概念

2019年2月26日 14:23

永远都是True：tautology
永远都是false：contradiction
要么真要么假，除了上面两个以外的：contingency
equivalent：永远都有相同的真值

Converse:反命题，条件和结论互换
Contrapositive：逆否命题
Inverse：否命题

逻辑表达式

2019年3月3日 12:12

否（negation）：¬

逻辑与（Conjunction）∧

逻辑或（Disjunction）∨

Exclusive or（异或）⊕
当只有一个为真时结果为真
其余为假
相加模2

非运算符优先级最高，
其次是与和或，
最后是蕴含和互推关系

p→q
只有当P为true，q为false时结果为false
其余全是true

相当于承诺
得到100分，就给A+
得到100分相当于p
给A+相当于q

p→q等价于
Q unless ¬p
P only if q

逻辑互推（Biconditional）
p<->q两个是可以互推的

两个都是false或者两个都是true是结果才是true
其余全是false

注意：
<->指的是一个逻辑关系
<=> 代表两者等价
含义是不一样的

逻辑等价式

2019年3月3日 12:30

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

这个等价式可通过布尔函数来记忆

p + (q * r) = (p + q) * (p + r)

$\mathrm{p} \rightarrow q \equiv (\neg p) \vee q$

$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$

$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$

$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

$\mathrm{p} \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

断言逻辑（Predicates logic）

2019年2月26日 15:14

任意：Universal quantifier:∀(for all)
对每一个都成立（与）

存在：Existential：∃(there exists)

可以通过找特例的方式来判断两个语句是否等价

对于断言逻辑，必须要指定作用域，即x的范围，然后才能指定x的范围
变量X一定要指定范围，如果没有指定范围（universal 或 Existential），他就不是逻辑命题

任何断言逻辑都比逻辑表达式有更高的优先级
∀x P(x) ∨ Q(x) 意思是 (∀x P(x)) ∨ Q(x) 而不是 ∀x (P(x) ∨ Q(x))

对于任意，存在这些量词，都比其他逻辑运算符拥有更高的优先级

量词（∀□∃）放在不同的位置可能会表示不同的逻辑
如果∀和∃放在一起，改变两者的位置就会表示不同的逻辑
但是如果一个命题只有∀或∃这两个量词存在，那么改变这些量词的顺序就不会改变其语义

断言逻辑等价式

2019年3月3日 16:23

$\forall x \neg P(x) \equiv \neg \exists x P(x)$

$\neg \exists x\ \mathrm{Perfect}(x) \equiv \forall x\ \neg \mathrm{Perfect}(x)$

练习

2019年3月1日 16:45

For every real number x, there exists a real number y such that xy = 1
$\forall x \exists y (xy = 1) \equiv \exists x \forall y (xy \neq 1)$

L(x,y)指的是x喜欢y

则There is exactly one person whom everybody loves. 可以表示为?
$\exists y(\forall x L(x,y) \wedge \forall z(\forall x L(x,z) \rightarrow y = z))$

判断两个是否逻辑等价（对于逻辑推理这种题目，我们一般只看正确的结论，即在正确的前提下讨论能否推出这个结果）

1. (∃x P(x)) → (∃x Q(x)) and ∃x (P(x) → Q(x)) （证明逆否命题）

   False，原因：

   方法一：逻辑等价的条件是：在所有可能的条件下都有相同的真值

   对于这道题，完全可以找到一个反例

P(x): x<0	Q(x):x>=0

   对于第一个式子来说：当左边的x<0，右边x>=0时为结果为真

   对于第二个式子来说：当x<0时结果为假，就不符合条件

   其实，对于这种逻辑判断的题来说，有些时候需要相信直觉

   方法二：对于左边推右边，已知的是(∃x P(x)) → (∃x Q(x))，∃x P(x)，需要推到的是对于这个特定的x，Q(x)也要成立，所以说不一定，有可能使得P(x)和Q(x)成立的值不一样，即只有P(a)为真且Q(b)为真，这样子是怎么也不能推出Q(a)为真的，所以不成立

2. ∃x (P(x) → Q(x)) and ∀x P(x) →∃x Q(x)（证明逆否命题）

论域是南科大的学生
P:students who take CS201
Q:student is CS-major
Anyone who takes CS201 is CS-major
$\forall x, (P(x) \rightarrow Q(x))$
$\forall x, (P(x) \wedge Q(x))$
能正确表示的是第一个
第二个表示的是：
对于任意的南科大学生，他们既上CS201，又是CS的
Someone who takes CS201 is CS-major
$\exists x, (P(x) \rightarrow Q(x))$
$\exists x, (P(x) \wedge Q(x))$
正确表达的是第二个
第一个意思是：
存在一个南科大学生，如果他上CS201，那么他是CS系的（言外之意是：如果这个学生没有上CS201，他也有可能是计算机系的），因为根据->的真值表，如果p是错的，那么结果一定是对的，不管q是否正确，这样就与原来的意思表达不符
总结：对于任意的修饰词，用->关系
对于存在这类修饰词，用逻辑与的关系

True，原因：

由于这个是逻辑等价，所以要从左边能证到右边，也要从右边证到左边

对于右边证到左边，取一个满足条件的值a，使得$P(a) \to Q(a)$为真，那么这个式子就满足了左边命题的定义，即存在性定义

对于左边证到右边，由于通常是在已知正确结论下的讨论，所以$\forall x\ P(x)$是必然成立的，所以说我们的前提是：$\exists x\ (P(x) \to Q(x))$，$\forall x\ P(x)$，需要推到的结论是$\exists x\ Q(x)$。这也是取一个满足条件的值a，使得$P(a) \to Q(a)$为真，由于是任取，所以单独的$P(a)$也为真，故此时的$Q(a)$必须为真，所以推到的结果成立，说明两个式子逻辑等价

命题逻辑

2019年3月10日 12:10

肯定前件式

modus ponens

$(p \wedge (p \rightarrow q)) \rightarrow q$

已知p->q，p为真，那么推出q也为真

否定后件式

modus tollens

$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

已知p->q，非p为真，那么非q也为真

假言三段论

hypothetical syllogism

$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

已知p->q，q->r

那么可以推出p->r

选言三段论

disjunctive syllogism

$(\neg p \wedge (p \vee q)) \rightarrow q$

带有量词的逻辑证明：

对于任意性量词，假设任意的一个数字a即可

对于存在性量词，就设一个特定的数字a即可

Addition

$p \rightarrow (p \vee q)$

Conjunction

$((p) \wedge (q)) \rightarrow (p \wedge q)$

Universal Instantiation

$\forall x P(x)$

$\therefore P(c)$

Simplication

$(p \wedge q) \rightarrow p$

Resolution

$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

Existential Instantiation

$\exists x P(x)$

$\therefore P(c)$ for some element c

Existential Generalization

P(c) for some element c

$\therefore \exists x P(x)$

Universal Generalization

P(c) for an arbitary c

$\therefore \forall x P(x)$

集合的定义

2019年3月10日 13:05

Two sets A,B are equal if and only if $\forall x\ (x \in A \leftrightarrow x \in B)$.

power set，幂集，写做P(S).指的是一个集合，这个集合里面包含了集合A所有的子集

笛卡儿积：Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a,b), where $a \in A$ and $b \in B$. Hence $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$，就是把一维元素的集合变成二维的

同理，还有N维的$A1 \times A1 \times \cdots \times An = \{(a1,a2,\ldots,an) \mid ai \in Ai \text{ for } i = 1,2,\ldots,n\}$

cardinality of S, denoted by |S|.指的是S集合中元素的个数

真子集：proper subset，符号是：$A \subset B$

并集：Union

$A \cup B$, is the set $\{x \mid x \in A \vee x \in B\}$.

补集：Complement

$\bar{A}$，$U - A$, $\bar{A} = \{x \in U \mid x 6\in A\}$.

交集：Intersection

$A \cap B$, is the set $\{x \mid x \in A \wedge x \in B\}$.

差集：Difference

$A - B$，$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}$

disjoint，即A和B的交集为空集

集合真值表

2019年3月10日 13:17

证明$\overline{A \cap B} = \bar{A} \cup \bar{B}$:

通过真值表可以证明，此时的真值表是针对元素而言，即判断这个元素在不在集合里面

使用0代表不在集合里面，1代表在集合里面

A	B	$\bar{A} \cup \bar{B}$	$\overline{A \cap B}$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

所以通过真值表得到相关的证明

集合的性质

2019年3月10日 13:16

$|A \times B| = |A| \times |B|$

$|A \cup B| = |A| + |B| - |A \cap B|$

Cardinality

2019年3月12日 15:22

对于两个有限元素的集合A和B，他们的Cardinality就是他们集合的元素个数
如果对于两个无限元素的集合A和B，如果他们的Cardinality相同，则他们集合之间的元素能建立一一对应的关系（bijection）
要么集合有限，要么能和正整数集合建立一一对应的关系（映射），就是可数集合（countable）
否则，就是uncountable
Countable set 可以将集合中的元素一一列举（通过和正整数集合建立一一对应的关系）出来

可数集的子集也可数

对于集合是否可数，通过集合的交并补来构造解答

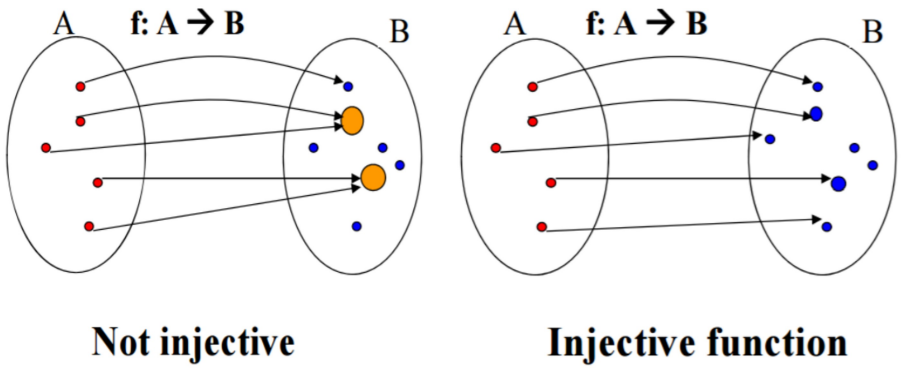
函数定义

2019年3月17日 12:34

函数指的是两个集合之间的映射，指的是集合A映射到集合B，记为f:A->B
对于函数，A中所有的元素都要和B中的元素产生一一对应的关系，而且A中的任意一个元素都只能对应B集合中的一个值

若f是A到B的函数，则称A是f的定义域，B是f的陪域（codomain）
值域指的是A中所有像（image）的集合

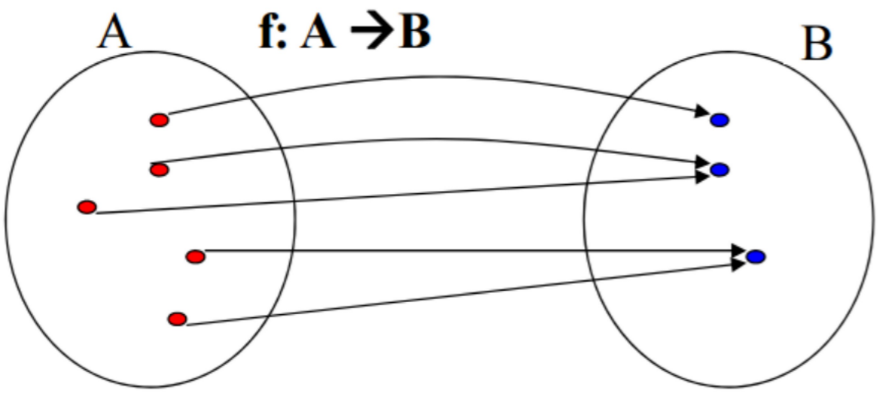
Injective Function（一对一函数）：指的是A集合中的每一个元素分别对应B中不同的值
如果这个函数是一对一函数，那么对任意A集合中的两个值x，y，f(x) = f(y)<=> x = y



Bijective Function：
当且仅当这两个函数既是一对一函数，又是映上函数

复合函数：$(f \circ g)(x) = f(g(x))$

Surjective（Onto） Function：映上函数
指的是函数的值域等于陪域
函数f是映上函数当且仅当对任意b∈B，存在a∈A使得f(a) = b


A
f: A → B
B

要点

2019年3月17日 12:52

“For a function f : A → B with |A| = |B| = n, f is one-to-one if and only if f is onto.对于这句话，是对的

“For a function f from A to itself, f is one-to-one if and only if f is onto, where A is infinite.对于这句话，就是错的

第二个例子的反例：假设陪域和定义域都是正整数,f(x) = 2 * x，这个值域就只有偶数而没有奇数

对于有限的集合A和B，如果f不是bijective，那么他们就没有反函数

$\subsetneq$

指的是真子集 $B - A = B \cap \bar{A}$

概念

2019年3月17日 13:09

对于任意的$n>n0$，都存在C使得$|f(n)| \le C|g(n)|$，则称$f(n) = O(g(n))$
对于任意$n>n0$，都存在C使得$|f(n)| \ge C|g(n)|$, 则称$f(n) = \Omega(g(n))$
$f(n) = O(g(n))$ and $g(n) = O(f(n))$当且仅当$f(n) = \Theta(g(n))$

$n! = O(n^n)$
$\log(n!) = O(n\log(n))$

$(f1 + f2)(x) = O(\max(|g1(x)|, |g2(x)|))$

主定理

2019年6月1日 14:03

假设我们有递推关系式：

$T(n) = aT\left(\frac{n}{b}\right) + f(n)$

其中，n为问题的规模、a为递推下子问题的数量，$\frac{n}{b}$为每个子问题的规模，$f(n)$为递推后做的额外的计算工作。

1.假设存在常数$\epsilon > 0$，使得$f(n) = O(n^{\log_b(a)-\epsilon})$，则$T(n) = \Theta(n^{log_b a})$。

具体意思是f(n)的上界是n的幂次，且$log_b(a)$比这个幂次要大，则时间复杂度为这个n的$log_b(a)$次。

例子：二叉树的遍历。$T(n) = 2T\left(\frac{n}{2}\right) + \Theta(1)$。其中$a = 2$，$b = 2$，$f(n) = 1$，此时$\epsilon = 1$。$T(n) = \Theta(n)$。

2.假设存在常数$k \geq 0$，使得$f(n) = \Theta(n^{\log_b a} \log^k n)$，则$T(n) = \Theta(n^{log_b a} \log^{k+1} n)$。

具体意思是f(n)是n的$log_b(a)$次，再乘以一个log，则复杂度是f(n)的复杂度再乘以一个log。

例子：归并排序。$T(n) = 2T\left(\frac{n}{2}\right) + \Theta(n)$。其中$a = 2$，$b = 2$，$f(n) = n$，此时$k = 0$。$T(n) = \Theta(n \log_2 n)$。

例子：二分搜索（折半搜索）。$T(n) = T\left(\frac{n}{2}\right) + \Theta(1)$，其中$a = 1$，$b = 2$，$f(n) = 1$，此时$k = 0$，则$T(n) = \Theta(log_2 n)$。

3.假设存在常数$\epsilon > 0$，有$f(n) = \Omega(n^{\log_b(a)+\epsilon})$，同时存在常数$c < 1$以及充分大的$n$满足$af\left(\frac{n}{b}\right) \leq cf(n)$那么$T(n) = \Theta(f(n))$。

这个感觉没啥用啊。。。

NP完全问题

2019年3月15日 17:38

具有相同的类型：
如果f（n）和g（n）有相同的类型，那么对f（n）和g（n）有f(n ^a)b1<=
多项式都是相同的类型，指数和多项式是不同的类型

NP完全问题是一类问题。如果对于一个NP完全问题有解，那么可以通过这个NP完全问题的解答来推出其他问题的解。但是，目前对于任何一个NP完全问题都没有一个有效的解答，所以说NP完全问题很有可能是NP难问题

优化问题和decision problem

2019年3月15日 17:42

Decision problem指的是输出是yes还是no
优化问题指的是最快的方式求出解
每一个优化问题都对应着Decision Problem

其中，输入的大小要求是用二进制的位数来表示，不是数据的个数！

通常，要想解决优化问题的关键是解决Decision Problem
所以，证明dicision问题难，就可以证明优化问题难
复杂度理论：将dicision问题划分成三类
简单，难，很难
如果是多项式时间，这个算法就是高效的
如果运行时间是O(n ^ k)，k是常数，n是输入大小，那么这个算法就是高效的

要点

2019年3月15日 17:55

定义Class P：P是所有的可以在多项式内解决的decision问题的集合
certificate：输出yes的特定的值
定义Class NP：要用多项式时间来验证一个certificate是不是yes-input

NP：不是确定性的多项式时间“nondeterministic polynomial-time”
根据NP的定义，故所有的P问题都属于NP
确定是不是合数属于NP问题

satisfiable：对于布尔代数，有一种方式使得结果为1
SAT问题：属于NP

计算机需要解决最重要的问题之一是：$P = NP$或$P \neq NP$，即是否存在一个算法使得所有的问题都有多项式时间的解，这里的NP指的是不确定是不是多项式时间，而不是非多项式时间！

时间复杂度

2019年3月17日 13:28

判断一个算法是不是多项式时间的时间复杂度，此时不仅要看执行了多少个指令，还要看数据量大小
其中，数据量的大小指的是输入数据的最小bit位数（如果输入数据是7，那么就占用三个bit位宽，所以数据量就是3）时间复杂度的真正表示方法是用数据量的函数来表示

例如，判断一个数是不是合数，采取的算法是从1到n依次遍历，通过迭代看看是不是符合要求
假设这个数据的大小为n，那么数据量大小为$size(n) = \log_2(n)$，所需要的指令数是$O(n)$（如果算上除法的时间复杂度，则需要的时间更多），所以用$O(2^{size(n)})$，故为指数的时间复杂度
例如，将n个数排序，那么数据量就是这n个数，假设这n个数平均每个数的大小是a，那么数据量就是$n\log_2(a_{max} + 1)$，排序算法的时间复杂度是$O(n^2)$，所以总的时间复杂度是$O(\frac{size(input)^2}{\log_2^2(a_{max}+1)})$

定义两个函数有相同的类型当且仅当$c_1 g(n^{a_1})^{b_1} \le f(n) \le c_2 g(n^{a_2})^{b_2}$，而对于所有的多项式都是有相同类型，但是指数和多项式不是相同的类型

加减乘除，指数取余复杂度

2019年3月27日 15:42

定义

假设有两个数a和b，这两个数用二进制表示时，其位数都是n

$a = (a_{n-1}a_{n-2}\ldots a_1a_0)$，$b = (b_{n-1}b_{n-2}\ldots b_1b_0)$

加法的复杂度（减法的处理和加法一样）

则a，b两个数相加，就需要先从低位开始算出结果和进位，依次计算直到高位

所以说，复杂度是O（n）

乘法的复杂度

a，b两个数相乘，相当于b中每个位置上的位数相加

$ab = a(b_0 2^0 + b_1 2^1 + \ldots + b_{n-1} 2^{n-1})$

$= a(b_0 2^0) + a(b_1 2^1) + \ldots + a(b_{n-1} 2^{n-1})$

对于a乘以b中的每一个位置的数来说，由于有次方，所以就相当于做移位操作

每一次移位操作需要消耗O（1）的时间复杂度，对于最后一项，需要消耗O（n）的时间复杂度，总共有n的数字，所以移位的时间复杂度是O（n^2）

对于加法，每一次加法都消耗O（n）的时间复杂度，总共要加n-1次，所以相加的总时间复杂度是O（n^2）

综上，乘法的时间复杂度是O（n^2）

除法的复杂度

除法算法参照机组Week6

循环的次数是被除数的总位数，

每一次循环都是相减，相减的时间复杂度是O（n）

所以说总的时间复杂度是O（n^2）

n指的是除数和被除数的总位数，

如果数值为a，则n = log（a）

对于指数取余运算

假设需要算的是$b^n \bmod m$，其中，b的大小是n，m是非零整数

$b^n = b^{a_{k-1}\cdot 2^{k-1}+\ldots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}}\ldots b^{a_1\cdot 2}\cdot b^{a_0}$

由于a_i只能取0和1，所以说b^{a_i}可以通过O（1）的算出

所以只需要算出b^k（k = 0，1，2...）即可

下面为其算法

```
procedure modular exponentiation(b: integer, n = (a_{k-1}a_{k-2}...a_1a_0)_2 , m: positive
    integers)
 x := 1
power := b mod m
for i := 0 to k − 1
      if a_i = 1 then x := (x·power) mod m
      power := (power·power) mod m
return x {x equals b^n mod m }
```

这个式子循环log（n）次，每一次做多做两次相乘运算，量词模运算

这些运算的时间复杂度是O（$(\log m)^2$）（因为结果都在0~m的范围内运算，所以最多是$(\log m)^2$）

所以整个运算的时间复杂度是O（$(\log m)^2\cdot\log(n)$）

整除

2019年3月22日 16:43

整除定义

对于整数a（$a \neq 0$），b，如果存在整数c，使得 $ab = c$，则称a能被b整除，记为$a|b$

整除性质

(i) if $a|b$ and $a|c$, then $a|(b + c)$

(ii) if $a|b$ then $a|bc$ for all integers c

(iii) if $a|b$ and $b|c$, then $a|c$

对等式 $a = dq + r$，a叫被除数（dividend），d叫除数（divisor）q叫商（quotient），r叫余数（remainder）

最大公约数

2019年3月22日 17:54

gcd（greatest common divisor）最大公约数
lcm（least common multiple）最小公倍数
大多定理都要使用北祖等式来证

北祖等式推论：
已知 a|bc，gcd（a，b） = 1
求证：a|c
证明：
gcd(a,b) = 1
=> 1 = sa + tb(s，t是整数)
=> c = sac + tbc
等式两边同时除a
得到左边a|c
所以等式得证

实际上，想要证明和gcd相关的问题，相关方法有：

1. 北祖等式推论
2. 北祖等式
3. 欧拉算法
4. 通过同余的变换来化简

北祖等式：
任意两个数的gcd一定可以表示成这两个数的线性组合
gcd(a,b) = sa + tb
证明：辗转相除法倒推即可

欧拉定理：用来寻找两个数的最大公约数
对于求gcd（a,b）如果a = b*q + r（q为整数，q<0）
则相当于求gcd（b，r）
通过这个定理，就可以不停的相除，取余数，即可找到最大公约数
证明欧拉定理：
已知：对于任意整数a，b，a = b*q + r
求证：gcd（a，b）= gcd（b，r）
证明：
假设gcd（a，b）=d,a = d * a'，则相当于证明d|r
则可以列出等式b*q + r = d * a'
等式两边同时除以d，得到r一定会被d整除所以得证

同余

2019年3月27日 16:47

同余（Congruent modulo）定义

a ≡ b(modm) 代表a和b同余

a mod m = b 是一种运算，b是在[0,m]范围内

性质

如果a ≡ b(modm)还有c ≡ d(modm)那么

c + a ≡ b + d(modm)，ac ≡ bd(modm)

注意：

如果a ≡ b(modm)，c是任意非零整数，则不能说a/c ≡ b/c (mod m)

例子：14 ≡ 8 (mod 6) but 7 !≡ 4 (mod 6)

证明同余的整体思路：

转换成 m|a - b

定理：m是正整数，ac ≡ bc(modm)，gcd（c，m）=1，

求证：a ≡ b(modm)

证明：证明思路和北祖等式的推论证明一样

意义：指明了什么时候可以被c可以被约掉

若$a \equiv b \mathrm{mod} m$，有$a^k \equiv b^k \mathrm{mod} m$

线性同余式

2019年3月26日 14:36

线性同余式指的是：

$ax \equiv b(\mathrm{mod}m)$，其中a，b，m都是整数，需要求x的解集

模逆定义：

找到一个整数$\bar{a}$，使得对于特定整数a，有下面等式成立：

$a \cdot \bar{a} \equiv 1(\mathrm{mod}m)$

对于解线性同余式

由$ax \equiv b(\mathrm{mod}m)$，得到$a \cdot \bar{a} \cdot x \equiv b \cdot \bar{a}(\mathrm{mod}m)$

又$a \cdot \bar{a} \equiv 1(\mathrm{mod}m)$，故$x \equiv b \cdot \bar{a}(\mathrm{mod}m)$

当a和m的gcd = 1，模逆存在且唯一

当a和m的gcd不为1，则模逆有多个，但是这里不考，所以不证

证明：

使用北祖等式1 = s*a + t*m

可以认为$s = \bar{a}$，可以证明此时$s \cdot a \equiv 1(\mathrm{mod}m)$（北祖等式同时除以m即可得到）

逆着欧拉算法就能找到s的值，通过北祖等式可以证明模逆的唯一性

北祖等式证明其存在

通过证明其唯一性：乘上a1

寻找模逆的方法：只需要找到m和a的gcd，并用北祖等式表示即可

eg：找101 mod 4620的模逆

$$
\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
1 &= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
1 &= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75 \\
1 &= 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75 \\
&= 26 \cdot 101 - 35 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\
&= -35 \cdot 4620 + 1601 \cdot 101
\end{aligned}
$$

所以1601就是101 mod 4620的模逆

求解线性同余式组

2019年3月27日 17:39

中国剩余定理

问题：

求解如下线性同余方程组

$x \equiv a1 \pmod{m_1}$

$x \equiv a2 \pmod{m_2}$

...

$x \equiv an \pmod{m_n}$

要求：

mi两两互素

方法：

令$m = m_1 m_2 \ldots m_n$，$M_k = m/m_k$

由于gcd（M_k，m_k）=1，就存在y_k，使得$M_k \cdot y_k \equiv 1 \pmod{m_k}$

令$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots + a_n \cdot M_n \cdot y_n$，则x就是这个线性同余方程组mod m的唯一解

注意：

如果mi不是两两互素，则可以通过拆分模的数将其转换成互素的数

但是这样子会使得式子增多

eg：

$x \equiv 8 \pmod{15}$

=> $x \equiv 8 \pmod{3}$, $x \equiv 8 \pmod{5}$

向后置换法

对于线性同余式，一开始设一个数，代换，不停的化简即可

eg：

$x \equiv 2 \pmod{3}$ ①

$x \equiv 3 \pmod{5}$ ②

$x \equiv 2 \pmod{7}$ ③

求解：

令$x = 3k + 2$

带入②，化简，再带到③，得到最终的表达式

费马小定理

2019年3月29日 16:25

令p为素数，令x为整数，x! ≡ 0modp（不和modp同余），也就是说p不能被x整除

则有：$x^{p-1} \equiv 1(\mathrm{mod}p)$

证明：

{1，2……，p-2，p-1}和{a，2a……，（p-2）a，（p-1）a}这两个集合内部的元素中，任意两个都不是模p同余的，而且模p同余就只有这么p-1种情况（除了整除）

1. {1，2……，p-2，p-1}和{a，2a……，（p-2）a，（p-1）a}这两个集合的乘积模p同余
2. $(p-1)! \equiv a^{p-1}(p-1)!\,(\mathrm{mod}p)$（阶乘）
3. $(p-1)! = (p-1)\cdot(p-2)\cdot\ldots\cdot 2\cdot 1$，每一个数模p都不等于零，故$(p-1)!$模p不等于0，故$(p-1)!$和p互素
4. 上式约掉$(p-1)!$，令a为x，即可得到结果

欧拉定理

2019年3月29日 16:26

令欧拉函数：$\phi(n)$为1到n中与n互素的正整数的个数

故对于任意素数p，q：

$\phi(p) = p - 1$
$\phi(p \cdot q) = (p - 1)(q - 1)$
$\phi(p^i) = p^i - p^{i-1}$

欧拉定理：

令n为正整数，令x为整数，gcd（x，n）=1

则有：$x^{\phi(n)} \equiv 1 (\mathrm{mod} n)$

证明略

本原根

2019年3月29日 16:35

本原根指的是一个数a的任意次方模本原根得到的值要填充{1，2……p-1}中所有的数
要模一个素数
3是模7的本原根
3的n次方模7的值等于1到6中的值，而且是全覆盖类型

模n有本原根只有4种情况，n = 2，4，p的e次方，2p的e次方，e是任意整数

RSA

2019年3月30日 11:59

选2个很大的素数p，q，令n=pq，$\phi(n) = (p-1)(q-1)$，令任意整数e，d满足以下性质

$\gcd(e, \phi(n)) = 1$，$ed \equiv 1 (\mathrm{mod}\, \phi(n))$

则$C = M^e \mathrm{mod} n$，称为加密；$M = C^d \mathrm{mod} n$，称为解密

这里用到的是NP难问题，也就是找到一个很大的数字p和q很容易，但是，将n分解成一个两个素数的乘积很难

对外界公布的是n和e

自己掌握的是p，q和$\phi(n)$

对于证明RSA的正确性，也就是说，需要证明：

令p，q为奇素数，令n = pq，令e为正整数，gcd（e，$\phi(n)$）=1，令d为正整数，$ed \equiv 1 (\mathrm{mod}\, \phi(n))$，则对于x在0<x<n的范围内有：

$x^{ed} \equiv x (\mathrm{mod}\, n)$（通过加密和解密合并得到的式子）

证明：

由于0<x<n故只需证明$x^{ed} \mathrm{mod} n = x$

由gcd（e，$\phi(n)$）=1，根据北祖等式得到$\exists a, b$,使得$a \cdot e = 1 + b \cdot \phi(n)$,其中a=d

带入上式得$x^{1+b \cdot \phi(n)} \mathrm{mod} n = x$

整理得 $x \cdot \left(x^{\phi(n)} \mathrm{mod} n\right)^b \mathrm{mod} n) \mathrm{mod} n = x$

根据欧拉定理得$x \cdot \left((1)^b \mathrm{mod} n\right) \mathrm{mod} n = x$

故源式得证

对称和非对称密码学

2019年3月30日 11:58

对限制条件要求很高
在传递的过程中，密钥的要求很高

加密的密钥和解密的密钥不一样
不需要进行提前的密钥协商
每个人才能有自己独特的解密钥匙

RSA相关证明

2019年4月22日 21:15

RSA描述：

选2个很大的素数p，q，令n=pq，$\phi(n) = (p-1)(q-1)$，令任意整数e，d满足以下性质

$\gcd(e, \phi(n)) = 1$，$ed \equiv 1 (\mathrm{mod}\, \phi(n))$

则$C = M^e \mathrm{mod} n$，称为加密；$M = C^d \mathrm{mod} n$，称为解密

证$M = C^d \mathrm{mod} n$

证明：

1. gcd（n，M）=1

   也就是证明：$M = M^{ed} \mathrm{mod} n$

   假设$ed = 1 + k\phi(n)$

   所以有：$M = M^{1+k\phi(n)} \mathrm{mod} n$

   所以就是证明$M(M^{k\phi(n)} - 1) \mathrm{mod} n = 0$

   就是证明$(M^{k\phi(n)} - 1) \mathrm{mod} n = 0$

   这里由费马定理可以很容易得到

2. gcd(n,M)=p

   令M=tp

   所以就是证明$M(M^{k\phi(n)} - 1) \mathrm{mod} n = 0$

   只需证明$(M^{k\phi(n)} - 1) \mathrm{mod} q = 0$即可

   只需证明$(M^{k(p-1)\phi(q)} - 1) \mathrm{mod} q = 0$，该等式可以通过费马定理得到

3. gcd(n,M)=q

   同上

4. gcd(n,M)=pq

   易得

Consider the RSA system. Let (e, d) be a key pair for the RSA. Define λ(n) = lcm(p − 1, q − 1) and compute $d' = e^{-1} \mathrm{mod} \lambda(n)$. Will decryption using d 0 instead of d still work? (prove $C^{d'} \mathrm{mod} n = M$)

证明：

1. gcd（n，M）=1

   即证明$M^{ed'} \mathrm{mod} n = M$

   由$d' = e^{-1} \mathrm{mod} \lambda(n)$，设$ed' = k\lambda(n) + 1$

   即证明$M^{k\lambda(n)+1} \mathrm{mod} n = M$

   即证明$M(M^{k\lambda(n)} - 1) \mathrm{mod} n = 0$

   即证明$M(M^{k\phi(n)/\gcd(p-1,q-1)} - 1) \mathrm{mod} n = 0$

   此时，根据费马定理易得

2. gcd（n，M）=p

   即证明$M(M^{k\phi(n)/\gcd(p-1,q-1)} - 1) \mathrm{mod} n = 0$

   也就是证明$(M^{k\phi(n)/\gcd(p-1,q-1)} - 1) \mathrm{mod} q = 0$

   分解$\phi(n)$即可证明，同左边

3. gcd（n，M）=q

   同2

4. gcd（n，M）=pq易得

数归两种方法

2019年4月9日 14:25

通过最小的反例来证明原命题正确
先假设最小的反例为m
先验证0是成立的
在n=m时，通过推导使得n=m时成立，所以推出矛盾

将反证法变成正向证明，就变成了数归

良序集才能用数归，例如自然数集

弱准则：
先证明最小的情况成立
在证明P（n-1）->P（n）
流程：

1. Base case
2. Inductive hypothesis（归纳假设）
3. Inductive step（推论）
4. Conclusion

强准则：
先证明P（0）正确，然后证明$P(0) \wedge P(1)$正确，
然后推到$P(0) \wedge P(1) \wedge \ldots\ldots P(k-1)$正确
要求证明P（k）正确
强准则和弱准则是等价的

递归

2019年4月9日 15:13

总体来说就是使用了分治的思想

关键是如何展开递推式

方法就是就是一步一步的写出来，找到规律即可

对$T(n)=\begin{cases} T(1), if\ n=1 \\ 2T(n/2)+n, if\ n\geq 2 \end{cases}$进行递推

得到结果$\mathrm{nT(1)+nlog_2n}$

$$\mathrm{T(n)}=\begin{cases} 1, \mathrm{if\,n=1} \\ \mathrm{f(n)T(n-1)+g(n), if\,n\geq 2} \end{cases}$$

一阶线性递推式

令$\mathrm{f(n)=r}$为常数，进行递推，得

$$\mathrm{T(n)=r^nT(0)+\sum_{i=0}^{n-1} r^i g(n-i)}$$

证明方法通过数归来证

例题

2019年5月3日 15:54

假设存在集合A，B，$|A| = m$，$|B| = n$

问：

1. 从A到B中有多少种onto-function
2. 有多少种function使得A到B的映射中B集合至少有一个元素没有被映射到

根据观察，可以发现，这两个问题的解集互为补集

也就是说$(1) + (2) = n^m$

所以，只要求解一个问题就解决了两个问题

对于第二个问题，假设E_i为集合B中第i个元素，这个元素没有被映射到

所以（2）的解答就是$|\cup_{i=0}^{n} E_i|$

通过公式，化简得到$\sum_{k=1}^{n}(-1)^{k+1}\sum_{1\le i_1<i_2\ldots<i_k\le n}^{\square}|E_{i_1}\cap E_{i_2}\ldots\cap E_{i_k}|$

由于$|E_i| = (n-1)^m$，$|E_{i_1}\cap E_{i_2}\ldots\cap E_{i_k}| = (n-k)^m$

所以结果是：$\sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}(n-k)^m$

判断能否构成三角形

2019年4月26日 16:41

将各个点进行升序排列，那么这个按照升序排列的元组就是从{1，2。。。n}中取三个元素组成集合的个数
证明：也就是证明一个元组到集合的函数是bijective

要点

2019年4月26日 16:44

两个集合的大小相同当且仅当存在一个函数，使得两个集合能建立一一对应关系

$$\binom{n}{k} = C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{k!\,(n-k)!}$$

Inclusion-Exclusion Principle：

指的是集合的并集关系

对于二元的等式：

$|A \cup B| = |A| + |B| - |A \cap B|$

对n维：

$$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 \le i_2 < \ldots < i_k < n} |E_{i_1} \cap E_{i_2} \cap \ldots \cap E_{i_k}|$$

Binomial Coefficients

2019年4月26日 17:34

要求：

证明$\sum_{i=0}^{n}\binom{n}{k}=2^n$

这里通过集合论的思想来证明

定义P为{1，2……n}中所有集合的子集

定义S_i为{1，2……n}中抽取i个元素组成的子集

则$|P|=\sum S_i=\sum_{i=0}^{n}\binom{n}{k}$(可以认为是对问题的具体化，方便找到一个bijective）

定义L为长度为n的bit字符串（每个位置上只能显示0和1）

则根据排列组合知道$|L|=2^n$。现在就是证明P到L是bijective

易证这两个函数为bijective，所以原命题得证

使用二项式定理可以证明关于二项式系数的不等式

通过数学归纳法来证明

杨辉三角

2019年4月26日 17:29

证明$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

这个定理是帕斯卡定理

分成两种不同的方式即可

这里采用一种递归的思想

$\binom{n}{k}$就相当于在装有n个小球的盒子中取出k个

右式分成两种情况，是否取某个特定的小球，其中$\binom{n-1}{k-1}$代表取这个小球，所以要在剩下的n-1个小球中取k-1个。

$\binom{n-1}{k}$代表不取这个小球，所以在剩下的n-1个小球中取k个

如图，函数为C（n，k）如果将表变成正的就变成了杨辉三角

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

二项式定理（Binomial Theorem）

2019年5月3日 16:43

使用排列组合的思想来证明的

如果未知数增多，就会产生三项式定理

$$(a+b+c)^n = \frac{n!}{k_1! \cdot k_2! \cdot k_3 \cdot !} a^{k_1} b^{k_2} c^{k_3} = \binom{n}{k_1\, k_2\, k_3} a^{k_1} b^{k_2} c^{k_3}$$

定义 2 设 u 是实数且 k 是非负整数。那么广义二项式系数 $\binom{u}{k}$ 定义为

$$\binom{u}{k} = \begin{cases} u(u-1)\cdots(u-k+1)/k! & k>0 \\ 1 & k=0 \end{cases}$$

定理 2 **广义二项式定理** 设 x 是实数，$|x|<1$，u 是实数，那么

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k$$

可以使用麦克劳林级数的理论证明定理 2，我们将这个证明留给熟悉这部分微积分的读者完成。

评注 当 u 是正整数时，广义二项式定理就归约到 6.4 节提出的二项式定理，因为如果 $k>u$，那么在这种情况下 $\binom{u}{k}=0$。

证明欧几里得算法

2019年5月5日 16:29

通过观察发现： $r_{i+2} = r_i \mathrm{mod} r_{i+1}$

要证明欧几里得算法是$O(\log n)$

所以也就是要证明：$r_{i+2} < \frac{1}{2} r_i$（i越高数字$r_i$越小）

通过对r_{i+1}进行分类讨论即可

1. $r_{i+1} \leq \frac{1}{2} r_i$

   由于模性质$r_{i+2} < r_{i+1}$，则必有$r_{i+2} < \frac{1}{2} r_i$

2. $r_{i+1} > \frac{1}{2} r_i$

   由于$r_{i+1} < r_i$，则此时余数必定为1

   故原式可化简为：$r_i = r_{i+1} + r_{i+2}$

   由于$r_{i+1} > \frac{1}{2} r_i$，则必有$r_{i+2} < \frac{1}{2} r_i$

综上，原命题得证

k阶线性齐次方程

2019年5月5日 16:34

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$

齐次：要求有关于和ai相关的数

对于上式，就是k阶线性齐次方程

$A_n = A_{n-1} + 1$就不是线性齐次方程（不满足齐次性）

对于线性齐次方程，如果不给初始值则有很多个解

如果给了初始值，则解唯一

通过特征方程，猜其解的形式来解

解的方法在于化成特征方程，然后求解

对于该方程$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$

化成$x^k = c_1 x^{k-1} + c_2 x^{k-2} + \ldots + c_k$

然后求解，即可

考虑二阶的特征方程

如果这有两个根，那么解的形式当且仅当为

$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$

证明：

也就是要证明：$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$为一个解的形式

还要证明解的形式只有可能为：$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$

对于证明第一种，只需要带进去即可

对于第二种的证明：通过数学归纳法即可证明，证明略

考虑二阶的特征方程

如果$r^2 - c_1 r - c_2 = 0$只有一个解

则$a_n = \alpha_1 r_1^n + \alpha_2 n r_2^n$

证明解的形式：

利用重根的条件

$\begin{cases} f(r) = 0 \\ f'(r) = 0 \end{cases}$（最大值在顶点处取得，导数为0）

等式两边乘上r的n次方，求导，发现nr^n也能满足条件，所以用nr^n来代替r2

对于$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + \mathrm{f(n)}$

就有通解和特解，通解和特解相加变成了最终解

通解指的是先解

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$

得到的是通解

然后通过构造法，得到特解

例如：

$a_n = 3a_{n-1} + 2n$，$a_1 = 3$

首先只看$a_n = 3a_{n-1}$，得到$a_n = \alpha 3^n + p(n)$

通过构造法得到由于f（n）是一次，所以设p（n）为一次多项式

令$p(n) = cn + d$，得到$cn + d = 3(c(n-1) + d) + 2n$

解方程式，得到c = −1 and d = −3/2

所以$p(n) = -n - \frac{3}{2}$

代入a_1得到最终结果

生成函数

2019年5月5日 17:36

作用在于证明递推式，证明组合恒等式等等，关键点在于求和和找幂级数前面的系数
只要幂级数前面的系数相同，生成函数就相等

一个数列的生成函数在于，对数列$\{a_k\}$，其生成函数为$\sum_{k=0}^{\infty} a_k x^k$，其中，这个加和是无穷级数
对于数列$\{a_k\}$，有$a_k = 3$，则其生成函数为$\sum_{k=0}^{\infty} 3x^k$
对于$a_k = 2^k$，其生成函数为$\sum_{k=0}^{\infty} 2^k x^k$
当a_{n+1}，a_{n+2}……等为零时，就变成了有穷加和（在排列组合中用到很多）
对于$a_k = C(m,k)$，其生成函数为$\sum_{k=0}^{m} C(m,k)x^k = (1+x)^m$

令$f(x) = \sum_{k=0}^{\infty} a_k x^k$，$g(x) = \sum_{k=0}^{\infty} b_k x^k$
则$f(x) + g(x) = \sum_{k=0}^{\infty} \left(a_k + b_k\right) x^k$

$$f(x)g(x) = \sum_{k=0}^{\infty} \left(x^k \times \sum_{j=0}^{k} a_{k-j} b_j \right)$$

对于生成函数的结果表示
和无穷级数很相似（例如幂级数等等）

eg：
求$x_1 + x_2 + x_3 = 17$，解的个数
其中$2 \le x_1 \le 5, 3 \le x_2 \le 6, 4 \le x_3 \le 7$
解法是：$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$
计算上述多项式中x^{17}前面的系数

定义

2019年5月13日 13:14

任何关系R都是笛卡儿积的子集
在关系代数中我们只研究集合A对集合A的关系
而且我们研究binary relation，这种关系可以在01矩阵中表示

研究的是从A到A自身的关系

a R b，指的是（a，b）这个元素在R这个关系中
有时也记作a->b

一般的，通过01矩阵可以表示这个关系
01矩阵中的每个位置代表着对应的元素是否在关系R中
对于A R B，横坐标代表A的元素，纵坐标代指B的元素

通过01矩阵，或者通过有向图表示binary relation

五种重要的关系

2019年5月13日 13:20

Reflexive relation
自反性：在A集合对应的关系R中
（a，a）都在R中
主对角线上的元素都是1
其余随意

Irreflexive relation
在A集合对应的关系R中
任意（a，a）都不在R中
主对角线都为0
其余随意

Symmetric relation
对称性：
若（a，b）∈R，则（b，a）也要∈R
对称矩阵（转置于其本身都是一样的）
主对角线随意

Antisymmetric relation
如果（b，a）∈R且（a，b）∈R推得a=b对任意a，b∈A
上三角部分可以是1，可以是0
上三角部分及其对称部分不能同时为1
主对角线随意
Mij = 1推得mji = 0

Transitive relation
若（a，b）∈R，（b，c）∈R，则（a，c）也要属于R
transitive在01矩阵中

Composite of relations

2019年5月7日 14:35

令R为集合A到B的关系，S为集合B到C的关系
若$a \in A$，$b \in B$，$c \in C$且$(a,b) \in R$，$(b,c) \in S$
则定义$S \circ R$为R和S的组合，其中（a，b）和（b，c）
得到的结果为（a，c）

关系R的n次幂：
$R^1 = R$，$R^{n+1} = R^n \circ R$

在集合A中的关系R为transitive当且仅当$R^n \subseteq R$
证明必要性
这里令n=2，这里已知$(a,b) \in R, (b,c) \in R$
根据R^2的定义，$a(c) \in R^2$
由$R^n \subseteq R$，故$(a,c) \in R$，故R为transitive
证明充分性
当n = 1时，$R \subseteq R$
假设当$1 \leq n \leq k$时等式成立，即$R^n \subseteq R$
当n = k+1时
假设$(a,b) \in R^{k+1}$，则根据$\mathrm{R}^{\mathrm{k}+1} = \mathrm{R}^{\mathrm{k}} \circ \mathrm{R}$
存在$x \in A$使得$(a,x) \in R$，$(x,b) \in R^k$
则根据由于$R^k \subseteq R$，故$(x,b) \in R$
由R为transitive，故$(a,b) \in R$
故$R^{k+1} \subseteq R$

要点：
需要注意的是符号标记$S \circ R$是反着的
真正的操作步骤是R和S进行结合
R找第二个元素，S里面找第一个元素，首尾相接
注意composition是反着的
转化成01矩阵就是R和S矩阵相乘，如果矩阵相乘结果大于1，则结果就是1

n元关系

2019年5月13日 22:18

设$A_1, A_2 \ldots A_n$为集合，定义在这些集合上的n元关系是$A_1 \times A_2 \times \ldots A_n$的子集
$A_1, A_2 \ldots A_n$称为这个关系的域，n称为关系的阶

Functional：
n元组中一个属性唯一标识这个元组
Composite key：
多个属性唯一标识这个元组

闭包

2019年5月13日 22:25

令S为R的闭包
闭包有三种情况：
reflexive，symmetic，transitive closures
（剩下的两种性质不管如何加元素，都不能满足闭包的性质）
对于任意性质的闭包，都要满足以下三种性质：

1. Minimal set，即原集合的最小生成集合（证明对任意包含集合R且满足性质P的关系Q，证明$S \subseteq Q$）
2. Contain R，元素需要包含原集合
3. 满足P（reflexive，symmetic，transitive）性质

由于可以很容易的得到reflexive和symmetic的闭包，这里不再说明
关键是得到transitive的闭包
使用图表示闭包，发现得到transitive closure的关键在于
在有向图中，使用有向路径找到所有连接的元素

令R为A对应的关系，a，b为A中的元素
则存在从a到b长度为n的路径当且仅当$(a, b) \in R^n$
证明：

1. 使用数归，当n = 1时，显然成立
2. 假设为n时条件成立
3. n+1时，设该路径为$x_0 \to x_1 \to x_2 \to \ldots \to x_n$，将这条路径在$x_0 \to x_1$处截断，由于$x_0 \to x_1$长度为1，属于$R^1$，$x_1 \to x_2 \to \ldots \to x_n$长度为n，属于$R^n$，而$x_i$这n个点相互不相同，根据$R^{n+1} = R^n \circ R$，得到$(x_0, x_n) \in R^{n+1}$，而且$x_0$到$x_n$长度为n+1,故得证

令$R^* = \cup_{k=0}^{\infty} R^k$，则对任意两点a，b，都存在一条确定长度的路径
则R^*就是R的transitive clousure
由于R^i代表着有向图中长度为i的点

现在证明R*就是transitive closures
Transitive closures需要满足三个性质
minimal set，contain R，满足transitive性质
（1）由$R^* = \cup_{k=0}^{\infty} R^k$，故Contain R易证
（2）证明R*是transitive
如果（a,b）联通且（b，c）联通，则一定存在一条路径使得（a，c）联通（从a到b，再从b到c）
（3）证minimal set，也就是证：对任意包含R且满足transitive的关系S，$R^* \subseteq S$
由于S是transitive，则$S^n \subseteq S$（根据一个证明过的性质）
而且S^n也为闭包（这个使用数归，将（a，b）拆分成（a，x）和（b，x），（a，c）同理），得到最终结果
故$S^* \subseteq S$，由于R*是R的最小生成集，故$R^* \subseteq S^*$
故$R^* \subseteq S^* \subseteq S$，原命题得证

使用warshell算法可以计算R的闭包，此算法将计算简化成了n^3
步骤如下：

procedure Warshall ($\mathbf{M}_R$: zero-one $n \times n$ matrix)
// computes R^* with zero-one matrices
$W := \mathbf{M}_R$;
for $k := 1$ to n
  for $i := 1$ to n

则R^*就是R的transitive clousure

由于R^i代表着有向图中长度为i的点

假设R中有n个点，故该有向图中最大的长度为n

所以不需要进行到∞次才能得出结果，只需进行n次幂集，将前n次的结果取并集，即可得到R*

```
W := M_R;
for k := 1 to n
  for i := 1 to n
    for j := 1 to n
        w_ij := w_ij ∨ (w_ik ∧ w_kj)
return W
// W is the zero-one matrix for R*
```

关键思路在于k指的是集合中每一个元素，i和j指的是遍历矩阵每一次循环都添加进一个点，加入的这个点使得矩阵尽可能联通，从而声称闭包

第k个点的遍历代表经过k个点的路径有哪些

等价关系和等价类

2019年5月13日 23:16

设关系R作用在集合A中

如果R满足reflexive, symmetric, and transitive的性质，则称R为等价关系

reflexive，自反性

symmetric，对称性

transitive，传递性

令R为集合A中的等价关系

与A中一个元素a有关系的所有元素的集合叫a的等价类，简称$[a]_R$

Eg:

$$A = \{0, 1, 2, 3, 4, 5, 6\}$$
$$R = \{(a, b) : a \equiv b \bmod 3\}$$

$$[0] = [3] = [6] = \{0, 3, 6\}$$
$$[1] = [4] = \{1, 4\}$$
$$[2] = [5] = \{2, 5\}$$

设R是A中的等价关系

则关于集合A中的两个元素a，b的命题是逻辑等价的

(i) a R b （$(a, b) \in R$） (ii) [a] = [b] (iii)$[a] \cap [b] \neq \emptyset$

证明方法主要是通过等价关系的三个性质得来的

证 首先证明(i)推出(ii)。假设 aRb，我们将通过$[a]\subseteq[b]$和$[b]\supseteq[a]$来证明$[a]=[b]$。假设 $c\in[a]$，那么 aRc。因为 aRb 且 R 是对称的，所以 bRa。又由于 R 是传递的以及 bRa 和 aRc，就得到 bRc，所以 $c\in[b]$。这就证明了$[a]\subseteq[b]$。类似地，可证明$[b]\subseteq[a]$，证明留给读者作为练习。

其次我们将证明(ii)推出(iii)。假设$[a]=[b]$。这就证明了$[a]\cap[b]\neq\varnothing$，因为$[a]$是非空的(由 R 的自反性 $a\in[a]$)。

下面证明(iii)推出(i)。假设$[a]\cap[b]\neq\varnothing$，那么存在元素 c 满足 $c\in[a]$且 $c\in[b]$。换句话说，aRc 且 bRc。由对称性，有 cRb。再根据传递性，由 aRc 和 cRb，就有 aRb。

由于这3个性质，可以将R分成若干个等价类

偏序

2019年5月13日 23:33

设定义在集合S上的关系R，如果R是reflexive, antisymmetric, and transitive
则称R是偏序的，集合S和偏序R一起被称为偏序集，记为（S，R）poset
集合S称为偏序集中的元素

偏序集中若$a \prec b$或者$b \prec a$，则称a，b两个元素可比

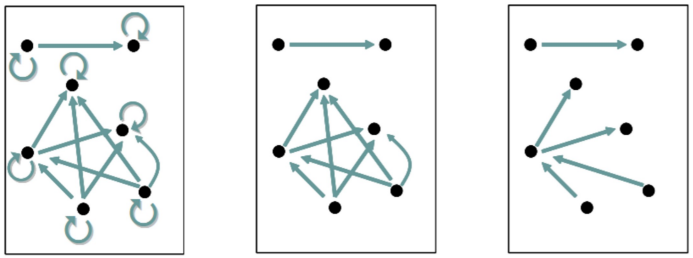
Example:

$S = \{1, 2, 3, 4, 5, 6\}$, R denotes the "$|$" relation

$2, 4$ are comparable, $3, 5$ are incomparable.

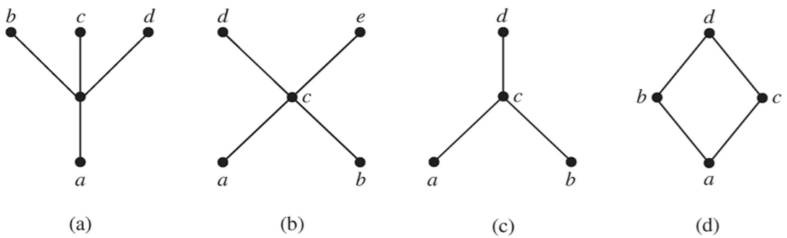
因为（2，4）在R中，而（4，2）不在R中，所以2，4可比
而（3，5），（5，3）都不在R中，所以不可比

可比性可以形成一条链
由此可以构造Hasse Diagram
简单来说就是去掉自反的路径，比较长的路径（满足传递性的路径）



由此可以定义极大值，极小值，最大值，最小值

Example



(a) 中极小值是a，极大值是b，c，d，最小值是a，没有最大值
(b) 中极小值是a,b，极大值是d,e，没有最小值，没有最大值
(c) 中极小值是a,b，极大值是d，没有最小值，最大值是d
(a) 中极小值是a，极大值是d，最小值是a，最大值是d

令A为偏序集S的子集
令u∈S为upper bound，若所有A中的元素都大于u
同样的可以定义lower bound

例 18 找出图 7 中的哈塞图所示的偏序集的子集$\{a, b, c\}$、$\{j, h\}$和$\{a, c, d, f\}$的下界和上界。

解 $\{a, b, c\}$的上界是 e、f、j 和 h，它的唯一的下界是 a。$\{j, h\}$没有上界，它的下界是 a、b、c、d，e 和 f。$\{a, c, d, f\}$的上界是 f、h 和 j，它的下界是 a。◀

令x∈S为least upper bound，若x是A中的upper bound，且比其他的upper bound都小
同样的可以定义greatest lower bound

例 19 在图 7 所示的偏序集中，如果存在，求出$\{b, d, g\}$的

(a) 中极小值是a，极大值是d，最小值是a，最大值是d

注意：偏序要求的是自反，反对称，传递

等价类要求的是自反，对称，传递

例 19 在图 7 所示的偏序集中，如果存在，求出$\{b, d, g\}$的最大下界和最小上界。

解 $\{b, d, g\}$的上界是 g 和 h。因为 $g \prec h$，所以 g 是最小上界。$\{b, d, g\}$的下界是 a 和 b。因为 $a \prec b$，所以 b 是最大下界。◀

要点

2019年5月7日 15:02

relation个数：2^{n^2}个
reflexive个数：$2^{n(n-1)}$个
irreflexive个数：$2^{n(n-1)}$个
Symmetric个数：$2^{\frac{n(n+1)}{2}}$个（上三角加上主对角线）
antisymmetric个数：$2^n \times 3^{\frac{n(n+1)}{2}}$个

偏序关系
满足reflexive，antisymmetric，transitive性质，称R为poset

可比性
首先要是poset，要么（a，b）属于R，要么（b，a）属于R
这个是针对单一的某个元素

Total ordering
如果这个集合的任意两个元素都具有可比性，那么就是total ordering，就可以形成一条链

Lexicographic ordering

定义

2019年5月25日 16:28

每一条边由一个或两个点相连

Each edge has either one or two vertices associated with it, called its endpoints.

An edge is said to be incident to (or connect) its endpoints.

图的边可以是曲线，也可以是直线

简单图

最多有一条边连接图中的任意两个点（没有重边）

完全图K_n

图中任意两个点都有一条边连接

Neighborhood$N(v)$

指的是和点v相邻的点的集合

$\deg(v)$

指点v的度

bipartite（二分图）

V可以被分成V_1和V_2

每一条边都连接V_1和V_2上的某个点

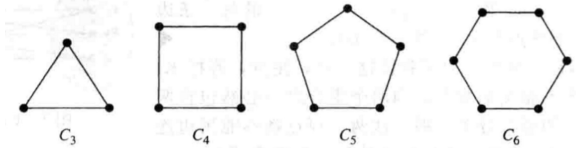
另外一种定义是：

能对图中的每个顶点赋予两种不同的颜色，且

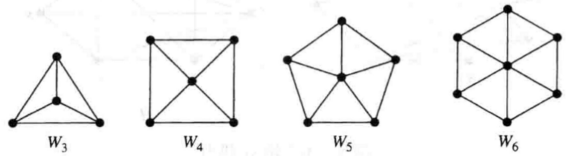
使得没有两个相邻的顶点被赋予相同的颜色

Complete Bipartite Graphs （完全二分图）

环：要求成环的边个数至少是3条边（C_n）

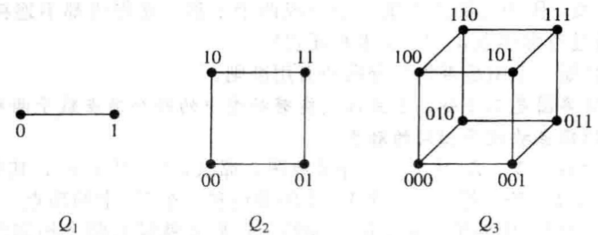


wheel：环加上一个顶点（W_n）



N-dimensional Hypercube（N立方体图）

例 8　n 立方体图　**n 立方体图**记作 Q_n，是用顶点表示 2^n 个长度为 n 的位串的图。两个顶点相邻，当且仅当它们所表示的位串恰恰有一位不同。图 6 显示了图 Q_1、Q_2 和 Q_3。



Complete Bipartite Graphs （完全二分图）

二分图中，V_1上每一个顶点，都有一条边连接到V_2的任意一个顶点上

$K_{2,3}$

Q_1 Q_2 Q_3

无向图性质

2019年5月25日 16:38

Handshaking theorem
若G是无向图，有m条边
则$2m = \sum_{v \in V} \deg(v)$

无向图有偶数个度为奇数的顶点

有向图性质

2019年5月25日 16:54

入度：$\deg^{-}(v)$

出度：$\deg^{+}(v)$

令E为图G上的边，则

$$|E| = \sum \deg^{-}(v) = \sum \deg^{+}(v)$$

二分图匹配

2019年5月27日 19:57

给定一个二分图，定义最大匹配为：
最多数量的边能重合
对于一个在二分图G = （V，E），其二分顶点的集合为(V1, V2)，其匹配为M，则M为完全匹配当且仅当V1中每一个端点都在M中，即 |M| = |V1|.

霍尔定理：
带有二部划分的（V_1，V_2）的二分图G = （V，E）中有一个V_1到V_2的完全匹配当且仅当对于V_1的所有子集A，有$|N(A)| \geq |A|$
证明充分性：
对于二分图中V_1的任何子集A，由于其是二分图，所以一定是联通的，所以对于$a \in A$，$\deg(a) \geq 1$
所以$|N(A)| \geq |A|$
证明必要性：
当n = 1时，$|V_1| = 1$，为二分图
当$0 \leq n \leq k$时，假设原定理成立
n = k+1时，分两种情况

1. 对于$1 \leq j \leq k$，W_1中的这些元素都与V_2中至少j+1个顶点相邻
   则一定存在一个点v属于$v \in W_1$，其对应点为w
   删去v和w及其相关联的点，得到剩余的点，其满足假设，等式成立，得证
2. 对于$1 \leq j \leq k$，V_1中的这些元素都与V_2中恰好j个顶点相邻
   假设这j个顶点组成的集合为$W_1{}'$，对应的邻居为$W_2{}'$
   则删去这些点$(V_1 - W_1{}', V_2 - W_2{}')$，剩下的顶点恰好组成了一个完全的二分图
   为了证明$(V_1 - W_1{}', V_2 - W_2{}')$是完全二分图，也就是证明对于$V_1 - W_1{}'$的所有子集A，有$|N(A)| \geq |A|$
   只需反证其存在一个子集，少于t个即可

图的表示方法

2019年5月28日 14:32

邻接表

对于每一个顶点，在链表中记录其相邻的顶点

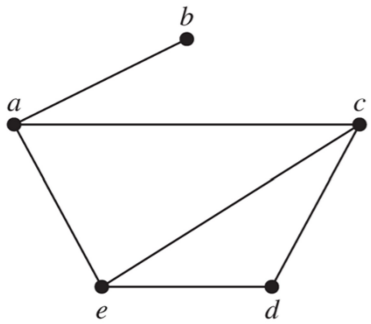


TABLE 1 An Adjacency List for a Simple Graph.

Vertex	*Adjacent Vertices*
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

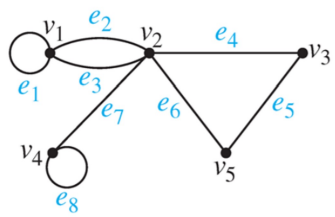
关联矩阵（Incidence matrix）

行是顶点，列是边

如果是1代表第j条边是否与第i个

顶点相连

否则就是0



$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

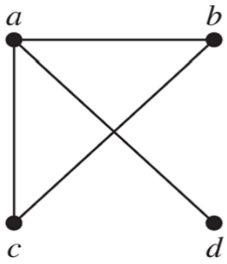
邻接矩阵

行和列分别是顶点组成的集合，代表行中的元素指向列中的元素

使用邻接矩阵可以表示多个边，也可以表示非简单图

$\mathbf{A}_G = [a_{ij}]_{n \times n}$, where

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \text{ is an edge of } G, \\ 0 & \text{otherwise.} \end{cases}$$



$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

同构图

2019年5月21日 15:06

设图$G_1 = (V_1, E_1)$，$G_2 = (V_2, E_2)$都是简单图，若存在从V_1到V_2one-to-one 还有onto function f
且f具有如下性质：对 V_1中任意两点a，b来说，a和b在G_1中相邻当且仅当f(a)和f（b）在G_2中相邻
则称G_1和G_2是同构（isomorphism）的

如果两个图有相同的长度为k的回路，则这两张图为同构图

在变换的过程中，不变的有

1. 度的个数及其数量
2. 顶点的个数
3. 边的个数

关键在于：同构图中映射的对应点的度的个数都要一样

凸多面体一定可以压到纸上，使得边与边之间不相交

联通

2019年5月28日 14:59

如果图是强连通的，则对于有向图的任意两个顶点都存在路径
如果图是弱联通的，则对于无向图的任意两个顶点，都存在路径

点联通性
定义$\kappa(G)$是使G变成不连通的图或者只含有一个顶点的图所需删除的最小顶点数
若G中含有n个结点，则$0 \leq \kappa(G) \leq n-1$
$\kappa(G)$越大，说明联通性越好
边联通性
定义$\lambda(G)$为边割集（需要消除什么边才能使得图不连通）中最小的边数
若G本身就不连通，则$\lambda(G)=0$

割点（cut vertices）
如果去掉这个点及其对应边，则这个图就不联通
割边（cut edge）
去过去掉这个边，这个图就不联通

要点

2019年5月24日 16:45

凸多面体一定存在球面嵌入和平面嵌入

r个邻接矩阵相乘，结果是图中长度为r的矩阵的条数
其中，数值代表长度为r的路径的个数
通过数归证明

最短路径问题：dijkstra算法

欧拉回路和哈密顿回路

2019年5月29日 14:30

欧拉回路：经过所有点的简单回路（一笔画问题产生了回路，要求回到起点）
欧拉路径：经过所有点的简单路径（一笔画问题产生的路径，不要求回到起点）

构成欧拉回路的充要条件
每一个顶点的度必须是偶数
由于要构成回路，所以每一个顶点要有一个出的边和一个进入的边
综上，每一个顶点的度必须是偶数

构成欧拉路径的充要条件
图中恰好有两个顶点度为奇数
需要从起点到终点，所以一个出，一个入，就是恰好两个度为奇数顶点

哈密顿回路：
图中恰好经过每个点一次

判断哈密顿回路只有充分条件
若G是顶点数$n \geq 3$的简单图，且G中每一个顶点的度$\geq n/2$，则G为哈密顿回路
若G是顶点数$n \geq 3$的简单图，且对于G中每一对不相邻的两个顶点u和v来说，都有$\deg(u) + \deg(v) \geq n$，则G有哈密顿回路

平面图

2019年5月29日 14:47

若可以在一个平面中画出一张图而边没有任何交叉，则这个图是平面图（边可以是弯曲的）

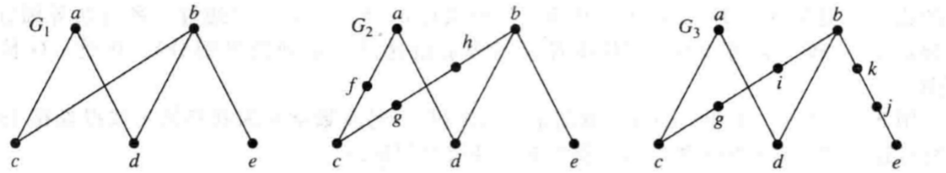
$K_{3,3}$和K_5不是平面图

一个图是非平面图当且仅当它包含于一个同胚于$K_{3,3}$或K_5的子图

Kuratowski’ s Theorem

如果一个图是平面图，则通过删除一条边{u，v}并增加新的顶点w和两条边{u，w}和{w，v}获得的新图也是平面图，且称这两个图是同胚的

eg：



欧拉公式

2019年5月24日 16:46

r：G的平面图表示的面数

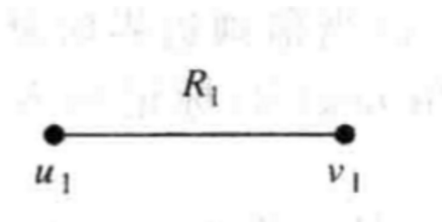
e：G中边的数量

v：G中顶点的数量

G为简单联通平面图，则$r = e - v + 2$

使用数归来证

N = 2时，情况如图



关系易得

假设n = k时，条件成立

N = k+1时，分成两种情况

1. 点的数量没有增加，只是添加了新的边
   则r->r+1,e->e+1,v不变，等式仍成立
2. 点的数量增加了，并且连接上了新的边
   则r不变,e->e+1,v->v+1，等式仍成立

综上，欧拉公式得证

正多面体也满足欧拉公式

每一个面是全等的正多边形

二分图的回路至少是4

推论1：

若G是平面简单联通图，$v \geq 3$，则$e \leq 3v - 6$

证：由于是简单平面联通图，所以一个面至少包含了三条边，即

$2e = \sum \deg(v) \geq 3r$，通过欧拉公式，消去r，即可得到推论中的不等式

即$e \leq 3v - 6$

推论2：

如果G是联通简单平面图，则G中顶点的度不超过5

证：假设G中的任意顶点的度至少为6，则$2e = \sum \deg(v) \geq 6v$

化简得$e \geq 3v$

这个与$e \leq 3v - 6$矛盾，所以原命题正确

推论3：

在一个简单联通平面图G中，若G有e个边，v个顶点

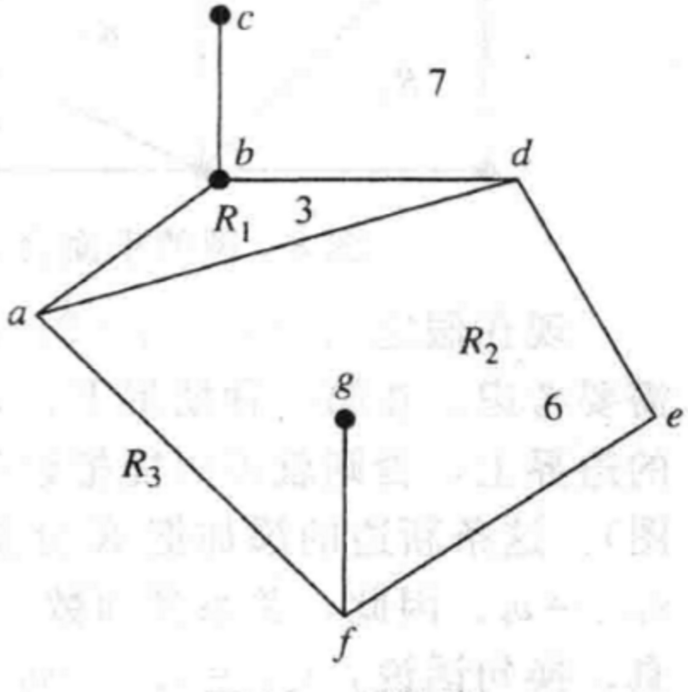
且$v \geq 3$且没有长度为3的回路，则$e \leq 2v - 4$

证：没有长度为3的回路意味着面的度长度至少为4，证明方法和推论1相似，这里略

可以通过推论1和推论3来证明K_5和$K_{3,3}$不是平面图（反证法）

在证明之前，先定义Region of degree，指的是这个面的边界上的边数，当一条边在边界上出现了两次，则其贡献就是2

由于要证明的图是简单图，所以一个面的region of degree肯定至少有三条边



四色定理

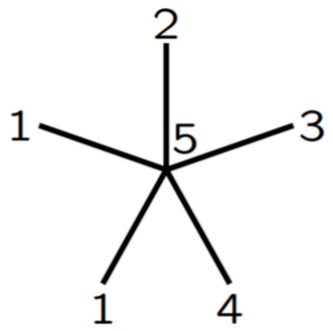
2019年5月24日 17:41

针对于平面图来说
是对顶点染色，其实对边染色也可以
证明五色定理：分类讨论，判断是否是成环，不可能有两个环（这是一个平面图）

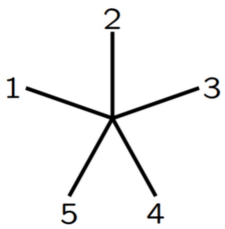
图G的着色数（chromatic number）是着色这个图所需要的最少颜色数，记为$\chi(G)$
四色定理证明的内容是：
只要是一个图是平面图，则这张图最多只需要四种颜色即可完成染色

证明五色定理
N = 1时，易证
假设当n = k时，能用最多五种颜色完成染色
N = k+1时，由推论2（the graph has a vertex of degree 5 or fewer）
去掉这个度≤5的点，由假设，可以用五种颜色完成染色，此时再加上这个点

1. 如果这个点的度小于5，则直接染上下一种颜色即可
2. 如果这个点的度等于5，仍有可能有相同颜色，此时只需染第五种颜色即可



3. 如果这个点的度等于5，且每一个区域颜色都不同，如图



如果这五个区域是分开的，直接变换一个区域，变成相同的颜色，即可完成染色
如果这五个区域不是独立的，由于平面图的性质，只可能有一个环，就是只可能有最多两个区域有联系
此时变换颜色，即可得证

Assignment1

2019年4月19日 11:08

证明$(p \to q) \to ((r \to p) \to (r \to q))$是永真式

$$
\begin{aligned}
&(p \to q) \to ((r \to p) \to (r \to q)) \\
&\equiv \neg(\neg p \vee q) \vee (\neg(\neg r \vee p) \vee (\neg r \vee q)) \quad \text{Useful} \\
&\equiv \neg(\neg p \vee q) \vee ((r \wedge \neg p) \vee (\neg r \vee q)) \quad \text{De Morgan} \\
&\equiv \neg(\neg p \vee q) \vee ((r \vee (\neg r \vee q)) \wedge (\neg p \vee (\neg r \vee q))) \quad \text{Distributive} \\
&\equiv \neg(\neg p \vee q) \vee (((r \vee \neg r) \vee q) \wedge (\neg p \vee (\neg r \vee q))) \quad \text{Associative} \\
&\equiv \neg(\neg p \vee q) \vee ((T \vee q) \wedge (\neg p \vee (\neg r \vee q))) \quad \text{Complement} \\
&\equiv \neg(\neg p \vee q) \vee (T \wedge (\neg p \vee (\neg r \vee q))) \quad \text{Identity} \\
&\equiv \neg(\neg p \vee q) \vee (\neg p \vee (\neg r \vee q)) \quad \text{Identity} \\
&\equiv \neg(\neg p \vee q) \vee ((\neg p \vee q) \vee \neg r) \quad \text{Associative} \\
&\equiv (\neg(\neg p \vee q) \vee (\neg p \vee q)) \vee \neg r \quad \text{Associative} \\
&\equiv T \vee \neg r \quad \text{Complement} \\
&\equiv T \quad \text{Identity.}
\end{aligned}
$$

Thus, it is a tautology.

□

关键点：对于第三步，可以将非r和q看成一个整体

True并上q是True

Q.5 Prove that if $p \wedge q$, $p \to \neg(q \wedge r)$, $s \to r$, then $\neg s$.

Solution:

(1)	$p \wedge q$	Premise
(2)	p	Simplication of (1)
(3)	$p \to \neg(q \wedge r)$	Premise
(4)	$\neg(q \wedge r)$	Modens ponens (2) (3)
(5)	$\neq q \vee \neg r$	De Morgan
(6)	q	Simplication of (1)
(7)	$\neg r$	Disjunctive syllogism (6) (7)
(8)	$s \to r$	Premise
(9)	$\neg s$	Modus tollens (7) (8)

□

关键点在于能熟练的背出对应的逻辑推断依据

Let C(x) be the statement “x has a cat”, let D(x) be the statement “x has a dog” and let F(x) be the statement “x has a ferret.” Express each of these sentences in terms of C(x), D(x), F(x), quantifiers, and logical connectives. Let the domain consist of all students in your class.

(d) No student in your class has a cat, a dog, and a ferret.

(e) For each of the three animals, cats, dogs, and ferrets, there is a student in your class who has this animal as a pet

(d) $\neg\exists x(C(x) \wedge D(x) \wedge F(x))$

(e) $(\exists xC(x)) \wedge (\exists xD(x)) \wedge (\exists xF(x))$

这里需要注意的点在于：没有人，指的是不存在

Let L(x, y) be the statement “x loves y”, where the domain for both x and y consists of all people in the world. Use quantifiers to express each of these statement.

(g) There is exactly one person whom every body loves.

(h) There are exactly two people whom Lynn loves.

(j) There is someone who loves no one besides himself or herself.

(g) $\exists x(\forall yL(y, x) \wedge \forall z((\forall wL(w, z)) \to z = x))$

(d) $\neg\exists x(C(x) \wedge D(x) \wedge F(x))$
(e) $(\exists xC(x)) \wedge (\exists xD(x)) \wedge (\exists xF(x))$
这里需要注意的点在于：没有人，指的是不存在

For each of these arguments, explain which rules of inference are used for each step.
(a) "Each of five roommates, A, B, C, D, and E, has taken a course in discrete mathematics. Every student who has taken a course in discrete mathematics can take a course in algorithms. Therefore, all five roommates can take a course in algorithms next year."
(b) "All movies produced by John Sayles are wonderful. John Sayles produced a movie about coal miners. Therefore, there is a wonderful movie about coal miners."

Solution:
(a) Let r(x) be "r is one of the five roommates listed", let d(x) be "x has taken a course in discrete mathematics", and let a(x) be "x can take a course in algorithms".
We are given premises $\forall x(r(x) \rightarrow d(x))$, $\forall x(d(x) \rightarrow a(x))$, and we want to conclude $\forall x(r(x) \wedge a(x))$.
Step Reason
1. $\forall x(r(x) \rightarrow d(x))$ Hypothesis
2. $r(y) \rightarrow d(y)$ Universal Instantiation using 1.
3. $\forall x(d(x) \rightarrow a(x))$ Hypothesis
4. $d(y) \rightarrow a(y)$ Universal instantiation using 3.
5. $r(y) \rightarrow a(y)$ Hypothetical syllogism using 2. and 4.
6. $\forall x(r(x) \rightarrow a(x))$ Universal generalization using 5.

(b) let s(x) be "x is a movie produced by sayles," let c(x) be "x is a movie about coal miners", and let w(x) be "movie x is wonderful".
we are given premises $\forall x(s(x) \rightarrow w(x))$ and $\exists x(s(x) \wedge c(x))$, and we want to conclude $\exists x(c(x) \wedge w(x))$.
step reason

herself.

(g) $\exists x(\forall yL(y, x) \wedge \forall z((\forall wL(w, z)) \rightarrow z = x))$
(h) $\exists x\exists y(x \neq y \wedge L(Lynn, x) \wedge L(Lynn, y) \wedge (\forall z(L(Lynn, z) \rightarrow (z = x \vee z = y)))$
(j)$\exists x\forall y(L(x, y) \leftrightarrow x = y)$
这道题的关键点在于能正确表达excatly one person的意思

1. $\exists x(s(x) \wedge c(x))$ hypothesis
2. $s(y) \wedge c(y)$ existential instantiation using 1.
3. $s(y)$ simplification using 2.
4. $\forall x(s(x) \rightarrow w(x))$ hypothesis
5. $s(y) \rightarrow w(y)$ universal instantiation using 4.
6. $w(y)$ modus ponens using 3. and 5.
7. $c(y)$ simplification using 2.
8. $w(y) \wedge c(y)$ conjunction using 6 and 7.
9. $\exists x(c(x) \wedge w(x))$ existential generalization using 8.

Assignment 2

2019年4月20日 15:21

Show that log n! is O(n log n)

证明：

也就是证明$\log n! \leq c_1 n \log n$

由于$n! = n \cdot (n-1) \cdot \ldots \cdot 1$
$\leq n \cdot n \cdot \ldots \cdot n$

不等式两边加上对数，即可证明

Show that n log n is O(log n!)

证明：

n！容易被放缩成n^n

但是不能逆推，所以最好是从系数下手

也就是证明$n \log n \leq c_1 \log n!$

将c_1抽调一个2，有$(n!)^2$

将两个n!倒序相乘，也就是证明(n-i)*i<n

所以原命题得证

Assginment 3

2019年4月22日 10:43

Suppose that gcd(a, y) = d1 and gcd(b, y) = d2. Prove that gcd(gcd(a, b), y) = gcd(d1, d2).
方法是假设x=gcd(gcd(a,b),y)，然后根据x|a,x|b,x|y得到x|gcd(d1,d2)
设z=gcd(d1,d2),同理可得z|gcd(gcd(a,b),y)
又x|z,z|x，故x = z，原命题得证

Suppose that gcd(b, a) = 1. Prove that gcd(b + a, b − a) ≤ 2.
反证法，先将gcd(b+a,b-a)用欧拉定理转换成gcd(b-a,2a)
再通过设未知数转换成gcd(b-a,a)
由欧拉定理gcd(b,a)=gcd(b-a,a),gcd(b-a,a)>1，故推得矛盾，原命题成立

Let a and b be positive integers. Show that gcd(a, b) + lcm(a, b) = a + b if and only if a divides b, or b divides a.
对于证明必要性，不妨设a|b，故有gcd(a,b)=a,lcm(a,b)=b，故等式成立
对于证明充分性，设gcd(a,b)=d,由gcd(a,b)*lcm(a,b)=ab,带入原等式中，有d + ab/d = a+b，将原等式看作为关于d的方程，解得d=a，或d=b，故命题成立

Prove that if a and m are positive integer such that gcd(a, m) = 1 then the function
$f : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$
defined by $f(x) = (a \cdot x) \bmod m$ is a bijection.
要证明是bijection，也就是证明one-to-one还有onto
先证明one-to-one，令(a*x)mod m = (a*y)mod m
由gcd(a,m)=1,故存在a mod m的模逆，故有x mod m = y mod m
由x，y∈{0, . . . , m − 1}，故x=y，one-to-one性质证明完毕
现证明onto，假设z是陪域中的任意一个元素，且假设x=bz mod m
则ax ≡ abz ≡ zmodm，根据z的范围，得到ax mod m = z，所以证明onto性质（这里的b是存在性，因为只需要证明存在一个x即可，而z是任意的）

Prove that there are infinitely many primes of the form 4k + 3, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes q1, q2, . . . , qn, and consider the number 4q1q2 · · · qn − 1.]
这道题使用反证法，也就是假设有有限多个4k+3的质数q1,q2...qn
也就是需要寻找一个新的质数，证明其是4k+3的形式

所以得到了$4q_1q_2 \cdots q_n - 1$

1. 如果$4q_1q_2 \cdots q_n - 1$是质数，其形式为$4k+3$，使得与原假设矛盾
2. 如果$4q_1q_2 \cdots q_n - 1$是合数，也就是证明$4q_1q_2 \cdots q_n - 1$包含了$4k+3$的质数，所以要用反证法假设没有对应的质数

   由于架设了没有对应的$4k+3$的质数，所以就只有$4k+1$的质数，$4k+1$的质数不论如何相加都不可能除4余3，所以和原假设矛盾，原命题成立

Assignment 4

2019年5月3日 15:48

Find f(n) when n = 4k, where f satisfies the recurrence relation f(n) = 5f(n/4) + 6n, with f(1) = 1.

方法就是简单的迭代

$$f(n) = 5f(\frac{n}{4}) + 6n$$

$$= 5(5f(\frac{n}{4^2}) + 6\frac{n}{4^1}) + 6n$$

$$= 5^2 f(\frac{n}{4^2}) + 5^1 \cdot 6 \cdot \frac{n}{4^1} + 6n$$

$$= 5^k f(\frac{n}{4^k}) + \sum_{i=1}^{k} 5^{i-1} \cdot 6 \cdot \frac{n}{4^{i-1}}$$

$$= 5^k + 24n\left(\left(\frac{5}{4}\right)^k - 1\right)$$

$$= 25n^{\log_4 5} - 24n$$

Assignment 5

2019年6月1日 14:04

16 points are chosen inside a 5×3 rectangle. Prove that two of these points lie within $\sqrt{2}$ of each other.

这道题是抽屉原理的直接应用

面积是15，但是有16个点

说明至少有一个区域内有两个点

一个单位面积的区域内最长线段为$\sqrt{2}$，说明必然存在一对点，使得点之间的距离小于$\sqrt{2}$

Prove the hockeystick identity

$$\sum_{k=0}^{r}\binom{n+k}{k}=\binom{n+r+1}{r}$$

whenever n and r are positive integers,

(a) using a combinatorial argument

(b) using Pascal's identity.

（a）如果使用二项式定理来证明这道题，就是使用01bit串来进行构造

根据右边的形式，构造r个为0的bit串，n+1个为1的bit串

这（n+r+1）个bit串中选出r个，代表这些（n+r+1）位的bit串中，r个为0的bit串有多少个

左式是根据位数为1的bit串进行分类，$\binom{n+i}{i}$指的是最后一个1出现在第n+i+1位时，该01串出现的可能数，当最后一个1出现在第n+i+1位时，后面全部填充0的到一个完整的字符串，又每一项互不重叠，所以直接算出加和即可

（b）帕斯卡定理如下：

$\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$，指的是杨辉三角中上一层左右两项之和等于下一层

Q.14

(a) Find all solutions of the recurrence relation $a_n =$

(b) Find the solution of the recurrence relation in p

（a）首先列出特征方程$x=2$

所以$a_n=\alpha 2^n$，由于后面有多项式，所以a_n必定含有a_n

所以必定有$p_2n^2+p_1n+p_0=2(p_2(n-1)^2+p_1(n-1)$

合并同类项得$(-p_2-2)n^2+(4p_2-p_1)n+(-2p_2+2p_1$

所以有

$$\begin{cases}-p_2-2=0\\4p_2-p_1=0\\-2p_2+2p_1-p_0=0\end{cases}$$

解得$\begin{cases}p_2=-2\\p_1=-8\\p_0=-12\end{cases}$

所以，$a_n=\alpha 2^n-2n^2-8n-12$

（b）带入a_1，得$\alpha=13$

带入α即可

Q.15 Use generating functions to prove Pascal's i

1) when n and r are positive integers with r < n.

[Hint: Use the identity $(1+x)^n=(1+x)^{n-1}+x(1+$

$$(1+x)^n=\sum_{i=0}^{n}C_n^i x^i$$

$= 2a_{n-1} + 2n^2$.

part (a) with initial condition $a_1 = 4$

Suppose that the relation R is symmetric. Show that R∗ is symmetric.

$= p_2n^2 + p_1n + p_0$

$+ p_0) + 2n^2$（通过迭代系数得到）

$- p_0) = 0$

dentity: C(n,r) = C(n −1 ,r) + C(n−1,r−

$x)^{n-1}$.]

（b）帕斯卡定理如下：

$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ 指的是杨辉三角中上一层左右两项之和等于下一层

将等式中 $\binom{n+1}{1}$ 拆成 $\binom{n+1}{0} + \binom{n}{1}$ 并和第一项相加

$\binom{n}{0} + \binom{n}{1} = \binom{n+1}{1}$, $\binom{n+1}{1} + \binom{n+1}{0} = \binom{n+2}{1}$

$\binom{n+2}{1} + \binom{n+2}{2} = \binom{n+3}{2}$ ……从而完成迭代

变成右式

$$(1+x)^n = \sum_{i=0}^{n} C_n^i x^i$$

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

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

$$= \sum_{i=1}^{n} C_{n-1}^{i-1} x^i$$

所以 $\sum_{i=0}^{n} C_n^i x^i = \sum_{i=0}^{n-1} C_{n-1}^i x^i + \sum_{i=1}^{n} C_{n-1}^{i-1} x^i$

所以 $1 + (\sum_{r=1}^{n-1} C_n^r x^r) + x^n = 1 + \left(\sum_{r=1}^{n-1} (C_{n-1}^r + C_{n-1}^{r-1}) x\right.$

所以得到C(n,r) = C(n −1 ,r) + C(n−1,r−1)

需要注意的是：使用聚合函数时要化成相同的相加项，

$^{r}) + x^{n}$

才能变成这种形式

Assignment 6

2019年6月1日 15:48

Q.4 Let $n \geq 5$ be an integer. Consider the graph G_n whose vertices are the sets $\{a, b\}$, where $a, b \in \{1, \ldots, n\}$ and $a \neq b$, and whose adjacency rule is *disjointness*, that is, $\{a, b\}$ is adjacent to $\{a', b'\}$ whenever $\{a, b\} \cap \{a', b'\} = \emptyset$.

(a) Draw G_5.

(b) Find the degree of each vertex in G_n.

解: