简单的逻辑和朴素集合论

AUGPath

2022 年 11 月 14 日

1 数理逻辑

1.1 命题

从高中开始, 我们似乎就开始处理各种各样的命题. 下面我们加一层抽象, 这样, 我们就可以把一些繁琐的内容交给计算机完成, 并且在探索的过程中对 “什么是有效的推理” 有一个更深的理解.

定义 1.1 (命题 (Proposition))**.** **命题**是可以判定真假的陈述句 (不可既真又假).

1.2 命题逻辑

1.2.1 命题逻辑的语言

所以, 要完成这项任务, 第一步就是尽可能地形式化的描述一下这些一直在用的语言.

定义 1.2 (命题逻辑的语言)**.** 命题逻辑的语言有且仅有如下的内容构成:

- 任意多的命题符号
- 5 个逻辑连接词 (见下表1.2.1)
- 左括号, 右括号

定义 1.3 (公式)**.** 如果一个串是公式, 那么:

- 每个命题符号都是公式;

符号	名称	英文读法	中文读法	LaTeX
$\neg$	negation(否定)	not	非	`\lnot`
$\wedge$	conjunction(合取)	and	与	`\land`
$\vee$	disjunction(析取)	or	或	`\lor`
$\rightarrow$	conditional	implies(if then)	蕴含 (如果, 那么)	`\to`
$\leftrightarrow$	biconditional	if and only if	当且仅当	`\leftrightarrow`

- 如果 α 和 β 都是公式, 则 $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \to \beta)$ 和 $(\alpha \leftrightarrow \beta)$ 也是公式;
- 除此之外, 别无其它.

这里出现了很类似定义自然数的定义方法, 一个很自然的想法是我们能不能在这里运用数学归纳法. 答案是可以的. 我们称作 “归纳原理”.

定理 1.1 (归纳原理)**.** 令 $P(\alpha)$ 为一个关于公式的性质. 假设

- 对所有的命题符号 A_i, 性质 $P(A_i)$ 成立; 并且
- 对所有的公式 α 和 β, 如果 $P(\alpha)$ 和 $P(\beta)$ 成立, 则 $P((\neg\alpha))$, $P((\alpha * \beta))$ 也成立,

那么 $P(\alpha)$ 对所有的公式 α 都成立.

> **思考题**
>
> 数学归纳法可以在正整数上使用, 但是不能再 $\mathbb{R}$ 上使用, 却可以在上面定义的结构中使用, 为什么? 什么样的结构可以运用数学归纳法?

规定了符号, 就一定要有对应的运算规律. 因此, 我们就给出如下定义, 和高中的内容类似.

定义 1.4 (命题符号的运算规则)**.** 一般地, 命题记号遵循如下的运算规则:

- 最外层的括号可以省略
- 优先级: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$
- 结合性: 右结合 $(\alpha \wedge \beta \wedge \gamma,\ \alpha \to \beta \to \gamma)$

有了命题, 我们很多时候希望 “假定” 这些命题的真假, 来考察最终结论的真假, 或者从中找到一点规律. 这样做其实有一个更专业的名字叫 “真值指派”.

定义 1.5 (真值指派 (v))**.** 令 S 为一个命题符号的集合. S 上的一个**真值指派** v 是一个从 S 到真假值的映射

$$v : S \to \{T, F\}.$$

如果对于只能指派一个的话太局限了, 我们不妨把所有可能的情况都枚举一遍映射过去. 也就是真值指派的 “扩张”.

定义 1.6 (真值指派的扩张 $(\overline{v})$)**.** 令 S 为一个命题符号的集合. 令 $\overline{S}$ 为只含有 S 中命题符号的公式集.

S 上的**真值指派** v **的扩张**是一个从 $\overline{S}$ 到真假值的映射

$$\overline{v} : \overline{S} \to \{T, F\}.$$

定义 1.7 (满足 (Satisfy))**.** 如果 $\overline{v}(\alpha) = T$, 则称真值指派 v **满足**公式 α.

很多时候一些逻辑表达式看上去就是废话. 比如 “如果我后天知道了考试的成绩, 那我明天就知道了”. 数学上面对这类问题有一个定义叫做 “重言蕴含”.

定义 1.8 (重言蕴含 (Tautologically Implies))**.** 设 Σ 为一个公式集.

Σ **重言蕴含**公式 α, 记为 $\Sigma \models \alpha$,

如果每个满足 Σ 中所有公式的真值指派都满足 α.

定义 1.9 (重言式/永真式 (Tautology))**.** 如果 $\emptyset \models \alpha$, 则称 α 为**重言式**, 记为 $\models \alpha$.

反之, 就是永远都不能成立的矛盾的形式.

定义 1.10 (矛盾式/永假式 (Contradiction))**.** 若公式 α 在所有真值指派下均为假, 则称 α 为**矛盾式**.

定义 1.11 (重言等价 (Tautologically Equivalent))**.** 如果 $\alpha \models \beta$ 且 $\beta \models \alpha$, 则称 α 与 β **重言等价**, 记为 $\alpha \equiv \beta$.

1.2.2 命题逻辑的运算律

上面我们发现了有很多的废话, 但是, 有时候 "废话" 并不是显然的. 这就需要一些推理规律来帮助我们联通看上去毫不相干的逻辑符号.

命题 1.1. (逻辑的运算律)

- 交换律:

$$(A \wedge B) \leftrightarrow (B \wedge A)$$

$$(A \vee B) \leftrightarrow (B \vee A)$$

- 结合律:

$$((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$$

$$((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$$

- 分配律:

$$(A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$$

$$(A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$$

- De Morgan 律:

$$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$$

$$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$$

- 双重否定律:

$$\neg\neg A \leftrightarrow A$$

- 排中律:

$$A \vee (\neg A)$$

- 矛盾律:

$$\neg(A \wedge \neg A)$$

- 逆否命题:

$$(A \to B) \leftrightarrow (\neg B \to \neg A)$$

那么, 这些内容化简到最后有没有一个目标呢? 其实是有的. 任何一个命题都可以写成 “合取范式 (CNF)” 或者 “析取范式” 的形式. 下面给出定义.

定义 1.12 (合取范式 (Conjunctive Normal Form))**.** 我们称公式 α 是**合取范式**, 如果它形如

$$\alpha = \beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_k,$$

其中, 每个 β_i 都形如

$$\beta_i = \beta_{i1} \vee \beta_{i2} \vee \cdots \vee \beta_{in},$$

并且 β_{ij} 或是一个命题符号, 或者命题符号的否定.

定义 1.13 (析取范式 (Disjunctive Normal Form))**.** 我们称公式 α 是**析取范式**, 如果它形如

$$\alpha = \beta_1 \vee \beta_2 \vee \cdots \vee \beta_k,$$

其中, 每个 β_i 都形如

$$\beta_i = \beta_{i1} \wedge \beta_{i2} \wedge \cdots \wedge \beta_{in},$$

并且 β_{ij} 或是一个命题符号, 或者命题符号的否定.

> **思考题**
>
> 根据上述的演算的规则, 有没有一种操作方法, 应该怎样把一个命题化作一个 CNF 或者 BNF?

1.2.3 命题逻辑的演算

命题逻辑的演算有时候也可以帮助我们理解命题之间的等价关系.

引入假设.

$$\frac{}{[x : P]} \quad \texttt{(assumption)}$$

所有引入的假设最终必须被 “**释放**” (discharged) 所谓释放, 其实就是在使用假设 α 作为假设的前提下推出了 β, 最后要写成 $\alpha \to \beta$ 的形式. 这就是假设的释放.

“$\wedge$” 推理规则.

$$\frac{P \qquad Q}{P \wedge Q} \quad \wedge\texttt{-intro}$$

$$\frac{P \wedge Q}{P} \quad \wedge\texttt{-elim-left}$$

$$\frac{P \wedge Q}{Q} \quad \wedge\texttt{-elim-right}$$

下面这条规则描述了双重否定的性质.

“$\neg\neg$” 推理规则.

$$\frac{\alpha}{\neg\neg\alpha}\neg\neg\texttt{-intro}$$

$$\frac{\neg\neg\alpha}{\alpha}\neg\neg\texttt{-elem}$$

“$\rightarrow$” 推理规则.

$$\frac{\alpha\rightarrow\beta \qquad \alpha}{\beta} \quad \rightarrow\texttt{-elim (modus ponens)}$$

$$\frac{\alpha\rightarrow\beta \qquad \neg\beta}{\neg\alpha}\texttt{modus tollens}$$

$$\begin{array}{c}[x:\alpha]\\ \vdots\\ \beta\end{array}$$

$$\frac{\beta}{\alpha\rightarrow\beta} \quad \rightarrow\texttt{-intro}/x$$

`Assumption` x `is discharged`

$\vee$ 推理规则.

$$\frac{\alpha}{\alpha\vee\beta} \quad \vee\texttt{-intro-left}$$

$$\frac{\alpha\vee\beta \qquad \alpha\rightarrow\gamma \qquad \beta\rightarrow\gamma}{\gamma} \quad \vee\texttt{-elim; (分情况分析)}$$

$\perp$ 推理规则.

$$\frac{\alpha \qquad \neg\alpha}{\perp} \quad \perp\texttt{-intro}$$

$$\frac{\perp}{\alpha} \quad \perp\texttt{-elim(Principle of Explosion)};$$

“$\neg$”. 推理规则

$$\frac{\alpha\rightarrow\perp}{\neg\alpha} \quad \neg\texttt{-intro}\frac{\neg\alpha}{\alpha\rightarrow\perp} \quad \neg\texttt{-elim}$$

定理 1.2 (命题逻辑的可靠性 (Soundness))**.** 如果 $\Sigma\vdash\alpha$, 则 $\Sigma\models\alpha$.

定理 1.3 (命题逻辑的完备性 (Completeness))**.** 如果 $\Sigma\models\alpha$, 则 $\Sigma\vdash\alpha$.

1.3 谓词逻辑

我们发现命题逻辑无法表达部分与整体的关系.

1.3.1 谓词逻辑的语法

定义 1.14 (谓词逻辑的构成).

逻辑联词: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

量词符号: $\forall$ (forall; 全称量词), $\exists$ (exists; 存在量词)

变元符号: $x, y, z, \ldots$

左右括号: $(,)$

常数符号: 零个或多个常数符号 $a, b, c, \ldots$, 表达特殊的个体

函数符号: n-元函数符号 $f, g, h, \ldots$ $(n \in \mathbb{N}^+)$, 表达个体上的运算

谓词符号: n-元谓词符号 $P, Q, R, \ldots$ $(n \in \mathbb{N})$, 表达个体的性质与关系

定义 1.15 (项 (Term)).

1. 每个变元 $x, y, z, \ldots$ 都是一个项;
2. 每个常数符号都是一个项;
3. 如果 $t_1, t_2, \ldots, t_n$ 是项, 且 f 为一个 n-元函数符号,
   则 $f(t_1, t_2, \ldots, t_n)$ 也是项;
4. 除此之外, 别无其它.

定义 1.16 (公式 (Formula)).

- 如果 $t_1, \ldots, t_n$ 是项, 且 P 是一个 n 元谓词符号,
  则 $P(t_1, \ldots, t_n)$ 为公式, 称为**原子公式**;
- 如果 α 与 β 都是公式, 则 $(\neg\alpha)$ 与 $(\alpha * \beta)$ 都是公式;
- 如果 α 是公式, 则 $\forall x.\ \alpha$ 与 $\exists x.\ \alpha$ 也是公式;
- 除此之外, 别无其它.

举个例子:

- 0 不是任何自然数的后继

$$\forall x.\ \neg(Sx = 0)$$

- 两个自然数相等当且仅当它们的后继相等

$$\forall x.\ \forall y.\ (x = y \leftrightarrow Sx = Sy)$$

- x 是素数 ($x > 1$ 且 x 没有除自身和 1 之外的因子)

$$\mathrm{Prime}(x) : S0 < x \wedge \forall y.\ \forall z.\ (y < x \wedge z < x) \rightarrow \neg(y \times z = x)$$

- 哥德巴赫猜想 (任一大于 2 的偶数, 都可表示成两个素数之和)

$$\forall x.\ (SS0 < 2 \wedge (\exists y.\ 2 \times y = x)) \rightarrow$$
$$(\exists x_1.\ \exists x_2.\ \mathrm{Prime}(x_1) \wedge \mathrm{Prime}(x_2) \wedge x_1 + x_2 = x)$$

定义 1.17 (作用域 (Scope)、约束变元 (Bind)、自由变元 (Free))**.** [(1)]

1. $\forall x.\ (P(x) \to Q(x))$
2. $(\forall x.\ P(x)) \to Q(x)$
3. $\forall x.\ \Big(P(x) \to \big(\exists y.\ R(x,y)\big)\Big)$
4. $\Big(\forall x.\ \forall y.\ \big(P(x,y) \land Q(y,z)\big)\Big) \land \exists x.\ P(x,y)$

定义 1.18 (改名 (Rename))**.** 为尽量避免重名, 可将约束变元或自由变元改名为新鲜 (fresh)变元

定义 1.19 (t is free for x in α)**.**

$$y - 1 \text{ is free for } x \text{ in } \exists z.\ (z < x)$$

$$y - 1 \text{ is } \textit{not} \text{ free for } x \text{ in } \exists y.\ (y < x)$$

在公式 α 中, 项 t 可以替换变量 x 写作 ($\alpha[t/x]$)

1.3.2 谓词逻辑的语义

在这里, 情况变复杂了. 我们需要考虑对象所处的数学空间来下结论. 也就是一个表达式的语义取决于:

- 对量词论域 (universe) 的解释, 限定个体范围
- 对常数符号、函数符号、谓词符号的解释
- 对自由变元的解释 (赋值函数 s)

也就是这种 "解释" 将公式映射到一个数学结构 $\mathcal{U}$ 上, 决定了该公式的语义.

定义 1.20 ($(\mathcal{U}, s) \models \alpha$)**.** $\mathcal{U}$ 与 s 满足公式 α:

$$(\mathcal{U}, s) \models \alpha$$

- 将 α 中的常数符号、函数符号、谓词符号按照结构 $\mathcal{U}$ 进行解释,
- 将量词的论域限制在集合 $|\mathcal{U}|$ 上,
- 将自由变元 x 解释为 $s(x)$,
- 这样就将公式 α 翻译成了某个数学领域中的命题,
- 然后, 使用数学领域知识我们知道该命题成立

例如,

$$\alpha : \forall x.\ (x \times x \neq 1 + 1)$$

在 α 在数学结构 $\mathcal{U} = \mathbb{Q}$ 中为真, 在数学结构 $\mathcal{U} = \mathbb{R}$ 中为假.

定义 1.21 (语义蕴含 (Logically Imply))**.** 令 Σ 为一个公式集, α 为一个公式.

Σ **语义蕴含** α, 记为 $\Sigma \models \alpha$, 如果每个满足 Σ 中所有公式的结构 $\mathcal{U}$ 与赋值 s都满足 α. 记作

$$\{\forall x.\ P(x)\} \models P(y)$$

举例: 假设有

$$\alpha : \forall x \forall y \forall z((P(x, y) \land P(y, z)) \to P(x, z))$$

$$\beta : \forall x \forall y((P(x, y) \land P(y, x)) \to x = y)$$

$$\gamma : \forall x \exists y P(x, y) \to \exists y \forall x P(x, y)$$

那么我们还不可以推断出 $\{\alpha, \beta\} \models \gamma$, 除非我们知道 $\mathcal{U} = \mathbb{N}$, $P(x, y) : x \leq y$.

定义 1.22 (语义等价 (Logically Equivalent))**.** 如果 $\alpha \models \beta$ 且 $\beta \models \alpha$, 则称 α 与 β **语义等价**, 记为 $\alpha \equiv \beta$.

例如: $\neg(\forall x.\ \alpha) \equiv \exists x.\ \neg\alpha$. 这就相当于命题逻辑中的 “重言式”, 可用于公式推导.

定义 1.23 (普遍有效的 (Valid))**.** 如果 $\emptyset \models \alpha$, 则称 α 是**普遍有效的**, 记为 $\models \alpha$.

普遍有效的公式在所有可能的结构 $\mathcal{U}$ 与所有可能的赋值 s下均为真.
下面来看几组普遍有效的公式:

定理 1.4. (普遍有效的公式)

$$\boxed{\neg\forall x\alpha \leftrightarrow \exists x\neg\alpha}$$

$$\boxed{\neg\exists x\alpha \leftrightarrow \forall x\neg\alpha}$$

$$\neg(\forall x \in A.\ \alpha) \leftrightarrow \exists x \in A.\ \neg\alpha$$

$$\forall x \forall y \alpha \leftrightarrow \forall y \forall x \alpha$$

$$\exists x \exists y \alpha \leftrightarrow \exists y \exists x \alpha$$

$$\forall x\alpha \land \forall x\beta \leftrightarrow \forall x(\alpha \land \beta)$$

$$\exists x\alpha \lor \exists x\beta \leftrightarrow \exists x(\alpha \lor \beta)$$

$$\forall x\alpha \to \exists x\alpha$$

$$\exists x \forall y \alpha \to \forall y \exists x \alpha$$

$$\forall x \alpha \vee \forall x \beta \to \forall x (\alpha \vee \beta)$$

$$\exists x (\alpha \wedge \beta) \to \exists x \alpha \wedge \exists x \beta$$

对于 β 不含 x:

$$\forall x.\ (\alpha \vee \beta) \leftrightarrow (\forall x.\ \alpha) \vee \beta$$

$$\forall x.\ (\alpha \wedge \beta) \leftrightarrow (\forall x.\ \alpha) \wedge \beta$$

$$\exists x.\ (\alpha \vee \beta) \leftrightarrow (\exists x.\ \alpha) \vee \beta$$

$$\exists x.\ (\alpha \wedge \beta) \leftrightarrow (\exists x.\ \alpha) \wedge \beta$$

注意这条公式不成立: $\forall y \exists x \alpha \not\to \exists x \forall y \alpha$. 我们有反例: $U = \{a, b\}$, 关系 $P(a,b), P(b,a)$, $\forall y \exists x P(y,x) \equiv T$ $\exists x \forall y P(y,x) \equiv F$.

1.3.3 谓词逻辑的推演

定理 1.5. ($\forall$-elim)

$$\frac{\forall x.\ \alpha}{\alpha[t/x]} \quad (\forall x\text{-elim})$$

where t is free for x in α

例子:

$$\forall x.\ P(x) \vdash P(c) \quad (c \text{ 是任意常元符号})$$

$$\forall x.\ \exists y.\ (x < y) \vdash \exists y.\ (z < y) \quad (z \neq y \text{ 是任意变元符号})$$

$$\forall x.\ \exists y.\ (x < y) \nvdash \exists y.\ (y < y) \quad (y \text{ is } \textit{not} \text{ free for } x \text{ in } \alpha)$$

定理 1.6.

$$\frac{\begin{array}{c}[t] \\ \vdots \\ \alpha[t/x]\end{array}}{\forall x.\ \alpha} \quad (\forall x\text{-intro})$$

where, t is a fresh variable

这个定理的意思是任取 t, 如果能证明 α 对 t 成立, 则 α 对所有 x 成立. 例如:

$$\Big\{P(t), \forall x(P(x) \to \neg Q(x))\Big\} \vdash \neg Q(t)$$

我们可以有如下的推理:

$$\begin{aligned} P(t) &\quad (\text{前提}) &(1)\\ \forall x.\,(P(x)\to\neg Q(x)) &\quad (\text{前提}) &(2)\\ P(t)\to\neg Q(t) &\quad (\forall\text{-elim},(2)) &(3)\\ \neg Q(t) &\quad (\to\text{-elim},(1),(3)) &(4) \end{aligned}$$

另一个例子:

$$\Big\{\forall x.\,(P(x)\to Q(x)),\forall x.\,P(x)\Big\}\vdash\forall x.\,Q(x)$$

$$\begin{aligned} \forall x.\,(P(x)\to Q(x)) &\quad (\text{前提}) &(1)\\ \forall x.\,P(x) &\quad (\text{前提}) &(2)\\ [x_0] &\quad (\text{引入变量}) &(3)\\ P(x_0)\to Q(x_0) &\quad (\forall\text{-elim},(1),(3)) &(4)\\ P(x_0) &\quad (\forall\text{-elim},(2),(3)) &(5)\\ Q(x_0) &\quad (\to\text{-elim},(4),(5)) &(6)\\ \forall x.\,Q(x) &\quad (\forall\text{-intro},(3)-(6)) &(7) \end{aligned}$$

定理 1.7 ($\exists$-intro)**.**

$$\frac{\alpha[t/x]}{\exists x.\,\alpha}\quad(\exists x\text{-intro})$$

where t is free for x in α

也就是说如果 α 对某个项 t 成立, 则 $\exists x.\,\alpha$ 成立. 也就是说我们有

$$P(c)\vdash\exists x.\,P(x)\quad c\text{ 是任意常元符号}$$

如果变量不是自由的, 那么就不能做这样的替换, 如下所示

$$\forall y.\,(y=y)\nvdash\exists x.\,\forall y.\,(x=y)\quad (y\text{ is }\textit{not}\text{ free for }x\text{ in }\alpha)$$

定理 1.8 ($\exists$-elim)**.**

$$\frac{\exists x.\,\alpha\qquad [x_0]\qquad \begin{matrix}[\alpha[x_0/x]]\\ \vdots\\ \beta\end{matrix}}{\beta}\quad(\exists\text{-elim})$$

where x_0 is free for x in α

这句话的意思是假设 x_0 使得 α 成立, 如果从 $\alpha[x_0/x]$ 可以推导出 β, 则从 $\exists x.\,\alpha$ 可以推导出 β. 看如下的例子:

$$\forall x.\,P(x)\vdash\exists x.\,P(x)$$

有如下的证明:

$$\forall x.\ P(x) \quad \text{(前提)} \tag{1}$$
$$[x_0] \quad \text{(引入变量)} \tag{2}$$
$$P(x_0) \quad (\forall\text{-elim}, (1), (2)) \tag{3}$$
$$\exists x.\ P(x) \quad (\exists\text{-intro}, (3)) \tag{4}$$

1.4 数学归纳法

定理 1.9 (第一数学归纳法 (The First Mathematical Induction))**.** 设 $P(n)$ 是关于自然数的一个性质. 如果

1. $P(0)$ 成立;
2. 对任意自然数 n, 如果 $P(n)$ 成立, 则 $P(n+1)$ 成立.

那么, $P(n)$ 对所有自然数 n 都成立.

翻译成形式化的方法, 也就是

$$\frac{P(0) \qquad \forall n \in \mathbb{N}.\ \Big(P(n) \to P(n+1)\Big)}{\forall n \in \mathbb{N}.\ P(n)} \quad \text{(第一数学归纳法)}$$

$$\Big(P(0) \wedge \forall n \in \mathbb{N}.\ \Big(P(n) \to P(n+1)\Big)\Big) \to \forall n \in \mathbb{N}.\ P(n).$$

定理 1.10 (第二数学归纳法 (The Second Mathematical Induction))**.** 设 $Q(n)$ 是关于自然数的一个性质. 如果

1. $Q(0)$ 成立;
2. 对任意自然数 n, 如果 $Q(0), Q(1), \ldots, Q(n)$ 都成立,
   则 $Q(n+1)$ 成立.

那么, $Q(n)$ 对所有自然数 n 都成立.

同样的, 翻译成形式化的表示形式, 也就是

$$\frac{Q(0) \ \ \forall n \in \mathbb{N}.\ \Big(\big(Q(0) \wedge \cdots \wedge Q(n)\big) \to Q(n+1)\Big)}{\forall n \in \mathbb{N}.\ Q(n)} \quad \text{(第二数学归纳法)}$$

$$\Big(Q(0) \wedge \forall n \in \mathbb{N}.\ \Big(\big(Q(0) \wedge \cdots \wedge Q(n)\big) \to Q(n+1)\Big)\Big) \to \forall n \in \mathbb{N}.\ Q(n).$$

定理 1.11 (数学归纳法)**.** 第一数学归纳法与第二数学归纳法等价.

第二数学归纳法也被称为**“强” (Strong)** 数学归纳法, 它强在可以使用的条件更多了. 我们可以来证明这件事情.

引理 1.1. 第一数学归纳法蕴含第二数学归纳法.

证明. 要证第二类数学归纳法,也即任给一个命题 F ,若满足 $F(1)$ 及 $(F(1)\wedge F(2)\wedge\cdots\wedge F(n))\Rightarrow F(n+1)$ ，则有 $\forall k\in\mathbb{N}.F(k)$. 那么，我们可以构造命题 $G(n):=F(1)\wedge F(2)\wedge\cdots\wedge F(n)$. 显然，$G(n)\Rightarrow F(n+1)$ ，又有 $G(n)\Rightarrow G(n)$ ，则 $G(n)\Rightarrow(F(n+1)\wedge G(n))$ ，而后者即为 $G(n+1)$. 故，命题 G 满足第一类数学归纳法的条件，所以 $\forall k\in\mathbb{N}$. $G(k)$ 成立. 而 $G(k)\Rightarrow F(k)$ ，故 $\forall k\in\mathbb{N}$. $F(k)$ ，也即第二类数学归纳法成立. □

引理 1.2. 第二数学归纳法蕴含第一数学归纳法.

证明. 要证第一类数学归纳法，也即任给一个命题 F ，若满足 $F(1)$ 及 $F(n)\to F(n+1)$ ，则有 $\forall k\in\mathbb{N}$. $F(k)$. 显然，F 是满足第二类数学归纳法的条件的 (因为 1 的条件比 2 强)，故根据第二类数学归纳法，$F(k)$ 对所有正整数 k 成立，也即第一类数学归纳法成立. □

数学归纳法的更深层次的结果是自然数的 Peano 公理. Peano 公理体系刻画了**自然数的递归结构**.

定义 1.24 (Peano Axioms)**.** 自然数的 Peano 公理有如下几条:

1. 0 是自然数;
2. 如果 n 是自然数, 则它的后继 $\mathbf{S}n$ 也是自然数;
3. 0 不是任何自然数的后继;
4. 两个自然数相等当且仅当它们的后继相等;
5. **数学归纳原理:** 如果
   (a) $P(0)$ 成立;
   (b) 对任意自然数 n, 如果 $P(n)$ 成立, 则 $P(n+1)$ 成立.

   那么, $P(n)$ 对所有自然数 n 都成立.

自然数集具有良序原理.

定义 1.25 (良序原理 (The Well-Ordering Principle))**.** 自然数集的任意非空子集都有一个最小元.

定理 1.12. 良序原理与 (第一) 数学归纳法等价.

引理 1.3. (第一) 数学归纳法蕴含良序原理.

证明. By mathematical induction on the size n of non-empty subsets of $\mathbb{N}$.

$$P(n):\text{All subsets of size } n \text{ contain a minimum.}$$

Inductive Hypothesis:

- Basis Step: $P(1)$

- Inductive Hypothesis: $P(n)$
- Inductive Step: $P(n) \to P(n+1)$
  - $A' \leftarrow A \setminus a$
  - $x \leftarrow \min A'$
  - Compare x with a

□

> **例子:**
>
> Of the 1000 islanders, it turns out that **100 of them have blue eyes** and **900 of them have brown eyes**, although the islanders are not initially aware of these statistics (each of them can of course only see 999 of the 1000 tribespeople).
>
> One day, a **blue-eyed foreigner** visits to the island and wins the complete trust of the tribe.
>
> One evening, he addresses the entire tribe to thank them for their hospitality.
>
> However, not knowing the customs, the foreigner makes the mistake of mentioning eye color in his address, remarking "**how unusual it is to see another blue-eyed person like myself in this region of the world**".
>
> **What effect, if anything, does this *faux pas* (失礼) have on the tribe?**

定理 1.13. Suppose that the tribe had $n > 0$ blue-eyed people.

Then n days after the traveller's address, all n blue-eyed people commit suicide.

证明.

基础步骤: $n = 1$.

这个**唯一的蓝眼人**的内心独白: **"你直接念我身份证吧"**

归纳假设: 有 n 个蓝眼人时, 前 $n-1$ 天无人自杀, 第 n 天集体自杀.

归纳步骤: 考虑恰有 $n+1$ 个蓝眼人的情况.

每个**蓝眼人**都如此推理: 我看到了 n 个蓝眼人, 他们应该在第 n 天集体自杀.

但是, 每个蓝眼人都在等其它 n 个蓝眼人自杀, 因此, 第 n 天无人自杀.

每个**蓝眼人**继续推理: 一定不止 n 个蓝眼人, 但是我看到的其余人都不是蓝眼.

所以, **"小丑竟是我自己"**. □

这就像是考虑 $n = 1, n = 2$ 的简单情况, 出现了类似 "我知道你知道我知道 ..." 的思维递归情形.

2 朴素集合论

2.1 公理体系

在中学的时候，我们定义的集合是如下的一个数学对象：集合就是任何一个有明确定义的对象的整体.

定义 2.1 (集合)**.** 我们将集合理解为任何将我们思想中那些确定而彼此独立的对象放在一起而形成的聚合.

这也引出了概括原则:

定理 2.1 (概括原则)**.** 对于任意性质/谓词 $P(x)$, 都存在一个集合 X:

$$X = \{x \mid P(x)\}$$

很多时候我们需要判别两个集合是不是相等, 那么我们有外延性原理:

定义 2.2 (外延性原理 (Extensionality))**.** 两个集合相等 $(A = B)$ 当且仅当它们包含相同的元素.

$$\forall A.\, \forall B.\, \Big(\big(\forall x.\, (x \in A \leftrightarrow x \in B)\big) \leftrightarrow A = B\Big)$$

这条公理意味着集合这个对象完全由它的元素决定.

有时候我们需要从一个集合里面抽出一部分, 也就是寻找一个集合的子集. 因此我们有如下的定义.

定义 2.3 (子集)**.** 设 A、B 是任意两个集合.

$A \subseteq B$ 表示 A 是 B 的子集 (subset):

$$A \subseteq B \iff \forall x \in A.\, (x \in A \to x \in B)$$

$A \subset B$ 表示 A 是 B 的真子集 (proper subset):

$$A \subset B \iff A \subseteq B \wedge A \neq B$$

我们还可以证明两个集合相等, 当二者互为对方的子集时候.

定理 2.2. 两个集合相等当且仅当它们互为子集.

$$A = B \iff A \subseteq B \wedge B \subseteq A$$

2.2 简单操作

现在我们不妨把高中定义的文字性的内容重新定义一下:

定义 2.4 (集合的并 (Union))**.**

$$A \cup B \triangleq \{x \mid x \in A \vee x \in B\}$$

定义 2.5 (集合的交 (Intersection))**.**

$$A \cap B \triangleq \{x \mid x \in A \land x \in B\}$$

定理 2.3 (分配律 (Distributive Law))**.**

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

对于这样的命题, 我们同样给出证明.

证明. 对任意 x,

$$\begin{aligned}
& x \in A \cup (B \cap C) && (5)\\
\iff & (x \in A) \vee (x \in B \land x \in C) && (6)\\
\iff & (x \in A \vee x \in B) \land (x \in A \vee x \in C) && (7)\\
\iff & (x \in A \cup B) \land (x \in A \cup C) && (8)\\
\iff & x \in (A \cup B) \cap (A \cup C) && (9)
\end{aligned}$$

□

同样, 像命题符号一样, 集合的运算也遵循吸收率:

定理 2.4 (吸收律 (Absorption Law))**.**

$$A \cup (A \cap B) = A$$

$$A \cap (A \cup B) = A$$

证明. 对任意 x,

$$\begin{aligned}
& x \in A \cup (A \cap B) && (10)\\
\iff & x \in A \vee (x \in A \land x \in B) && (11)\\
\iff & x \in A && (12)
\end{aligned}$$

□

有了这个我们就可以使用这个证明一个比较重要的习题.

定理 2.5.

$$A \subseteq B \iff A \cup B = B \iff A \cap B = A$$

证明. 对任意 x

$$\begin{aligned}
& x \in B && (1)\\
\implies & x \in A \vee x \in B && (2)\\
\implies & x \in A \cup B && (3)
\end{aligned}$$

□

定义 2.6 (集合的差 (Set Difference); 相对补 (Relative Complement))**.**

$$A \setminus B = \{x \mid x \in A \land x \notin B\}$$

定义 2.7 (绝对补 (Absolute Complement); $\overline{A}, A', A^c$)**.** 设全集为 U.

$$\overline{A} = U \setminus A = \{x \in U \mid x \notin A\}$$

期中, 全集 U (Universe) 是当前正在考虑的所有元素构成的集合. 一般均默认存在. 注意: 不存在 "包罗万象" 的全集.

相对补和绝对补之间存在一些联系.

定理 2.6 ("相对补" 与 "绝对补" 之间的关系)**.** 设全集为 U.

$$\boxed{A \setminus B = A \cap \overline{B}}$$

证明. 对任意 x,

$$\begin{aligned}
& x \in A \setminus B && (1)\\
\iff & x \in A \land x \notin B && (2)\\
\iff & x \in A \land (x \in U \land x \notin B) && (3)\\
\iff & x \in A \land x \in \overline{B} && (4)\\
\iff & x \in A \cap \overline{B} && (5)
\end{aligned}$$

□

定理 2.7 (德摩根律 (绝对补))**.** 设全集为 U.

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

证明. 对任意 x,

$$\begin{aligned}
& x \in \overline{A \cup B} && (1)\\
\iff & x \in U \land \neg(x \in A \lor x \in B) && (2)\\
\iff & x \in U \land x \notin A \land x \notin B && (3)\\
\iff & (x \in U \land x \notin A) \land (x \in U \land x \notin B) && (4)\\
\iff & x \in \overline{A} \land x \in \overline{B} && (5)\\
\iff & x \in \overline{A} \cap \overline{B} && (6)
\end{aligned}$$

□

定理 2.8 (德摩根律 (相对补))**.**

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$$
$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

证明.

$$
\begin{aligned}
& C \setminus (A \cup B) && (1)\\
\iff & C \cap \overline{A \cup B} && (2)\\
\iff & C \cap (\overline{A} \cap \overline{B}) && (3)\\
\iff & (C \cap \overline{A}) \cap (C \cap \overline{B}) && (4)\\
\iff & (C \setminus A) \cap (C \setminus B) && (5)
\end{aligned}
$$

□

由此, 我们可以在集合的操作的层面上证明如下四个定理而不需要取集合中的一个元素进行证明.

定理 2.9.

$$A \cap (B \setminus C) = (A \cap B) \setminus C = (A \cap B) \setminus (A \cap C)$$

$$A \setminus (B \setminus C) = (A \cap C) \cup (A \setminus B)$$

$$A \subseteq B \implies \overline{B} \subseteq \overline{A}$$

$$A \subseteq B \implies (B \setminus A) \cup A = B$$

这里面有一个类似一个异或操作的运算符: 对称差.

定义 2.8 (对称差 (Symmetric Difference))**.**

$$A \oplus B = (A \setminus B) \cup (B \setminus A) = (A \cap \overline{B}) \cup (B \cap \overline{A})$$

2.3 高级集合操作

既然集合的对象是一组元素, 那么集合也是对象, 集合中的元素自然也可以被传进去看作运算. 由此, 我们需要定义关于集合的集合的运算.

定义 2.9 (广义并 (Arbitrary Union))**.** 设 $\mathbb{M}$ 是一组集合 (a *collection* of sets)

$$\bigcup \mathbb{M} = \left\{ x \mid \exists A \in \mathbb{M}.\ x \in A \right\}$$

举一些例子, 比如 $\mathbb{M} = \Big\{ \{1,2\}, \{\{1,2\},3\}, \{4,5\} \Big\}$, 那么 $\bigcup \mathbb{M} = \Big\{ 1,2,3,4,5,\{1,2\} \Big\}$. 注意元素只被解开了一次而不是一次解包到我们认为的 “基本元素”. 因为有时候 “基本元素” 也是用集合定义的. 我们后来会发现我们可以把整个数学基础建立到集合论的基础上.

和求和记号一样, 为了方便书写, 我们也有类似的记号:

$$\bigcup_{j=1}^{n} A_j \triangleq A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcup_{j=1}^{\infty} A_j \triangleq A_1 \cup A_2 \cup \cdots$$

$$\bigcup_{\alpha \in I} A_\alpha \triangleq \left\{ x \mid \exists \alpha \in I.\ x \in A_\alpha \right\}$$

和广义并一样, 我们还有广义交. 定义如下:

定义 2.10 (广义交 (Arbitrary Intersection))**.** 设 $\mathbb{M}$ 是一组集合 (a *collection* of sets)

$$\bigcap \mathbb{M} = \left\{ x \mid \forall A \in \mathbb{M}.\ x \in A \right\}$$

同样的, 如果 $\mathbb{M} = \left\{ \{1,2\}, \{\{1,2\},3\}, \{4,5\} \right\}$ 是全集, $\bigcap \mathbb{M} = \emptyset$. 同样只是展开一次就行了. 注意一个有趣的情况: $\bigcap \emptyset = U$. "包含所有元素的集合" 在后面会发现会导出一个矛盾, 有时候我们也会认为这样说的结果是未定义的.

那么类似的, 我们也希望广义集合里面有没有像普通集合的一些操作. 答案是肯定的. 下面我们来探讨一些有趣的内容.

定理 2.10 (德摩根律)**.**

$$X \setminus \bigcup_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I} (X \setminus A_\alpha)$$

$$X \setminus \bigcap_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} (X \setminus A_\alpha)$$

证明. 对任意 x,

$$\begin{aligned}
& x \in X \setminus \bigcup_{\alpha \in I} A_\alpha && (1)\\
\iff & x \in X \wedge \neg(\exists \alpha \in I.\ x \in A_\alpha) && (2)\\
\iff & x \in X \wedge (\forall \alpha \in I.\ x \notin A_\alpha) && (3)\\
\iff & \forall \alpha \in I.\ (x \in X \wedge x \notin A_\alpha) && (4)\\
\iff & x \in \bigcap_{\alpha \in I} (X \setminus A_\alpha) && (5)
\end{aligned}$$

□

我们同样可以用这条规律来化简集合, 而不用真正在一个集合的集合里面取出来一个元素.

举例:

如果

$$X_n = \{-n, -n+1, \cdots, 0, \cdots, n-1, n\}$$

请化简:

$$A = \mathbb{R} \setminus \bigcap_{n \in \mathbb{Z}^+} (\mathbb{R} \setminus X_n)$$

证明.

$$\begin{aligned}
A &= \mathbb{R} \setminus \bigcap_{n \in \mathbb{Z}^+} (\mathbb{R} \setminus X_n)\\
&= \mathbb{R} \setminus \left(\mathbb{R} \setminus \bigcup_{n \in \mathbb{Z}^+} X_n \right)\\
&= \mathbb{R} \setminus \left(\mathbb{R} \setminus \mathbb{Z} \right)\\
&= \mathbb{Z}
\end{aligned}$$

□

2.4 集合的操作: 排列的力量

在高中, 我们学习了排列组合. 如果对于集合中的元素进行 “选择性缺席”, 这样就可以让我们构造出更加复杂而全面的集合了.

定义 2.11 (幂集 (Powerset))**.**

$$\mathcal{P}(A) = \Big\{ X \mid X \subseteq A \Big\}$$

这个之所以强大, 是因为给定一个 A, 就有如下的内容可以被生成.

$$A = \{1, 2, 3\}$$

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

因为对于 $|A| = n$ 的句子, $|\mathcal{P}(A)| = 2^n$, 因此有时候也写做 2^A 或者 $\{0, 1\}^A$.
接下来看一个 (看似) 没啥用的定理:

定理 2.11.

$$S \in \mathcal{P}(X) \iff S \subseteq X$$

这个定理的作用是在 $\in$ 和 $\subseteq$ 之间转换, 同时脱去一层 $\mathcal{P}()$ 记号.

> **举例:**
> 请证明:
> $$\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(S)))$$

证明. 根据上面的定理, 我们有

$$\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(S))) \iff \{\emptyset, \{\emptyset\}\} \subseteq \mathcal{P}(\mathcal{P}(S)).$$

分别证明之:

$$\begin{aligned} &\emptyset \in \mathcal{P}(\mathcal{P}(S)) \\ &\iff \emptyset \subseteq \mathcal{P}(S) \end{aligned}$$

$$\begin{aligned} &\{\emptyset\} \in \mathcal{P}(\mathcal{P}(S)) \\ &\iff \{\emptyset\} \subseteq \mathcal{P}(S) \\ &\iff \emptyset \in \mathcal{P}(S) \\ &\iff \emptyset \subseteq S \end{aligned}$$

□

其实幂集生成之间也有一些关系. 不妨看一看.

定理 2.12. 证明:

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$$

证明. 对于任意 x,

$$\begin{aligned} & x \in \mathcal{P}(A) \cap \mathcal{P}(B) \\ \iff & x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B) \\ \iff & x \subseteq A \wedge x \subseteq B \\ \iff & x \subseteq A \cap B \\ \iff & x \in \mathcal{P}(A \cap B) \end{aligned}$$

□

定理 2.13. 证明:

$$\bigcap_{\alpha \in I} \mathcal{P}(A_\alpha) = \mathcal{P}(\bigcap_{\alpha \in I} A_\alpha)$$

证明. 对于任意 x,

$$\begin{aligned} & x \in \bigcap_{\alpha \in I} \mathcal{P}(A_\alpha) \\ \iff & \forall \alpha \in I.\, x \in \mathcal{P}(A_\alpha) \\ \iff & \forall \alpha \in I.\, x \subseteq A_\alpha \\ \iff & x \subseteq \bigcap_{\alpha \in I} A_\alpha \\ \iff & x \in \mathcal{P}(\bigcap_{\alpha \in I} A_\alpha) \end{aligned}$$

□

2.5 悖论的出现

前面我们提到 “不存在含有任何东西的集合”. 这就是我们以前知道的通俗讲述的 “理发师悖论”. 形式化的, 根据概括原则, 如果性质 P 是 $P(x) \triangleq$ “$x \notin x$”, 集合 $R = \{x \mid x \notin x\}$, 那么 $R \in R$ 吗?

> “悖论出现于数学的边界上, 而且是靠近哲学的边界上”
> — 哥德尔

之后, 数学家们提出了 ZF(ZFC) 公理化集合论, 避免了这样的内容. 通过粗暴的避免了这种情况, 我们得到了一个还可以使用, 但是丧失了一部分确定性的集合.

定理 2.14 (Russell's Paradox)**.**

$$\{x \mid x \notin x\} \text{ is } \textit{not} \text{ a set.}$$