第一章 预备知识

上次内容

- 什么是逻辑?
  - 推理
  - 概念
  - 悖论
- 什么叫数理逻辑?
- 为什么要学数理逻辑?

上次内容

- 什么是逻辑?
  - 推理: (1930)数理逻辑
  - 概念
  - 悖论
- 什么叫数理逻辑?
- 为什么要学数理逻辑?

上次内容

- 什么是逻辑?
  - 推理: (1930)数理逻辑Mathmetical logic
  - 概念: (1990)描述逻辑Description logics
  - 悖论
- 什么叫数理逻辑?
- 为什么要学数理逻辑?

今天内容

- 集合, 集合之间的关系, 集合运算
- 关系, 函数及其分类
- 结构: 偏序, 布尔代数, 布尔代数基本定理
- 基数: Cantor定理, 对角线方法
- 数学归纳法

集合(set): 具有某种性质的元素(对象)的汇集(collection).

集合(set): 具有某种性质的元素(对象)的汇集(collection). 性质称为集合的**内含**, 所有满足性质的对象组成集合的**外延.**

对象: a;

集合: S;

断言: $a \in S, a \notin S$.

概念与集合的差别

张三是一个人;
(*) 我是这个班;
(*) 我是共产党;
我是这个班的同学;
我是共产党党员.

概念与集合的差别

张三是一个人;
($*$) 我是这个班;
($*$) 我是共产党;
我是这个班的同学;
我是共产党党员.
概念: x是一个A;
集合: x是集合A的一个成员.

概念与集合的差别

张三是一个人;
$(*)$ 我是这个班;
$(*)$ 我是共产党;
我是这个班的同学;
我是共产党党员.
概念: x是一个A;
集合: x是集合A的一个成员.
集合是一个个体;
概念不是一个个体; 是一个(复合)个体: 概念的外延和概念的内涵.

集合之间的关系

学一个概念，首先搞清楚
(1) 概念的内涵是什么;

集合之间的关系

学一个概念, 首先搞清楚

(1) 概念的内涵是什么. 比如: 一个集合是具有某个性质的元素的集体.

学一个概念，首先搞清楚
(1) 概念的内涵是什么.
(2) 有什么特殊的外延元素;

集合之间的关系

学一个概念，首先搞清楚
(1) 概念的内涵是什么.
(2) 有什么特殊的外延元素; $N = \{0, 1, 2, 3, \ldots\}$

集合之间的关系

学一个概念, 首先搞清楚
(1) 概念的内涵是什么.
(2) 有什么特殊的外延元素.
(3) 外延元素之间的相等关系.
注意: 相等关系可以通过其它基本关系定义. 比如有自然数上的大小关系$\leq$, 那么自然数上的相等关系$=$定义为: 对任何自然数n, m,

$$n = m \text{ iff } n \leq m \& m \leq n.$$

集合之间的关系

相等: $S = T$ iff 对所有的x, $x \in S$当且仅当$x \in T$.
子集(subset): $S \subseteq T$ iff **对所有的**x, 如果$x \in S$则$x \in T$.
真子集(proper subset): $S \subset T$.

集合之间的关系

事实上, 子集关系是基本关系.
对任何集合S, T,

$$S = T \text{ iff } S \subseteq T \& T \subseteq S.$$

集合之间的关系

事实上, 子集关系是基本关系.
对任何集合S, T,

$$S = T \text{ iff } S \subseteq T \& T \subseteq S.$$

子集关系又是通过属于关系定义的. 对任何集合S, T,

$$S \subseteq T \text{ iff 对任何的} x, x \in S \text{ 蕴涵 } x \in T.$$

集合之间的关系

事实上, 子集关系是基本关系.
对任何集合S, T,

$$S = T \text{ iff } S \subseteq T \& T \subseteq S.$$

子集关系又是通过属于关系定义的. 对任何集合S, T,

$$S \subseteq T \text{ iff 对任何的} x, x \in S \Rightarrow x \in T.$$

因此, 在集合论中只需要一个关系

$$\in \text{关系}.$$

结论

由相等的定义可以推出:
构成集合的元素与集合中元素的**次序**和是否**重复**无关.
$\{0,0,1\} = \{0,1\}$;
$\{0,1\} = \{1,0\}$.

空集

空集$\emptyset$: 不含任何元素的集合.
空集是唯一的.

结论

空集是任何集合的子集.

结论

空集是任何集合的子集.
任给一个集合A, 有
$$\emptyset \subseteq A.$$

结论

空集是任何集合的子集.
任给一个集合A, 有
$$\emptyset \subseteq A.$$
我们需要证明: 对任何元素x, 如果$x \in \emptyset$ 则$x \in A$.
因为$x \in \emptyset$为假. 如果前提为假, 则整个蕴涵式句子为真*, 与蕴涵式句子的结论的真假值无关.
$*$ 注意: 这只是逻辑学的一个约定.

集合的表示

$$S = \{x | P(x)\},$$

其中$P(x)$是关于x的性质.
$\{x | x < 100,$ 并且x是素数$\}$.

集合的表示

$$S = \{x | P(x)\},$$

其中$P(x)$是关于x的性质.

$\{x | x < 100,$ 并且x是素数$\}$.

注意两点:

(1) 属于这个集合的元素具有性质P;

(2) 不属于这个集合的元素不具有性质P.

$P(x)$表示元素(个体) x事例(instantiates)性质P, 或者x满足性质P.

Russell悖论

设$P(x): x \notin x$是一个关于x的性质.

Russell悖论

设$P(x): x \notin x$是一个关于x的性质.
定义集合

$$V = \{x | x \notin x\}.$$

Russell悖论

设$P(x): x \notin x$是一个关于x的性质.
定义集合
$$V = \{x | x \notin x\}.$$
问题: 是否$V \in V$?

Russell悖论

设$P(x): x \notin x$是一个关于x的性质.
定义集合

$$V = \{x | x \notin x\}.$$

问题: 是否$V \in V$?
如果$V \in V$则V满足定义集合的性质, 即$V \notin V$;
如果$V \notin V$则V满足性质, 因此$V \in V$.

Russell悖论的推动作用

由朴素集合论(naive set theory)变成
(1) **公理化(axiomatic)集合论**;
解决办法: $\{x \in A | P(x)\}$;
数理逻辑的组成部分: 模型论, 集合论, 递归论和证明论.

Russell悖论的推动作用

由朴素集合论(naive set theory)变成
(1) **公理化(axiomatic)集合论**;
解决办法: $\{x \in A | P(x)\}$;
(2) 类型论(type theory)的产生.
解决办法: 所有的集合分成类型, 低类型的集合才可以构成高类型的集合.
类型论是现代程序语言设计的基本理论.

序对(pairs)

有序偶:

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}.$$

命题. $\langle a, b\rangle = \langle c, d\rangle$ 当且仅当$a = c$并且$b = d$.

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}.$$

集合的运算: 集合交和并

在包含关系下, 集合S和T的并:

$$S \cup T = \{x : x \in S \text{或} x \in T\};$$

集合S和T的交:

$$S \cap T = \{x : x \in S \text{且} x \in T\}.$$

交和并的性质

集合交和并满足下列公式:

交换律(communitive)	$S \cup T = T \cup S$;
	$S \cap T = T \cap S$;
结合律(associative)	$S \cup (T \cup U) = (S \cup T) \cup U$;
	$S \cap (T \cap U) = (S \cap T) \cap U$;
分配律	$S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$;
	$S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$.

分配律的证明

证明: 对任何集合S, T, U,

$$S \cap (T \cup U) = (S \cap T) \cup (S \cap U).$$

分配律的证明

要证明

$$S \cap (T \cup U) = (S \cap T) \cup (S \cap U),$$

需要证明

$$S \cap (T \cup U) \subseteq (S \cap T) \cup (S \cap U) \tag{1}$$

并且

$$(S \cap T) \cup (S \cap U) \subseteq S \cap (T \cup U). \tag{2}$$

$S \cap (T \cup U) \subseteq (S \cap T) \cup (S \cap U)$

对任何x, 假定$x \in S \cap (T \cup U)$. 则$x \in S$, 且$x \in T \cup U$;

$S \cap (T \cup U) \subseteq (S \cap T) \cup (S \cap U)$

对任何x, 假定$x \in S \cap (T \cup U)$. 则$x \in S$, 且$x \in T \cup U$;
即$x \in S$, 且$x \in T$或$x \in U$;

$S \cap (T \cup U) \subseteq (S \cap T) \cup (S \cap U)$

对任何x, 假定$x \in S \cap (T \cup U)$. 则$x \in S$, 且$x \in T \cup U$;
即$x \in S$, 且$x \in T$或$x \in U$;
即$x \in S$ 且$x \in T$, 或$x \in S$ 且$x \in U$;

$S \cap (T \cup U) \subseteq (S \cap T) \cup (S \cap U)$

对任何x, 假定$x \in S \cap (T \cup U)$. 则$x \in S$, 且$x \in T \cup U$;
即$x \in S$, 且$x \in T$或$x \in U$;
即$x \in S$ 且$x \in T$, 或$x \in S$ 且$x \in U$;
即$x \in S \cap T$, 或$x \in S \cap U$;

$S \cap (T \cup U) \subseteq (S \cap T) \cup (S \cap U)$

对任何x, 假定$x \in S \cap (T \cup U)$. 则$x \in S$, 且$x \in T \cup U$;
即$x \in S$, 且$x \in T$或$x \in U$;
即$x \in S$ 且$x \in T$, **或**$x \in S$ 且$x \in U$;
即$x \in S \cap T$, 或$x \in S \cap U$;
即$x \in (S \cap T) \cup (S \cap U)$.

$(S \cap T) \cup (S \cap U) \subseteq S \cap (T \cup U)$

对任何x, 假定$x \in (S \cap T) \cup (S \cap U)$. 则$x \in S \cap T$, 或$x \in S \cap U$;
即$x \in S$且$x \in T$, 或$x \in S$且$x \in U$;

$(S \cap T) \cup (S \cap U) \subseteq S \cap (T \cup U)$

对任何x, 假定$x \in (S \cap T) \cup (S \cap U)$. 则$x \in S \cap T$, 或$x \in S \cap U$;
即$x \in S$且$x \in T$, 或$x \in S$且$x \in U$;
即$x \in S$, 且$x \in T$或$x \in U$;

$(S \cap T) \cup (S \cap U) \subseteq S \cap (T \cup U)$

对任何x, 假定$x \in (S \cap T) \cup (S \cap U)$. 则$x \in S \cap T$, 或$x \in S \cap U$;
即$x \in S$且$x \in T$, 或$x \in S$且$x \in U$;
即$x \in S$, 且$x \in T$或$x \in U$;
即$x \in S$,且$x \in T \cup U$;

$(S \cap T) \cup (S \cap U) \subseteq S \cap (T \cup U)$

对任何x, 假定$x \in (S \cap T) \cup (S \cap U)$. 则$x \in S \cap T$, 或$x \in S \cap U$;
即$x \in S$且$x \in T$, 或$x \in S$且$x \in U$;
即$x \in S$, 且$x \in T$或$x \in U$;
即$x \in S$,且$x \in T \cup U$;
即$x \in S \cap (T \cup U)$.

$(S \cap T) \cup (S \cap U) \subseteq S \cap (T \cup U)$

对任何x, 假定$x \in (S \cap T) \cup (S \cap U)$. 则$x \in S \cap T$, 或$x \in S \cap U$;
即$x \in S$且$x \in T$, 或$x \in S$且$x \in U$;
即$x \in S$, 且$x \in T$**或**$x \in U$;
即$x \in S$,且$x \in T \cup U$;
即$x \in S \cap (T \cup U)$.
注意: $\cup$和$\cap$的分配性是由自然语言中的"或"和"且"的分配性所决定的.

集合差

集合S和T的差:

$$S - T = \{x : x \in S, \text{且} x \notin T\}.$$

幂集

给定一个集合S，S的所有子集的集合称为S的幂集，记为$\wp(S)$.

- 每个$\wp(S)$的元素是集合;
- $\wp(S)$中包含一个最大的元素S和
- 一个最小的元素$\emptyset$.

幂集

不同集合的子集可以不同, 除了空集.
每个集合有空集作为子集.
空集是每个集合的子集.
这个性质只有空集具有.

幂集的例子1

例子: 集合$\{a, b\}$的幂集为

$$\{\emptyset, ..., S\}.$$

幂集的例子1

例子: 集合$\{a, b\}$的幂集为

$$\wp(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, S\} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

幂集的例子2

例子: 集合$\{a, b, c\}$的幂集为

$$\wp(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, S\}.$$

幂集的例子3

例子: 集合$\{a,\{b,c\}\}$的幂集为

$$\wp(\{a,\{b,c\}\}) = \{\emptyset, ..., S\}.$$

幂集的例子3

例子: 集合$\{a, \{b, c\}\}$的幂集为

$$\wp(\{a, \{b, c\}\}) = \{\emptyset, \{a\}, \{b, c\}, \{a, \{b, c\}\}\}.$$

幂集的例子3

例子: 集合$\{a, \{b, c\}\}$的幂集为

$$\wp(\{a, \{b, c\}\}) = \{\emptyset, \{a\}, \{b, c\}, \{a, \{b, c\}\}\}.$$

对吗?

幂集的例子3

例子: 集合$\{a, \{b, c\}\}$的幂集为

$$\wp(\{a, \{b, c\}\}) = \{\emptyset, \{a\}, \{\{b, c\}\}, \{a, \{b, c\}\}\}.$$

幂集的例子4

例子: 集合$\emptyset$的幂集为

$$\wp(\emptyset) = \{\emptyset, ..., S\};$$

幂集的例子4

例子: 集合$\emptyset$的幂集为

$$\wp(\emptyset) = \{\emptyset, \emptyset\} = \{\emptyset\}.$$

注意: $\{\emptyset\}$与$\emptyset$的差别.

幂集的例子4

例子: 集合$\emptyset$的幂集为

$$\wp(\emptyset) = \{\emptyset, \emptyset\} = \{\emptyset\}.$$

无中生有
$2^{n+1} = 2^n \cdot 2.$
$2^0 = 1.$

幂集的例子5

例子: 集合$\{\emptyset, \{\emptyset\}\}$的幂集为

$$\wp(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, ..., \{\emptyset, \{\emptyset\}\}\};$$

幂集的例子5

例子: 集合$\{\emptyset, \{\emptyset\}\}$的幂集为

$$\wp(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

补集

给定一个集合S和S的一个子集X，X的补定义为

$$-X = S - X.$$

注意补集与集合差之间的差别: 相对性和绝对性.

差满足的性质

设X, Y, Z为S的子集,

幂等律(idempotent)	$-(-X) = X$;
	$X \cup (-X) = S$;
	$X \cap (-X) = \emptyset$;
De Morgan律	$-(X \cup Y) = (-X) \cap (-Y)$;
	$-(X \cap Y) = (-X) \cup (-Y)$.

自然语言上的"否定"与"或, 且"之间的De Morgan律决定了$-$与$+, \times$之间的De Morgan律.

De Morgan律: $-(X \cup Y) = (-X) \cap (-Y)$

对任何元素x, 假设$x \in -(X \cup Y)$.
则$x \notin X \cup Y$, 即$x \in X$或者$x \in Y$的否定;
也就是$x \in X$的否定并且$x \in Y$的否定;
即$x \notin X$并且$x \notin Y$;
即$x \in -X$并且$x \in -Y$,
即$x \in -X \cap -Y$.

笛卡儿乘积

$$S \times T = \{\langle x, y\rangle | x \in S, y \in T\}.$$

线段与线段的笛卡儿乘积是面;
线段与面的笛卡儿乘积是立方体

关系(relation)

给定集合S和T, 一个S与T之间的关系R就是$S \times T$的一个子集. 即

$$R \subseteq S \times T.$$

函数

函数

S到T的一个函数f 是一个S与T之间的关系, 满足下面条件:
对任何$x \in S$和$y, y' \in T$, 如果$(x, y), (x, y') \in f$ 则$y = y'$.

函数

S到T的一个函数f 是一个S与T之间的关系, 满足下面条件:
对任何$x \in S$和$y, y' \in T$, 如果$(x, y), (x, y') \in f$ 则$y = y'$.
记唯一的y为$f(x)$.
函数f的定义域(domain)

$$\mathrm{dom}(f) = \{x \in S : \exists y((x, y) \in f)\};$$

值域(range)

$$\mathrm{ran}(f) = \{y \in T : \exists x((x, y) \in f)\};$$

函数

结论: 如果f是S到T的一个函数, 则

$$\mathrm{dom}(f) \subseteq S;$$
$$\mathrm{ran}(f) \subseteq T.$$

函数

设$S = \{a, b\}$, $T = \{a, c, d\}$.
关系$R = \{(a, a), (a, c), (b, d)\}$不是一个函数.
关系$f = \{(a, a), (b, d)\}$是一个函数, 其定义域为

$$\mathrm{dom}(f) = \{a, b\},$$

值域为

$$\mathrm{ran}(f) = \{a, d\}.$$

什么是函数依赖(关系数据库)?

函数的种类

一一函数(injective): 对任何$x, x' \in S$, 如果$x \neq x'$则$f(x) \neq f(x')$.
映上函数(surjective, 满射): 对任何$y \in T$, 存在至少一个$x \in S$使得$f(x) = y$.
双射(bijective): 一一的满射.
$f = \{(a, a), (b, c)\}$是一个一一的,但非映上的函数, 其中$S = \{a, b, c\} = T$.

一个集合上的一元关系

一元关系也称为谓词.
S上的一元关系就是S的一个子集.
事实上, 在数理逻辑学中, 关系就是谓词, 谓词就是关系.

一个集合上的二元关系

S上的二元关系$R \subseteq S \times S$.
R是自反的(reflexive), 如果**对任何**$x \in S$, xRx;
R是对称的(symmetric), 如果**对任何**$x, y \in S$, 如果xRy 则yRx;
R是传递的(transitive), 如果**对任何**$x, y, z \in S$, 如果xRy且yRz则xRz;

等价关系

集合S上二元关系R是一个等价关系(equivalence relation), 如果R是自反的, 对称的且传递的.
等价关系R的等价类X是S的最大子集使得X中每两个元素具有关系R.
给定一个$x \in S$, 子集

$$\overline{x} = \{y \in S| \quad xRy\}$$

是包含x的唯一的等价类.

结论. 两个等价类X和Y相等, 即$X = Y$, 当且仅当存在$x \in X, y \in Y$使得xRy.

一个集合的划分

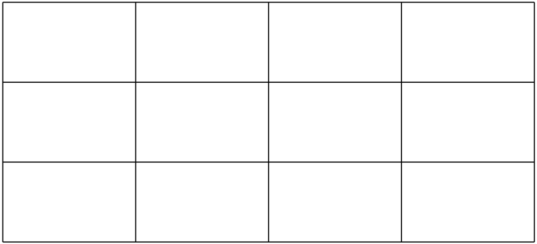
集合S的子集的集合P是S的一个划分(partition), 如果P的元素两两不相交, 并且所有P的元素的并等于S.
对任何$x \in P, x \subseteq S$, 而不是$x \in S$.

一个集合的划分

S的子集的集合P是S的一个划分(partition), 如果P的元素两两不相交, 并且所有P的元素的并等于S.

一个集合的划分

S的子集的集合P是S的一个划分(partition), 如果P的元素两两不相交, 并且所有P的元素的并等于S.



等价关系与划分的关系

基本性质. 给定集合S上的一个等价关系R，R的所有等价类组成S的一个划分;

等价关系与划分的关系

给定S的一个划分P, 定义关系R_P使得对任何$x, y \in S$,

$$xR_Py \text{当且仅当 存在一个} X \in P \text{使得} x, y \in X.$$

则R_P是一个等价关系.

二元关系: 一种否定的方式

R不是自反的, 如果**存在**$x \in S$使得$(x, x) \notin R$;
R不是对称的, 如果**存在**$x, y \in S$使得xRy并且$(y, x) \notin R$;
R不是传递的, 如果**存在**$x, y, z \in S$使得xRy, yRz且$(x, z) \notin R$.
R是自反的(reflexive), 如果对任何$x \in S$, xRx;
R是对称的(symmetric), 如果对任何$x, y \in S$, 如果xRy 则yRx;
R是传递的(transitive), 如果对任何$x, y, z \in S$, 如果xRy且yRz则xRz;

二元关系: 第二种否定的方式

R是非自反的(irreflexive), 如果**对任何**$x \in S, (x, x) \notin R$;
R是非对称的(asymmetric), 如果**对任何**$x, y \in S, xRy$蕴涵$(y, x) \notin R$;
比如, "大于", "小于"是非对称关系.
R是自反的(reflexive), 如果对任何$x \in S$, xRx;
R是对称的(symmetric), 如果对任何$x, y \in S$, 如果xRy 则yRx;

二元关系: 第三种否定的方式

R是非自反的(irreflexive), 如果对任何$x \in S, (x,x) \notin R$;
R是非对称的(asymmetric), 如果对任何$x, y \in S, xRy$蕴涵$(y,x) \notin R$;
R是反对称的(anti-symmetric), 如果**对任何**$x, y \in S, xRy$且yRx蕴涵$x = y$;
比如, "不小于", "不大于"是反对称关系.
R是自反的(reflexive), 如果对任何$x \in S$, xRx;
R是对称的(symmetric), 如果对任何$x, y \in S$, 如果xRy 则yRx;
R是传递的(transitive), 如果对任何$x, y, z \in S$, 如果xRy且yRz则xRz;

二元关系

关系	关系名称
$\forall x \exists y (xRy)$	序列的Serial
$\forall x (xRx)$	自反的Reflexive
$\forall x, y, z (xRy \wedge yRz \to xRz)$	传递的Transitive
$\forall x, y (xRy \to yRx)$	对称的Symmetric
$\forall x, y, z (xRy \wedge xRz \to yRz)$	欧几里德的Euclidean
$\forall x, y, z (xRy \wedge xRz \to y = z)$	函数式的functional
$* \ \forall x, y (xRy \to yRy)$	移位自反的Shift Reflexive
$\forall x, y (xRy \to \exists z (xRz \wedge zRy))$	稠密的Dense
$* \forall x, y, z, u (xRy \wedge xRu \to \exists z (yRz \wedge uRz))$	收敛的Convergent

二元关系

任何元的关系可以用若干个二元关系表示.
课外作业.
因此, 只需要考虑二元关系.

前序

定义. 一个集合S上的自反, 传递的关系R称为S上的一个前序(也称伪序, pre-order).
如果R是自反的, 反对称的, 传递的, 称R为S上的一个偏序(partial order).
一个偏序R是线性的(或称为全序, linear order), 如果对任何$x, y \in S$, 要么xRy要么yRx.
通常, 我们用$\leq$表示偏序.

二元关系

一个偏序$\leq$是良定的(well-founded), 如果它不包含无限的降链.
比如,自然数的序:

$$0 < 1 < 2 < 3 < ...,$$

是良定的线性序, 但整数上的序:

$$... < -3 < -2 < -1 < 0 < 1 < 2 < 3 < ...$$

不是良定的线性序.

上确界与下确界

假设R是一个集合S上的偏序, 且x, y是S的元素. 一个元素$z \in S$称为x和y的并(最小上界, 上确界, join, supremum) 如果

1. xRz, yRz,且
2. 对任何元素$a \in S$使得xRa且yRa, 我们有zRa.

上确界与下确界

假设R是一个集合S上的偏序, 且x, y是S的元素. 一个元素$z \in S$称为x和y的并(最小上界, 上确界, join, supremum) 如果

1. xRz, yRz,且
2. 对任何元素$a \in S$使得xRa且yRa, 我们有zRa.

一个元素$z \in S$称为x和y的交(最大下界, 下确界, meet, infimum), 如果

1. $z \leq x, z \leq y$, 且
2. **对任何元素**$b \in S$使得$b \leq x$ 且$b \leq y$, 我们有$b \leq z$.

最大公因子, 最小公倍数

定义$m|n$, 如果n能被m整除.
$|$是一个偏序.
给定$m, n \in \omega$,
(1) m, n的下确界是m, n的最大公因子(m, n);
(2) m, n的上确界是m, n的最小公倍数$[m, n]$.

布尔代数

一个布尔代数B是由集合U, 运算$+, \times, -$, 和常元$0, 1$组成的, 并且
(1) $+, \times$满足交换律, 结合律, 分配律;
(2) $-$满足幂等律$(-(-x) = x)$;
(3) $+, \times, -$满足De Morgan律; 并且
(4) 对任何$x \in U, x + (-x) = 1, x \times (-x) = 0$.

典型的布尔代数

$(\wp(S), \cup, \cap, -, S, \emptyset)$是一个布尔代数.

最简单的布尔代数$\mathbf{B}_0$

设$U = \{0,1\}$, $\mathbf{B}_0 = (\{0,1\}, +, \times, -, 0, 1)$.

1. 二元加法$+$:

$$0+0=0, 0+1=1=1+0, 1+1=1;$$

2. 二元乘法$\times$:

$$0\times 0=0\times 1=1\times 0=0, 1\times 1=1;$$

3. 一元逆函数$-$:

$$-0=1, -1=0.$$

最简单的布尔代数

对任何$x, y, z \in \{0, 1\}$,

- 结合律:

$$x + (y + z) = (x + y) + z;$$
$$x \times (y \times z) = (x \times y) \times z.$$

- 分配律:

$$x \times (y + z) = (x \times y) + (x \times z);$$
$$x + (y \times z) = (x + y) \times (x + z).$$

-

$$-(-x) = x;$$
$$-(x \times y) = (-x) + (-y);$$
$$-(x + y) = (-x) + (-y);$$
$$x + (-x) = 0;$$
$$x \times (-x) = 1.$$

布尔代数与偏序

给定一个布尔代数$\mathbf{B} = (U, +, \times, -, 0, 1)$, 可以定义$U$上的一个偏序$\leq$使得对任何$x, y \in U$,

$$x \leq y \text{ 当且仅当 } x + y = y;$$

等价地,

$$x \leq y \text{ 当且仅当 } x \times y = x.$$

在偏序$\leq$下, x和y的上确界为$x + y$, 下确界为$x \times y$.

典型的布尔代数

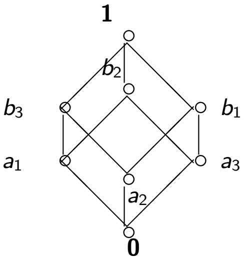
给定一个集合S, 所有的S的子集$\mathcal{P}(S)$ (S的幂集)在集合交, 并, 差运算下是一个布尔代数.

布尔代数基本定理

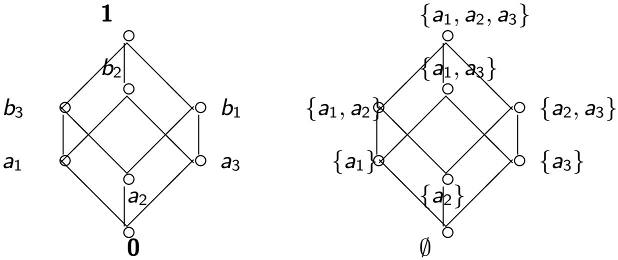
定理. 任何一个布尔代数$(U,+,\times,-,0,1)$, 存在一个集合S和一个双射$f:U\to\wp(S)$使得对任何$x,y\in U$,

$$
\begin{aligned}
&f(0)=\emptyset;\\
&f(1)=S;\\
&f(x+y)=f(x)\cup f(y);\\
&f(x\times y)=f(x)\cap f(y);\\
&f(-x)=-f(x).
\end{aligned}
$$

布尔代数基本定理的证明思路



证明思路2



$\mathbf{1}$
b_2
b_3
b_1
a_1
a_3
a_2
$\mathbf{0}$
$\{a_1, a_2, a_3\}$
$\{a_1, a_3\}$
$\{a_1, a_2\}$
$\{a_2, a_3\}$
$\{a_1\}$
$\{a_3\}$
$\{a_2\}$
$\emptyset$

布尔代数的表示

命题. 任给一个布尔代数$\wp(S)$,

$$\wp(S) \cong \{0,1\}^S = (\mathbf{B}_0)^S.$$

证明: 对任何子集$X \in S$, 定义

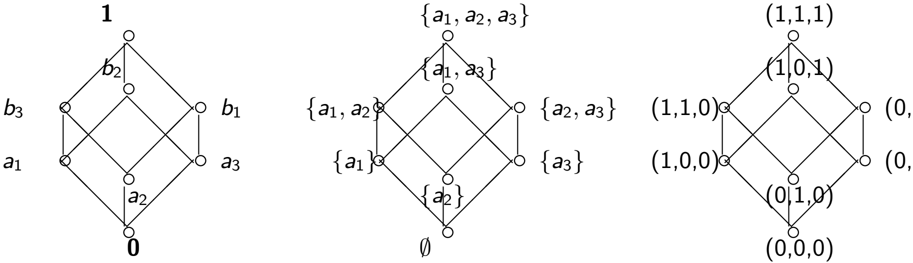
$$\sigma(X) = \chi_X,$$

其中χ_X是X的特征函数, 即对任何$x \in S$,

$$\chi_X(x) = \begin{cases} 1 & \text{如果} x \in X \\ 0 & \text{如果} x \notin X. \end{cases}$$

则σ是$\wp(S)$到$\{0,1\}^S$上的同构. $\square$

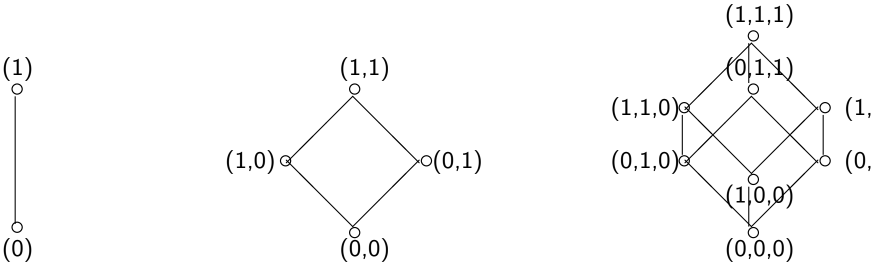
证明思路



$\mathbf{1}$
b_2
b_3
b_1
a_1
a_3
a_2
$\mathbf{0}$
$\{a_1, a_2, a_3\}$
$\{a_1, a_3\}$
$\{a_1, a_2\}$
$\{a_2, a_3\}$
$\{a_1\}$
$\{a_3\}$
$\{a_2\}$
$\emptyset$
(1,1,1)
(1,0,1)
(1,1,0)
(0,
(1,0,0)
(0,
(0,1,0)
(0,0,0)

布尔代数的表示1

推论. 任给一个布尔代数A 可以表示为布尔代数$\mathbf{B}_0$的乘积.



分析哲学的逻辑基础;
计算机科学的理论基础.

格

如果集合U上的偏序$\leq$使得每两个元素的上确界$\cup$和下确界$\cap$存在, 则$(U, \leq, \cap, \cup)$称为一个格(lattice).
一个布尔代数是一个格.

计数

计数是在确定相等之后的第一件事情.
3是人类智力上的大突破.
乌鸦至多计数到2.

等势/基数

两个集合S和T称为等势的，如果存在S到T的双射.
一个集合S是可数的，如果S与自然数是等势的.
一个集合S是有限的，如果S与某个自然数是等势的.
基数是等势的等价类. 给定一个集合S，S的基数是

$$|S| = \{T : T\text{与}S\text{是等势的}\}.$$

个数

定义: $\mathbf{n} = \{T : T有n个元素\}$.
每个自然数对应一个且唯一一个基数.
$\aleph_0 = |\omega|, \aleph_1, \aleph_2, \ldots$
定义: 序数. $\omega + 1, \omega + \omega, \omega \times \omega$不是基数.
$*$ $\aleph$读着aleph.

基数的运算

宇宙旅馆

可数无穷集合的并是可数无穷的;

可数无穷集合的笛卡儿乘积是可数无穷的.

基数的运算

$$
\begin{tikzcd}
(0,0) \arrow[r] & (0,1) \arrow[dl] & (0,2) \arrow[r] & (0,3) \arrow[dl] & \cdots \\
(1,0) \arrow[d] & (1,1) \arrow[ur] & (1,2) \arrow[dl] & (1,3) & \\
(2,0) \arrow[ur] & (2,1) \arrow[dl] & (2,2) \arrow[ur] & (2,3) & \\
(3,0) \arrow[d] & (3,1) \arrow[ur] & (3,2) & (3,3) & \\
(4,0) \arrow[ur] & & & & \\
\vdots & & & &
\end{tikzcd}
$$

$$\tau(x,y) = \frac{(x+y)^2 - x - 3y + 2}{2};$$

$$x(z) = z - \frac{1}{2}\left(\sqrt{2z - \tfrac{7}{4}} - \tfrac{1}{2}\right)\left(\left(\sqrt{2z - \frac{7}{4}} - \frac{1}{2}\right) + 1\right);$$

$$y(z) = \left(\sqrt{2z - \tfrac{7}{4}} - \tfrac{1}{2}\right) - x(z) + 2.$$

幂集的个数

定理. 元素个数为n的集合S的幂集含有2^n个元素.
证明: 当$n=0$时, S为空集, $\wp(S)=\{\emptyset\}$含有一个元素.
假设定理对n成立, 我们证明对$n+1$也成立. 设S是一个含有$n+1$个元素的集合, 从S中任取一个元素, 设a. 设$S=S'\cup\{a\}$.
则

$$\wp(S) = \wp(S')\cup(\wp(S')+a),$$

其中$\wp(S')+a=\{T\cup\{a\}:T\in\wp(S')\}$.

幂集的个数

比如, 设$S=\{a,b,c\}$. 则$S=S'\cup\{a\}$, 其中$S'=\{b,c\}$.

$$\begin{aligned}
\wp(S) &= \{\emptyset,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\} \\
&= \{\emptyset,\{b\},\{c\},\{b,c\}\}\cup\{\{a\},\{a,b\},\{a,c\},\{a,b,c\}\} \\
&= \{\emptyset,\{b\},\{c\},\{b,c\}\}\cup(\{\emptyset,\{b\},\{c\},\{b,c\}\}+\{a\}) \\
&= \wp(S')\cup(\wp(S')+a)
\end{aligned}$$

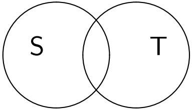
集合的势与集合运算

给定集合S和T,

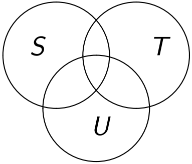
$$|S \cup T| \leq |S| + |T|,$$

并且$|S \cup T| = |S| + |T|$当且仅当$S \cap T = \emptyset$.

$$|S \cup T| = |S| + |T| - |S \cap T|.$$

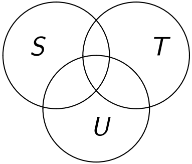


??



S
T
U

??



$$
\begin{aligned}
|S \cup T \cup U| &= |S| + |T| + |U| \\
&\quad -|S \cap T| - |S \cap U| - |T \cap U| \\
&\quad +|S \cap T \cap U|
\end{aligned}
$$

比如, 设$S = \{a, b, c\}$, $T = \{b, c, d, e, f\}$.

$$
\begin{aligned}
|S \cup T| &= |\{a, b, c, d, e, f\}| = 6; \\
|S \cap T| &= |\{b, c\}| = 2; \\
|S| &= 3; \\
|T| &= 5; \\
6 &= 3 + 5 - 2.
\end{aligned}
$$

定理的证明

$$
\begin{aligned}
|\wp(S)| &= |\wp(S')| + |\wp(S') + a| \\
&= 2^n + 2^n \\
&= 2^{n+1}.
\end{aligned}
$$

实数的不可数性

每个实数$r \in [0,1]$可以表示为{0,1,...,9}的无穷串:

$$r = 0.r_1 r_2 r_3 \cdots ,$$

其中$r_i \in \{0, 1, ..., 9\}$, 且

$$0 = 0.0000 \cdots ,$$
$$1 = 0.9999 \cdots .$$

实数的不可数性

$$
\begin{array}{c|ccccccc}
r_0 & 0.r_{00} & r_{01} & r_{02} & \cdots & r_{0n} & \cdots \\
r_1 & 0.r_{10} & r_{11} & r_{12} & \cdots & r_{1n} & \cdots \\
r_2 & 0.r_{20} & r_{21} & r_{22} & \cdots & r_{2n} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
r_m & 0.r_{m0} & r_{m1} & r_{m2} & \cdots & r_{mn} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

实数的不可数性

$$
\begin{array}{c|ccccccc}
r_0 & 0.r_{00}+1 & r_{01} & r_{02} & \cdots & r_{0n} & \cdots \\
r_1 & 0.r_{10} & r_{11}+1 & r_{12} & \cdots & r_{1n} & \cdots \\
r_2 & 0.r_{20} & r_{21} & r_{22}+1 & \cdots & r_{2n} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
r_n & 0.r_{n0} & r_{n1} & r_{n2} & \cdots & r_{nn}+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

其中$9+1=0$.

实数的不可数性

$$
\begin{array}{c|lllllll}
 & 0. & & & & & & \\
r_0 & 0.r_{00}+1 & r_{01} & r_{02} & \cdots & r_{0n} & \cdots \\
r_1 & 0.r_{10} & r_{11}+1 & r_{12} & \cdots & r_{1n} & \cdots \\
r_2 & 0.r_{20} & r_{21} & r_{22}+1 & \cdots & r_{2n} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
r_n & 0.r_{n0} & r_{n1} & r_{n2} & \cdots & r_{nn}+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

其中$9+1=0$.

对角线方法

定义一个实数r使得对任何i,

$$r(i) = \begin{cases} r_{ii} + 1 & \text{如果} r_{ii} \neq 9 \\ 0 & \text{否则}. \end{cases}$$

则$r \in [0, 1]$, 且存在一个j使得

$$r = r_j.$$

实数的不可数性

$$
\begin{array}{c|llllll}
r_0 & 0.r_{00} & r_{01} & r_{02} & \cdots & r_{0j} & \cdots \\
r_1 & 0.r_{10} & r_{11} & r_{12} & \cdots & r_{1j} & \cdots \\
r_2 & 0.r_{20} & r_{21} & r_{22} & \cdots & r_{2j} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
r_j & 0.r_{00}+1 & r_{11}+1 & r_{22}+1 & \cdots & r_{jj}+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

对角线方法

计算$r(j)$.

$$r(j) = r_j(j) = r_{jj};$$
$$r(j) = \begin{cases} r_{jj} + 1 & \text{如果} r_{jj} \neq 9 \\ 0 & \text{否则.} \end{cases}$$

实数的不可数性

$$
\begin{array}{c|cccccc}
r_0 & 0.r_{00} & r_{01} & r_{02} & \cdots & r_{0j} & \cdots \\
r_1 & 0.r_{10} & r_{11} & r_{12} & \cdots & r_{1j} & \cdots \\
r_2 & 0.r_{20} & r_{21} & r_{22} & \cdots & r_{2j} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
r_j & 0.r_{00}+1 & r_{11}+1 & r_{22}+1 & \cdots & r_{jj}+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

$$
r_j = \quad 0.r_{00}+1 \quad r_{11}+1 \quad r_{22}+1 \quad \cdots \quad r_{jj}+1 \quad \cdots
$$

实数的不可数性

$$
\begin{array}{c|lllllll}
r_0 & 0.r_{00} & r_{01} & r_{02} & \cdots & r_{0j} & \cdots \\
r_1 & 0.r_{10} & r_{11} & r_{12} & \cdots & r_{1j} & \cdots \\
r_2 & 0.r_{20} & r_{21} & r_{22} & \cdots & r_{2j} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
r_j & 0.r_{00}+1 & r_{11}+1 & r_{22}+1 & \cdots & r_{jj}+1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

$$
\begin{array}{llllllll}
r_j = & 0.r_{00}+1 & r_{11}+1 & r_{22}+1 & \cdots & r_{jj}+1 & \cdots \\
r_j = & 0.r_{j0} & r_{j1} & r_{j2} & \cdots & r_{jj} & \cdots
\end{array}
$$

幂集的基数

实数集合的基数是自然数的幂集的基数.

$$|\mathbf{R}| = |2^{\mathbf{N}}| = |\{f : \mathbf{N} \to \{0,1\}\}|.$$

幂集的基数

实数集合的基数是自然数的幂集的基数.

$$|\mathbf{R}| = |2^{\mathbf{N}}| = |\{f : \mathbf{N} \to \{0, 1\}\}|.$$

结论. 自然数的幂集基数严格大于自然数的基数.

幂集的基数

实数集合的基数是自然数的幂集的基数.

$$|\mathbf{R}| = |2^{\mathbf{N}}| = |\{f : \mathbf{N} \to \{0,1\}\}|.$$

结论. 自然数的幂集基数严格大于自然数的基数.
推广结论为:
定理. 任何集合的幂集的基数严格大于该集合的基数. 即任给集合A,

$$|\mathcal{P}(A)| > |A|.$$

幂集的基数

定理. $|\mathcal{P}(A)| > |A|$.
证明: 反证法. 假设存在A到$\mathcal{P}(A)$的双射f. 定义集合

$$D = \{a \in A : a \notin f(a)\}.$$

则$D \subseteq A$. 由于f是映上的, 存在一个A中的元素x使得

$$f(x) = D.$$

问$x \in D$?

幂集的基数

定理. $|\mathcal{P}(A)| > |A|$.
证明: 反证法. 假设存在A到$\mathcal{P}(A)$的双射f. 定义集合

$$D = \{a \in A : a \notin f(a)\}.$$

则$D \subseteq A$. 由于f是映上的, 存在一个A中的元素x使得

$$f(x) = D.$$

问$x \in D$?
若$x \in D$, 则$x \notin f(x) = D$, 即$x \notin D$;
若$x \notin D$, 即$x \notin f(x)$, 则$x \in D$.

无穷的不可掌握性

实数的基数记为$2^{\aleph_0}$, 可以是任何大于$\aleph_0$的基数.
平面几何中唯一的涉及无穷的公理是平行公理:
两条平行线不会相交.
非欧几何: 两条平行线在无穷远处相交, 或者相距无穷远.

自然数

$$\omega = \{0, 1, 2, ...\}.$$

自然数可以由一个常元0和一个函数符号s表示:

$$\begin{aligned}
0 &= s^0(0) = 0;\\
1 &= s(0) = s^1(0);\\
2 &= s(1) = s(s(0));\\
3 &= s(2) = s(s(s(0)));\\
n+1 &= s(n) = \overbrace{s(s\cdots(s(0))\cdots)}^{n+1\text{-个 } s}.
\end{aligned}$$

自然数的表示2

自然数可以由空集$\emptyset$表示:

$$
\begin{aligned}
0 &= \emptyset; \\
1 &= \{\emptyset\}; \\
2 &= \{\emptyset, 1\} = \{\emptyset, \{\emptyset\}\}; \\
3 &= \{\emptyset, 2\} = \{\emptyset, \{\emptyset, \{\emptyset\}\}\}; \\
n+1 &= \{\emptyset, n\} = \overbrace{\{\emptyset, \{\emptyset, \cdots \{\emptyset, \{\emptyset\}\} \cdots\}\}}^{(n+1)\text{-个 }\}}.
\end{aligned}
$$

自然数上一般归纳原理

公理: 假定P是自然数上一个谓词. 则
如果$P(0)$
且对所有的i, $P(i)$ 蕴涵$P(i+1)$,
则$P(n)$对所有的n 成立.

例子

证明: 对任何自然数n, $1+2+\cdots+n=\dfrac{n(n+1)}{2}$.

$P(0)$: 左边=0=右边;

假定$P(i)$: $1+2+\cdots+i=\dfrac{i(i+1)}{2}$. 则

$$
\begin{aligned}
1+2+\cdots+i+(i+1) &= \frac{i(i+1)}{2}+(i+1) \\
&= \frac{(i+1)}{2}(i+2) \\
&= \frac{(i+1)(i+2)}{2}.
\end{aligned}
$$

自然数上的完全归纳原理

公理: 假定P是自然数上一个谓词. 则
如果对每个自然数n,
假定$P(i)$对所有的$i < n$, 我们能证明$P(n)$,
则$P(n)$对所有的n成立.

字典序归纳原理

定义. 自然数序对上的字典序定义如下: $(m, n) \le (m', n')$当且仅当或者$m < m'$ 或者$m = m'$且$n \le n'$.

公理: 假设P是自然数上一个谓词.

如果对每个自然数序对(m, n),

假定$P(m', n')$对所有的$(m', n') < (m, n)$, 我们能证明$P(m, n)$,

则$P(m, n)$对所有的m, n成立.

结构归纳法

结构归纳定义
结构归纳证明
计算机科学的哲学基础是分析哲学.

下载

文件名	:	$L13 \star .pdf$
文件名(打印用)	:	$L13 \star a.pdf$
email	:	$yfsui@ict.ac.cn$
		$yuefeisui@sina.com$, 密码：123456
电话	:	62600538, 13911230027
办公室	:	计算所538房间