命题逻辑, 布尔代数和选举

哲学数学计算机中的逻辑课程 (2016 年秋)

王彦晶
北大哲学系

2016 年 11 月 10 日

完全性

布尔代数

超滤子与选举

回顾

- 演绎定理: $\vdash$ 与 $\rightarrow$ 的关系
- 可靠性: 公理系统中可证的都是语义上有效的
- 一致性: 公理系统系统不能推出矛盾
- 公理独立性: 公理系统的公理缺一不可
- 紧致性: 语义上公式集的有穷子集都可满足则整个集合可满足
- 完全性: 语义上有效的都能在公理系统系统中证明出来

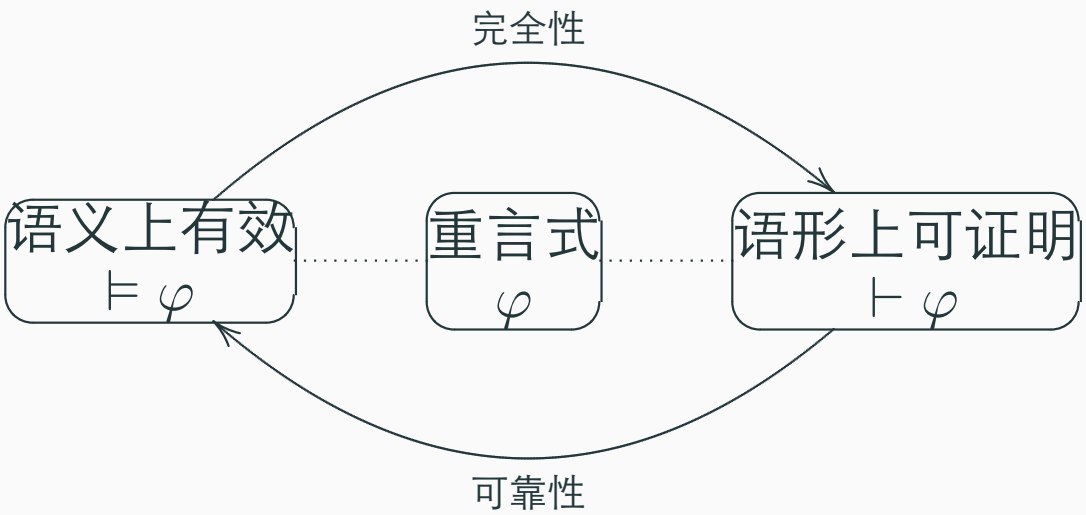
完全性

语形与语义

语义的可满足关系 $V\models\varphi$ (“两道杠”), $\models\varphi$ 表示 φ 是有效的 (放之四海模型皆真), $\Gamma\models\varphi$ 表示语义后承 (语义上对任何模型你真我就真).

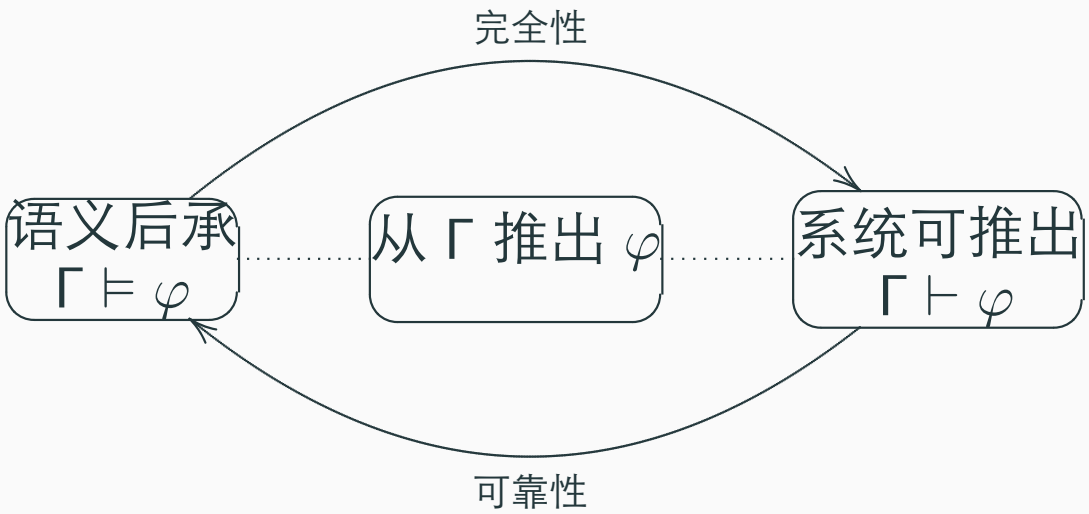
语形上公理系统 S 的可证明关系 $\vdash_S\varphi$ (“一道杠”), $\Gamma\vdash_S\varphi$ 表示可在 S 里从 Γ 的前提推出 φ.

可靠性与完全性: 语义, 语形下对同一堆公式的不同看法



公理系统中的很多事情就是按规则改写符号串, 不太需要脑子和创造力, 可以交给机器做, 这时候可以忘掉语义也没关系.

可靠性与完全性: 更强的版本



一种“构造性”的(弱)完全性证明 $\vDash \varphi \Longrightarrow \vdash \varphi$

关键: 怎么从语义上有效跨越到语形上可以证明? 原则上得每个有效式都找到证明才行啊!

思路:

- 从语义与语形最相似的地方入手跨过语义-语形的这道坎
- 推广到一般情形

一种 “构造” 的完全性证明 (用 $\vdash p \vee \neg p$ 排中律)

1. 每个公式 φ 的真值表的每一行 l 都可以写出来:
   - 1.1 写出模型 V 来: 如果 $V(p) = 1$ 则 $l(p) = p$, 反之 $l(p) = \neg p$
   - 1.2 类似的, 公式 φ 可以根据真值写 φ 或者 $\neg\varphi$, 定义为 $l(\varphi)$
   - 1.3 可以归纳证明, 对任意一行真值表, $l(p_1), \ldots, l(p_n) \vdash l(\varphi)$
2. 假设 $\vDash \varphi$, 则对任意 V 中一行 l: $l(p_1), \ldots, l(p_n) \vdash \varphi$
3. 想办法把前提们弄掉
   - 3.1 找两行 l, l' 只在 p_n 处不一样, 有 $l(p_1), \ldots l(p_{n-1}), p_n \vdash \varphi$, 有 $l(p_1), \ldots l(p_{n-1}), \neg p_n \vdash \varphi$
   - 3.2 用演绎定理: $l(p_1), \ldots, l(p_{n-1}) \vdash p_n \to \varphi$, $l(p_1), \ldots, l(p_{n-1}) \vdash \neg p_n \to \varphi$, 用排中律有 $l(p_1), \ldots, l(p_{n-1}) \vdash \varphi$
   - 3.3 对某个 l''(与 l 只在 p_{n-1} 上不同的) 重复上面两步可得 $l(p_1), \ldots, l''(p_{n-1}) \vdash \varphi$ 这里 $l''(p_{n-1}) \neq l(p_{n-1})$.
   - 3.4 可继续消去 p_{n-1} 等, 直到得到$\vdash \varphi$.

从弱完全性到强完全性

有了 $\vDash \varphi \implies \vdash \varphi$, 怎么得到 $\Gamma \vDash \varphi \implies \Gamma \vdash \varphi$?

可以用紧致性:

1. 假设 $\Gamma \vDash \varphi$
2. 则按照紧致性, 可以找到 Γ 的有穷子集 Δ 使得 $\Delta \vDash \varphi$
3. 按语义定义, 可得 $\vDash \bigwedge \Delta \to \varphi$ ($\bigwedge \Delta$ 是 Δ 里公式的合取)
4. 按弱完全性有 $\vdash \bigwedge \Delta \to \varphi$
5. 按 $\vdash$ 定义有 $\Delta \vdash \varphi$
6. 按 $\vdash$ 定义有 $\Gamma \vdash \varphi$

强完全性: 另一种证明方法.

要证: 任意 Γ, φ: $\Gamma \vDash \varphi \implies \Gamma \vdash \varphi$.

证逆否: 任意 Γ, φ: $\Gamma \nvdash \varphi \implies \Gamma \nvDash \varphi$

- $\Gamma \nvdash \varphi$ iff $\Gamma \cup \{\neg\varphi\}$ 一致 (推不出矛盾).
- $\Gamma \nvDash \varphi$ iff $\Gamma \cup \{\neg\varphi\}$ 可满足 (有满足它的模型).

转化为要证: 任意 Γ, φ: $\Gamma \cup \{\neg\varphi\}$ 一致则 $\Gamma \cup \{\neg\varphi\}$ 可满足. 其实只需证明: 任意 Γ, Γ 一致则 Γ 可满足, 本质上变成了找模型的任务!

思想: 用一致的公式集造一个模型 (对命题变元的赋值). 考虑最简单的情况, 如果这个一致的公式集包括 $\{p_1, \neg p_2, \neg p_3, \dots\}$, 它几乎就是一个模型了, 按它说的赋值应该不会错 (需证明). 当然最好这个公式集就明确告诉我对所有公式来说哪些是真的哪些假的.

证明一致则可满足: 扩充一致集给我足够多的信息!

如果语言里的命题变元可以数出来:$p_1, p_2, \ldots$, 我们也可以给公式排个序数出来: $\varphi_1, \varphi_2, \ldots$ 可以用哥德尔配数 (Gödel numbering)

假设 Γ 是一致的,

1. 要证明: Γ 可以扩充成某个极大一致集(再加啥都不一致)
   - 1.1 令 $\Gamma_0 = \Gamma$
   - 1.2 令 $\Gamma_{k+1} = \begin{cases} \Gamma_k \cup \{\varphi_{k+1}\} & \text{如果 } \Gamma_k \cup \{\varphi_{k+1}\} \text{ 是一致的} \\ \Gamma_k \cup \{\neg\varphi_{k+1}\} & \text{否则} \end{cases}$
   - 1.3 证明每个 Γ_i 都是一致的 (证明如果 Γ_k 一致则 Γ_{k+1} 肯定一致)
   - 1.4 证明 $\Sigma = \bigcup_0^\infty \Gamma_i$ 是极大一致集 (反证, 若不一致则有穷步就不一致)
2. 用上面的 Σ 定义一个模型 V^c: $V^c(p) = 1$ iff $p \in \Sigma$
3. 证明对任何 φ: $V^c \vDash \varphi \iff \varphi \in \Sigma$ (极大一致集有一些好性质).

极大一致集 (MAXIMAL CONSISTENT SET) 有和语义很像的好性质

证明对任何 φ: $V^c \vDash \varphi \iff \varphi \in \Sigma$ 需要依赖如下性质:

- $\neg\varphi \in \Sigma \iff \varphi \notin \Sigma$
- $\varphi \to \psi \in \Sigma \iff \neg\varphi \in \Sigma$ 或者 $\psi \in \Sigma$

和语义是不是长得很像:

$V \vDash p$	$\Leftrightarrow$	$V(p) = 1$
$V \vDash \neg\varphi$	$\Leftrightarrow$	$V \nvDash \varphi$
$V \vDash \varphi \to \psi$	$\Leftrightarrow$	$V \nvDash \varphi$ 或者$V \vDash \psi$

注意: 完全性证明应用到所有公理和规则 (除非它们不是必须的).

强完全性可以用来证明紧致性

可靠性与完全性: $\Gamma \vdash \varphi \iff \Gamma \vDash \varphi$.

紧致性: Γ 有穷可满足则可满足.

假设 Γ 有穷可满足, 要证 $\Gamma \nvdash \bot$.

证明:

1. 对任意 $\Delta \subseteq_f \Gamma$, $\Delta \nvDash \bot$.
2. 由可靠性, 对任意 $\Delta \subseteq_f \Gamma$, $\Delta \nvdash \bot$.
3. 由 $\vdash$ 定义, $\Gamma \nvdash \bot$.
4. 由完全性 $\Gamma \nvDash \bot$.

布尔代数

布尔代数 (BOOLEAN ALGEBRA)

布尔 (George Boole (1815–1864)): 自学成才的英国数学家, 在 The Laws of Thought 中提出用代数的方法研究逻辑.

布尔代数是一种抽象代数: 并不预设个体和运算的解释, 而是给出一些公理, 满足这些公理的具体代数就是布尔代数.

一个布尔代数首先是一个数学结构 $\langle A, +, \cdot, -, 0, 1\rangle$ 其中 A 是一堆东西, $+$ 和 $\cdot$ 是这些东西上的二元运算, $-$ 是一个一元运算, $0, 1$ 是 A 中两个特殊的元素 (可以相同).

这种数学结构还需要满足很多性质 (下一页).

布尔代数对任意 $x, y, z \in \mathbf{A}$ 要满足:

结合律 (Associativity)	$x + (y + z) = (x + y) + z$
	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
交换律 (Commutativity)	$x + y = y + x$
	$x \cdot y = y \cdot x$
同一律 (Identity)	$x + 0 = x$
	$x \cdot 1 = x$
分配率 (Distributivity)	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
	$x + (y \cdot z) = (x + y) \cdot (x + z)$
互补率 (Complementation)	$x + (-x) = 1$
	$x \cdot (-x) = 0$

布尔代数是有补分配格 (Complemented distributive lattice)

可以用这些公理作证明

德摩根率 (de Morgan's law):

$$-(x+y) = -x \cdot -y \qquad -(x \cdot y) = -x + -y$$

证明步骤:

1. 证明 $-x$ 是 x 唯一 (满足互补率) 的补.
2. 证明 $(x+y) \cdot (-x \cdot -y) = 1$
3. 证明 $(x+y) + (-x \cdot -y) = 0$
4. $-(x+y) = -x \cdot -y$

布尔代数的具体例子: 幂集代数 (POWER SET ALGEBRA)

取具体集合上 W 的并交补, $\langle \mathcal{P}(W), \cup, \cap, \bar{}, \emptyset, X \rangle$ 是一个布尔代数:

结合律 (Associativity)	$x \cup (y \cup z) = (x \cup y) \cup z$
	$x \cap (y \cap z) = (x \cap y) \cap z$
交换律 (Commutativity)	$x \cup y = y \cup x$
	$x \cap y = y \cap x$
同一律 (Identity)	$x \cup \emptyset = x$
	$x \cap W = x$
分配率 (Distributivity)	$x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$
	$x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$
互补率 (Complementation)	$x \cup \bar{x} = W$
	$x \cap \bar{x} = \emptyset$

和命题逻辑的关系

把 A 看成公式集, $\cdot$ 看成 $\wedge$, $+$ 看成 $\vee$, $-$ 看成 $\neg$, $=$ 看成 $\leftrightarrow$:

结合律 (Associativity)	$x \vee (y \vee z) \leftrightarrow (x \vee y) \vee z$
	$x \wedge (y \wedge z) \leftrightarrow (x \wedge y) \wedge z$
交换律 (Commutativity)	$x \vee y \leftrightarrow y \vee x$
	$x \wedge y \leftrightarrow y \wedge x$
同一律 (Identity)	$x \vee \bot \leftrightarrow x$
	$x \wedge \top \leftrightarrow x$
分配率 (Distributivity)	$x \wedge (y \vee z) \leftrightarrow (x \wedge y) \vee (x \wedge z)$
	$x \vee (y \wedge z) \leftrightarrow (x \vee y) \wedge (x \vee z)$
互补率 (Complementation)	$x \vee (\neg x) \leftrightarrow \top$
	$x \wedge (\neg x) \leftrightarrow \bot$

林登鲍姆-塔斯基代数 (LINDENBAUM-TARSKI ALGEBRA)

把 $\leftrightarrow$ 变成真正的相等:

A 是命题逻辑公式的等价类 的集合 $\{[\varphi] \mid \varphi$ 是命题逻辑公式$\}$, 其中 $[\varphi] = \{\psi \mid \vdash \varphi \leftrightarrow \psi\}$.

定义: $[\varphi] + [\psi]$ 为 $[\varphi \vee \psi]$, $[\varphi] \cdot [\psi]$ 为 $[\varphi \wedge \psi]$, $-[\varphi]$ 为 $[\neg\varphi]$, 1 为 $[p \vee \neg p]$, 0 为 $[p \wedge \neg p]$.

可以证明这也是一个布尔代数, 例如互补率:

$$[\varphi] + -[\varphi] = [\varphi] + [\neg\varphi] = [\varphi \vee \neg\varphi] = [p \vee \neg p]$$

斯通表示定理 (STONE'S REPRESENTATION THEOREM)

这么看来布尔代数的具体例子似乎千奇百怪 (因为定义只要求满足特定公理就好了), 但是这只是表面现象, 我们有如下的表示定理 (任意符合抽象要求的都有有特定的具体形式):

Theorem

每个布尔代数都同构于某个集代数 *(Ser algebra)*.

集代数是幂集代数的子代数 (不需要 W 所有子集, 只要对几种运算封闭的子集们即可).

"同构" 先可以简单的理解为数学上看具有同样的性质 (可以看成是一样的). 这个定理把抽象的和具体的联系起来了!

用表示定理证明命题逻辑的完全性

令 SET 表示所有集合代数的类, BA 表示所有布尔代数的类. 可以把逻辑的语义和证明系统代数化 ($\Vdash$ 通过用代数结构来给 φ 真假):

- $\vDash \varphi \iff \mathbf{SET} \Vdash \varphi$ ($\vDash$ 和 SET 比较接近)
- $\vdash \varphi \iff \mathbf{BA} \Vdash \varphi$ ($\vdash$ 和 BA 比较接近)

代数语义的基本想法就是把命题变元解释成代数里的元素, 连接词解释成相应的布尔算子, φ 在一个代数结构上有效当且仅当不管把 φ 中的命题变元解释成什么, φ 对应的代数式子都等于该代数中的 1. $\mathbf{SET} \Vdash \varphi$ 表示 φ 在所有集合代数上都有效.

每个集合代数都是布尔代数, 而斯通表示定理又告诉我们每个布尔代数也可以看成某个集合代数, 因此: $\mathbf{SET} \Vdash \varphi \iff \mathbf{BA} \Vdash \varphi$ 所以我们有 $\vDash \varphi \iff \vdash \varphi$.

斯通表示定理的证明

Theorem

所有布尔代数都同构于某个集代数.

证明? 不讲!

思想: 任给个布尔代数, 得用它弄出个合适的集合来, 这里面用到一个对逻辑和数学都很重要且有意思的概念:

超滤子 (ultrafilter)

超滤子与选举

布尔代数上的滤子 (FILTER)

给定一个布尔代数 $\langle A, +, \cdot, -, 0, 1\rangle$, 它上面的一个滤子 F 是一个 A 的子集满足:

- $1 \in F$
- F 对 $\cdot$ 封闭: 若 $a, b \in F$ 则 $a \cdot b \in F$
- F 向上封闭: $a \in F$ 且 $a \leq b$ (即 $a + b = b$) 则 $b \in F$

一个真滤子 (proper filter) 是一个不包含 0 的滤子.

一个超滤子是真滤子且满足对任意 $a \in A$, $a \in F$ 或者 $-a \in F$.

公式集上的滤子

- $\top \in F$
- 若 $\varphi, \psi \in F$ 则 $\varphi \wedge \psi \in F$
- $\varphi \in F$ 且 $\varphi \to \psi$ 则 $\psi \in F$

一个真滤子是一个不包含 $\bot$ 的滤子.

一个超滤子是真滤子且满足对任意 $\varphi \in A$, $\varphi \in F$ 或者 $\neg\varphi \in F$.

超滤其实就是极大一致集! 真滤子是一致集.

等等: 为啥叫 “滤子”(FILTER)?

留下特大的东西, 放走小东西!

集合上的滤子

给定一个集合 W, 一个 W 上的滤子 F 是一个 W 子集的集合满足:

- $W \in F$
- $X, Y \in F \implies X \cap Y \in F$
- $X \in F$ 且 $X \subseteq Y \implies Y \in F$

一个真滤子是一个不包含空集的滤子.

真滤子的例子

令 $\mathbb{N}$ 为所有自然数的集合,

$$\{X \mid X \text{ 是 } \mathbb{N} \text{ 的余有穷子集}\} = \{X \mid \mathbb{N} \backslash X \text{ 是有穷的}\}$$

是一个真滤子: 验证那四条性质.

一个集合上的超滤子是一个真滤子而且对任何一个 W 的子集 X, X 在其中或者 X 的补集在其中.

上面的例子不是超滤子: 奇数的集合和偶数的集合都不在里面.

$\mathbb{N}$ 上超滤子的例子: $\{X \mid 1 \in X \subseteq \mathbb{N}\}$, 验证那五条性质.

主超滤子和非主超滤子

主超滤子(principal ultrafilter) 是由一个元素 “生成” 的超滤子 (是包含那个元素的所有子集的集合), 其他的超滤子称为非主超滤子 (non-pricipal ultrafilter). 显然只要一个超滤子里有一个单元集 (只有一个元素的集合) 那么这个超滤就是主超滤子 (由向上封闭性).

非主超滤子只能包括无穷子集 (想想为什么?). 所以全集是有穷的时候只有主超滤子(重要!).

Theorem (超滤定理)

每个真滤都可以扩充成一个超滤.

想想我们造极大一致集的时候: 一致公式集可以扩充成极大一致集.

换种说法: 找对象满足多少条件就足够好了?

给定一个女孩, 一个她各种要求的集合 W, 不太可能有男孩满足所有这些条件, 那么满足多少算 “足够好” 呢? 令 “足够好” 的 W 的子集的集合为 F, F 直观上应满足:

- $W \in F$
- $\emptyset \notin F$
- $X \in F$ 且 $X \subseteq Y \implies Y \in F$
- 如果 $X, Y \in F$ 那么 $X \cap Y$ 非空
- 如果 $X \in F$ 且 $Y \subset X$ 但 $Y \notin F$ 则 $X \backslash Y \in F$

这其实就是等价的超滤的定义 (自己试试看怎么证明)!

因而: 如果女孩的条件一共只有有穷多条 (W 有穷), 那么肯定存在某个条件, 只要满足这一个条件, 女孩就嫁了 (只存在主超滤子)!

超滤子可以看成 w 上的有穷可加的 0 – 1 测度

从数学上看哪些子集是 “大” 的子集?

一个 0 – 1 测度函数 $\mu : \mathcal{P}(W) \to \{0, 1\}$ 需要满足:

- $\mu(W) = 1$
- 如果 $Y_1, \ldots, Y_n$ 是两两不交的 W 的子集, 那么 $\mu(\bigcup_{k \leq n} Y_k) = \sum_{i \leq n} \mu(Y_i)$. 一大块东西的大小通过测量不相交的部分再相加得到.

给定一个这样的测度, 测度为 1 的子集们组成一个超滤子.

我们在逻辑里我们还使用超滤子帮助我们把一堆小模型揉在一起, 使得在 “几乎所有” 的小模型上都是真的的公式在揉起来的大模型上还是真的. 可用来构造特殊饱和模型和证明逻辑的紧致性.

阿罗不可能定理 (ARROW'S IMPOSSIBILITY THEOREM)

令 W 是一个选民的集合, C 是候选人的集合. 令 Π_C 是所有候选人的可能排序的集合. 一个公平的选票聚合函数 (vote aggregation function) (VA) $f : \Pi_C^W \to \Pi_C$ (输入所有人对候选人的排序, 输出一个排序作为聚合结果) 直观上应该满足:

- 无异议性 (Unanimity, U): 所有人都投了同样的排序则 f 也输出一样的排序.
- 无关事件独立性 (Independence of Irrelevant Alternatives, IIA): 在 f 输出的结果中两个候选人的相对排序只和每个人投票中这两个人的相对排序有关.
- 没有独裁 (no dictator): 没有一个人可以独自决定选举的结果.

阿罗不可能定理 (ARROW'S IMPOSSIBILITY THEOREM)

定理: 如果 W 是有穷的且 $|C| \geq 3$, 满足 U 和 IIA 的 VA 函数一定会导致有一个独裁者 (他投啥结果就是啥)!

(一个) 证明思路:

1. 给定一个满足 U 和 IIA 的 VA 函数 f
2. 我们关心那些选民的决定集们 (decisive sets): 只要这伙人选啥结果就是啥 (可以看成对独裁者的多人推广, 显然根据 U, W 是这样一个集合).
3. 我们证明这些 f-决定集构成一个在选民集合 W 上的超滤子.
4. 因为 W 是有穷的所以这个超滤子必须是主超滤子, 也就是说存在一个只有一个人的决定集, 显然这个人就是一个独裁者.

社会选择理论 (SOCIAL CHOICE THEORY)

和逻辑的关系: 公理化性质, 寻找逻辑上不相容的性质集合, 然后想解决办法,

投票水很深 (同样的投票, 根据不同聚合办法得到的结果可能千差万别)! 延伸阅读: 《选举几何学》

计算社会选择理论 (Computational social choice theory): 用计算复杂性防止坏情况的发生

逻辑与社会选择的更多关系

- 形式化半自动证明
- 用逻辑做投票协议验证
  - 隐私性: 没有别人能知道你投的是谁 (在你不主动说的情况下)
  - 无收据性: 你不能证明给别人你投了特定人的票
  - 个体可核查性: 你自己能检查你的票是不是被算进去了
  - 公平性: 之前投票的部分结果不会影响之后投票的结果

祝大家双十一快乐!