. If the point showing up is not one, then Amy will take her turn. The same rule is also available for Amy. Let P_n be the probability that Tom will take the n-th turn. What is the value of $\lim_{n\to\infty} P_n$?

Example Problems

Answer

The basic strategy is the same as that in the previous problem. We can first try to find the relation between P_n and P_{n+1}. From the description:

$$P_{n+1} = \frac{1}{6}P_n + \frac{5}{6}P_{n+1}$$

To find the limit, we first notice that

$$\lim_{n\to\infty} P_n = lim_{n\to\infty} P_{n+1} = x$$

Therefore, we can solve the equation

$$x = \frac{1}{6}x + \frac{5}{6}(1-x) \Rightarrow x = \frac{1}{2}$$

Example Problems

Question

Randomly choose three numbers from $1, 2, 3, ..., 2013$. What is the probability that these three numbers can form an ascending arithmetic progression?

Example Problems

Answer

Let these three numbers to be a, $a+d$ and $a+2d$. Then it is obvious that $d \leqslant 1005$ must hold true. For a particular d, a can be the value from 1 to $2013-2d$. Therefore, the sum of such arithmetic progression can be calculated as:

$$\sum_{d=1}^{1005}(2013-2d) = 1007 * 1005$$

Therefore, calculate this probability as

$$\frac{1007 * 1005}{C_{2013}^{3}}$$

Example Problems

Question

Four people are playing bridge cards. What is the probability that Tom has more than one "King"
(1) if he claims that he has a "King"
(2) if he claims that he has a spade "King"

Example Problems

Answer

These two problems are all about conditional probability.
For the first problem, there are C_{48}^{13} conditions when Tom has no "King"; there are $C_{48}^{12} * 4$ conditions when Tom has exactly one "King"; there are $C_{52}^{13} - C_{48}^{13} - C_{48}^{12} * 4$ conditions when Tom has at least two "King"s. Hence, the probability that Tom has more than one "King" is

$$\frac{C_{52}^{13} - C_{48}^{13} - C_{48}^{12} * 4}{C_{52}^{13} - C_{48}^{13}} \approx 0.37$$

For the second problem, there are C_{51}^{12} conditions when Tom has a spade "King"; there are C_{48}^{12} conditions when Tom has no other kinds of "King"s. Hence, the probability that Tom has more than one "King" is

$$\frac{C_{51}^{12} - C_{48}^{12}}{C_{51}^{12}} \approx 0.56$$

Example Problems

Question

There are two people whose probability to tell the truth is $\frac{1}{3}$. One of them says "Austin is a girl." The other say "Yes." What is the probability that Austin is really a girl under this circumstance?

Example Problems

Answer

Let A be the event that Austin is a girl. Let B be the event that the second person says yes. Then $P(A \cap B) = \frac{1}{9}$ and $P(B) = \frac{1}{3} \cdot \frac{1}{3} + \frac{2}{3} \cdot \frac{2}{3} = \frac{5}{9}$. What we want can be presented as the conditional probability

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{1}{5}$$

Definition Checklist

- inhomogeneous / homogeneous recurrence relation, Catalan numbers
- divide-and-conquer algorithm, master theorem
- generating function, Cauchy product, binomial series
- inclusion-exclusion principle

Additional Materials

It is highly recommended for you to remember the following elementary generating functions.

g(x)	a_k	g(x)	a_k
$(1+ax)^n$	$C_n^k a^k$	$(1+x^r)^n$	$C_n^{k/r}$ for $r \mid k$
$\frac{1-x^{n+1}}{1-x}$	1 for $k \leqslant n$	$\frac{1}{1-ax}$	a^k
$\frac{1}{1-x^r}$	1 for $r \mid k$	$\frac{1}{(1-ax)^n}$	$C_{n+k-1}^k a^k$
$\frac{1}{(1+x)^n}$	$(-1)^k C_{n+k-1}^k$	e^k	$\frac{1}{k!}$
ln(1+x)	$\frac{(-1)^{k+1}}{k}$		

Additional Materials

We can also use generating functions to solve any linear homogeneous recurrence of order k with constant coefficients.Let's go through the following example. Let $h_0, h_1, ..., h_n, ...$ be a sequence of numbers satisfying the recurrence relation

$$h_n + h_{n-1} - 16h_{n-2} + 20h_{n-3} = 0 \text{ for } n \geqslant 3$$

where $h_0 = 0$, $h_1 = 1$ and $h_2 = -1$. Then, we can set the generating function $g(x)$ as $h_0 + h_1x + h_2x^2 + ... + h_nx^n + ...$ for $h_0, h_1, ..., h_n, ...$ Add the following four equations,

$$\begin{aligned} g(x) &= h_0 + h_1x + h_2x^2 + h_3x^3 + ... + h_nx^n + ... \\ xg(x) &= h_0x + h_1x^2 + h_2x^3 + ... + h_{n-1}x^n + ... \\ -16x^2g(x) &= -16h_0x^2 - 16h_1x^3 - ... - 16h_{n-2}x^n + ... \\ 20x^3g(x) &= 20h_0x^3 + ... + 20h_{n-3}x^n + ... \end{aligned}$$

Additional Materials

Then we can derive the relation that

$$\begin{aligned}(1+x-16x^2+20x^3)g(x) =& h_0+(h_1+h_0)x+(h_2+h_1-16h_0)x^2+\\ & (h_3+h_2-16h_1+20h_0)x^3+\ldots+\\ & (h_n+h_{n-1}-16h_{n-2}+20h_{n-3})x^n+\ldots\end{aligned}$$

Since $h_n+h_{n-1}-16h_{n-2}+20h_{n-3}=0$ for $n\geqslant 3$ and since $h_0=0, h_1=1$ and $h_2=-1$, we get

$$(1+x-16x^2+20x^3)g(x)=x$$

Hence, by the partial fraction expansion, we derive that

$$g(x)=-\frac{2}{49(1-2x)}+\frac{7}{49(1-2x)^2}-\frac{5}{49(1+5x)}$$

Additional Materials

From the table of elementary generating function. We can obtain that

$$g(x) = -\frac{2}{49}(\sum_{k=0}^{\infty} 2^k x^k) + \frac{7}{49}(\sum_{k=0}^{\infty}(k+1)^k x^k) - \frac{5}{49}(\sum_{k=0}^{\infty}(-5)^k x^k)$$
$$= \sum_{k=0}^{\infty}[-\frac{2}{49}2^k + \frac{7}{49}(k+1)2^k - \frac{5}{49}(-5)^k]x^k$$

That is to say, it follows that

$$h_n = -\frac{2}{49}2^n + \frac{7}{49}(n+1)2^n - \frac{5}{49}(-5)^n$$

Example Problems

Question

Prove that the number of 2-by-n matrix that can be made from the numbers $1, 2, 3, ..., 2n$ such that

$$x_{11} < x_{12} < x_{13} < ... < x_{1n}$$
$$x_{21} < x_{22} < x_{23} < ... < x_{2n}$$
$$x_{1i} < x_{21} \text{ for } 1 \leqslant i \leqslant n$$

equals the n-th Catalan number.

Example Problems

Answer

We can consider the sequences $a_1, a_2, ..., a_{2n}$ of "("s and ")"s obtained by taking a_i to be "(" if i is in the first row of the matrix and ")" if i is in the second row.

Example Problems

Question

Solve the nonhomogeneous recurrence relation

$$h_n = 4h_{n-1} + 3 \times 2^n \text{ for } n \geqslant 1$$
$$h_0 = 1$$

Example Problems

Answer

$$
\begin{aligned}
h_n &= 4h_{n-1} + 3 \times 2^n \\
&= 4^2 h_{n-2} + 3 \times 2^{n+1} + 3 \times 2^n \\
&= \ldots \\
&= 4^n h_0 + 3 \times 2^n \sum_{i=0}^{n-1} 2^i \\
&= 4^{n+1} - 3 \times 2^n
\end{aligned}
$$

Example Problems

Question

Solve the nonhomogeneous recurrence relation

$$h_n = h_{n-1} + 9h_{n-2} - 9h_{n-3} \text{ for } n \geqslant 3$$
$$h_0 = 1, h_1 = 1, h_2 = 2$$

Example Problems

Answer

Both method of generating function and method of characteristic equation can be applied here. Since the process is easy, the answer will be given directly as

$$h_n = -\frac{-3 + 4 \times 3^n - (-3)^n}{12}$$

Example Problems

Question

Describe the sequence with the generating function

$$(1+x+x^2+x^3+x^4+x^5)(1+x+x^2)(1+x+x^2+x^3+x^4)$$

Example Problems

Answer

The number of integral solutions of $a+b+c=n$ where $0 \leqslant a \leqslant 5$, $0 \leqslant b \leqslant 2$ and $0 \leqslant c \leqslant 4$.

Example Problems

Question

Determine the generating function for the number of solutions of the equation

$$e_1 + e_2 + ... + e_k = n$$

in nonnegative odd integers.

Example Problems

Answer

$$g(x) = (x + x^3 + x^5 + ...)^k = (\frac{1}{1-x} - \frac{1}{1-x^2})^k = \frac{x^k}{(1-x^2)^k}$$

Example Problems

Question

Determine the number of ways to color the square of a 1-by-n board with the colors red, white and blue, where the number of red squares is even and there is at least one blue square.

Example Problems

Answer

Let the answer be a_n, then we know that $\{a_n\}$ is a sequence whose terms count permutations instead of combinations. Hence, we should use the exponential generating function instead of the polynomial generating function.

$$\begin{aligned} g(x) &= (1+\frac{x^2}{2!}+\frac{x^4}{4!}+...)(1+\frac{x}{1!}+\frac{x^2}{2!}+...)(\frac{x}{1!}+\frac{x^2}{2!}+...) \\ &= \frac{e^x+e^{-x}}{2}e^x(e^x-1) \\ &= -\frac{1}{2}+\sum_{n=0}^{\infty}\frac{(3^n-2^n+1)x^n}{2n!} \end{aligned}$$

Thus, we obtain that

$$h_n = \frac{3^n-2^n+1}{2} \text{ for } n \neq 0 \text{ and } h_0 = 0$$

Example Problems

Question

Determine the number of permutations of the multiset

$$S = \{3 \cdot a, 4 \cdot b, 2 \cdot c\}$$

where, for each type of letter, the letters of the same type do not appear consecutively. (Thus, *abbbbcaca* is not allowed, but *abbbacacb* is.)

Example Problems

Answer

Here, we should use the inclusion-exclusion principle. The answer can be given as

$$\frac{9!}{3!4!2!} - \left(\frac{7!}{4!2!} + \frac{6!}{3!2!} + \frac{8!}{3!4!}\right) + \left(\frac{4!}{2!} + \frac{6!}{4!} + \frac{5!}{3!}\right) - 3!$$

Example Problems

Question

Let D_n be the number of derangement of $\{1, 2, 3..., n\}$. Prove that for $n \geqslant 1$:

$$D_n = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ... + (-1)^n \frac{1}{n!})$$
$$D_n = (n-1)(D_{n-2} + D_{n-1}) \text{ for } n \geqslant 3$$
$$D_n = nD_{n-1} + (-1)^n \text{ for } n \geqslant 2$$

Example Problems

Answer

The first equation can be derived from the inclusion-exclusion principle by fixing elements.

$$\begin{aligned} D_n &= n! - C_n^1(n-1)! + C_n^2(n-2)! - \ldots + (-1)^n C_n^n(n-n)! \\ &= n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}) \end{aligned}$$

Let's verify the second recurrence relation combinatorially in detail. All derangements can be partitioned into $n-1$ parts according to which of the integers $2, 3, \ldots, n$ is in the first place. Thus, we have the relation that $D_n = (n-1)d_n$, where d_n is the number of derangements in which 2 is in the first place. These d_n derangements can be partitioned further into two subparts according to whether 1 is in the second place or not.

Example Problems

Answer

Hence, we can further obtain $D_n = (n-1)(d'_n + d''_n)$, where d'_n is the number of derangements in which 2 is in the first place and 1 is in the second place and d''_n is the number of derangements in which 2 is in the first place and 1 is not in the second place.

Observe that d'_n is the same as the number of derangements for permutations of $\{3, 4, ..., n\}$ in which 3 is not in the first place, 4 is not in the second place, and so on. Thus, $d'_n = D_{n-2}$. Similarly, d''_n is the same as the number of derangements for permutations of $\{1, 3, 4, ..., n\}$ in which 1 is not in the first place, 3 is not in the second place, and so on. Thus, $d'_n = D_{n-1}$.

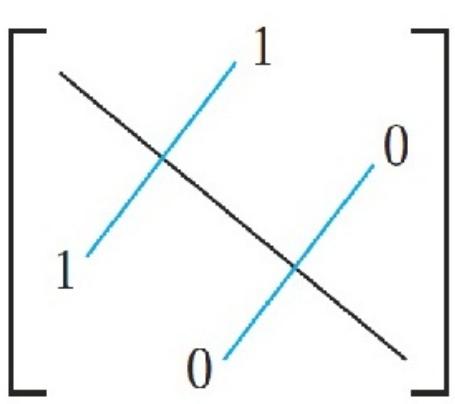
By now, we conclude that $D_n = (n-1)(D_{n-2} + D_{n-1})$ for $n \geqslant 3$. Since $D_2 = 1$ and $D_1 = 0$, we can further conclude that $D_n = nD_{n-1} + (-1)^n$ for $n \geqslant 2$.

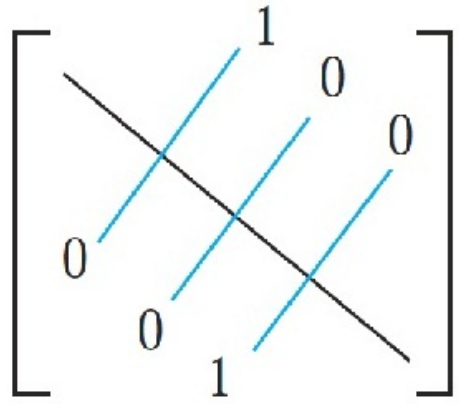
Definition Checklist

- matrix, Boolean Product
- reflexive, symmetric, transitive, antisymmetric, composing relation
- digraph, path, connectivity, closure
- partial ordering, total ordering, lexicographic ordering
- Hasse Diagram, maximal/minimal element
- subset, bound, lattice, topological sorting

Additional Materials

It is a common question to ask whether a particular relation is reflexive, symmetric, antisymmetric or transitive. We have already learnt how to solve these kinds of problems by examining the definitions at the beginning of this course. Now, let's consider this problem from the view of zero-one relation matrix. As shown in the graph, the first matrix represents the reflexive relation; the second matrix represents the symmetric relation; the third matrix represents the antisymmetric relation. These three relations are easy to identify.





Additional Materials

To determine whether a relation is transitive or not, we should judge whether $\mathbf{M}_R \vee \mathbf{M}_{R^*}$ is equal to $\mathbf{M}_R$ or not. Here, $\mathbf{M}_R$ means the zero-one relation matrix for this relation R and $\mathbf{M}_{R^*}$ means the zero-one relation matrix for its transitive closure. That is to say, we just need to care about finding the transitive closure of one relation. In the lecture slides, a naive algorithm to compute the transitive closure is introduced. However, its time complexity is $O(n^4)$, which is not efficient enough. The following algorithm, Warshall's Algorithm, is recommended in the real world calculation.

procedure: *Warshall*$(\mathbf{M}_R)$

$\mathbf{W}_0 := \mathbf{M}_R$;
for $k := 1$ to n **do**
  for $i := 1$ to n **do**
    for $j := 1$ to n **do**
      $\mathbf{W}_k(i,j) := \mathbf{W}_{k-1}(i,j) \vee \mathbf{W}_{k-1}(i,k) \wedge \mathbf{W}_{k-1}(k,j)$
$\mathbf{W}_n$; is the desired transitive closure

Additional Materials

Let's discuss the procedure in detail. Suppose that we have an initial relation matrix $\mathbf{W}_0$. The first column tells us that we should apply an OR operation with the first row to the second and third row to get $\mathbf{W}_1$. Then, since the elements in the second row of $\mathbf{W}_1$ are all zero, we derive that $\mathbf{W}_2$ is the same as $\mathbf{W}_1$. Similarly, apply an OR operation with the third row of $\mathbf{W}_2$ to the second and forth row to obtain $\mathbf{W}_3$ and apply an OR operation with the forth row of $\mathbf{W}_3$ to the first three rows to obtain $\mathbf{W}_4$.

$$\mathbf{W}_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \rightarrow \ldots \rightarrow \mathbf{W}_4 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Example Problems

Question

A relation R is called circular if aRb and bRc imply that cRa. Show that R is reflexive and circular if and only if it is an equivalent relation.

Example Problems

Answer

First suppose that R is reflexive and circular. We need to show that R is symmetric and transitive. Let $(a, b) \in R$. Since $(b, b) \in R$, it follows by circularity that $(b, a) \in R$; this proves symmetry. Now if $(a, b) \in R$ and $(b, c) \in R$, by circularity again, $(c, a) \in R$. By symmetry, $(a, c) \in R$ as well. Hence, reflexive and circular relation is also symmetric and transitive.

Conversely, transitivity and symmetry immediately imply circularity. Therefore, we can draw the conclusion.

Example Problems

Question

How many relations are there on a set with n elements that are
(a) symmetric?
(b) antisymmetric?
(c) reflexive and symmetric?

Example Problems

Answer

It will be easy to solve these kinds of problems if a relation matrix is taken into account.

For (a), we do not need to care about the diagonal elements. This will lead to 2^n conditions. For the remaining $n^2 - n$ elements, we should keep them symmetric. By the principle of multiplication, the total number should be $2^{n(n+1)/2}$ relations.

For (b), we also do not need to care about the diagonal elements as well. However, since the remaining elements cannot be symmetric at all, they lead to $3^{(n^2-n)/2}$ conditions. By the principle of multiplication, the total number should be $2^n 3^{n(n-1)/2}$ relations.

For (c), the diagonal elements should all be one. Therefore, there are $2^{n(n-1)/2}$ reflexive and symmetric relations.

Example Problems

Question

Use the naive computing procedure and Warshall's Algorithm to find the transitive closure of the following relation on the set $\{1, 2, 3, 4\}$:

$$\{(2, 1), (2, 3), (3, 1), (3, 4), (4, 1), (4, 3)\}$$

Example Problems

Answer

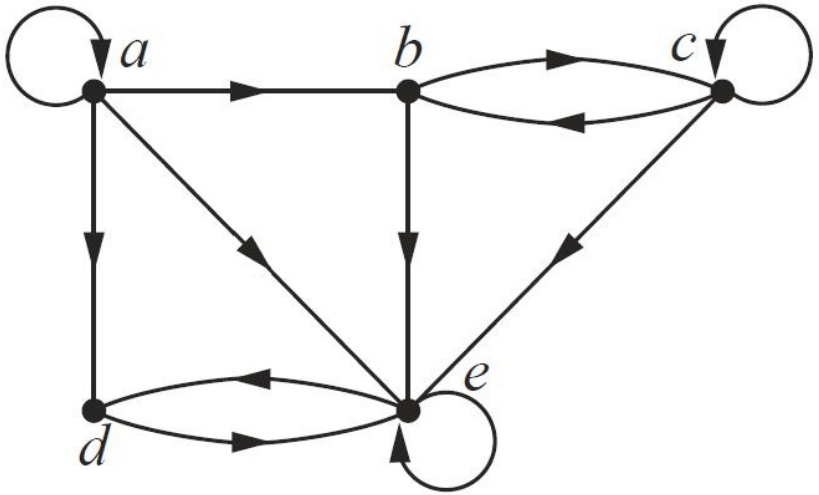
The detailed steps are ignored. The relation matrix of this transitive closure is:

$$\mathbf{W}_0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \rightarrow \ldots \rightarrow \mathbf{W}_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Example Problems

Question

Determine whether there is a path in the following graph beginning at the first vertex given and ending at the second vertex given. If such a path exists, is it necessary for vertex e to be on this path? Moreover, it is possible that the path has a exact length of two, if such a path exists?
(a) b,a; (b) b,d; (c) a,c



Example Problems

Answer

Build the relation matrix of the transitive closure for this relation with Warshall's Algorithm. From $\mathbf{W}_5$, only path (a) does not exist. From $\mathbf{W}_4$, vertex e must be on path (b).

$$\mathbf{W}_0 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow \ldots \rightarrow \mathbf{W}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow$$

$$\mathbf{W}_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Example Problems

Answer

To discuss the length of a path, Warshall's Algorithm will not work. Instead, we should use the naive computing procedure. In this problem, to get the paths with the length of two, we should observe $\mathbf{W}_1$. Therefore, there exist a path with the length of two between b and d as well as between a and c.

$$\mathbf{W}_0 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow \mathbf{W}_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Example Problems

Question

For the poset $(\{3, 5, 9, 15, 24, 45\}, |)$:
(a) Find the maximal elements.
(b) Find the minimal elements.
(c) Find the greatest element, if exists.
(d) Find the least element, if exists.
(e) Find all upper bounds of $\{3, 5\}$.
(f) Find the least upper bound of $\{3, 5\}$, if exists.
(g) Find all lower bounds of $\{15, 45\}$.
(h) Find the greatest lower bound of $\{15, 45\}$, if exists.

Example Problems

Answer

From the Hasse diagram for this poset, we can easily get the final answer:
(a) 24,45
(b) 3,5
(c) No
(d) No
(e) 15,45
(f) 15
(g) 15,5,3
(h) 15

Example Problems

Question

Show that every nonempty finite subset of a lattice has a least upper bound and a greatest lower bound.

Example Problems

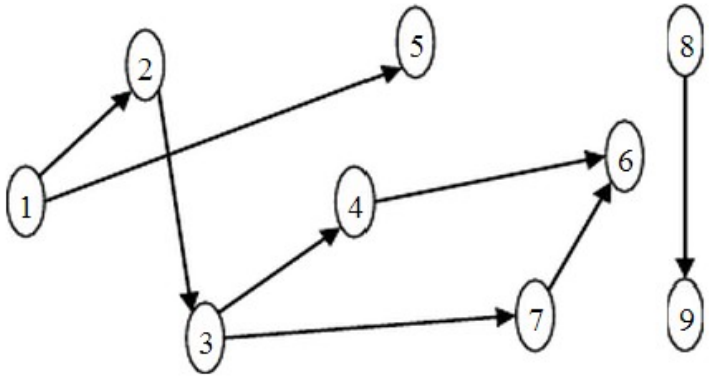
Answer

Let $P(n)$ be "every subset with n elements from a lattice has a least upper bound and a greatest lower bound." Then, $P(1)$ is true because the least upper bound and greatest lower bound of $\{x\}$ are both x.
Assume that $P(k)$ is true. Let S be a set with $k+1$ elements. Let $x \in S$ and $S' = S - \{x\}$. Because S' has k elements, by the inductive hypothesis, it has a least upper bound y. Now because we are in a lattice, there is an element $z = \text{lub}(x, y)$. To show that z is the least upper bound of S, note that if $w \in S$, then $w = x$ or $w \in S'$. If $w = x$, then $w \preceq z$ because z is the least upper bound of x and y. If $w \in S'$, then $w \preceq z$ because $w \preceq y$, which is true because y is the least upper bound of S', and $y \preceq z$, which is true because $z = \text{lub}(x, y)$. To see that z is the least upper bound of S, suppose that u is an upper bound of S. Note that such an element u must be an upper bound of x and y, but because $z = \text{lub}(x, y)$, it follows that $z \preceq u$. We omit the similar argument for the greatest lower bound of S.

Example Problems

Question

Given the following graph, determine the number of different topological sequences for the set $\{1, 2, ..., 9\}$.



Example Problems

Answer

We first notice that 8 and 9 can be inserted to any position of the sub-sequence generated by $\{1, 2, ..., 7\}$ in this order. So we will discuss two conditions based on whether 8 and 9 are adjacent or not. Since $\{1, 2, ..., 7\}$ can produce 8 empty positions, then we can $C_8^1 + C_8^2$ ways to determine the position of 8 and 9. Then we will discuss the situation when 1 has been deleted from the set $\{1, 2, ..., 7\}$. Similarly, we have C_6^1 ways to put 5 among the sub-sequence generated by $\{2, 3, 4, 6, 7\}$. After 2 is also deleted, we can obtain two different topological sequences produces by $\{3, 4, 6, 7\}$. Therefore, the final answer is:

$$2C_6^1(C_8^1 + C_8^2) = 432$$

Definition Checklist

- graph, directed graph, vertex, edge, adjacent, isolated, pendant
- complete graph, cycle, wheel, hypercube, bipartite graph
- adjacent table, adjacent matrix, incidence matrix
- handshaking theorem, isomorphism graph, homeomorphic graph
- cut vertex, cut edge, Euler circuit, Hamilton path
- shortest path, Dijkstra Algorithm
- planar graph, Kuratowski's Theorem
- marriage theorem, perfect matching, Harem Theorem

Additional Materials

To find the Euler Circuit of a given graph one can use the Hierholzer's Algorithm. The time-complexity of this algorithm is $O(E)$. The main idea of this algorithm is to find the sub-circuits and to insert them into the circuit maintained.

procedure: *Hierholzer*(G)

cir := an arbitrary initial circuit in G;
$G := G$ - cir
while G has edges **do**
$sub - cir$:= an arbitrary circuit in G;
$G := G$ - $sub - cir$
Insert $sub - cir$ into cir;
cir is the desired Euler Circuit

Additional Materials

The following theorem provides a useful criterion for determining whether a graph is bipartite.

Theorem

A simple graph is bipartite if and only if it has at least two vertices and the length of all circuits are even.

The proof for this theorem is ignored.
One more thing to emphasize is that the best algorithm for determining whether two graphs are isomorphic have exponential worst-case time complexity. So, when solving this kind of problem by yourself, just check the following five points:

- the number of edges
- the number of vertices
- the number of degrees for each vertice
- the paths with the same length
- the isomorphic sub-graphs

Example Problems

Question

The complementary graph $\overline{G}$ of a simple graph G has the same vertices as G. Two vertices are adjacent in $\overline{G}$ if and only if they are not adjacent in G. A simple graph G is called self-complementary if G and $\overline{G}$ are isomorphic. Show that if G is a self-complementary simple graph with v vertices, then $v \equiv 0$ or $1 (\mathrm{mod}\ 4)$.

Example Problems

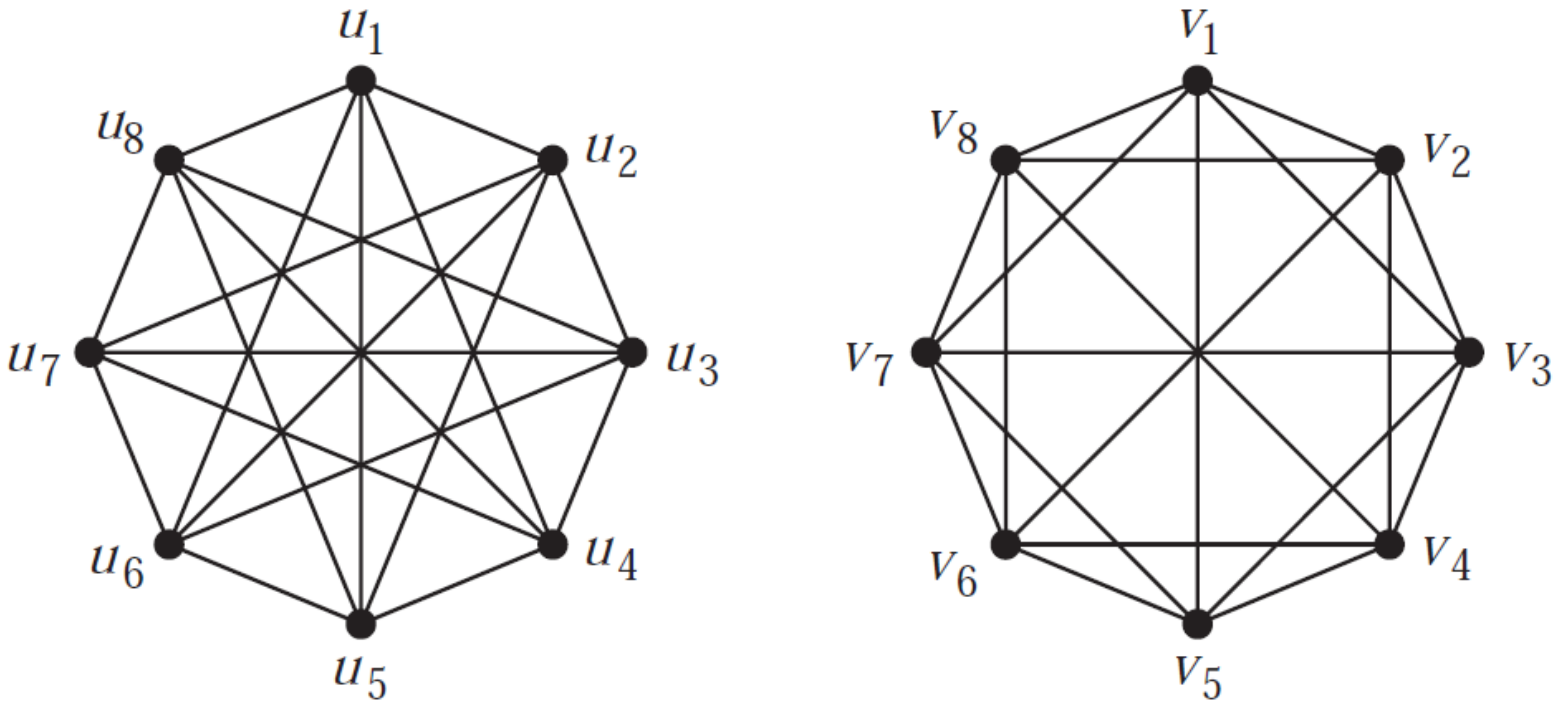
Answer

If G is self-complementary, then the number of edges in G must be equal to the number of edges of $\overline{G}$. But the sum of these two numbers is $v(v-1)/2$. Therefore, the number of edges in G must be $v(v-1)/4$. Since this number must be an integer, we can check that $v \equiv 0$ or $1 (\text{mod } 4)$.

Example Problems

Question

Determine whether the given pair of graphs is isomorphic or not.



Example Problems

Answer

The easiest way to show that these graphs are not isomorphic is to look at their complement. The complement of the left graph consists of two 4-cycle. The complement of the right graph is an 8-cycle. Since the complements are not isomorphic, the graphs are also not isomorphic.

Example Problems

Question

Show that if a simple graph G has k connected components and these components have $n_1, n_2, ..., n_k$ vertices, respectively, then the number of edges of G does not exceed

$$\sum_{i=1}^{k} C_{n_i}^2$$

Further, show that

$$\sum_{i=1}^{k} n_i^2 \leqslant n^2 - (k-1)(2n-k)$$

Finally, show that a simple graph with n vertices and k connected components has at most $(n-k)(n-k+1)/2$ edges.

Example Problems

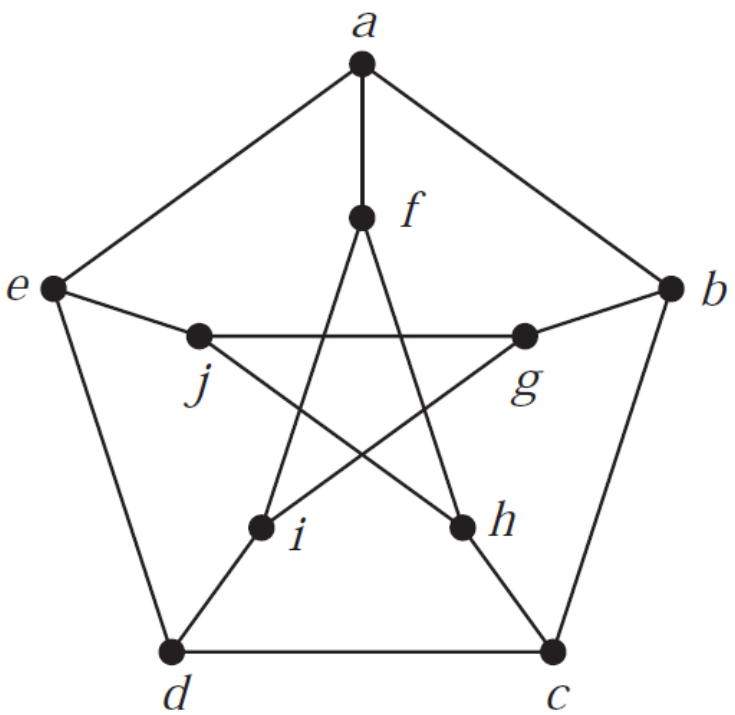
Answer

An edge cannot connect two vertices in different connected components. Because there are at most $C_{n_i}^2$ edges in the connected components with n_i vertices, it follows that there are at most $\sum_{i=1}^{k} C_{n_i}^2$ edges in the graph.
Observe that the maximum value of $\sum n_i^2$, subject to the constraint that $\sum n_i = n$, is obtained when one of the n_i's is as large as possible, namely $n-k+1$, and the remaining n_i's are equal to 1. Hence, $\sum_{i=1}^{k} n_i^2 \leqslant n^2 - (k-1)(2n-k)$ also holds true.
Since the number of edges of the given graph does not exceed $\sum_{i=1}^{k} C_{n_i}^2 = \sum_{i=1}^{k}(n_i^2 - n_i)/2 = ((\sum_{i=1}^{k} n_i^2) - n)/2$. Applying the inequality above, we see that this does not exceed $(n^2 - (k-1)(2n-k) - n)/2$, which after a little algebra is seen to equal $(n-k)(n-k+1)/2$.

Example Problems

Question

Show that the Peterson graph does not have a Hamilton circuit, but that the subgraph obtained by deleting a vertex v and all edges incident with v, does have a Hamilton circuit.



Example Problems

Answer

We do the easy part first, showing that the graph obtained by deleting a vertex from the Pertesen graph has a Hamilton circuit. By symmetry, it makes no difference which vertex we delete, so assume that it is vertex j. Then a Hamilton circuit in what remains is $a, e, d, i, g, b, c, h, f, a$.

Now we show that the entire graph has no Hamilton circuit. Assume that a Hamilton circuit exists. Not all edges around the outside can be used, so without loss of generality, assume that $\{c, d\}$ is not used. Then $\{e, d\}, \{d, i\}, \{h, c\}, \{b, c\}$ must all be used. If $\{a, f\}$ is not used, then $\{e, a\}, \{a, b\}, \{f, i\}, \{i, h\}$ must all be used, forming a premature circuit. Therefore, $\{a, f\}$ is used. Without loss of generality, assume that $\{e, a\}$ is used and $\{a, b\}$ is not used. Then $\{b, g\}$ is also used, and $\{e, j\}$ is not. But this requires $\{g, j\}$ and $\{h, j\}$ to be used, forming a premature circuit. Therefore, the Peterson graph does not have a Hamilton circuit.

Example Problems

Question

Given a simple graph with all edge weights larger than one. Define the weight of a path as the product of all the edge weights on this path. How to find the path with the smallest weight between two vertices with Dijkstra's Algorithm?

Example Problems

Answer

Take the logarithm to all the edge weights, then we can change "multiplication" to addition. Since all the edge weights are larger than one, their logarithm should be larger than zero. Hence, this algorithm still works.

Example Problems

Question

Suppose that a connected planar simple graph with e edges and v vertices contains no simple circuit of length 4 or less. Show that $e \leqslant (5/3)v - (10/3)$ if $v \geqslant 4$.

Example Problems

Answer

We first define the degree of a region to be the number of edges on the boundary of this region. In this problem, the degree of each region is at least five. Therefore, we always have

$$2e = \sum deg(R) \geqslant 5r \Rightarrow (2/5)e \geqslant r$$

Combined with the Euler's Formula $r = e - v + 2$, we obtain

$$e \leqslant (5/3)v - (10/3)$$

Example Problems

Question

Prove that every planar graph G can be colored using five or fewer colors.

Example Problems

Answer

Suppose that $G = \langle V, E \rangle$, then it is obvious that this saying holds true when $\mid V \mid \leqslant 5$. Suppose that this saying is true for $\mid V \mid \leqslant k$, then let's consider $G_1 = \langle V_1, E \rangle$, where $\mid V_1 \mid = k + 1$. Then there exists a vertex v_0 whose degree is not exceeding five. For the graph $G_1 - v_0$, we can always color it with no more than five colors. Now, we should discuss several conditions according to v_0.
(1) When the vertices adjacent to v_0 needs no more than four colors, then we can color v_0 directly.
(2) When $d(v_0) = 5$ and all it adjacent vertices are in different colors, we can name these adjacent vertices v_1, v_2, v_3, v_4, v_5 clockwise and define their colors as c_1, c_2, c_3, c_4, c_5. Consider the sub-graph H of $G_1 - v_0$ with the color of c_1 or c_3. Then obviously, v_1 and v_3 should be in H. We should discuss two sub-conditions here.

Example Problems

Answer

(2a) If v_1 and v_3 belongs to two separate connected components in H, then we can swap the color c_1 and c_3 in the connected components containing v_1. Thus, we can color v_0 with c_1.
(2b) If v_1 and v_3 are in the same connected components in H, then in the graph $H \cup \{v_0\}$, there exists a circuit $v_0, v_1, v_3, ..., v_1, v_0$. Then v_2 and v_4 cannot be inside or outside this circuit at the same. Thus, we derive the condition (2a) again.
To conclude, we prove the correctness of the five-color theorem by mathematical induction.

Definition Checklist

- tree, rooted tree, m-ary tree, balanced tree
- binary search tree, decision tree, Huffman tree
- preorder, inorder, postorder
- spanning tree, minimum spanning tree
- depth-first search, breadth-first search

Additional Materials

An m-ary Huffman code for a set of N symbols can be constructed analogously to the construction of a binary Huffman code. At the initial step, $(N-1)\mathrm{mod}(m-1)+1$ trees consisting of a single vertex with least weights are combined into a rooted tree with these vertices as leaves. At each subsequent step, the m trees of least weight are combined into an m-ary tree.

For example, if we want to use ternay Huffman coding to encode these letters with the given frequencies: A:0.25, E:0.30, N:0.10, R:0.05, T:0.12, Z:0.18, we will derive the coding as: A:2, E:1, N:010, R:011, T:02, Z:00.

Example Problems

Question

Prove the Kraft Inequality, saying that if $d(x)$ means the depth of a leaf x in a binary tree, then for all leaves x, $\sum 2^{-d(x)} \leqslant 1$ holds true.

Example Problems

Answer

Let T be a binary tree and let T' be the binary tree obtained by attaching a leaf to any node of T that has exactly one child so that T' is full. every node of T' has exactly two or zero children. Every leaf of T is present in T' so we immediately have

$$\sum_{x \in leaves(T)} 2^{-d(x)} \leqslant \sum_{x \in leaves(T')} 2^{-d(x)}$$

Consider the random walk that starts at the root of T' and repeatedly moves to the left or right child of the current node, with equal probability, until it reaches a leaf. The probability that this walk reaches a particular leaf, x, is exactly $2^{-d(x)}$. Therefore, we obtain that

$$\sum_{x \in leaves(T)} 2^{-d(x)} \leqslant \sum_{x \in leaves(T')} 2^{-d(x)} = 1$$

Example Problems

Question

Given a binary tree, prove that it is possible to divide all the nodes into three sets A, B and C, so that $max\{card(A), card(B), card(C)\} - min\{card(A), card(B), card(C)\} \leqslant 1$, when we cannot find any child in the same set with its father.

Example Problems

Answer

We use the induction loading to prove that if the root of this tree is in set A, then $max\{card(A), card(B), card(C)\} - min\{card(A), card(B), card(C)\} = card(A) - min\{card(A), card(B), card(C)\} \leqslant 1$. This is obviously true when this tree is an empty tree or a single node. Otherwise, suppose that this proposition is true for its left sub-tree and its right sub-tree and the three set for these two sub-trees are defined as A_1, B_1, C_1, A_2, B_2 and C_2. Notice that if $card(A_1) = n$ and $card(A_2) = m$, then we just need to list all the possible cardinality of B_1, C_1, B_2 and C_2 to find that it is possible to construct A, B and C when the root, A_1 and A_2 are in different sets.

Example Problems

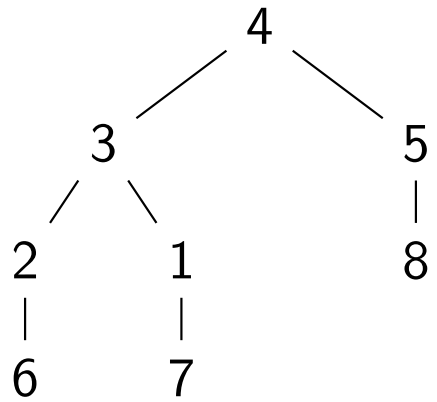
Question

Give the BFS sequence and the DFS sequence, how to reconstruct the original tree?

Example Problems

Answer

Let's use the example of the BFS sequence 4,3,5,2,1,8,6,7 and the DFS sequence 4,3,2,6,1,7,5,8. The first node 4 must be the root of this tree. All the nodes on the next level should appear in the same order in both sequences. So, the root has two children 3 and 5. Also, in the DFS sequence, all the nodes between 3 and 5 can form the sub-tree of node 3. So we can use the strategy above iteratively.



Example Problems

Question

Suppose that $d_1, d_2, ..., d_n$ are n positive integers with sum $2n-2$. Show that there is a tree that has n vertices such that the degrees of these vertices are $d_1, d_2, ..., d_n$.

Example Problems

Answer

We prove this by induction on n. The problem is trivial if $n \leqslant 2$, so assume that the inductive hypothesis holds and let $n \leqslant 3$. First note that at least one of the positive integers, d_i, must be equal to 1. Without the loss of generality assume that $d_n = 1$. Now it is impossible that for the remaining d_i's to be equal to 1. Without the loss of generality, assume that $d_1 > 1$. Now apply the inductive hypothesis to the sequence $d_1 - 1, d_2, d_3, ..., d_{n-1}$. There is a tree with these degrees. Add an edge from the vertex with degree $d_1 - 1$ to a new vertex, and we have the desired tree. By mathematical induction, this saying is true.

Example Problems

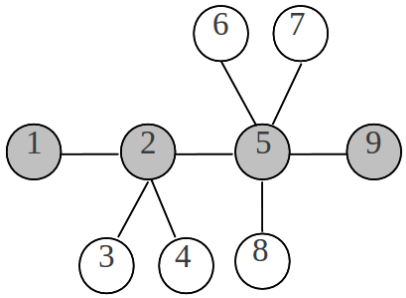
Question

A caterpillar is a tree with n nodes containing a main chain. All the nodes are on this main chain or adjacent to one node on the main chain. Also, a tree with n nodes is called graceful if we can label all its nodes with 1, 2, ..., n so that all the $n-1$ absolute values of the difference between two adjacent nodes are different. How to build a graceful caterpillar?

Example Problems

Answer

Let's first look at the following example:



The "main chain" is playing an important role in this problem, so we start with this part. Naturally, we may label node 1 with 1, then we can immediately find that its adjacent node should be labeled as 9. Since the node labeled as 2 must be adjacent to the node labeled as 9, so we choose node 3 as this node. By the same method, we can label node 4 with 3, label node 5 with 4, label node 6 with 8, label node 7 with 7, label node 8 with 6 and label node 9 with 5.

Example Problems

Answer

Now, make a guess that we can use the following strategy:
At the beginning, label the leftmost node on the main chain with 1. When we want to label the nodes adjacent to node k on the main chain, which is labeled as x, we first deal with the nodes not belonging to the main chain and deal with the other adjacent node on the main chain in the end. If the remaining numbers are all larger than x, then choose the largest remaining number every time. If the remaining numbers are all smaller than x, then choose the smallest remaining number every time.
Let's show that this strategy is correct. We can always get the difference $n-1$ easily. Suppose that the last two numbers we use to label the nodes are k_1 and k_2 $(k_1 < k_2)$ to get the difference $k_2 - k_1$. Then next time we will choose either $k_1 + 1$ or $k_2 - 1$ to get the difference $k_2 - (k_1 + 1)$ or $(k_2 - 1) - k_1$. They are both $k_2 - k_1 - 1$. By the mathematical induction, this strategy is correct.

Example Problems

Question

How to judge whether a simple graph G is bipartite with BFS?

Example Problems

Answer

First, we can print all the nodes with the color of white. After the BFS, we print all the nodes on the even level with the color of blue and all the nodes on the odd level with the color of red. In the end, check whether there exist any adjacent nodes in the original graph G with the same color.

Example Problems

Question

How to find the cut vertices and cut edges in an undirected graph with DFS?

Example Problems

Answer

Let T be the spanning tree obtained from DFS. For a node v, we should also record its depth d_v in T, the amount of its children tot_v in T and the depth low_v of the lowest ancestor adjacent to v and its posterity. Moreover, a node should have three different states: before it is visited, it has the color of white; after it is visited and checked, it has the color of black; after it is visited and when it is being checked, if has the color of grey.

Now, let's consider the property of cut vertices. If the root x of T has more than two children, then they can only be connected with x. If the node x is not the root of T, then we should focus on one of its children y. Notice that: y can never be connected with any black nodes; all the white nodes connected with y will become its posterity; all the grey nodes connected with y will become its ancestor. If y and all posterity of y is not connected with any ancestor of x, then x will become a cut vertex.

Example Problems

Answer

To find the cut edge, we can use a similar strategy. The conclusion is that if y and all posterity of y is not connected with any ancestor of x or x, then the edge (x, y) will become a cut edge.
I may upload a C++ code to SAKAI. You can have a look if you are interested. There is also a method to find the strong connected component with DFS. You can search this algorithm online called Tarjan's Algorithm.

Example Problems

Question

Prove that if after we delete all the edges with the weight larger than d in a simple graph G, the MST is divided into k connected components, then G is also divided into k connected components.

Example Problems

Answer

Suppose that G is divided into k' connected components and $k' \neq k$. It is impossible to obtain $k' > k$, hence $k' < k$. Therefore, in one connected components, the MST must be divided into at least two parts T_1 and T_2. Since they are in the same connected component, there exist $x \in T_1$ and $y \in T_2$ such that $w(x, y) \leqslant d$. Since in the MST, on the path from x to y, there exist an edge $w(e) > d$. So, delete e and add (x, y), we can get a smaller spanning tree. This is a contradiction.

Example Problems

Question

Prove that T is the spanning tree of a simple graph G with the minimized maximum weight of its edges, if T is the MST.

Example Problems

Answer

Suppose that there exists a spanning tree T' with a smaller maximum weight of its edges than T. Let e_0 be the edge in T with the maximum weight, then e_0 will divide T into two connected components X and Y. Since T is the MST, then for an arbitrary edge e connecting X and Y, the weight of e is not smaller than the weight of e_0. In T', since an edge connecting two vertices from X and Y must have a weight not smaller than the weight of e_0, we get the contradiction.

References

[Brualdi, 2010] Brualdi, R. A. (2010).
Introductory Combinatorics, 5th ed.
Pearson Education, Inc.

[Leiserson et al., 2001] Leiserson, C. E., Rivest, R. L., Stein, C., and Cormen, T. H. (2001).
Introduction to algorithms, 2rd ed.
The MIT press.

[Rosen, 2012] Rosen, K. H. (2012).
Discrete Mathematics and Its Applications, 7th ed.
McGraw-Hill, Inc.

[Stallings, 2011] Stallings, W. (2011).
Cryptography and Network Security, Principles and Practice, 5th ed.
Pearson Education, Inc.