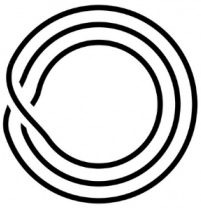

INFORMAL NOTES ON MATHEMATICS
2021.08.04

一个友好的布尔代数简介

数学

7月前

Yuanjue Chou 1楼 2021年8月4日

本文假设读者有初中的理解能力，主要受众为中学生及部分低年级本科生；本文力求通俗易懂，有不严谨之处请加以指正。

开了个大坑，讲的东西比较简单。写这玩意是源头是看一篇文章将topos的对偶logos与Boolean algebra的对偶Stone space放在一张表格里比对，后来又在彭柯尧老师的推荐下看了一点Heyting algebra，于是想写点东西科普一下。本来是打算作为@Geek学院 的一个沙龙，但太初等的话讲不完，直接讲我想讲的不是很多人能听——毕竟布尔代数很少有人专门去看，所以决定还是在论坛上写一点。目前打算还是从零开始慢慢讲，但实在太elementary了，我已经快写不下去哩

本帖不介意插楼

Il nous montre une correspondance subtile et fine, comme venue du vide.

Yuanjue Chou 2楼 2021年8月4日

1.简介

让我们从二猫同学很久之前的一个问题开始：

> 布尔代数是计算机概念，不是数学内容吧

这是一种常见的错觉（也许）。我们现在先来大致了解什么是布尔代数：

布尔代数是只有句义连词（sentential connectives）的双值逻辑的代数，也可以说是集合的并和补下的代数（此处代数指一种代数结构）。这个概念在逻辑学、集合论、拓扑学、测度论（可见 P. Halmos, *Measure Theory*）和环论（布尔环）中都有根源和应用。

布尔代数的理论是由英国数学家 George Boole 在 1847 年创立的。他把它设想为一种适合于逻辑分析的“算术”。他的“算术”的形式与 1864~1895 年期间出现的现代版本相当不同（见诸 Boole’s Algebra Isn’t Boolean Algebra）。

某种意思上说，布尔代数可以说存在感既低又不低。学计科的同学可能对此概念比较熟悉；在计科中的运用不予介绍。这里的“存在感既低又不低”是针对数学壬来说的。想必诸位在学抽象代数时见过该概念：通常作为环/代数的一个 Example。大家对此的认知往往停留在“哦，是一种环/代数，其上的运算是逻辑运算”，或者知道“集合的交并补构成布尔代数”，然而仅此而已了。这篇文章旨在告诉这些同学——当然也包括二猫，布尔代数比诸君想象的更“复杂”。例如以下定义：

> 定义1.1
>
> 布尔代数是一个满足排中律的 Heyting 代数 H.
>
> 这意味着
>
> $$\neg\neg = \mathrm{id} : H \to H$$
>
> ；或等价地说
>
> $$\forall_{x\in H}\ x \vee \neg x = \top$$
>
> ⌃⌃

至于何为 Heyting 代数，我们会在这篇极长的文章末尾再次与它见面。

本文假设读者有相对扎实的集合论及逻辑基础，同时希望读者掌握一定的抽象代数、拓扑及范畴论等基础，但这并非必要——需要时我们会单独列出一节介绍。本文的目标暂定为讲到 Stone space 及 Stone duality，可能在结尾处讲一些 Heyting algebra。本文主要参考书籍为 P.Halmos, *Lectures on Boolean Algebras*, 一本简短的小册子，有兴趣者可以看看。

标题处标有 * 号的章节有基础者可自行选择跳过，标有 $^\top$ 号的章节不是需要掌握的内容，可能是我一时兴起写的，可以跳过或另找时间阅读。

Il nous montre une correspondance subtile et fine, comme venue du vide.

Yuanjue Chou 3楼 2021年8月4日

2^*.一点群、环、格

注： 本节写的很敷衍，只是供读者了解目前需要了解的概念的名目，具体详细的学习请参考专门的抽象代数教材。一个典型的例子是 T.Hungerford, *Algebra*，虽然为研究生教材但并非非常难读；看 Hungerford 吃力的同学可以看 T.Feil, *A First Course in Algebra*，简单到不行；还有其它经典教材不再列举。

假设 S 是一个非空集，那么 S 上的二元运算就是一个函数 $S\times S=\{(s,t):s,t\in S\}$ 。对于二元运算下的 (a,b) 的像，有几种常用的符号： ab（乘法符号）、$a+b$（加法符号）、$a-b$ 、$a*b$ 等。为方便起见，我们在本节中通常使用乘法符号，并将 ab 称为 a 和 b 的积（部分书中常用 $a\circ b$ 指代二元运算）。由此我们可以定义一些熟悉的代数结构。

定义2.1

一个半群是指一个非空集合 G 及 G 上满足

(i) $a(bc)=(ab)c\ (\text{for all } a,b,c\in G)$ 的一个二元运算。如果一个半群 G 包含有一个

(ii) (双侧) 幺元素 $e\in G$, 使得 $ae=ea=a\ (\text{for all } a\in G)$, 且

(iii) 存在 (双侧) 逆元素 $a^{-1}\in G\ (\text{for all } a\in G)$, 使得 $a^{-1}a=aa^{-1}=e$

便称 G 是一个群。半群 G 的二元运算如果满足

(iv) $ab=ba\ (\text{for all } a,b\in G)$, 便称 G 为交换半群或者 Abel 半群。

定义2.2（群的一摊东西）

(i) 群同态的定义（自己找吧）

(ii) 假设 $f:G\to H$ 为群同态， $\mathrm{Ker}f:=\{a\in G\mid f(a)=e\in H\}$ ，称为 f 的核；
$\mathrm{Im}f:=\{b\in H\mid b=f(a),$
$\text{for some } a\in G\}$
，称为 f 的像。

(iii) 假设 G 是群， H 是它的非空子集并且对于 G 中的乘积运算封闭。如果 H 本身对于 G 中这个乘积运算是群，则称 H 为 G 的子群，并且表示成 $H<G$ 。对于每个 $a\in G$ ，定义 $\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\}$ ，则 $\langle a\rangle$ 为 G 的一个子群，称之为由 a 生成的循环子群。

(iv) H 是群 G 的子群，对于某一 $g\in G$ ， $\{gh\mid \text{for all } h\in H\}$ 表示 H 的一个左陪集，记作 gH ; $\{hg\mid \text{for all } h\in H\}$ 表示 H 的一个右陪集，记作 Hg 。

(v) 若 N 为 G 的一个子群，N 在 G 中的每个左陪集均为 N 在 G 中的右陪集，则称 N 是 G 的正规子群，写作 $N \lhd G$ 。

(vi) 若 N 为 G 的正规子群，G/N 为 N 在 G 中所有 (左) 陪集构成的集合，称之为 G 对于 N 的商群，其上群运算为 $(aN)(bN) = abN$ 。

现在很快（强行）来到了环。群的许多定理完全没有提及，譬如群同态三大定理、群同构定理等，并且定义也只是需要了解的最少的量，所以只是简单地了解一下，后期酌情补充。环的很多概念与群相似，不再多做介绍，因为我实在没有劲写了。

定义2.3

一个环 R 是一个集合，其上定义了两个二元运算，即加法 $(+)$ 和乘法 $(\cdot)$ （注意此处加法和乘法不一定是我们熟知的数之间的加和乘）满足以下属性：$(a, b, c \in R)$

(i) $a + b = b + a$

(ii) $(a + b) + c = a + (b + c)$

(iii) 存在一个元素 $0 \in R$ 使得 $a + 0 = a$

(iv) 存在一个元素 $x \in R$ 使得 $a + x = 0$ for all $a \in R$

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(vi)
$a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a$
$= b \cdot a + c \cdot a$

可以注意到，加法的结合律、交换律、幺元和逆的存在性，乘法的结合律和分配律必须成立：这称为环的公理。可以发现，乘法的交换法则不需要在任意环中成立；如果它成立，该环就被称为是交换环。此外，一个环并不总是需要有一个乘法幺元，即存在 $e \in R$ 使得 $a \cdot e \left(\text{or } e \cdot a\right) = a$；如果它有，则其被称为有单位的环 (ring with unit)。

环的理想及商环的定义与群的某些概念相似，请自行了解；该概念会在后续文章中经常使用。

若一个交换环 F ，其上增加二元运算除法，使得所有 $a \in R - \{0\}$ 可以作除法运算，即每个非零的元素都有乘法逆元，则称其为域，在此不多做赘述。

定义2.4

一个格是一个*偏序集*，允许所有有限 meets 及 joins。

（若将一个偏序集看做一个 $(0,1)$ -范畴，则其为一个偏序集允许所有有限积 (product) 和余积 (coproduct)。）

格也以后再细讲罢。。。马上我们进入布尔代数的正式内容。

Il nous montre une correspondance subtile et fine, comme venue du vide.

Yuanjue Chou 4楼 2021年8月4日

3.布尔环及布尔代数

让我们先回顾一下环。

除了我们熟知的整数环，还有许多其他环的例子。其中最平凡的情况是只有一个元素 0 所构成的环；这就是所谓的退化环。最简单的有单位的非退化环只有两个元素：0 和 1。加法和乘法的运算由以下算术表描述：

$+$	0	1
0	0	1
1	1	0

and

$\cdot$	0	1
0	0	0
1	0	1

观察表格，可以发现这个环有一些特殊的性质，我们关注的是： $p \cdot p = p$

满足这个条件的元素称之为幂等的 (idempotent)。若一个环中所有元素皆幂等，则称该环也幂等。现在我们来看布尔环最常见的定义：

定义3.1

若一个有单位的环是幂等的，则称之为布尔环。（实际上有单位的条件并非必要，每个无单位的布尔环皆可拓展为一个有单位的布尔环，试证明（该结论由 M. H. Stone 证明）。）

布尔环定义中的幂等条件对这类环的结构有相当强的影响。它的两个有趣的结论是：一个布尔环内元素总是满足 $p + p = 0$；且一个布尔环总是可交换的。（为什么？）

现在让我们看另一个布尔环的例子：

例子3.2

考虑一个集合 R，其元素为四个有序对： $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$. 这个集合我们记为 2^2 （类似于 $\mathbb{R}^2$ ）。我们定义 2^2 上有序对的加法及乘法如下：

$$
\begin{aligned}
&(p_0, p_1) + (q_0, q_1) \\
&= (p_0 + q_0, p_1 + q_1), (p_0, p_1) \\
&\cdot (q_0, q_1) = (p_0 \cdot q_0, p_1 \cdot q_1)
\end{aligned}
$$

那么其上的 0 和 1 (e ，即单位) 分别为 $(0,0)$ 和 $(1,1)$ 。易得 R （更严谨地， $(R,+,\cdot)$ ）为布尔环。

（试用同样的方法定义 2^n ，并说明它是布尔环）

另一个常见的例子来源于 P. Halmos, *Measure Theory*:

例子3.3 (P. Halmos)

考虑一个集合的类 R ，使得如果 $E \in R, F \in R$ ，那么 $E \cup F \in R$ 且 $E - F \in R$.

有些同学第一次看这个例子可能比较迷惑，但请注意，如果我们将集合的差记作“ $+$ ”，将集合的并记作“ $\cdot$ ”，这就又回到我们熟悉的形式。我们可以注意到：
$0 := \emptyset = E + E\,(E - E)$ ， $E = E \cdot E\,(E \cup E)$ 。（那么环上的 1 是什么？）

例子3.4

取任意集合 X ， 2^X 表示所有函数 $f : X \to 2$ 所构成的集合。

试定义 2^X 上的加法和乘法，并指出该定义下的 0 和 1 ，使其能成为一个布尔环。（若 $X = \emptyset$ ，你将得到什么？）

现在我们来看看布尔代数。

设 X 是任意集合， $\mathcal{P}(X)$ 是 X 的所有子集的类(X 的幂集)。 $\mathcal{P}(X)$ 上的三种集合运算是二元运算并 $\cup$ 和交 $\cap$ ，以及一元运算补 ^{c} 。关于这三种运算的法则，请拿出任意一本集合论教材，翻开，我们马上就会用到。

我们先来定义一下布尔代数

定义3.5

布尔代数是一个非空集 A ，连同两个二元运算 $\vee$ 和 $\wedge$ (在 A 上)，一个一元运算 $'$ ，以及两个元素 0 和 1，满足下列公理：

$$
\begin{aligned}
0' &= 1, & 1' &= 0 \\
p \wedge 0 &= 0, & p \vee 1 &= 1 \\
p \wedge 1 &= p, & p \vee 0 &= p \\
p \wedge p' &= 0, & p \vee p' &= 1 \\
(p')' &= p, & & \\
p \wedge p &= p, & p \vee p &= p, \\
(p \wedge q)' &= p' \vee q', & (p \vee q)' &= p' \wedge q' \\
p \wedge q &= q \wedge p, & p \vee q &= q \vee p, \\
p \wedge (q \wedge r) &= (p \wedge q) \wedge r, & p \vee (q \vee r) &= (p \vee q) \vee r, \\
p \wedge (q \vee r) &= (p \wedge q) \vee (p \wedge r), & p \vee (q \wedge r) &= (p \vee q) \wedge (p \vee r)
\end{aligned}
$$

试对照你的集合论教材，将其与集合的运算法则一一对应。

上方的运算 $\vee, \wedge$ 和 $'$，我们将其分别称为 meet、join 和补（我们在第二节“格”处也见过，以后我们会了解格及布尔代数的关系）。

meet 和 join 的乘法表为

$\vee$	0	1
0	0	1
1	1	1

and

$\wedge$	0	1
0	0	0
1	0	1

并且补为 $0 \mapsto 1$ 的一元运算。我们应当很快发现，该代数和二元布尔环是相互定义的。为此，我们可以用同样的符号 2 来表示这两种结构。布尔代数与布尔环的理论有着非常密切的联系，或者不如说，它们只是看待同一学科的不同方式。更确切地说，每一个布尔代数都可以通过定义适当的加法和乘法运算变成一个布尔环；反之，每一个布尔代数都可以通过定义适当的 meet, join 和补运算变成一个布尔代数。

通过比较 X 的所有子集构成的布尔代数 $\mathcal{P}(X)$ 和 X 上所有二元函数的布尔环 2^X，可以阐明这一点，X 的每个子集 $P_i \in \mathcal{P}(X)$ 都与一个函数 $p_i : X \to 2$ 自然地关联（此处 i 并非指标，只是为了方便辨识），即 P_i 的特征函数：

$$
p_i(x) = \begin{cases} 1 & \text{if } x \in P \\ 0 & \text{if } x \notin P \end{cases}
$$

这应当同样解决了部分同学学数分时的一个疑惑：为什么可以把 X 的幂集 $\mathcal{P}(X)$ 写作 2^X。这不完全是所谓记号上的约定俗成，而是存在双射 $\mathcal{P}(x) \xrightarrow{\cong} 2^X,\ P_i \mapsto p_i(x)$。

由此我们定义

$$
\begin{aligned}
(p+q)(x) &= p(x)+q(x) \\
&= \begin{cases} 1 & \text{if } p(x) \neq q(x), \\ 0 & \text{if } p(x) = q(x) \end{cases}
\end{aligned}
$$

和

$$
\begin{aligned}
(p \cdot q)(x) &= p(x) \cdot q(x) \\
&= \begin{cases} 1 & \text{if } p(x) = q(x) = 1, \\ 0 & \text{otherwise} \end{cases}
\end{aligned}
$$

若 $p(x)$ 和 $q(x)$ 的值不同，仅当其中一个是 1 而另一个是 0，也就是说，仅当 $x \in P, x \notin Q$ ，反之亦然。若 $p(x)$ 和 $q(x)$ 均为 1，则恰好 $x \in P, x \in Q$ 。观察可得 $\mathcal{P}(X)$ 上的环加法及乘法：

$$
\begin{aligned}
P + Q = (P \cap Q^c) \cup (P^c \cap Q) \quad &\text{and} \\
P \cdot Q = P \cap Q &
\end{aligned}
$$

（这里的加法即所谓的对称差），同样可得 $0 = \emptyset$ 且 $1 = X$ 。
（回顾例子 3.3，试着用类似的方法定义布尔代数）

同样，每个布尔环都可以转化为具有相同 0 和单位的布尔代数，只需定义 meet, join 和补运算如下：

$$
\begin{aligned}
p \vee q = p + q + p \cdot q, \quad p \wedge q = p \cdot q, \\
p' = p + 1
\end{aligned}
$$

（为什么？）

本节最后，对逻辑比较熟悉的同学想必感觉到了布尔代数与逻辑的关系，可以试着将定义 3.5 中的公理用一阶逻辑重写一遍；与逻辑的关系还可见这个视频 A Quick View of Bool. Alg.，十几分钟，茶都没凉（雾）就能看完哩。

Il nous montre une correspondance subtile et fine, comme venue du vide.