# 内容

# 1 基础:逻辑和证明

## 关键条款和结果

**条款**

**命题:**是真或假的陈述

**命题变量(proposition** variable):表示命题**的变量**

**真值:**真或假

**¬*p* (p的否定):**真值与p的真值相反的命题

**逻辑运算符(Logical operator):**用于组合命题的运算**符**

**复合命题:**用逻辑运算符组合命题而构成**的命题**

**真值表:**显示命题所有可能真值的表

***P*∨*q*(P与*q*的析取):**命题“P或q”，当且仅当P与q中至少有一个为真时为真

**$p \wedge q$ (p 与 q 的合取):**命题“p 与 q”，

当且仅当 p 和 q 都是真 **$p \oplus q$(不等于或等于 p 和 q):**命题“p *XOR* q，”

当 p 和 q 正好有一个为真 **$p \rightarrow q$ (p 暗含 q):**命题“如果 p，则 q”，当且仅当 p 为真且 q 为假时，哪个为真

**$p \rightarrow q$ 的逆命题:**条件语句 $q \rightarrow p$ **的逆命题:**条件语句 $q \rightarrow p$

**$p \rightarrow q$ 的反命题:**条件语句 $\neg p \rightarrow \neg q$ **$p \leftrightarrow q$(双条件):**命题“p 当且仅当 q”，当且仅当 p 和 q 具有相同的真值时为真

**Bit:**要么 0，要么 1

**布尔变量**(Boolean variable):值为 0 或 1 **位的变量。操作**(operation):对一个或多个比特**的操作**

**位串(Bit string):**位的列表

**位操作(Bitwise** operations):位字符串上的操作，对一个字符串中的每个比特和另一个字符串中对应的比特**进行操作**

**逻辑门(Logic gate):**一种逻辑元件，它对一个或多个位进行逻辑运算，产生一个输出位

**逻辑电路:**由产生一个或多个输出位的逻辑门组成的开关电路

**重言式:**总是真命题的复合命题**矛盾:**总是假命题的复合命题

**偶然性:一个**时而真时而假的复合命题

**一致的复合命题:**对这些复合命题有一个赋值给变量的真值，使所有这些命题都为真

**可满足的复合命题:**一个复合命题，对其变量有真值赋值，使其为真

**逻辑等价复合命题:**总是具有相同真值的复合命题

**谓词(Predicate):**句子中把属性归给主语的部分

**命题函数(**proposition function):一个包含一个或多个变量的语句，当其中的每个变量被赋值或被量词绑定时，它就成为**一个命题**

**论域(或论域):**命题函数中的变量可能接受的值

**$\exists x P(x)$ (P(x)的存在量词):**当且仅当域中存在一个 x 使 P(x)为真时为真的命题

**$\forall x P(x)$ (P(x)的普遍量化):**当且仅当 P(x)对域中的每个 x 都为真时为真的命题

**逻辑等价表达式(logical** equivalent expressions):无论使用哪个命题函数和值域，都具有相同真值**的表达式**

**自由变量(Free variable):**不受命题函数约束的变量

**绑定变量(Bound** variable):被量化**的变量**

**量词作用域(Scope** of a quantifier):量词绑定其变量的语句部分

**参数(Argument):**语句的序列

**论元形式(Argument form):**包含命题变量的复合命题序列

**前提:**一个陈述，在一个论证中，或论证形式，除了最后一个

**结论:**论证或论证形式中的最后陈述

**有效论证形式:**包含命题变量的复合命题序列，其中所有前提的真值都隐含结论的真**值**

**有效论证(Valid** argument):具有有效论证形式的论证

**推理规则:**一种有效的论据形式，可用于证明论据是有效**的**

**谬论(Fallacy):**一个无效的论证形式，经常被错误地用作推理规则(或者有时，更一般地说，是一个不正确的论证)

**循环推理或求问题:一种**推理，其中一个或多个步骤是基于被证明的陈述的真实性

**定理:**可以证明为真的数学断言

**猜想:**被提出为真，但尚未被证明的数学断言

**证明:**证明一个定理是正确**的**

**公理(Axiom):一种**被假定为真并且可以用作证明定理的基础的陈述

**引理(Lemma):**用来证明其他定理的定理

**推论:**作为一个刚刚被证明的定理的结果，可以被证明的命题

**空洞证明:**基于 p 为假的事实，证明 $p \rightarrow q$ 为真

**琐碎证明:**基于 q 为真这一事实，证明 $p \rightarrow q$ 为真

**直接证明:**一个 $p \rightarrow q$ 为真的证明，通过证明当 p 为真时 q 必须为真

**逆反证明:通过**证明当 q 为假时，p 一定为假，从而证明 $p \rightarrow q$ 为真

**反证法:**基于条件语句 $\neg p \rightarrow q$ 的真值来证明 p 为真，其中 q 是一个矛盾体

**穷举证明:**通过检查所有可能情况的列表来建立一个结果的证明

**按案例证明(Proof by cases):**分解成单独的案例的证明，这些案例涵盖了所有的可能性

**无损失通用性:一**种证明中的假设，通过减少证明中考虑的情况数量来证明定理

**反例:**使 P (x)为假的元素 x

**构造性存在证明:**证明具有特定性质的元素存在，明确地找到这样的元素

**非构造性存在证明:**证明具有指定性质的元素存在，但没有显式找到这样的元素

**有理数:**可以表示为两个整数 p 和 q 之比，使 q =0 的一个数

**唯一性证明(唯一性**证明):证明只有一个元素满足指定的性质

## 结果

在 1.3 节的表 6、7 和 8 中给出的逻辑等价。

关于量词的德·摩根定律。

命题演算的推理规则。量化语句的推理规则。

## 审查问题

**1. a)**定义一个命题的否定。

**b)**“这是一门无聊的课程”的否定是什么?

**2. a)**定义(使用真值表)命题 p 和 q 的析取、合取、排他或、条件式和双条件式。

**b)“我**今晚要去看电影”和“我要完成离散数学作业”这两个命题的析取、合取、排他或、条件或双条件是什么?

**3.a)**用英语描述条件语句 p→q至少五种不同的写法。

**b)**定义 econverseandcontrapositiveofconditional 语句。

**c)**陈述条件句“如果明天是晴天，那么我将去树林里散步”的反命题和逆反命题。

**4. a)**两个命题在逻辑上等价意味着什么?

**b)**描述显示两个复合命题在逻辑上等价的不同方法。**c)**至少用两种不同的方式表明复合命题¬p∨(r→¬q)和¬p∨(q∨)r是等价的。

**5.** *(取决于 1.3 节中设置的练习)*

**a)**给定一个真值表，说明如何用析取范式构造一个由该真值表构造的复合命题。

**b)**解释为什么(a)部分显示算子∧、∨和¬是功能完备的。

**c)**是否存在这样一个算子，使得仅包含这个算子的集合是功能完备的?

**6.** 谓词 P (x)的全称量词和存在量词是什么?它们的否定是什么?

**7. a)**量化∃ x∀ yP (x, y)和∀ y∃ xP (x, y)之间有什么区别?其中 P (x, y)是谓词?

**b)**给出一个谓词 P (x, y)的例子，使得∃ x∀ yP (x, y)和∀ y∃ xP (x, y)有不同的真值。

**8.** 描述命题逻辑中的有效论证是什么意思，并表明这个论证“如果地球是 flat，那么你可以航行离开地球的边缘”，“你不能航行离开地球的边缘”，因此，“地球不是平的”是一个有效论证。

**9.** 用推理规则证明，如果前提“所有的斑马都有条纹”和“马克是斑马”为真，那么结论“马克有条纹”为真。

**10. a)**描述条件语句 p→q 的直接证明、对位证明和矛盾证明的含义。

**b)**给出一个直接证明，一个逆反命题证明和一个矛盾证明:“如果 n是偶数，那么 n+4是偶数。”

**11. a)**描述一种方法来证明双条件 p□ q。

**b)**证明这个语句:“整数 3n + 2是奇时且仅当整数 9n + 5是偶数时，其中 n是整数。”

**12.** 要证明语句 p1、p2、p3 和 p4 是等价的，是否足以证明条件语句 p→p、4 p→2p、3 p1→pare1 有效?2 如果不能，提供另一组条件语句，可以用来证明这四个语句是等价的。

**13. a)**假设一个形式为∀ xP (x)的陈述是假的。如何证明这一点?

**b)**证明“对于每一个正整数 n,n2≥2n”的说法是错误的。

**14.** 构造性存在证明和非构造性存在证明的区别是什么?分别举一个例子。**15。** 证明存在唯一性的要素是什么

元素 x使 P (x)，其中 P (x)是一个命题函数?

**16.** 解释如何用案例证明来证明一个关于绝对值的结果，例如对于所有实数 x和 y， |xy| = |x||y|。

# 2/基本结构:集合、函数、序列、和和矩阵

## 关键术语和结果

**条款**

**集合(Set):**不同对象的集合

**公理(Axiom):**理论的基本假设

**悖论:**逻辑上的不一致

**元素，集合中的一员:集合**中的一个对象

**花名册方法(Roster method):**通过列出集合的元素来描述集合的方法

**集合构造法:**通过陈述来描述集合的表示法

一个元素的属性必须是成员∅ **(空集，空集):**没有成员的集合
**泛集:**包含所考虑的所有对象的集合

**文氏图:**一个集合或集合 ***S*** = ***T*** 的图形表示**(集合相等):**S 和 T具有相同的元素

***S*** ⊆ ***T*** **(*S*是 T的子集):**S 的每个元素也是 T的元素

***S*** ⊂ ***T*** **(*S*是 T的真子集):**S 是 T的子集，S 且=

**有限集:一个**有 n个元素的集合，其中 n是一个非负整数

**无限**集合:不有限的集合

|***S***| **(S 的基数):*SP*(S)**中的元素个数***(S*的幂集*)*:**S 的所有子集的集合

A∪B **(*A*与 *B*的并集):**包含在 中 A与 B中至少有一个的元素的集合

A∩B **(*A*和 *B*的交集):**包含在 A和 B中同时存在的那些元素的集合。

A− B **(*A*与 *B*之差):**包含在 A中但不在 B中的那些元素的集合

**A‾(A的补集):**全称集合中不属于 A的那些元素的集合

A⊕B **(*A*和 *B*的对称差):**包含 A和 B中恰好有一个中的那些元素的集合

**隶属度表(Membership** table):显示集合中元素的隶属度**的表**

**从 *A*到 *B*的函数:将** B的一个元素精确地赋值给 A的每个元素

***f*的定义域:**集合 A，其中 f是一个从 A到 B的函数 ***f*的上域:**集合 B，其中 f是一个从 A到 B的函数 ***B*是 *A*在 *f*下的像:**B = f(A)

**A是 b在 f下*的原像*:**f(A) = b

***f*的值域:*f*的**像的集合

**在函数上，surection:一个**从 a到 B的函数，使得 B的每个元素都是 a中某个元素的像

**一对一函数，注入:**一种函数，使其定义域内元素的图像是不同**的**

**一对一对应，双射:一种**同时是一对一和映上的函数

***f*的逆:**反转 f给出的对应关系的函数(当 f是双射时)

***F*∘ *g*(F和 *g*的组成):**将 F(g(x))分配到 x的功能

⌊ *x*⌋ **(地板功能):**不超过 x的最大整数

⌈ *x*⌉ **(取顶函数):**大于等于 x的最小整数

**偏函数(Partial function):**给定义域子集中的每个元素赋值一个上域中**唯一的元素**

**序列(Sequence):**定义域上是整数集合的一个子集的函数

**几何级数:**形式为 a,ar, ar 2，…，其中 a和 r都是实数

**等差数列:**a、a + d、a + 2d、……形式的数列。，其中 a和 d为实数**串:**有限数列

**空字符串(Empty** string):长度为 0的字符串

**递归关系:**用序列的一个或多个前一项 n来表示序列的第 n项 a，对于所有大于某一特定整数 n的整数

”∏Nni = 1ai:总和 a1 + a2+ • • • + an∏I = 1ai:乘积 a1a2 • • • an

**基数:**两个集合 A和 B具有相同的基数 if

a和 B之间存在一一对应的**可数集合:**一个集合要么是有限的，要么可以放在其中

**不可数集合(Uncountable** set):不可**数的集合**

ℵ 0 **(aleph null):**可数集合的基数 c:**实数集合的基数**

**康托对角化论证(Cantor diagonalization argument):**一种证明技术，用来证明实数集是不可数**的**

**可计算函数(Computable** function):一种函数，某种编程语言的计算机程序可以为它找到值

**不可计算函数(Uncomputable** function):一种程序设计语言中没有计算机程序为其寻找值**的函数**

**连续统假设:**不存在这样的集合 A:ℵ 0 < |A| < c**矩阵:**一个矩形数组

**矩阵加法:**见第 178 页

**矩阵乘法:**见第 179 页

**I**n **(n阶单位矩阵):*n*×** n的矩阵，其对角线上的元素等于 1，其他地方为 0

**A**t **(transpose ofA):通过**行列**互换由 ma得到的矩阵**

**对称矩阵:**如果一个矩阵等于它的转置，那么这个矩阵就是对称**的**

**0 - 1矩阵:**一个矩阵，每个元素要么等于 0，要么等于 1

**A∨B (A与 B的连接):**见第 181 页

**A∧B (A与 B的交点):**见第 181 页 **A⊙B (A与 B的布尔和):**见

**结果**

2.2节表 1中给出的集合恒等式 2.4节表 2中的求和公式有理数的集合是可数的。实数的集合是不可数的。

## 审查问题

**1.** 解释一个集合是另一个集合的子集意味着什么。如何证明一个集合是另一个集合的子集?

**2.** 什么是空集?表明空集是每个集合的子集。

**3.a)**定义|S|，集合 S的基数 **b)**给出|a∪b|的公式，其中 a和 b为集合。

**4. a)**定义一个集合 S的幂集。

**b)**什么时候空集在集合 S的幂集中?

**c)一个**有 n个元素的集合 S的幂集有多少个元素?

**5. a)**定义两个集合的并、交、差和对称差。

**b)**正整数集合和奇整数集合的并、交、差和对称差是什么?

**6. a)**解释两个集合相等的含义。

**b)**尽可能多地描述表明两个集合相等的方法。

**c)**以至少两种不同的方式展示集合

$A - (B \cap C)$ and $(A - B) \cup (A - C)$ are equal.

**7.** 解释逻辑等价和集合恒等式之间的关系。

**8. a)**定义函数的定义域、上域和值域。

**b)**设 f(n)为从整数集合到整数集合的函数，使 f(n) = n2+1。这个函数的定义域、上定义域和值域是什么？

**9. a)**定义一个函数从正整数集合到正整数集合是一对一的意味着什么。

**b)**定义一个函数从正整数集合到正整数集合是映上的意义。

**c)**给出一个从正整数集合到正整数集合的函数的例子，该函数既是一对一的也是映上的。

**d)**给出一个从正整数集合到正整数集合的函数的例子，这个正整数集合是一对一的，但不是映上的。

**e)**给出一个从正整数集合到不是一对一但是映上的正整数集合的函数的例子。

**f)**给出一个从正整数集合到既不是一对一也不是映上的正整数集合的函数的例子。

**10. a)**定义函数的逆函数。

**b)**函数什么时候有逆函数？

**c)**从整数集合到整数集合的函数 f (n) = 10− n是否有逆?如果有，它是什么？

**11. a)**定义从实数集合到整数集合的下限和上限函数。

**b)**对于哪个实数 x，⌊ x⌋ =⌈ x⌉ 是正确的?

**12.** 猜想一个以 8、14、32、86、248 开始的数列的项的公式，并找出数列的下三项。

**13.** 假设 $_n$n = 1,2， .. ..时，a= $a_{n-1}$ − 5为 a找一个 $_n$ 公式。

**14.** 几何级数的项之和是多少

$$a + ar + \cdots + ar^n \text{ when } r \neq 1$$

**15.** 表明奇数的集合是可数的。

**16.** 举一个不可数集合的例子。

**17.** 定义两个矩阵 A和 **b的乘积，这个乘积什么时候定义?**

**18.** 证明矩阵乘法是不可交换的。

# 3 /算法

## 关键术语和结果

---

**条款**

**算法(Algorithm):**执行计算或解决问题的精确指令的有限序列

**搜索算法(Searching algorithm):在**列表中定位一个元素的问题

**线性查找算法(Linear search** algorithm):一个接一个地查找列表元素**的过程**

**二分查找算法(Binary search algorithm):**通过连续地将一个列表一分为二来查找一个有序列表的过程

**排序:将**列表中的元素按规定的顺序重新**排序**

***f*(*x*)是** O(***g*(*x*)):**|f (x)|≤C|g(x)|对于所有 x > k对于某些常数 C和 k

**根据关系 *f*(*x*)是** O(***g*(*x*)):对于**|f(x)|≤C|g(x)|每当 x >k*f*(*x*)是 !(*g*(*x*)):**对于所有的 x |f (x)|≥**C|g(x)|对于某些正常数 C和 k**

***f*(*x*)是** “(*g*(*x*)):f(x)既是 O(g(x))又是!(g(x))**ti**

**Me复杂度(Me complexity):**算法解决一个问题所需的时间量

**空间复杂度(Space** complexity):一个算法解决一个问题所需的计算机内存空间

**最坏情况时间复杂度(Worst-case** time complexity):算法解决给定大小的问题所需要的最大时间量

平均时间复杂度(average-case time complexity):一个算法解决给定规模的问题所需的平均时间

**算法范式(Algorithmic paradigm):一种**基于特定概念构造算法的通用方法

**蛮力(Brute force)**:基于从问题的陈述和定义中以一种朴素的方式构造算法来解决问题的算法范式

**贪心算法**(Greedy algorithm):一种算法，在每一步都根据某些指定条件做出最佳选择

**可处理问题**(problem):有一个最坏情况下的多项式时间算法可以解决的问题

**难解**问题:没有最坏情况多项式时间算法可以解决的问题

**可解决问题**(solved problem):可以用算法解决**的问题**

**不可解决的问题(Unsolvable problem):**算法无法解决的问题

**结果**

**线性和二分查找算法**:(在 3.1 节给出)**冒泡**排序:一种使用传递的排序，如果顺序错误，则交换连续元素

**插入排序:**当列表的第 j− 1个元素已经排好序时，在第 j步将第 j个元素插入到列表中的正确位置的排序

线性搜索在最坏情况下的时间复杂度为 O(n)。二分查找的最坏情况时间复杂度为 O(log n)。冒泡排序和插入排序的最坏情况时间复杂度为 O(n2)。

o (log n) !是 O(n log n)。

如果 $f_1(x)$ = O ($g_1(x)$)和 $f_2(x)$是 O ($g_2(x)$),然后($f_1$ + $f_2$) (x)

是 O (max (g1(x) g2(x)))和(f1 f2)(x)是 O ((g1g2(x))。如果 $a_1$0a，…， a是 $_n$ a=0的实数，$_n$ 则 axn +$_n$a(n)n− 1x。

$_{n-1}$+ · · • + a1x +$a_0$ 是"(xn)，因此 O(n)和

# 审查问题

**1. a)**定义*算法*这个术语。

**b)**描述算法有哪些不同的方式?

**c)解决问题的**算法和解决这个问题的计算机程序有什么区别?

**2. a)**用英语描述一个从 n 个整数的列表中找出最大整数的算法。

**b)**用伪代码表示这个算法。

**c)**算法使用了多少次比较?

**3.a)**陈述 f (n)是 O(g(n))这一事实的定义，其中 f (n)和 g(n)是从正整数集合到实数集合的函数。

**b)**直接用 f (n)是 O(g(n))这一事实的定义来证明或证伪 n2+18n + 107 是

O (n3)。

**c)**直接利用 f (n)是 O(g(n))这一事实的定义来证明或反驳 n3 是 O(n2+18n + 107)。

**7. a)**描述在整数列表中查找整数的线性查找和二分查找算法。

**b)**比较这两种算法在最坏情况下的时间复杂度。

**c)**是否其中一种算法总是比另一种算法快(以比较衡量)?**8**

。**a)**描述冒泡排序算法。

**b)**使用冒泡排序算法对列表 5、2、4、

1、3。

**c)**对冒泡排序使用的比较次数给出一个大 0 估计。

**9. a)**描述插入排序算法。

**4.** 将这些函数列出来，使每个函数都是列表中下一个函数的大 0√(log n)3，n/1000000，n，100n + 101，3n，n!2nn2。

**5. a)如果一个函数**是不同项的和，其中每一项是几个函数的乘积，那么你如何得到一个大 0 估计?

**b)**给出函数 f (n) =的大 0 估计

$(n! + 1)(2^n + 1) + (n^{n-2} + 8n^{n-3})(n^3 + 2^n)$. For the function $g$ in your estimate $f(x)$ is $O(g(x))$ use a

最小可能阶的简单函数。

**6. a)**定义一个在 n 个整数列表中找到最小整数的算法的最坏情况时间复杂度、平均情况时间复杂度和最佳情况时间复杂度(根据比较)的含义。

**b)**通过将每个整数与目前找到的最小整数进行比较，在 n 个整数的列表中找到最小整数的算法的最坏情况、平均情况和最佳情况时间复杂度是多少?

**b)**使用插入排序算法对列表 2、5、1、4、3 进行排序。

**c)对** 插入排序使用的比较次数给出一个大 o 估计。

**10. a)**解释贪婪算法的概念。

**b)**提供一个产生最优解的贪婪算法的例子，并解释它产生最优解的原因。

**c)**提供一个贪婪算法的例子，该算法并不总是产生最优解，并解释它为什么不能产生最优解。

**11.** 定义什么是可处理的问题，什么是可解决的问题。

# 关键术语和结果

## 条款

**A | b(A除 b):**存在一个整数 c，使 b = ac A**和** b**求模 m同余:**m**除** A− b**模算术:**对整数 m取模≥2的算术**素数:**大于 1的整数有两个正整数约数

**合数:**大于 1的非素数的整数。
**Mersenneprime:**aprimeofthe form2p− 1，而 p 是素数

**Gcd(a, b) (a和 b的最大公约数):**同时除 a和 b的最大整数

**相对质数**整数:使 gcd(a, b) = 1 的整数 a 和 b

**成对相对质数整数(Pairwise relative prime** integers):一组整数，其性质是每一对整数都是相对质数

**Lcm(a, b) (a和 b的** 最小公倍数):能被 a和 b整除的最小正整数

**A取 b模:**整数 A被正整数 b除的余数

**A≡b(对 m取模)(A与 b对 m取模相等):**A− b能被 m整除

**N = (**aak- 1 k⋯Aa1)0:b n的 b进制**表示二进制表示:整数的 2进制**表示八进制表示:**整数的 8进制**表示

**十六进制表示法(Hexadecimal representation):**整数的 16进制表示法

**a和 b的整数系数线性组合:**形式为 sa+ tb的表达式，其中 s和 t为整数

**Bézout a和 b的系数:**整数 s和 t使 **Bézout恒等式** sa+ tb = gcd(a, b)保持 **a对 m取模的逆:一个**使 *aa*≡1**(对 m取模)的整数 a**

**linear同余:**形式 ax≡b (mod m)的同余，其中 x 是一个整数变量

**以 b为底的伪素数:**一个复合整数 n，使 bn- 1≡1 **(mod n)**

**卡迈克尔数:**一个合数 n，使得 n是以 b为底数的所有正整数 b的伪素数，且 gcd(b, n) = 1

**一个素数 p的本原根:**z中的 p一个整数 r，**使得所有不能被 p整除的整数都能对 p的 r次方取模**

**a对以 r为底对 p取模**的离散对数:0≤e≤p− 1的整数 e，使得 re≡a(mod p)加密**:使消息秘密的过程**

**解密(Decryption):**将秘密消息还原为原始形式的过程

**加密密钥(Encryption key):**确定要使用加密函数族中的哪一个的值

**移位密码(Shift** cipher):将明文字母 p加密为(p + k)对整数 k**的 m取模的密码**

**仿射密码(Affine** cipher):用 gcd(a, 26) = 1字符密码(character cipher)将明文字母 p作为(ap + b) **mod m对整数 a和 b**进行加密的密码

**分组密码(Block** cipher):对固定大小的字符分组进行加密**的密码**

**密码分析(cryptanalysis):在不知道加密方法的**情况下，或者只知道加密方法，但不知道密钥的情况下，从密文中恢复明文的过程

**密码系统:**一个五元组(P, C, K, E, D)其中 P是明文消息集合，C是密文消息集合，K是密钥集合，E是加密函数集合，D是解密函数集合

**私钥加密:**加密密钥和解密密钥都必须保密**的加密**

**公钥加密:**加密密钥是公开知识，但解密密钥要保密**的加密**

**RSA密码系统:**P和 C都是 $\mathbf{Z}_{26}$的密码系统，K是对的集合 K = (n, e)其中 n = pq其中 P和 q是大素数，e是正整数，$e_k$ (P) = pemod **n**, D(C) = cdk mod n其中 D**是** e模(P− 1)的倒数(q− 1)

**密钥交换协议(Key exchange protocol):**用于双方生成共享密钥的协议

**数字签名:一**种接收方可以用来确定消息的所谓发送方实际上发送了消息的方法

## 结果

**除法算法:**设 a和 d为整数，其中 d为正。那么就有 0≤r < d这样唯一的整数 qand r

that $a = dq + r$.

设 b是一个大于 1的整数。那么如果 n是一个 pos-

式整数，则可以以唯一的形式表示

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

求整数以 b为基展开的算法the base b expan

(参见 4.2 节中的算法 1)

加法和乘法的传统算法模幂算法(参见《**欧几里得算法:**求最大公约数》中的算法 5 **Bézout 的定理:**如果 a 和 b 是正整数，那么整数 gcd(a, b)是 a和 b超过指定数 n的线性组合，在 4.3节中描述，可以唯一地写成质数的乘积，其中质数因子按大小递增的顺序排列。

通过连续使用除法算法(参见 4.3节中的算法 1)

**埃拉托色尼筛:**求小于 n的所有素数的程序 **算术基本定理:**每一个正整数如果 a 和 b 是正整数，那么 ab = gcd(a, b) • lcm(a, b)。如果 m是一个正整数，并且 gcd(a, m) = 1，那么 a有一个模 m的逆。

**中国剩余定理:**线性同余系统**费马小定理:**如果 p是素数和 a是那个

对两两相对素数求模对这些模的乘积求模有唯一解。

$$a^{p-1} \equiv 1 \pmod{p}.$$

## 审查问题

**1.** 找到 210 **div** 17 和 210 **mod** 17。

**2. a)**定义 a 和 b 对 7 取余的意义。

**b)**哪些整数对-11、- 8、- 7、- 1、0、3 和 17 是同余模 7?

**c)**表示如果 a 和 b 是同余模 7，那么 10a + 13 和− 4b + 20 也是同余模 7。

**3.**证明如果 a≡b (mod m)， c≡d (mod m)，那么 a + c≡b + d (mod m)。

**4.** 描述一个将整数的十进制(以 10 为基数)展开式转换为十六进制展开式的过程。

**5.** 将$(1101\ 1001\ 0101\ 1011)_2$转换为八进制和十六进制表示。

**6.** 将$(7206)_8$和$(A0EB)_{16}$转换为二进制表示。

**7.** 陈述算术基本定理。

**8. a)**描述一个求整数的质因数分解的过程。

**b)**用这个方法求 80,707 的质因数分解。

**9. a)**定义两个整数的最大公约数。

**b)**至少描述三种找到两个整数最大公约数的方法。每种方法在什么情况下最有效?

**c)**找出 1,234,567 和 7,654,321 的最大公约数。

**d)**求 2335577911 和 2937557313 的最大公约数。

**10. a)**如何找到两个整数的线性组合(系数为整数)，使其等于它们的最大公约数?

**b)**将 gcd(84,119)表示为 84 和 119 的线性组合。

**11. a) a** 是模 m 的逆是什么意思?

**b)**当 m 是一个正整数且 gcd(a, m) = 1 时，如何求模 m 的逆?

**c)**求模 19 的 7 的逆。

**12. a)**当 gcd(a, m) = 1 时，如何用模 m 的逆解全等性 ax≡b (mod m) ?**b)**求解线性同余性 7x≡13 (mod 19)。

**13. a)**陈述中国剩余定理。

**b)**求出系统 x≡1 (mod 4)、x≡2 (mod 5)和 x≡3 (mod 7)的解。

**14.** 假设 $2^{n-1}\equiv 1 \pmod n$， n 一定是素数吗?

**15.** 用费马小定理求 $9200$ **模** 19。

**16.** 解释如何找到 10 位 ISBN 的校验位。

**17.** 使用密钥 k = 13 的 shift 密码加密消息 APPLES AND ORANGES。

**18. a)**公钥密码系统和私钥密码系统的区别是什么?

**b)**解释为什么使用移位密码是一种私钥系统。

**c)**解释为什么 RSA 密码系统是一个公钥系统。

**19.** 解释在 RSA 密码系统中如何进行加密和解密。

**20.**描述两方如何使用 Diffie-Hellman 密钥交换协议共享密钥。

# 5 / InductionandRecursion

## 关键术语和结果

**条款**

**序列(Sequence):**定义域是整数集合的子集的函数

**几何级数:**形式 a,ar,ar 2，…的序列。，其中 a 和 r 是实数

**等差数列:**a、a + d、a + 2d 等形式的数列。，其中 a 和 d 是实数

**数学归纳法原理:**如果 P(1)为真，∀ k[P (k)→P (k + 1)]为真，则陈述∀ n P (n)为真。

**基步骤:**∀ nP (n)的数学归纳法证明中的 P(1)的证明

**归纳步骤:**在∀ nP 的数学归纳法证明中，对所有正整数 k 证明 P (k)→P (k + 1)

**强归纳:**∀ nP(n)为真若 P(1)为真且
∀ k[(P(1)∧・・・∧P(k))→P(k ＋ 1)]为真**良序性质:**每一个非负整数的非空集合都有一个最小元素。

**函数的递归定义:一个函数的**定义，指定一个初始值集，以及从它在较小整数上的值获得这个函数在整数上的值的规则

**集合的递归**定义:集合的定义，指定了集合中元素的初始集合，以及从集合中获取其他元素的规则

**结构归纳:一种**证明关于递归定义集合的结果的技术

**递归算法**(Recursive algorithm):一种算法，通过用更小的输入将一个问题归为同一个问题

**归并**排序(Merge sort):一种排序算法，通过将列表分成两部分，分别对两个结果列表进行排序，并将结果合并成一个排序列表

**迭代(Iteration):一种**基于循环中重复使用操作的过程

**程序正确性:**验证一个过程总是产生正确的结果

**循环不变式(Loop invariant):在循环的**每次遍历过程中都保持 true 的属性

**初始断言(Initial assertion):**指定程序输入值的属性的语句

**最终断言(Final assertion):在**程序正确运行的情况下，指定输出值应该具有的属性的语句

## 审查问题

**1. a)**你能利用数学归纳法的原理找到一个序列前 n项和的公式吗?

**b)**能不能用数学归纳法的原理来判断给定的一个序列前 n项和的公式是否正确?

**c)**找到前 n个偶数正整数和的公式，并用数学归纳法进行证明。

**2. a)**哪个正整数 n是 11n ＋ 17≤$_{2n}$?

**b)**用数学归纳法证明你在(a)部分所做的猜想。

**3.a)**使用 5分和 9分的邮票可以生成哪些数量的邮资?

**b)**用数学归纳法证明你的猜想。

**c)**用强归纳法证明你做出的猜想。

**d)**找到一个与你在(b)和(c)中给出的猜想不同的证明。

**4.**给出两个使用强归纳法的不同证明例子。

**5. a)**陈述正整数集合的良序性质。

**b)**利用这个性质来说明每个大于 1的正整数都可以写成质数的乘积。

**6. a)**解释一个函数 f从正整数集合到实数集合，如果它是通过指定 f(1)和从 f (n－ 1)找到 f (n)的规则递归定义的，为什么它是有定义的。

**b)**提供函数 f(n) =的递归定义

(n ＋ 1)!。

**7. a)**给出斐波那契数的递归定义。

**b)**证明当 n≥3时，$f_n > \alpha^{n-2}$，其中 $_n$ f为斐波那契数列的第 n√项，且 α =

$(1 + 5)/\overline{2}$。

**8. a)**解释为什么一个序列是 $_n$ 定义良好的，如果它是通过指定 a1 和 $_{a2}$ 递归定义的，以及一个从 $a_n$ a，⋯$_{12}$，$a_{n-1}$ for n = 3,4,5，. . . .

**b)**求 $a_n$ f a=$_1$ 1,$a_2$ = 2, a=$_n$ 的值

$$a_{n-1} + a_{n-2} + \cdots + a_1, \text{for } n = 3, 4, 5, \ldots .$$

**9.** 给出两个例子，说明如何为不同的元素和操作符集递归地定义格式良好的公式。

**10. a)**给出字符串长度的递归定义。

**b)**利用第(a)部分的递归定义和结构归纳法证明 l(xy) = l(x) ＋ l(y)。

**11. a)**什么是递归算法?

**b)**描述一个计算序列中 n个数字之和的递归算法。

**12.** 描述计算两个正整数的最大公约数的递归算法。

**13. a)**描述归并排序算法。

**b)**使用归并排序算法，将列表 4、10、1、5、3、8、7、2、6、9按递增顺序排列。

**c)**对归并排序使用的比较次数给出一个大 o估计。

**14. a)**测试一个计算机程序，看它是否对某些输入值产生正确的输出，是否验证该程序总是产生正确的输出?

**b)**显示计算机程序在初始断言和最终断言方面部分正确，是否证明该程序总是产生正确的输出?如果不是，还需要什么?

**15.** 你可以使用什么技术来证明一个很长的计算机程序在初始断言和最终断言方面是部分正确的?

**16.** 什么是循环不变式?如何使用循环不变量?

# 6 /计数

## 关键术语和结果

### 条款

**组合学:对象**排列的研究枚举:对象排列的计数**树图:由一个根，**离开根的分支，和其他分支离开分支的一些端点组成的图

**permutation:集合** 元素的有序排列 ***r*-permutation:**集合 **P(*n,r*)*的有序排列* *r-permutation:***n 个元素集合的 r-permutation 的个数 r-combination:**无序选择**集合 C(n,r)的 r 个元素的个数!r-组合的 n 个元素集合 n 的 r-组合

**二项式系数:**也是 r 组合的个数 r

n 个元素的集合的个数

**组合证明:一种**使用计数参数的证明

而不是用代数方法来证明**帕斯卡三角形的结果:**二项式!系数的表示

三角的第 i 行包含 ji&quot

$$j = 0, 1, 2, \ldots, i$$

***S*(*n, j*):*第***二类的斯特林数，表示将 n 个可区分的物体分配到 j 个不可区分的盒子中的方法的数量，这样就没有盒子是空*的***

### 结果

**计数的乘积法则:一个由**两个任务组成的程序的方法数是完成第一个任务的方法数和完成第一个任务后完成第二个任务方法数的乘积。

**集合的乘积法则:**有限集合的笛卡儿乘积中的元素个数是每个集合中元素个数的乘积。

**计数的和规则:用**两种方法中的一种来完成一项任务的方法数，是如果不能同时完成这些任务的方法数的总和。

**集合的和规则:两两**不相交的有限集合的并集的元素数是这些集合中元素数的和。

**集合的计数或容斥减法规则:**如果一项任务可以用 n1 种方式或 n2 种方式来完成，那么完成任务的方式数就是 n+ n 减去 2 1 两种不同方式共有的完成任务的方式数。

**集合的减法规则**或**容斥规则:**两个集合并集的元素数是这些集合中的元素数减去它们的交集中的元素数之和。

**计数的除法规则:**如果一个任务可以用一个可以以 n 种方式执行的过程来完成，那么就有 n/ ddn 种方式来完成它，而对于每一种方式 *w*, n 种方式中的 d 正好对应于方式 *w*。

**集合的除法规则:**假设一个有限集合 a 是 n 个互不相交的子集的并集，每个子集都有元素。则 n=|A|/d。

**鸽子洞原理:**当 k 个盒子里放置了 k 个以上的物体时，一定有一个盒子里包含了一个以上的物体。

**广义的鸽子洞原理:**当 N 个物体被放置在 k 个盒子里时，必须有一个盒子至少包含[ N/k] 个物体。

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

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

**帕斯卡二项式恒等式定理:**n+1k”(x+ =!k - ny)1”n+ =!%nk"n k=0 !nk " xn- kyk 当允许重复时，一个有 n 个元素的集合有 n个 rr 排列。

当允许重复时，含有 n 个元素的集合有 C(n + r⌐ 1,r) r 种组合。

有 n!/(n1!n2! • • • nk!) k 的 n 个对象的排列

类型，其中有 $n_i$ 个类型 I 的不可区分对象

$$\text{for } i = 1, 2, 3, \ldots, k.$$

生成集合{1,2，…的排列组合的算法。n}

## 审查问题

1. 解释如何使用和和乘积规则来找到长度不超过 10 的位串的数量。
2. 解释如何找到长度不超过 10 且至少有一个 0 位的位串的数量。

**3.a)**如何使用乘积法则来找出从 m 个元素的集合到 n 个元素的集合的函数数量?

**b)**从一个有 5 个元素的集合到一个有 10 个元素的集合有多少个函数?

**c)**如何利用乘积法则，从 m 个元素的集合到 n 个元素的集合，找出一对一函数的数量?

**d)**从一个有五个元素的集合到一个有 10 个元素的集合，有多少个一对一函数?

**e)**从一个有五个元素的集合到一个有 10 个元素的集合有多少个 onto 函数?

**4.** 如果第一支赢了 4 场比赛的球队赢得了季后赛，你怎么能在两支球队之间找到季后赛可能结果的数量?

**5.** 如何找到长度为 10、以 101 开始或以 010 结束的位串的个数?

**6. a)**阐述鸽子洞原理。

**b)**解释如何利用鸽子洞原理来表明任意 11 个整数中，至少有两个的最后一位数字必须相同。

**7. a)**陈述广义鸽子洞原理。

**b)**解释如何用广义鸽子洞原理来证明任意 91 个整数中，至少有 10 个是以相同的数字结尾的。

**8. a)有** n 个元素的集合的 r 组合和 *r* 置换有什么区别?

**b)**推导出一个等式，将 n 个元素的集合的 r-组合的数量和 r-置换的数量联系起来。

**c)**从 25 名学生中选出 6 名学生加入委员会有多少种方法?

**d)**有多少种方法可以从 25 名学生中选择 6 名学生在委员会中担任 6 个不同的管理职位?

**9. a)**什么是帕斯卡三角形?

**b)**如何从上面的三角形生成一行帕斯卡三角形?

**10.** 身份的组合证明是什么意思?这样的证明与代数证明有什么不同?

**11.** 解释如何用组合论证证明帕斯卡恒等式。

**12. a)**陈述二项式定理。

**b)**解释如何用组合论证来证明二项式定理。

**c)**在展开中找到 $x^{100}y^{101}$ 的系数

$$(2x + 5y)^{201}.$$

**13. a)**解释在允许重复且顺序无关紧要的情况下，如何找到从 n 个对象中选择 r 个对象的方法数量的公式。

**b)**如果相同类型的物体无法区分，那么从五种不同类型的物体中选择十几个物体的方法有多少种?

**c)**如果必须至少有 3 个对象属于第一种类型，那么从这 5 种不同类型中选择 12 个对象有多少种方法?

**d)**如果第一种类型的对象不能超过 4 个，从这 5 种不同类型中选择 12 个对象有多少种方法?

**e)**如果第一种类型的对象必须至少有两个，而第二种类型的对象不能超过三个，那么从这五种不同类型中选择十几个对象有多少种方法?

**14. a)**设 n 和 r 为正整数。解释为什么方程 $x_1 + x_2 + \cdots + x_n = r$ 的解的个数，其中 $x_i$ 是一个非负整数，对于 i = 1,2,3，…， n，等于一个包含 n 个元素的集合的 r 种组合的个数。

**b)**方程 $x_1 + x_2 + x_3 + x_4 = 17$ 的非负整数解有多少个?

**c)**第(b)部分的方程有多少个正整数解?

**15. a)**推导出 k 种不同类型的 n 个物体排列数的公式，其中有 $n_1$ 个类型 1 的不可区分物体，$n_2$ 个类型 2 的不可区分物体，…，以及 n 个 k 类不可区分 $_k$ 对象。

**b)**对单词 *indiscretness 的字母排序有多少种方法*?

**16.** 描述一个生成 n 个最小正整数集合的所有排列的算法。

**17. a)**从一副标准的 52 张牌中向 6 个玩家发 5 张牌有多少种方法?

**b)**有多少种方法可以将 n 个可区分的对象分配到 k 个可区分的盒子中，以便将无 $_i$ 对象放置在盒子 i 中?

**18.** 描述一个生成 n 个最小正整数集合的所有组合的算法。

# 7 / DiscreteProbability

## 关键术语和结果

### 条款

**样本空间:**一个实验事件的可能结果的集合**:一个事件的**实验概率的样本空间的子集**(拉普拉斯定义):**这个事件成功结果的数量除以可能结果的数量

**概率分布:**来自 all out-集合的一个函数 $p$

comes of a sample space $S$ for which $0 \leq p(x_i) \leq 1$ for $i = 1, 2, \ldots, n$ and $\sum_{i=1}^{n} p(x_i) = 1$, where $x_1, \ldots, x_n$ are the possible outcomes

**事件 *E的概率:*** $E$中所有结果的概率之和

**$p(E|F)$ (E给定 *F的条件概率*):**比值

$$p(E \cap F)/p(F)$$

**独立事件:**事件 $E$ 和 $F$，使得 $p(E \cap F) =$

$p(E)\ p(F)$

**成对独立事件:**事件 $E_1, E_2$，…，*恩这样*

that $p(E_i \cap E_j) = p(E_i)p(E_j)$ for all pairs of integers $i$ and $j$ with $1 \leq j < k \leq n$

**相互独立的事件:** *事件* $E_{21}, E$，…，*恩这样*

that $p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1})p(E_{i_2}) \cdots p(E_{i_m})$ whenever $i_j$, $j = 1, 2, \ldots, m$, are integers with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ and $m \geq 2$

**随机变量(Random variable):为**实验的每个可能结果分配一个实数的函数

**随机变量 *X* 的分布:**对的集合

$$(r, p(X = r)) \text{ for } r \in X(S)$$

**均匀分布:**对有限集合中的元素分配相等的概率

随机变量的**期望值:随机变量**的加权平均值，对随机变量的值加权?由结果的概率，即 $E(X) = \sum_{s \in S} p(s)X(s)$

**几何分布:**随机变量 X的分布，当 $k$= 1,2 *时*，$p(X = k) = (1 - p)^{k-1} p$。对于某实数 $p$，$0 \leq p \leq 1$。

**独立随机变量:**对于 *所有实数* 1 *rand* $r$，使 $p(X = r_{11}$ and $Y = r_{22}) = p(X = r)p(Y = r)$*的*随机变量 *X 和 Y*

**随机变量 X的方差:** *X 的*值与其期望值 *E(X)之差的平方的加权平均值*，带权重?由结果的概率给出，即 $V(X) = \sum_{s \in S} (X(s) - E(X))^2 p(s)$

**随机变量的标准差** $\sqrt{X}$**:** *X*方差的平方根，即 $\sigma(X) = V(X)$

**伯努利试验(Bernoulli trial):**有两种可能结果的实验

**概率(或蒙特卡洛)算法(probabilistic algorithm):**在一个或多个步骤中做出随机选择的算法

**概率方法(Probabilistic method):一种**证明集合中存在具有某些属性的对象的技术，通过给对象分配概率并显示一个对象具有这些属性的概率是正的来进行**处理**

### 结果

当进行 n 次独立伯努利试验时，正好 k 次成功*的概率等于* $C(n, k)p^k q^{n-k}$，其中 p *是*成功的概率，q = 1− p 是*失败的概率*。

**贝叶斯定理:**如果 $E$ 和 $F$ 是来自样本空间 $S$ 的事件，使得 $p(E)$?= 0 和 $p(F)$?= 0，那么

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}.$$

$$E(X) = \sum_{r \in X(S)} p(X = r)r.$$

**linearity of expectations:** $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$ if $X_1, X_2, \ldots, X_n$ are random variables

如果 $X$ 和 $Y$ 是独立随机变量，则 $E(XY) =$

$E(X)\ E(Y)$。

**毕纳梅尔公式:**如果 $X_1, X_2$，…，$x_n$ 都是独立的 random variables, then $V(X_1 + X_2 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$.

**Chebyshev'sinequality:** $p(|X(s) - E(X)| \geq r) \leq V(X)/r^2$,

其中 $X$ 是概率函数 $p$ 的随机变量，$r$ 是正实数。

# 审查问题

**1. a)**定义所有结果都是等可能的事件的概率。

**b)**如果从前 50 个正整数中选择 6 个不同的中奖号码，那么您选择 6个中奖号码的概率是多少?

**2. a)**分配给有限样本空间的结果的概率应该满足什么条件?

**b)**如果正面出现的次数是反面出现次数的三倍，正面出现的结果和反面出现的结果应分配什么概率?

**3.a)**给定事件 $F$，定义事件 $E$的条件概率。

**b)**假设 $E$ 是掷骰子时得到偶数的事件，$F$ 是掷骰子时得到 1 2或 3的事件。在给定 $E$的情况下，$F$的概率是多少?

**4. a)**什么时候两个事件 $E$和 $F$是独立的?

**b)**假设 $E$ 是掷出均匀骰子时出现偶数的事件，$F$ 是掷出 5或 6的事件。$E$和 $F$独立吗?

**5. a)**什么是随机变量?

**b)**将出现在两个骰子上的较大的数字赋给一个随机变量 $X$ 的可能值是什么?

**6. a)**定义一个随机变量 $X$的期望值。

**b)**给两个骰子的结果赋予两个骰子上出现的较大数字的随机变量 $X$的期望值是多少?

**7. a)**解释如何将具有有限多个可能输入值的算法的平均计算复杂性解释为期望值。

**b)**线性搜索算法的平均计算复杂度是多少，如果我们搜索的元素在列表中的概率是 1/3，并且这个元素出现在列表中 $n$个元素中的任意一个的可能性是相等的?

**8. a)**伯努利试验是什么意思?

**b)** $n$次独立伯努利试验中 $k$次成功的概率是多少?

**c)** $n$次独立伯努利试验中成功次数的期望值是多少?

**9.** a)多个变量的期望线性是什么意思?

**b)**当 hatcheck 的人随机归还帽子时，期望的线性如何帮助我们找到得到正确帽子的预期人数?

**10. a)**如果小概率的错误是可以接受的，那么如何用概率来解决决策问题呢?

**b)**如果我们愿意接受犯错的小概率，如何快速判断一个正整数是否为质数?

**11.**状态贝叶斯定理，并使用它来找到 $p(F|E)$if

$$p(E \mid F) = 1/3, \quad p(E \mid \bar{F}) = 1/4, \quad \text{and} \quad p(F) = 2/3,$$

其中 $E$和 $F$是来自样本空间 $S$的事件。

**12. a)**说一个随机变量有一个带有参数 $p$的几何分布是什么意思?

**b)**一个参数为 $p$的几何分布的均值是什么?

**13. a)**一个随机变量的方差是什么?

**b)**成功概率为 $p$的伯努利试验的方差是多少?

**14. a)** $n$个独立随机变量和的方差是多少?

**b)**当进行 $n$ 次独立的伯努利试验时，每次成功的概率为 $p$，成功次数的方差是多少?

**15.** 关于一个随机变量偏离其均值超过指定值的概率，切比雪夫不等式告诉我们什么?