arXiv:2305.01439v1 [cs.LO] 2 May 2023

证明论中基于归约的方法与基于模型的方法的趋同

Gilles Dowek*

摘要

近年来，用于证明切消去的基于归约的方法与基于模型的方法逐渐趋同，如今看来，它们恰如一枚硬币的两面。本文详细介绍了这一转变过程中的若干步骤。

引言

证明论中的许多结果，例如不可证性结果、各种证明搜索方法的完备性、构造性证明的析取性质和见证性质，以及从这类证明中提取程序的可能性，都依赖于切消去定理。这些定理断言：如果某个命题在某个理论中可证，那么它就有一种特殊形式的证明，即无切证明。

为证明这类切消去定理而发展出的方法，大体可分为两类：基于归约的方法和基于模型的方法。近来，我们见证了这两类方法逐渐趋于融合。本文将详细阐述这一转变的若干步骤；正是这一转变使人们开始将基于归约的方法和基于模型的方法视为同一枚硬币的两面。

1 公理问题

在基于归约的方法与基于模型的方法逐渐融合、以用于证明切消去的过程中，初步的一步是定义足够一般的切概念。而这本身又要求修改理论的概念。

我们先来看一个例子。切消去定理的一个推论是析取性质：在构造性自然演绎中，如果形如 $A \vee B$ 的命题可在空理论中证明，也就是说，无需公理即可证明，那么 A 或 B 必有一个可证。事实上，根据切消去定理，如果命题 $A \vee B$ 可证，那么它就有一个无切证明。接着，简单地对证明结构进行归纳

* ´巴黎综合理工学院和 INRIA，LIX， ´巴黎综合理工学院，法国 Palaiseau Cedex，91128，gilles.dowek@polytechnique.edu。

可知，在构造性自然演绎中，空理论下无切证明的最后一条规则是引入规则。因此，$A \vee B$ 的无切证明以析取的引入规则结束，且 A 或 B 可证。

无切证明的最后一个规则是引入规则这一事实，在加入公理后并不再成立。例如，如果命题 $A \vee B$ 是一个公理，那么它就有一个以公理规则结束的无切证明。因此，对于算术、简单类型论等理论，或者更简单地说，对于由公理 $P \Leftrightarrow (Q \Rightarrow R)$ 形成的理论，其析取性质无法以简单方式从谓词逻辑的切消去定理中推出。试图刻画能够保持无切证明通常性质（例如析取性质、见证性质，或最后一个规则是引入规则这一事实）的公理——如 Harrop 公式——最终得到的类别都相对较小；例如，它们从不包含算术的公理。事实上，不含公理的谓词逻辑的切消去定理可以在算术中得到证明，而算术中所有可证明命题都有一个以引入规则结束的证明，这一性质蕴含算术的一致性。因此，这一结果无法以初等方式从谓词逻辑的切消去定理中推出。

因此，要证明算术或简单类型论的析取性质，我们需要先扩展切消去定理。这也解释了为什么针对各种我们感兴趣的理论，会有若干种切消去定理。例如，在算术中，我们通常会引入一种针对归纳公理的新的切形式，并针对这种扩展后的切概念再次证明切消去定理。

为每种我们感兴趣的理论引入特定切概念的必要性，一直是发展一般切消去理论的障碍。模演绎 [11, 14] 试图部分解决这一问题。在模演绎中，形如 $\forall x_1 \ldots \forall x_n \, (t = u)$ 或 $\forall x_1 \ldots \forall x_n \, (P \Leftrightarrow A)$ 的公理（其中 P 是一个原子命题）会被重写规则 $t \longrightarrow u$ 或 $P \longrightarrow A$取代。例如，公理 $P \Leftrightarrow (Q \Rightarrow R)$ 会被重写规则 $P \longrightarrow (Q \Rightarrow R)$ 取代。然后，在这些规则生成的同余下进行演绎。例如，给定重写规则$P \longrightarrow (Q \Rightarrow R)$，蕴涵的一个消去规则实例为

$$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash R} \Rightarrow\text{-elim}$$

因为 P与 $Q \Rightarrow R$同余。许多理论（如果不是全部的话）都可以表述为重写系统：例如算术 [15, 1] 和简单类型论 [12]。

在模演绎中，切的定义与自然演绎中的相同：它是由一个引入规则后接一个消去规则构成的序列。在模演绎中，并非所有理论都具有切消去性质。例如，由规则 $P \longrightarrow (Q \Rightarrow R)$ 构成的理论具有该性质，由规则 $P \longrightarrow (Q \Rightarrow P)$ 构成的理论也具有该性质，但由规则$P \longrightarrow (P \Rightarrow R)$ 构成的理论则不具有。在模演绎中，纯计算理论中的无切证明（即包含重写规则但不含公理的理论）总是以一个引入规则结

束。因此，当一个纯计算理论具有切消去性质时，它就具有析取性质。

由于模演绎中的切只不过是由一个引入规则和一个消去规则构成的序列，因此切这一概念的定义与所关注的理论无关。现在，询问某个以重写系统表述的理论是否具有切消去性质，便是一个定义良好的问题。

事实上，Dag Prawitz 和其他人 [25, 6, 7, 19, 16] 此前也曾研究过类似的思想$\forall x_1 \ldots \forall x_n$，他们提出将形如$P \Leftrightarrow A($ A $)$的公理替换为非逻辑演绎规则，从而允许将 P折叠为 P，并将 A展开为 $P \Leftrightarrow$。例如，公理 $Q \Rightarrow R()$ 可以替换为两条规则

$$\frac{\Gamma \vdash Q \Rightarrow R}{\Gamma \vdash P}\,\text{fold}$$

and

$$\frac{\Gamma \vdash P}{\Gamma \vdash Q \Rightarrow R}\,\text{unfold}$$

最近，Benjamin Wack 引入了超自然演绎的概念 [29, 3]，：将 A 折叠为 P，并先对 A 的联结词和量词应用所有可能的引入规则；将 P 展开为 A 后，则自动接续相应的消去规则。例如，公理 $r : (P \Leftrightarrow (Q \Rightarrow R))$ 被替换为以下规则。

$$\frac{\Gamma, Q \vdash R}{\Gamma \vdash P}\,r\text{-intro}$$

and

$$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash R}\,r\text{-elim}$$

这就导出了非常自然的演绎规则；正如通常的数学实践中那样，联结词和量词几乎消失了。

有趣的是，在这三种形式体系中具有切消去性质的理论是相同的 [9, 4]。这表明了切这一概念的稳健性。

总而言之，可以 formulat e 一种适用于所有能够表示为重写系统的理论的一般切概念，而且这一切概念相当稳健。定义一种独立于所关注理论的切概念，是基于归约的方法与基于模型的方法趋于融合的先决条件；正因为如此，人们识别出了一大类适用于这些方法的问题。

2 模型

2.1 可靠性与完备性

可靠性定理断言，对于每个命题 A，如果 A 可在谓词逻辑中证明，那么对于每个模型 $\mathcal{M}$，A 在 $\mathcal{M}$中都是有效的。反之，

完备性定理断言，对于每个命题 A，如果对于每个模型 $\mathcal{M}$，A 在 $\mathcal{M}$中都是有效的，那么 A是可证明的。然而，在完备性定理的大多数证明中，所证明的是与之在经典逻辑上等价的表述：对于每个命题 A，存在一个模型 $\mathcal{M}$，使得如果 A 在 $\mathcal{M}$中有效，那么 A 是可证明的。

按照通常的二值模型概念，无法交换量词顺序并证明存在一个统一模型 $\mathcal{M}$，使得对于每个命题 A，如果 A 在 $\mathcal{M}$中有效，那么 A 就是可证明的。但是，如果扩展模型的概念，允许真值取自任意布尔代数的元素，那么这一论述便可以得到证明。此类模型的一个例子是这样的模型：项解释域是语言中的项的集合，而命题解释域是该语言的林登鲍姆代数，即该语言中命题的集合对关系 $\simeq$ 取商所得的集合，其中该关系定义为：若 $A \Leftrightarrow B$ 可证明，则 $A \simeq B$。在构造性逻辑中，必须用 Heyting 代数取代布尔代数，但仍然可以证明这一统一完备性定理。

2.2 基于模型的切消去证明

基于模型的切消去证明——例如 [26, 24, 28, 2, 8, 22] ——通过证明一个加强的完备性定理来进行：对于每个命题 A，如果对于每个模型 $\mathcal{M}$，A 在 $\mathcal{M}$中有效，那么 A 就有一个无切证明。切消去定理由可靠性定理和这个加强的完备性定理直接推出：如果一个命题有证明，那么根据可靠性定理，它在所有模型中都有效，因此根据加强的完备性定理，它有一个无切证明。

Olivier Hermant 已证明，这种基于模型的方法可用于证明模演绎中一大类理论的切消去 [20, 21]。他强化后的完备性定理具有一致性：通过构造一个模型 $\mathcal{M}$，使得对于所有 A，若 A 在 $\mathcal{M}$中有效，则 A 有无切证明。请注意，使用这种一致的强化完备性定理时，在切消去定理的证明中只需用到一次可靠性定理：即与强化完备性定理所给出的模型 $\mathcal{M}$ 相对应的那一次。可证命题在这个特定模型中有效，因此它们有无切证明。

3 归约

基于归约的方法通过展示一种算法来证明切消去定理，该算法将一个含有切的证明转换为另一个“更接近”无切证明的证明。这个转换过程称为证明归约，可以迭代进行；若最终终止，就会得到一个无切证明。

最早的基于归约的切消去证明之一，是使用 Tait 方法证明算术中证明归约的终止性 [27]。其思路是对证明结构进行归纳，证明所有证明都会终止；但要

使这一归纳论证成立，和通常的归纳证明一样，必须加强归纳假设，证明所有证明都满足一个比终止性更强的性质，称为可约性。可约性这一概念以该证明所证明的命题为参数。因此，在这个证明中，先对命题 A 的结构进行归纳，定义“是 A 的可约证明”这一概念；然后，再对证明结构进行归纳，证明所有 A 的证明都是 A 的可约证明。

一种等价的表述是使用 A 的可约证明集，而不是谓词“是 A 的可约证明”。谓词“是 A 的可约证明”是按 A 的结构归纳定义的，这一事实可以改述为：$A \Rightarrow B$ 的可约证明集由 A 的可约证明集和 B 的可约证明集通过对这些集合应用一个二元函数 $\dot{\Rightarrow}$ 得出；其他联结词和量词的情形也类似。

4 从归约到模型

弥合基于归约的方法与基于模型的方法之间的差距，需要经过若干步骤。

4.1 可约候选项

第一步是 Jean-Yves Girard 引入了可约性候选的概念，并以此为基础给出了简单类型论中切消去的归约证明 [17, 18]。

在该证明中，要定义某个命题 A 的可约证明集，就必须对所有命题B 的可约证明集进行量化。因此，直接尝试会导致循环定义。避免这种循环的一种方法是预先引入一个证明集的集合，即可约性候选集，并改为对所有这类可约性候选进行量化。这样便可以定义所有命题的可约证明集，而且事后可知，这些集合都是可约性候选。

引入这组可约性候选后，Jean-Yves Girard 定义了可约证明集所处的空间。Michel Parigot [23] 后来指出，这组可约性候选可以用一种简单的方式定义，即由运算 $\dot{\Rightarrow}$、$\forall$、.....封闭的证明集之集中的˜最小集合。

4.2 作为真值的可约候选项

在各种类型论表述的切消去证明中，特别是在 Benjamin Werner 关于归纳构造演算切消去的证明中，人们注意到，将证明集赋予每个命题，与在模型中将真值赋予每个命题，这两种做法十分相似。

特别值得一提的是，模型论记法$[\![A]\!]$ 已逐渐取代表示命题可约证明集的记法 R_A

，而“ A的解释”和“ A的指称”这两种表达也已逐渐取代“ A的可约证明集”这一表达。

4.3 引入论域

在 [14], 中，我们与 Benjamin Werner 一起，为模演绎中的一大类理论提出了基于归约的切消去证明，这些理论的特点是拥有一个以可约性候选为值的模型。

例如，为了证明规则 $P \longrightarrow (Q \Rightarrow R)$ 下的切消去，我们构造一个模型，其中每个命题都由一个可约性候选来解释，并且规则 $P \longrightarrow (Q \Rightarrow R)$ 有效，也就是说，该规则两边具有相同的指称。我们首先用任意可约性候选来解释命题符号 Q 和 R~，例如用包含所有强终止证明的候选 $\top$。然后，我们用候选 $[\![Q]\!] \Rightarrow [\![R]\!]$来解释命题符号 P~ ~，在这个例子中即为 $\top \Rightarrow \top$。接着，根据构造可得 $[\![P]\!] = [\![Q]\!] \Rightarrow [\![R]\!]$，也就是说，规则 $P \longrightarrow (Q \Rightarrow R)$ 在此模型中有效。并且，这种模型的存在足以证明该理论中证明归约的强终止性，因为我们可以证明，命题A 的所有证明都是候选 $[\![A]\!]$的元素。

在模演绎中，不同于类型论，理论中的项与证明项属于不同类型的实体，正如语言中的类与命题也属于不同类型。因此，除了使用可约性候选表示真值来解释命题之外，解释项也是顺理成章的。例如，要构造规则 $P(f(x)) \longrightarrow (P(x) \Rightarrow R)$ 的模型，我们可以先选择一个项解释域，例如自然数集合 $\mathbb{N}$，再为函数符号 f 指定一种解释，例如函数 $n \mapsto n+1$。接着，我们用任意可约性候选来解释命题符号 R，例如用 $\top$ 来解释~；然后用函数 α 来解释谓词符号 P。该函数将每个自然数映射到一个可约性候选，并按如下方式通过归纳定义：$\alpha(0)$~ 是任意候选，例如 $\top$；而 $\alpha(n+1) = \alpha(n) \Rightarrow [\![R]\!]$。然后，容易验证，对于所有赋值 ϕ，$[\![P(f(x))]\!]_\phi = [\![P(x) \Rightarrow R]\!]_\phi$，因此规则 $P(f(x)) \longrightarrow (P(x) \Rightarrow R)$ 在该模型中有效。

引入这个项解释域简化了我们的切消去证明，尤其是因为，我们无需将谓词符号的解释定义为一个把项映射到真值的函数，而可以将这一过程分为两步：先解释项，再将谓词符号的解释定义为一个把项解释域中的元素映射到真值的函数，这与模型中的通常做法一致。

因此，项解释域是在基于归约的切消去证明中引入的，并由此形成了以可约性候选为值的模型这一概念，称为预模型。

4.4 真值代数与超一致性

如前所述，通常的二值模型概念可以扩展为真值构成布尔代数或 Heyting 代数的模型。这引出了一个问题：能否将预模型视为这类以 Heyting 代数为值的模型？也就是说，能否在可约候选项集合上定义一种序，使其构成 Heyting 代数？遗憾的是，这~ ~ ~是不可能的，因为在所有 Heyting 代数中都有 ($\top \Rightarrow \top$) $= \top$，但在可约候选项代数中并非如此。因此，为了纳入可约候选项代数，必须将 Heyting 代数的概念推广为真值代数 [10]这一概念。

一个集合要作为真值集合使用，应当配备哪些关系和运算？事实上，它不必配备~序关系。只需配备一族运算 $\Rightarrow$、 $\forall$、 $\tilde{\wedge}$，.....，以便解释命题，并定义一种正真值的概念来刻画有效命题。为了使可靠性定理成立，这些正真值必须对推导规则封闭。例如，如果 $a \Rightarrow b$和 a 是正真值，那么 b 也必须是正真值。

Thierry Coquand 曾在一次私人交流中提出，在这样的代数中，总可以定义一种关系 $\leq$：若 $a \Rightarrow b$ 是正真值，则 $a \leq b$ 成立。他还注意到，配备这种关系的真值代数满足海廷代数的所有性质，唯独不满足关系 $\leq$的反对称性。因此，真值代数也可以定义为具有最大下界、最小上界和相对补的预序结构。与序结构不同，在预序结构中，最大下界和最小上界并不唯一~；此外，定义代数时，除了预序之外，还必须给定运算 $\Rightarrow$、 $\forall$、 $\tilde{\wedge}$、.....，因为必须明确指定 a 和 b 的哪个最大下界是元素 $a \tilde{\wedge} b$ 。

众所周知，在命题上由 $A \leq B$ if $A \Rightarrow B$is provable 定义的关系具有自反性和传递性；但若要使其具有反对称性并定义一种语言的林登鲍姆代数，就必须按照由 $\simeq$ defined by $A \simeq B$ if $A \Leftrightarrow B$ is provable 定义的关系，对命题集合取商。另一种“解决方案”是放弃反对称性这一要求。

配备运算是~的真值代数，取值于该代数的模型恰好就是我们与 ~ Benjamin Werner 一起定义的预模型。

令人惊讶的是，在这些构造中，并未用到可约候选项代数的任何特定性质。因此，它们可以推广到所有真值代数。这促使人们引入了超一致性的概念：如果一个理论对于所有真值代数都存在一个取值于 $\mathcal{B}$ 的模型，而不只是对于其中一种代数存在这样的模型，那么该理论就是超一致的 $\mathcal{B}$。例如，对于任意真值代数 $\mathcal{B}$，我们都可以通过将 Q 和 R 解释为真值 ~ ~ ~$\top$，将 P 解释为真值 $\top \Rightarrow \top$，来构造规则 $P \longrightarrow (Q \Rightarrow R)$ 的一个模型。因此，由重写规则 $P \longrightarrow (Q \Rightarrow R)$ 构成的理论是超一致的。同理，我们可以证明，算术和简单类型论都是超一致的。

超一致性是证明归约终止性的一种模型论充分条件。该条件是否也是必要条件，仍是一个悬而未决的问题。

4.5 从超一致性到基于模型的切消证明

我们与 Olivier Hermant 注意到，如果将目标限定为证明超一致性意味着所有可证明的命题都有无切证明 [13]，那么证明超一致性蕴含证明约简的终止性这一结论的证明可以简化。在这种情况下，我们不必确立证明的性质，只需确立命题和序列式的性质。因此，我们可以不使用以证明集为元素的代数，而改用一种更简单的代数，其元素是序列式集：在可约性候选中，每个证明都会归结为其结论。

Tait 引理指出，若 π 是命题 A的证明，则它是 A的可约证明集 $[\![A]\!]$ 中的一个元素；该引理由此简化为这样一个事实：若序列式$\Gamma \vdash A$ 可证明，则它是 $[\![A]\!]$ 的一个元素。这个模型还可以进一步转换为一个真值为上下文集的模型，这些上下文集构成一个 Heyting 代数，并且满足：若 $\Gamma \in [\![A]\!]$，则 $\Gamma \vdash A$ 有无切证明。于是，Tait 引理可改述为这样一个事实：若序列式 $\Gamma \vdash A$ 可证明，则$\Gamma \in [\![A]\!]$。

可以证明，若序列式 $\Gamma \vdash A$ 在此模型中有效，则$\Gamma \in [\![A]\!]$；而 Tait 引理归结为这样一个事实：若序列式 $\Gamma \vdash A$ 可证，则它在此模型中有效。与基于模型的证明一样，这只是对应于此模型的可靠性引理的一个实例。事实上，若序列式 $\Gamma \vdash A$ 在此模型中有效，则 $\Gamma \in [\![A]\!]$，因而$\Gamma \vdash A$ 有无切证明；这是一条统一的强化完备性定理。

结论

逐步地，基于归约的方法与基于模型的方法之间在证明切消去方面的鸿沟已被弥合；与此同时，新的理论也被证明具有切消去性质。这两类证明都可以分解为两个步骤：首先证明所关注的理论是超一致的，然后证明一个与所关注理论无关的结论，即超一致性蕴含切消去。两者唯一的区别在于，选择何种真值代数来从超一致性推导出切消去：用可约候选项代数证明证明归约的终止性；用更简单的序列式代数构造一个模型，使得有效性蕴含无切可证性。

一旦实现这种趋同，就值得探索若干方向。首先，我们或许可以直接从超一致性推导证明论结果，而不必先证明切消去。其次，我们或许可以将超一致性的概念扩展到类型论。近期这项将模演绎与类型论联系起来的 [5] 或许是一个良好的起点。

参考文献

[1] L. Allali. 海廷算术模理论中的算法等式。高阶重写，2007。[2] P.B. Andrews. 类型论中的归结。《符号逻辑杂志》，36(3)：414–432，1971。[3] P. Brauner, C. Houtmann, and C. Kirchner. 超演绎实践。《重写、计算与证明：为纪念 Jean-Pierre Jouannaud 六十岁生日而作的论文集》，《计算机科学讲义》4600，施普林格，132–166，2007。[4] P. Brauner, G. Dowek, and B. Wack. 超演绎与模演绎中的规范化。手稿，2007。[5]D. Cousineau and G. Dowek. 在模 λΠ 演算中嵌入纯类型系统。《类型化λ演算及其应用》，《计算机科学讲义》4583，施普林格，102–117，2007。[6] M. Crabb´é. Zermelo 理论的非规范化。手稿，1974。[7] M. Crabb´é. 分层与割消去。《符号逻辑杂志》，56(1)：213–226，1991。[8] M. De Marco and J. Lipton. 直觉主义类型论中的完备性与切消去。《逻辑与计算杂志》，15：821–854，2005。[9] G. Dowek. 关于折叠-展开割与模割。《逻辑与计算杂志》，11(3)：419–429，2001。[10] G. Dowek. 真值代数与证明规范化，TYPES 2006，《计算机科学讲义》4502，施普林格，2007。[11] G. Dowek, T. Hardin, and C. Kirchner. 模定理证明。《自动推理杂志》，31：32–72，2003。[12] G. Dowek, T. Hardin, and C. Kirchner. HOL-lambda-sigma：高阶逻辑的一种内涵式一阶表达。《计算机科学中的数学结构》，11：1–25，2001。[13] G. Dowek and O. Hermant. 超一致性蕴含切消去的一个简单证明。《重写技术及其应用》，《计算机科学讲义》4533，96–106，2007。[14] G. Dowek and B. Werner. 模证明规范化。《符号逻辑杂志》，68(4)：1289–1316，2003。[15] G. Dowek and B. Werner. 作为模理论的算术。《项重写及其应用》，《计算机科学讲义》3467，施普林格，423–437，2005。

[16] J. Ekman。集合论中的规范证明。博士论文，查尔姆斯理工大学与哥德堡大学，1994。[17] J.-Y. Girard。G´odel 解释向分析的扩展，以及其在分析和类型´理论中切消去方面的应用。第二届斯堪的纳维亚逻辑研讨会，Noth Holland，第63–92页，1971。[18] J.-Y. Girard，高阶算术中的函数解释与切消去。博士论文，巴黎第七大学，1972。[19] L. Halln¨as。论集合论中证明的规范化。博士论文，斯德哥尔摩大学，1983。[20] O. Hermant。模约简中的语义方法。博士论文，巴黎第七大学，2005。[21] O. Hermant。直觉主义序列演算中的语义切消去。类型化λ演算及其应用，《计算机科学讲义》第3461卷，施普林格，第221–233页，2005。[22] M. Okada。关于各种一阶与高阶逻辑的切消去及完备性的统一语义证明。《理论计算机科学》281：471–498，2002。[23] M. Parigot。二阶经典自然演绎的强规范化。《计算机科学中的逻辑》，第39–46页，1993。[24] D. Prawitz。高阶逻辑的主定理。《符号逻辑杂志》33：452–457，1968。[25] D. Prawitz。自然演绎：证明论研究。Almqvist and Wiksell，1965。[26] W. W. Tait。二阶谓词逻辑中 Gentzen 主定理的一个非构造性证明。《美国数学会通报》72：980–983，1966。[27] W. W. Tait。有限类型泛函 I 的意向解释。《符号逻辑杂志》32：198–212，1967。[28] M. o. Takahashi。简单类型论中切消去定理的一个证明。《日本数学会杂志》19：399–410，1967。[29] B. Wack。重写演算中的类型与演绎。博士论文，亨利·庞加莱大学南锡一大，2005。[30] B. Werner。归纳构造理论。博士论文，巴黎第七大学，1994。