arXiv:2304.05085v1 [cs.LO] 11 Apr 2023

补：有限证明与无限证明之间的桥梁

Gilles Dowek[1] 和 Ying Jiang[2]

[1] Inria 和 ´巴黎萨克雷高等师范学校，法国卡尚 94235，普雷西登特·威尔逊大道 61 号，gilles.dowek@ens-cachan.fr。[2] 中国科学院软件研究所计算机科学国家重点实验室，中国北京 100190，jy@ios.ac.cn。

摘要。当某个命题在一个推理系统中不可证时，有时构造一个反证会很有用，它能够逐步说明不可证的原因。一般来说，这种反证是在另一个推理系统中的（可能）无限余归纳证明。本文指出，对于某些可判定推理系统，这个（可能）无限证明可以表示为另一个系统中的有限证明，而该系统与前一个系统等价。反过来，为了更好地说明不可证的原因，我们提出一种高效方法，将有限证明转换为（可能）无限证明。我们通过交替下推系统中的不可达性证明展示了该方法的应用。

1 引言

当一个命题在某个推理系统中没有证明时，有时构造一个反证来解释其不可证性的原因会很有用。

为了说明反证这一概念，我们来考虑一个推理系统，以及一个在该系统中不可证的命题。对于该系统中每条能够导出此命题的推理规则，至少有一个前提是不可证的。要说明此命题不可证，一种方法是针对这些规则，指出其中一个不可证的前提。为了说明这些前提不可证，我们以相同的方式余归纳地进行，从而构造一棵（可能是）无限树，逐步解释最初命题不可证的原因。这棵树称为该命题的反证。

为了在单个系统中表达证明和反证，我们将原推理系统 $\mathcal{I}$ 扩展为一个完备系统 $\mathcal{I}_{\mathcal{J}}$，称为 $\mathcal{I}$的补，该系统允许导出形如 $\vdash A$ 的序列式（当命题 A 在 $\mathcal{I}$ 中有证明时），以及形如 $\nvdash A$ 的序列式（当它没有证明时）。因此，在系统 $\mathcal{I}_{\mathcal{J}}$中，形如 $\vdash A$ 的序列式的证明是有限的，而形如 $\nvdash A$ 的序列式的证明则是（可能）无限的。

在本文中，这一补的一般概念被专门应用于一些可判定系统。在 [8], 我们介绍了一种通用方法，通过将其转换为自动机来证明推理系统 $\mathcal{I}$ 中可证性的可判定性

$\mathcal{A}$—一种仅包含引入规则的推理系统—同时保持可证明性。在这个自动机中，自底向上搜索命题 A的证明：如果该命题有证明，搜索就会成功；如果没有证明，则会在有限时间后失败。这个自动机中的证明 $\mathcal{A}$ 可以轻松转换为原系统 $\mathcal{I}$ 中的证明，因为自动机的所有规则 $\mathcal{A}$ 都可以在 $\mathcal{I}$中导出。

与原系统 $\mathcal{I}$一样，自动机 $\mathcal{A}$ 可以扩展为一个完备系统 $\mathcal{A}_\mathcal{B}$。系统 $\mathcal{B}$ 同样也是一个自动机。因此，在系统 $\mathcal{A}_\mathcal{B}$中，证明总是有限的。我们以此表明，形如 $\vdash A$ 的序列式在 $\mathcal{I}_\mathcal{J}$ 中有一个（可能是）无限证明，当且仅当它在 $\mathcal{A}_\mathcal{B}$中有一个有限证明。换句话说，在 $\mathcal{I}_\mathcal{J}$ 中的一个（可能是）无限证明，总能作为 $\mathcal{A}_\mathcal{B}$中的证明而具有一个有限表示。

然而，序列式 $\vdash A$ 在 $\mathcal{A}_\mathcal{B}$ 中的证明并不十分有说明力，因为它只能解释该序列式在自动机 $\mathcal{A}$ 中不可证的原因，而无法解释其在原始系统 $\mathcal{I}$ 中不可证的原因。本文的第三项贡献是提出一种有效且高效的方法，将 $\vdash A$ 在 $\mathcal{A}_\mathcal{B}$ 中的有限证明转化为该序列式在系统 $\mathcal{I}_\mathcal{J}$ 中一个更有说明力的（可能是）无限证明。

本文的灵感来源有三：第一个灵感来源是用于在模型检测中构造反例 [5] 的方法。这种构造反例的能力是模型检测的主要优势之一，因为它能够帮助找出复杂设计中细微错误的原因。第二个来源是逻辑程序设计中的否定概念，通常是指在 Prolog [12] 和人工智能系统（如 Planner [9]）中使用的失败即否定 [4], 概念。第三个来源是余归纳定义和余归纳证明 [10,13], 的概念，尤其是归纳可定义集合与余归纳可定义集合之间的对偶性。

本文其余部分结构如下。第 2 节回顾证明的概念后，我们在第 3 节展示如何将推理系统 $\mathcal{I}$ 扩展为完备系统 $\mathcal{I}_\mathcal{J}$。第 4 节首先回顾与推理系统 $\mathcal{I}$ 相关联的自动机 $\mathcal{A}$ 的概念。随后，我们将该自动机补为系统 $\mathcal{A}_\mathcal{B}$，并证明在 $\mathcal{A}_\mathcal{B}$ 中的证明总是有限的，且 $\mathcal{A}_\mathcal{B}$ 与 $\mathcal{I}_\mathcal{J}$ 等价。第 5 节是本文的主要贡献：我们设计了一种高效算法，能够将 $\mathcal{A}_\mathcal{B}$ 中的有限证明余归纳地转换为 $\mathcal{I}_\mathcal{J}$ 中信息更丰富的（可能是）无限证明。第 6 节通过在交替下推系统 [1] 中应用不可达性证书来说明该方法。

2 有限证明和无限证明

设 $\mathcal{S}$ 是一个集合，其元素称为命题。

定义 1（推理规则、推理系统、结论有限）。

推理规则是从 $\mathcal{S}^n$ 到 $\mathcal{S}$ 的一个偏函数，其中 n 是某个自然数，称为该规则的前提数。推理系统 $\mathcal{I}$ 是一组推理规则。它定义了一个从 $\mathcal{P}(\mathcal{S})$ 到 $\mathcal{P}(\mathcal{S})$ 的函数 $F_\mathcal{I}$

$$F_\mathcal{I}(X) = \{f(A_1, ..., A_n) \mid f \text{ in } \mathcal{I} \text{ and } A_1, ..., A_n \text{ in } X\}$$

如果对于每个命题 B，只有有限多个命题序列 $\langle A_1^1$、...、$A_{n_1}^1\rangle$、...、$\langle A_p^p$、...、$A_{n_p}^p\rangle$能通过该系统中的某条规则推导出 B，那么这个推理系统在结论方面是有限的。

下一个定义允许我们将如下规则简化为

$$\frac{P(x)\quad P(x)}{Q(x)}$$

与之等价的规则

$$\frac{P(x)}{Q(x)}$$

定义 2（简化）。设 f 是一条推理规则，D 是其定义域。若存在 i 和 j、$i \neq j$，使得对于所有 $\langle x_1$、...、$x_n\rangle$ 属于 D、$x_i = x_j$，则我们可以将这条规则 f 替换为由下式定义的等价规则 f'

$$f'(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_{j-1}, x_{j+1}, ..., x_n) = f(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_{j-1}, x_i, x_{j+1}, ..., x_n)$$

定义 3（可导出规则）。若 g 是一条具有 n 个前提的推理规则，且 f_1、...、f_n 是函数，并且每个 f_i 要么是具有 m_i 个前提的推理规则，要么是恒等函数，此时 $m_i = 1$，那么由下式定义的规则 h

$$h(x_1^1, ..., x_{m_1}^1, ..., x_1^n, ..., x_{m_n}^n) = g(f_1(x_1^1, ..., x_{m_1}^1), ..., f_n(x_1^n, ..., x_{m_n}^n))$$

是通过复合 g 和 f_1、...、f_n 得到的可导出规则。

该函数的定义域是满足以下条件的集合 $\langle x_1^1$、...、$x_{m_1}^1$、...、x_1^n、...、$x_{m_n}^n\rangle$：$\langle x_1^1$、...、$x_{m_1}^1\rangle$ 属于 f_1 的定义域，$\langle x_1^n$、...、$x_{m_n}^n\rangle$ 属于 f_n 的定义域，并且$\langle f_1(x_1^1$、...、$x_{m_1}^1)$ ...、$f_n(x_1^n$、...、$x_{m_n}^n)\rangle$ 属于 g 的定义域。

定义 4（连续，余连续）。单调函数 F 从$\mathcal{P}(\mathcal{S})$ 到 $\mathcal{P}(\mathcal{S})$，如果对于 $\mathcal{P}(\mathcal{S})$ 中的所有递增序列 X_0, X_1,...，$F(\bigcup_n X_n) = \bigcup_n F(X_n)$，则称其为连续函数。如果对于 $\mathcal{P}(\mathcal{S})$ 中的所有递减序列X_0, X_1,...，$F(\bigcap_n X_n) = \bigcap_n F(X_n)$，则称其为余连续函数。

定义5（证明）。推理系统 $\mathcal{I}$ 中的一个（可能是）无限证明，也称为余归纳证明，是一棵标记有命题的（可能是）无限树，满足：当一个节点标记为命题 B，且其子节点标记为命题 A_1、...、A_n时，则可以使用 $\mathcal{I}$ 的一个规则，根据命题序列 $\langle A_1$、...、$A_n\rangle$推导出 B。如果一个证明的根标记为 A，则该证明是命题 A的证明。

作为有限树的证明称为有限证明。

命题 1. 设 $\mathcal{I}$ 是一个推理系统。如果 $\mathcal{I}$ 的结论是有限的，那么

– 函数 $F_{\mathcal{I}}$ 单调、连续且余连续，– 它具有一个最小不动点和一个最大不动点，– $\mathcal{S}$ 中的一个元素属于 $F_{\mathcal{I}}$ 的最小不动点，当且仅当它在 $\mathcal{I}$ 中具有一个有限证明；并且它属于 $F_{\mathcal{I}}$ 的最大不动点，当且仅当它在 $\mathcal{I}$中具有一个（可能是）无限证明。

证明。参见 [13]。

3 补

定义 6（补、补）。设 $\mathcal{I}$ 是一个结论有限的推理系统。若推理系统 $\mathcal{J}$ 同样是结论有限的，并且对于每个命题 B，如果 $\langle A_1^1$、……、$A_{n_1}^1\rangle$、……、$\langle A_1^p$、……、$A_{n_p}^p\rangle$ 是所有能够通过 $\mathcal{I}$中的某条规则推导出 B的前提序列，那么能够通过 $\mathcal{J}$ 中的某条规则推导出 B 的前提序列，就是对于某个序列 j_i而言，形如 $\langle A_{j_1}^1$、……、$A_{j_p}^p\rangle$的所有序列，则称推理系统 $\mathcal{J}$ 是 $\mathcal{I}$的补。

设 $\mathcal{S}'$ 为包含形如 $\vdash A$ 和 $\nvdash A$ 的序列式的集合，其中 A 属于 $\mathcal{S}$。设 $\mathcal{I}$ 为一个推理系统，$\mathcal{J}$ 为 $\mathcal{I}$ 的一个补。对于每条属于 $\mathcal{I}$ 的推理规则 f，将规则映射 $\vdash A_1$、…、$\vdash A_n$ 映射为 $\vdash f$（A_1、…、A_n）；对于每条属于 $\mathcal{J}$ 的推理规则 f，将规则映射 $\nvdash A_1$、…、$\nvdash A_n$ 映射为 $\nvdash f$（A_1、…、A_n）。由此得到的推理系统 $\mathcal{I}_{\mathcal{J}}$ 称为 $\mathcal{I}$ 的一个补。

例 1。考虑这样一种语言：它包含一个常量 ε、一个一元函数符号 a，以及一元谓词符号 P、Q、R、S、T、U 和 V。按照惯例，项 $a(t)$ 写作 at。设 $\mathcal{I}$ 为包含以下推理规则的推理系统

$$\frac{U(x)}{Q(ax)} \qquad \frac{V(x)}{Q(ax)} \qquad \frac{T(x)}{R(ax)} \qquad \frac{}{T(x)} \qquad \frac{Q(x)\ R(x)}{P(x)}$$

$$\frac{S(x)}{P(x)} \qquad \frac{P(ax)}{Q(x)}$$

那么，包含以下规则的系统 $\mathcal{J}$

$$\frac{Q(x)\quad S(x)}{P(x)} \qquad \frac{R(x)\quad S(x)}{P(x)} \qquad \frac{P(a)}{Q(\varepsilon)} \qquad \frac{P(aax)\quad U(x)\quad V(x)}{Q(ax)} \qquad \frac{}{R(\varepsilon)}$$

$$\frac{T(x)}{R(ax)} \qquad \frac{}{S(x)} \qquad \frac{}{U(x)} \qquad \frac{}{V(x)}$$

是 $\mathcal{I}$ 的补，以及包含这些规则的系统 $\mathcal{I}_{\mathcal{J}}$

$$\frac{\vdash U(x)}{\vdash Q(ax)} \qquad \frac{\vdash V(x)}{\vdash Q(ax)} \qquad \frac{\vdash T(x)}{\vdash R(ax)} \qquad \frac{}{\vdash T(x)} \qquad \frac{\vdash Q(x)\quad \vdash R(x)}{\vdash P(x)}$$

$$\frac{\vdash S(x)}{\vdash P(x)} \qquad \frac{\vdash P(ax)}{\vdash Q(x)}$$

$$\frac{\nvdash Q(x)\quad \nvdash S(x)}{\nvdash P(x)} \qquad \frac{\nvdash R(x)\quad \nvdash S(x)}{\nvdash P(x)} \qquad \frac{\nvdash P(a)}{\nvdash Q(\varepsilon)} \qquad \frac{\nvdash P(aax)\quad \nvdash U(x)\quad \nvdash V(x)}{\nvdash Q(ax)} \qquad \frac{}{\nvdash R(\varepsilon)}$$

$$\frac{\nvdash T(x)}{\nvdash R(ax)} \qquad \frac{}{\nvdash S(x)} \qquad \frac{}{\nvdash U(x)} \qquad \frac{}{\nvdash V(x)}$$

是 $\mathcal{I}$的补。

定义7（共轭函数）。函数 F 从$\mathcal{P}(\mathcal{S})$ 到 $\mathcal{P}(\mathcal{S})$ 的共轭 G 是从 $\mathcal{P}(\mathcal{S})$ 到 $\mathcal{P}(\mathcal{S})$ 的函数，其定义为

$$G(X) = \mathcal{S} \setminus F(\mathcal{S} \setminus X)$$

引理 1。如果函数 F 是连续的，那么函数 G 是余连续的，并且 F 的最小不动点的补是 G的最大不动点：

$$\mathcal{S} \setminus (\bigcup_n F^n(\varnothing)) = \bigcap_n G^n(\mathcal{S})$$

证明。根据 G 的定义以及 F 的连续性，我们得到 G 是余连续的。然后，通过对 n 进行归纳法，我们证明 $G^n(\mathcal{S}) = \mathcal{S} \setminus F^n(\varnothing)$。由于 $\mathcal{S} \setminus \bigcup_n F^n(\varnothing) = \bigcap_n (\mathcal{S} \setminus F^n(\varnothing))$，我们得出结论： $\mathcal{S} \setminus (\bigcup_n F^n(\varnothing)) = \bigcap_n G^n(\mathcal{S})$。

引理 2。设 $\mathcal{I}$ 是一个具有补 $\mathcal{J}$ 的推理系统。那么，函数 $F_{\mathcal{J}}$ 是函数 $F_{\mathcal{I}}$ 的共轭函数，即对于 $\mathcal{P}(\mathcal{S})$ 中的所有 X ， $F_{\mathcal{J}}(X) = \mathcal{S} \setminus F_{\mathcal{I}}(\mathcal{S} \setminus X)$。

证明。考虑一个命题 B，并设 $\langle A^1_1$、...、 $A^1_{n_1}\rangle$、...、 $\langle A^p_1$、...、 $A^p_{n_p}\rangle$ 是这样的 p 序列： B 可以通过 $\mathcal{I}$ 的一条规则从这些序列中导出。

– 如果 B 是 $F_{\mathcal{J}}(X)$ 的一个元素，那么它可以通过 $\mathcal{J}$ 的一条规则，由 X 中的前提 $A^1_{j_1}$、...、 $A^p_{j_p}$ 导出。因此，这些命题中没有一个属于 $\mathcal{S} \setminus X$。序列 $\langle A^1_1$、...、 $A^1_{n_1}\rangle$、...、 $\langle A^p_1$、...、 $A^p_{n_p}\rangle$ 中的每一个都包含一个不属于 $\mathcal{S} \setminus X$ 的命题，因此 B 不能通过 $\mathcal{I}$ 的一条规则，由 $\mathcal{S} \setminus X$ 中的命题导出。于是， B 是 $\mathcal{S} \setminus F_{\mathcal{I}}(\mathcal{S} \setminus X)$ 的一个元素。– 反之，如果 B 是 $\mathcal{S} \setminus F_{\mathcal{I}}(\mathcal{S} \setminus X)$ 的一个元素，那么它不能通过 $\mathcal{I}$ 的一条规则，由 $\mathcal{S} \setminus X$ 中的命题导出。于是，序列 $\langle A^1_1$、...、 $A^1_{n_1}\rangle$、...、 $\langle A^p_1$、...、 $A^p_{n_p}\rangle$ 中的每一个都包含一个不属于 $\mathcal{S} \setminus X$ 的元素 $A^i_{j_i}$。因此，所有命题 $A^1_{j_1}$、...、 $A^p_{j_p}$ 都属于 X，从而 B 可以通过 $\mathcal{J}$ 的一条规则，由 X 中的命题导出。因此， B 是 $F_{\mathcal{J}}(X)$ 的一个元素。

命题 2. 设 $\mathcal{I}$ 是一个具有补 $\mathcal{J}$ 的推理系统。那么，一个命题在 $\mathcal{J}$ 中具有一个（可能是）无限证明，当且仅当它在 $\mathcal{I}$ 中没有有限证明。

证明。命题 A 在 $\mathcal{J}$ 中有一个（可能是）无限证明，当且仅当它是余连续函数 $F_{\mathcal{J}}$的最大不动点的一个元素；当且仅当它是 $F_{\mathcal{I}}$ 的余连续共轭函数的最大不动点的一个元素（根据引理2）；当且仅当它不是函数 $F_{\mathcal{I}}$ 的最小不动点的一个元素（根据引理 1）；当且仅当它在 $\mathcal{I}$中没有有限证明。

定理1（完备性）。设 $\mathcal{I}$ 是一个具有补集 $\mathcal{J}$的推理系统。则，对于 $\mathcal{S}$中的所有命题 A ，$\vdash A$ 要么有有限证明，要么在 $\mathcal{I}_{\mathcal{J}}$中有（可能的）无限证明。因此，系统 $\mathcal{I}_{\mathcal{J}}$ 是完备的。

证明。根据命题 2。

例 2. 序列式 $\vdash P(a)$ 在例 1 的系统 $\mathcal{I}_{\mathcal{J}}$ 中没有有限证明，而序列式 $\nvdash P(a)$ 有一个无限证明。

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dots}{\nvdash P(aaa)} \quad \dfrac{}{\nvdash U(aa)} \quad \dfrac{}{\nvdash V(aa)}}{\nvdash Q(aa)} \quad \dfrac{}{\nvdash S(aa)}}{\nvdash P(aa)} \quad \dfrac{}{\nvdash U(a)} \quad \dfrac{}{\nvdash V(a)}}{\nvdash Q(a)} \quad \dfrac{}{\nvdash S(a)}}{\nvdash P(a)}$$

4 从无限证明到有限证明

定义8（引入规则、自动机）。考虑 $\prec$ on $\mathcal{S}$上的一个良基序。若命题 B 可由前提 A_1、.....、 A_n 通过规则 r 可导出，则称规则 r 是关于 $\prec$的引入规则，此时我们有 $A_1 \prec B$、.....、 $A_n \prec B$。自动机是一个结论有限且仅包含引入规则的推理系统。

命题 3. 自动机 $\mathcal{A}$ 的补 $\mathcal{B}$ 也是一个自动机。

证明。根据补的定义即可得出。

命题 4. 设 $\mathcal{B}$ 是一个自动机。那么， $F_{\mathcal{B}}$ 的最小不动点和最大不动点相同。也就是说，一个命题在 $\mathcal{B}$ 中有（可能是）无限证明，当且仅当它在 $\mathcal{B}$ 中有有限证明。

证明。由于序 $\prec$ 是良基的，因此证明中的每个分支都是有限的。

定理 2（有限证明和无限证明）。设 $\mathcal{I}$ 是一个系统，使得

– $\mathcal{I}$ 有一个补 $\mathcal{J}$，– $\mathcal{I}$ 等价于一个自动机 $\mathcal{A}$，– 自动机 $\mathcal{A}$ 有一个补 $\mathcal{B}$。

那么，当序列式具有形式 $\vdash A$ （此时证明是有限的）或（可能）具有形式 $\nvdash A$ （此时证明是无限的）时，它在 $\mathcal{I}_{\mathcal{J}}$中有证明，当且仅当它在 $\mathcal{A}_{\mathcal{B}}$中有有限证明。

证明。根据定理的假设和命题 2，系统 $\mathcal{I}_{\mathcal{J}}$ 和$\mathcal{A}_{\mathcal{B}}$ 等价。根据命题 4， $\mathcal{A}_{\mathcal{B}}$中的所有证明都是有限的。

例 3。例 1 中定义的推理系统 $\mathcal{I}$等价于包含以下规则的自动机 $\mathcal{A}$

$$\frac{U(x)\ T(x)}{P(ax)} \qquad \frac{V(x)\ T(x)}{P(ax)} \qquad \frac{U(x)}{Q(ax)} \qquad \frac{V(x)}{Q(ax)} \qquad \frac{T(x)}{R(ax)}$$

$$\frac{}{T(x)}$$

$\mathcal{A}$ 的补 $\mathcal{B}$ 包含以下规则

$$\frac{U(x)\ V(x)}{P(ax)} \qquad \frac{U(x)\ T(x)}{P(ax)} \qquad \frac{T(x)\ V(x)}{P(ax)} \qquad \frac{T(x)}{P(ax)} \qquad \frac{}{P(\varepsilon)}$$

$$\frac{U(x)\ V(x)}{Q(ax)} \qquad \frac{}{Q(\varepsilon)} \qquad \frac{T(x)}{R(ax)} \qquad \frac{}{R(\varepsilon)} \qquad \frac{}{S(x)}$$

$$\frac{}{U(x)} \qquad \frac{}{V(x)}$$

因此，系统 $\mathcal{A}_{\mathcal{B}}$，也就是 $\mathcal{A}$的补，包含这些规则

$$\frac{\vdash U(x) \quad \vdash T(x)}{\vdash P(ax)} \qquad \frac{\vdash V(x) \quad \vdash T(x)}{\vdash P(ax)} \qquad \frac{\vdash U(x)}{\vdash Q(ax)} \qquad \frac{\vdash V(x)}{\vdash Q(ax)} \qquad \frac{\vdash T(x)}{\vdash R(ax)}$$

$$\frac{}{\vdash T(x)}$$

$$\frac{\nvdash U(x) \quad \nvdash V(x)}{\nvdash P(ax)} \qquad \frac{\nvdash U(x) \quad \nvdash T(x)}{\nvdash P(ax)} \qquad \frac{\nvdash T(x) \quad \nvdash V(x)}{\nvdash P(ax)} \qquad \frac{\nvdash T(x)}{\nvdash P(ax)} \qquad \frac{}{\nvdash P(\varepsilon)}$$

$$\frac{\nvdash U(x) \quad \nvdash V(x)}{\nvdash Q(ax)} \qquad \frac{}{\nvdash Q(\varepsilon)} \qquad \frac{\nvdash T(x)}{\nvdash R(ax)} \qquad \frac{}{\nvdash R(\varepsilon)} \qquad \frac{}{\nvdash S(x)}$$

$$\frac{}{\nvdash U(x)} \qquad \frac{}{\nvdash V(x)}$$

很容易验证，在 $\mathcal{I}_{\mathcal{J}}$ 中具有无限证明的序列式 $\nvdash P(a)$，在 $\mathcal{A}_{\mathcal{B}}$ 中具有有限证明

$$\frac{\dfrac{}{\nvdash U(\varepsilon)} \quad \dfrac{}{\nvdash V(\varepsilon)}}{\nvdash P(a)}$$

5 构建无限证明的算法

由定理 2 可知，如果序列式 $\nvdash A$ 在系统$\mathcal{A}_{\mathcal{B}}$ 中有一个有限证明，那么它在系统 $\mathcal{I}_{\mathcal{J}}$ 中就有一个（可能是）无限证明。利用 $\mathcal{A}_{\mathcal{B}}$ 的可判定性，可以有效地构造出这个证明。

例如，考虑例 1 和例 3 中的系统，序列式 $\nvdash P(a)$ 在 $\mathcal{A}_{\mathcal{B}}$ 中有证明。因此，它在 $\mathcal{I}_{\mathcal{J}}$ 中必定有一个（可能是）无限证明。对 $\mathcal{I}_{\mathcal{J}}$ 规则的分析表明，该证明的最后一条规则要么是

$$\frac{\nvdash Q(a) \quad \nvdash S(a)}{\nvdash P(a)}$$

or

$$\frac{\nvdash R(a) \quad \nvdash S(a)}{\nvdash P(a)}$$

利用 $\mathcal{A}_{\mathcal{B}}$ 的可判定性，我们得知序列式 $\nvdash Q(a)$ 和 $\nvdash S(a)$ 在 $\mathcal{A}_{\mathcal{B}}$ 中有证明，但序列式 $\nvdash R(a)$ 没有。因此，$\mathcal{I}_{\mathcal{J}}$ 中证明的最后一条规则必定是这两条规则中的第一条。我们可以用这条规则开始证明。

$$\frac{\dfrac{\ldots}{\nvdash Q(a)} \quad \dfrac{\ldots}{\nvdash S(a)}}{\nvdash P(a)}$$

然后，我们考虑 $\mathcal{I}_{\mathcal{J}}$ 中最后使用的规则，分别用来证明序列式$\nvdash Q(a)$和 $\nvdash S(a)$），依此类推。根据 $\mathcal{A}_{\mathcal{B}}$的可判定性选取系统 $\mathcal{I}_{\mathcal{J}}$的规则的前提，对同一过程进行余归纳地应用，得到示例 2 中给出的无限证明。

这种方法利用 $\mathcal{A}_{\mathcal{B}}$ 的可判定性，从 $\mathcal{A}_{\mathcal{B}}$ 中的有限证明余归纳地构造出 $\mathcal{I}_{\mathcal{J}}$ 中（可能是）无限证明，虽然有效，但效率很低，因为在构造 $\mathcal{I}_{\mathcal{J}}$ 中的证明时，每一步都需要使用 $\mathcal{A}_{\mathcal{B}}$ 的完整判定算法。

在本节余下部分，我们将在某些特定情况下开发一种更高效的算法来构造这样的证明。该算法以如下命题的构造性证明形式给出：如果一个序列式在 $\mathcal{A}_{\mathcal{B}}$ 中有证明，那么它在 $\mathcal{I}_{\mathcal{J}}$ 中有余归纳证明（定理 3 ）。

5.1 饱和系统

与上一节一样，我们考虑命题上的良基序 $\prec$，并将规则分为引入规则和非引入规则。对于

对于每个非引入规则，我们选择将前提分为主要前提和非主要前提，使得每条规则至少有一个主要前提；我们称一个证明为切，当它以一条非引入规则结束，且其所有主要前提都由以引入规则结束的证明证明。

定义 9（切）。切是一种如下形式的证明:

$$\dfrac{\dfrac{\dfrac{\rho_1^1}{A_1^1}\ \ldots\ \dfrac{\rho_{k_1}^1}{A_{k_1}^1}}{A^1}\,\text{intro}\quad\ldots\quad\dfrac{\dfrac{\dfrac{\rho_1^m}{A_1^m}\ \ldots\ \dfrac{\rho_{k_m}^m}{A_{k_m}^m}}{A^m}\,\text{intro}\quad\dfrac{\pi_{m+1}}{A^{m+1}}\ \ldots\ \dfrac{\pi_n}{A^n}}{A}\,\text{non-intro}$$

其中 A^1,..., A^m 是非引入规则的主要前提。

如果一个证明的某个子树是切，那么该证明就包含一个切。

命题 5（无切证明）。证明是无切的，当且仅当它只包含引入规则。

证明。见 [8]。

定义 10（饱和系统）。如果一个推理系统每当包含

– 一个具有 n 个前提的非引入规则 g，其中最左边的 m 个前提是主要前提；– 引入规则 f_1、 ...、 f_m m

它还包含通过将 g 与 f_1、...、 f_m 以及恒等函数复合 $n-m$ 次而得到的可导出规则的简化。

在本节中，我们只考虑包含于某个饱和系统 $\mathcal{I}'$ 中且与之等价的推理系统 $\mathcal{I}$。

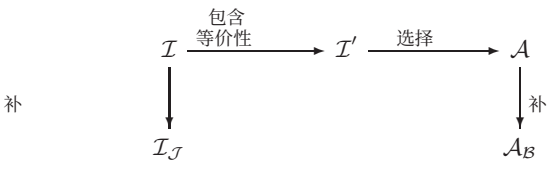
命题 6（切消去）。设 $\mathcal{I}'$ 是一个饱和系统。 $\mathcal{I}'$ 中的每个证明都可以化简为一个无切证明，其中只包含引入规则。

证明。由于 $\mathcal{I}'$ 是饱和的，我们可以用 $\mathcal{I}'$ 的一个可导出规则替换每个切规则。随着证明中的规则数量减少，这一过程最终会终止。

命题 7（自动机）。设 $\mathcal{I}'$ 是一个饱和系统。那么，由 $\mathcal{I}'$ 的引入规则构成的自动机 $\mathcal{A}$ 与 $\mathcal{I}'$ 等价。

证明。由命题 5 和 6。

推理系统 $\mathcal{I}$、 $\mathcal{I}_{\mathcal{J}}$、 $\mathcal{I}'$、 $\mathcal{A}$ 和 $\mathcal{A}_{\mathcal{B}}$ 之间的关系如下面的图所示。



例 4。例1 的系统 $\mathcal{I}$ 被包含在饱和系统 $\mathcal{I}'$中，该系统包含 $\mathcal{I}$ 的规则以及以下规则

$$\frac{U(x)\ T(x)}{P(ax)} \qquad \frac{V(x)\ T(x)}{P(ax)} \qquad \frac{U(x)\ T(x)}{Q(x)} \qquad \frac{V(x)\ T(x)}{Q(x)}$$

选择 $\mathcal{I}'$ 的引入规则可得到例 3 中的自动机 $\mathcal{A}$ 。

5.2 有限饱和系统中规则的秩

引理3。考虑一个非引入规则 r、一个由r 和引入规则得到的可导出规则 r' 、一个命题 A，以及一个前提序列 $\langle D_1$、...、 $D_n\rangle$，由此可以借助 r'导出 A。那么，存在一个前提序列 $\langle C_1$、...、 $C_p\rangle$，由此可以借助 r 和 $\{D_1, ..., D_n\} \prec_{DM} \{C_1, ..., C_p\}$导出 A，其中 $\prec_{DM}$ 是 $\prec$ [7]的多重集扩张。

证明。根据 r' 的构造，多重集 $\{D_1, ..., D_n\}$ 是通过从 $\{C_1, ..., C_p\}$ 中移除一些前提，并添加一些命题而得到的；这些命题可由严格小于被移除前提的引入规则推导出来。

引理4. 令 $\mathcal{I}'$ 为一个有限饱和规则集，且 r_1、 r_2、...、 r_k 为 $\mathcal{I}'$中的规则序列，使得该序列中的每条规则都是由前一条规则和引入规则得到的可导出规则。那么，该序列的长度 k 小于或等于 $\mathcal{I}'$中的规则数量。

证明。我们需要证明的只是，对于所有满足 $i < j$ 的 i 和 j ，都有$r_i \neq r_j$。假设 $r_i = r_j$。考虑一个命题 A 以及一个前提序列 $\langle D_1$、...、 $D_n\rangle$，由此可以借助 r_j 推导出 A 。根据引理3，存在一个前提序列 $\langle C_1$、...、 $C_p\rangle$，由此可以借助 r_i 推导出 A，并且$\{D_1, ..., D_n\} \prec_{DM} \{C_1, ..., C_p\}$。由于 $r_i = r_j$，我们可以构造一个严格递增的无限前提集合序列，由此可以借助 r_i证明 A ，这与 r_i 在结论方面是有限的这一事实相矛盾。

定义11（秩）。考虑一个有限饱和规则集。该集合中规则 r 的秩是从 r 开始的规则 r_1、 r_2、...、 r_k 的最长序列长度，其中规则 r_2、...、 r_k 中的每一条都是由前一条规则和引入规则得到的非引入可导规则。

5.3 构建无限证明

命题 8. 考虑一个自然数 $n \geq 1$、 n 集合族 $\langle H_1^1$、...、 $H_{k_1}^1\rangle$、...、 $\langle H_1^n$、...、 $H_{k_n}^n\rangle$ 以及一个集合 W，使得形如 $H_{j_1}^1 \cup ... \cup H_{j_n}^n$ 的每个 $k_1 \times ... \times k_n$ 集合都包含 W 的一个元素。那么，存在一个指标 l、 $1 \leq l \leq n$，使得集合 H_1^l、...、 $H_{k_l}^l$ 中的每一个都包含 W 的一个元素。

证明。对 n 进行归纳法。

如果 $n=1$，那么集合 H_1^1、.....、$H_{k_1}^1$ 中的每一个都包含 W 的一个元素。

然后，假设该性质对 n 成立，并考虑 $\langle H_1^1$、...、 $H_{k_1}^1\rangle$、...、 $\langle H_1^n$、...、 $H_{k_n}^n\rangle$、$\langle H_1^{n+1}$、...、 $H_{k_{n+1}}^{n+1}\rangle$，使得形如 $H_{j_1}^1 \cup ... \cup H_{j_n}^n \cup H_{j_{n+1}}^{n+1}$ 的每个 $k_1 \times ... \times k_n \times k_{n+1}$ 集合都包含 W 的一个元素。我们有

– 每一个形如 $(H_{j_1}^1 \cup ... \cup H_{j_n}^n) \cup H_1^{n+1}$ 的 $k_1 \times ... \times k_n$ 集合都包含 W 的一个元素，–...，– 每一个形如 $(H_{j_1}^1 \cup ... \cup H_{j_n}^n) \cup H_{k_{n+1}}^{n+1}$ 的 $k_1 \times ... \times k_n$ 集合都包含 W 的一个元素。

因此，

– 要么每个形如 $H_{j_1}^1 \cup ... \cup H_{j_n}^n$ 的 $k_1 \times ... \times k_n$ 集合都包含 W 的一个元素，要么 H_1^{n+1} 包含 W 的一个元素，–.....，– 要么每个形如 $H_{j_1}^1 \cup ... \cup H_{j_n}^n$ 的 $k_1 \times ... \times k_n$ 集合都包含 W 的一个元素，要么 $H_{k_{n+1}}^{n+1}$ 包含 W 的一个元素。

因此，

– 要么每个形如 $H_{j_1}^1 \cup ... \cup H_{j_n}^n$ 的 $k_1 \times ... \times k_n$ 集合都包含 W 的一个元素，– 要么 H_1^{n+1} 包含 W 的一个元素，.....，并且 $H_{k_{n+1}}^{n+1}$ 包含 W 的一个元素。

因此，根据归纳假设，要么存在一个指标 $l \leq n$，使得集合 H_1^l、.....、 $H_{k_l}^l$ 中的每一个都包含 W 的一个元素；要么集合 H_1^{n+1}、.....、 $H_{k_{n+1}}^{n+1}$ 中的每一个都包含 W 的一个元素。也就是说，存在一个指标 $l \leq n+1$，使得集合 H_1^l、.....、$H_{k_l}^l$ 中的每一个都包含 W 的一个元素。

命题 9。设 $\mathcal{I}$ 是一个推理系统，使得

– $\mathcal{I}$ 有一个补 $\mathcal{J}$，– $\mathcal{I}$ 被包含于一个饱和系统 $\mathcal{I}'$且与其等价，– 通过选择 $\mathcal{I}'$ 中的引入规则得到的自动机 $\mathcal{A}$ 有一个补 $\mathcal{B}$。

那么，如果 A 是一个命题，使得序列式 $\nvdash A$ 在 $\mathcal{A}_\mathcal{B}$ 和$\langle C_1$、.....、 $C_n\rangle$ 中有证明，而 $C_n\rangle$ 是一个前提序列， A可通过$\mathcal{I}$ 的一条规则导出，那么该序列中存在一个元素 C_i，使得序列式 $\nvdash C_i$ 在 $\mathcal{A}_\mathcal{B}$ 中有证明。

证明。对秩为 r 的规则进行归纳法，该规则允许在 $\mathcal{I}$ 中从$\langle C_1$、...、 $C_n\rangle$ 推导出 A 。

若 $r=0$，允许从 $\langle C_1$、...、 $C_n\rangle$ 推导出 A 的规则是引入规则。它也是 $\mathcal{A}$ 的规则，并且根据 $\mathcal{B}$的构造， $\langle C_1$、...、 $C_n\rangle$ 包含一个元素 C_i，使得序列式 $\nvdash C_i$ 在 $\mathcal{A}_\mathcal{B}$ 中有一个证明。

– 如果 $r > 0$，那么令 m 为满足以下条件的项：最左侧的 m 个前提是该规则的主要前提；并考虑以 C_1 为结论、相应前提集合分别为 H_1^1、...、$H_{k_1}^1$、... 的 k_1 个 $\mathcal{I}'$ 引入规则，以及以 C_m 为结论、相应前提集合分别为 H_1^m、...、$H_{k_n}^m$ 的 k_m 个 $\mathcal{I}'$ 引入规则。注意，所有这些规则也是 $\mathcal{A}$ 的规则。令 $k_{m+1} = ... = k_n = 1$ 和 $H_1^{m+1} = \{C_{m+1}\}$、...、$H_1^n = \{C_n\}$。由于系统 $\mathcal{I}'$ 是饱和的，它包含以 A 为结论且前提集合具有 $H_{j_1}^1 \cup ... \cup H_{j_n}^n$ 形式的 $k_1 \times ... \times k_n$ 条规则。这些规则的秩为 $< r$。根据归纳假设，这些 $k_1 \times ... \times k_n$ 个集合中的每一个都包含一个命题 K，使得 $\nvdash K$ 在 $\mathcal{A}_\mathcal{B}$ 中有证明。令 W 为这些 $k_1 \times ... \times k_n$ 个命题组成的有限集。根据命题 8，存在一个指标 l，使得每个 H_j^l 都包含一个属于 W 的命题 K_j^l。如果 $l \leq m$，那么序列式 $\nvdash K_j^l$ 在 $\mathcal{A}_\mathcal{B}$ 中有证明。因此，由于 $\mathcal{B}$ 是 $\mathcal{A}$ 的补，$\nvdash C_l$ 在 $\mathcal{A}_\mathcal{B}$ 中有证明。如果 $l > m$，那么 $K_1^l = C_l$，且 $\nvdash C_l$ 在 $\mathcal{A}_\mathcal{B}$ 中有证明。

定理 3（ $\mathcal{I}_\mathcal{J}$中反证的存在性）。设 $\mathcal{I}$ 是一个推理系统，使得

– $\mathcal{I}$ 有一个补 $\mathcal{J}$，– $\mathcal{I}$ 包含于一个饱和系统 $\mathcal{I}'$中，且与之等价，– 通过选取 $\mathcal{I}'$ 中的引入规则得到的自动机 $\mathcal{A}$ 有一个补 $\mathcal{B}$。

那么，若序列式 $\nvdash A$ 在系统 $\mathcal{A}_\mathcal{B}$中有一个证明，则它在系统 $\mathcal{I}_\mathcal{J}$中有一个（可能是）无限证明。

证明。根据命题 9，对于 $\mathcal{I}$中允许从 $\langle C_1,...,C_n\rangle$导出 A的每条规则，都存在一个 i，使得 $\nvdash C_i$ 在 $\mathcal{A}_\mathcal{B}$中可导出。由于 $\mathcal{J}$ 是 $\mathcal{I}$的补，因此存在一条 $\mathcal{I}_\mathcal{J}$ 中的规则，可从序列式 $\nvdash C_i$导出 $\nvdash A$。我们以余归纳的方式构造这些序列式的证明。

例 5。考虑例 1 和例 3 中的推理系统 $\mathcal{I}_\mathcal{J}$ 和 $\mathcal{A}_\mathcal{B}$。我们有 $\nvdash P(a)$ 在 $\mathcal{A}_\mathcal{B}$中的一个证明

$$\dfrac{\overline{\nvdash U(\varepsilon)} \quad \overline{\nvdash V(\varepsilon)}}{\nvdash P(a)}$$

为了将此证明转化为 $\mathcal{I}_\mathcal{J}$ 中一个（可能的）无限证明，我们逐步使用定理 3 的证明所描述的算法。由于此证明使用命题 9，而命题 9 的证明又使用命题 8，因此该算法使用命题 9 的证明所描述的算法，而后者又使用命题 8 的证明所描述的算法。我们依次描述这三个算法。

在 $\mathcal{I}$ 例 1中给出的推理系统里，有两条规则可以证明$P(a)$。第一条来自前提序列 $\langle Q(a)\ R(a)\rangle$，第二条来自前提序列 $\langle S(a)\rangle$。命题 9的证明在第一个序列中给出了命题 $Q(a)$，在第二个序列中给出了命题 $S(a)$以及证明

$\mathcal{A}_{\mathcal{B}}$ 中的 $\nvdash Q(a)$ 和 $\nvdash S(a)$:

$$\frac{\dfrac{}{\nvdash U(\varepsilon)} \quad \dfrac{}{\nvdash V(\varepsilon)}}{\nvdash Q(a)} \qquad \text{and} \qquad \frac{}{\nvdash S(a)}$$

由于 $\mathcal{J}$ 是 $\mathcal{I}$的补，补 $\mathcal{I}_{\mathcal{J}}$ 中存在一条规则，允许从 $\nvdash Q(a)$和 $\nvdash S(a)$推导出 $\nvdash P(a)$:

$$\frac{\nvdash Q(x) \quad \nvdash S(x)}{\nvdash P(x)}$$

所以我们用这条规则开始证明

$$\frac{\dfrac{\dots}{\nvdash Q(a)} \quad \dfrac{\dots}{\nvdash S(a)}}{\nvdash P(a)}$$

我们余归纳地将相同的过程应用于序列式 $\nvdash Q(a)$ 和 $\nvdash S(a)$，从而得到示例 2 中给出的无限证明。

现在让我们关注一下，命题9的证明如何在序列 $\langle Q(a)\ R(a)\rangle$中给出命题 $Q(a)$，并在 $\mathcal{A}_{\mathcal{B}}$ 中构造 $\nvdash Q(a)$ 的证明。

允许从 $\langle Q(a)\ R(a)\rangle$ 推导出 $P(a)$ 的 $\mathcal{I}$规则，在$\mathcal{I}'$ 的示例 4 中秩为 1。命题 $Q(a)$ 可以在 $\mathcal{I}$ 中使用来自集合 $H_1^1 = \{U(\varepsilon)\}$ 和 $H_2^1 = \{V(\varepsilon)\}$ 的引入规则得到证明。命题 $R(a)$ 可以在 $\mathcal{I}$ 中使用来自集合 $H_1^2 = \{T(\varepsilon)\}$ 的引入规则得到证明。由于系统$\mathcal{I}'$ 是饱和的，它包含两个可导出规则，允许分别直接从 $H_1^1 \cup H_1^2 = \{U(\varepsilon)\ T(\varepsilon)\}$ 和从 $H_2^1 \cup H_1^2 = \{V(\varepsilon)\ T(\varepsilon)\}$ 推导出 $P(a)$。这些规则是

$$\frac{U(x) \quad T(x)}{P(ax)} \qquad \text{and} \qquad \frac{V(x) \quad T(x)}{P(ax)}$$

而且二者的秩都小于 1，也就是 0。因此，它们是引入规则，进而也是 $\mathcal{A}$ 的规则。由此，命题 $P(a)$ 可分别从 $\mathcal{A}$ 中的前提序列 $\langle U(\varepsilon)\ T(\varepsilon)\rangle$ 以及前提序列 $\langle V(\varepsilon)\ T(\varepsilon)\rangle$ 推导出来。从 $\mathcal{A}_{\mathcal{B}}$ 中 $\nvdash P(a)$ 的证明可知，在这两个序列中各有一个命题 K，使得 $\nvdash K$ 在 $\mathcal{A}_{\mathcal{B}}$ 中有证明；也就是说，第一个序列中的 $U(\varepsilon)$ 和第二个序列中的 $V(\varepsilon)$，并且还有 $\mathcal{A}_{\mathcal{B}}$ 中的证明

$$\frac{}{\nvdash U(\varepsilon)} \qquad \text{and} \qquad \frac{}{\nvdash V(\varepsilon)}$$

设 $W = \{U(\varepsilon)\ V(\varepsilon)\}$。命题 8 的证明应用于 W、 H_1^1、 H_2^1和H_1^2，为我们给出了指标 1。因此，集合 H_1^1和 H_2^1都包含 W 的一个元素：$U(\varepsilon)$ 和 $V(\varepsilon)$，分别如此。由于这些命题属于 W，我们在 $\mathcal{A}_{\mathcal{B}}$ 中有序列式 $\nvdash U(\varepsilon)$ 和 $\nvdash V(\varepsilon)$的证明。通过构造 $\mathcal{B}$，系统$\mathcal{A}_{\mathcal{B}}$ 包含一条规则，允许从 $\nvdash U(\varepsilon)$和 $\nvdash V(\varepsilon)$ 推导出 $\nvdash Q(a)$。我们由此构造出 $\mathcal{A}_{\mathcal{B}}$ 中的证明

$$\frac{\dfrac{}{\nvdash U(\varepsilon)} \quad \dfrac{}{\nvdash V(\varepsilon)}}{\nvdash Q(a)}$$

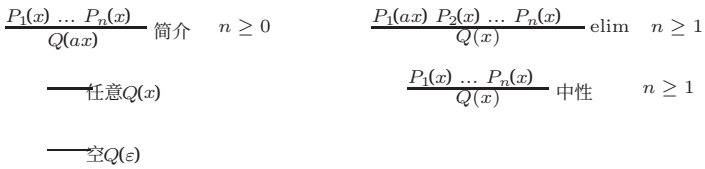


图 1. 交替下推系统

最后，让我们关注一下，命题8 的证明如何从集合 H_1^1、 H_2^1、 H_1^2 和 W得到指标1。注意，集合 $H_1^1 \cup H_1^2$是 $\{U(\varepsilon)\} \cup \{T(\varepsilon)\}$，而 $H_2^1 \cup H_1^2$是 $\{V(\varepsilon)\} \cup \{T(\varepsilon)\}$。那么，要么集合 $\{U(\varepsilon)\}$ 和 $\{V(\varepsilon)\}$ 中的每一个都包含 W 中的一个元素，要么 $\{T(\varepsilon)\}$ 包含一个元素。在这种情况下，集合 $\{U(\varepsilon)\}$ 和 $\{V(\varepsilon)\}$ 中的每一个都包含 W 中的一个元素。因此我们得到 $l = 1$。

6 应用

本节将通过一个关于交替下推系统的应用，阐述本文的主要结果。

定义 12（交替下推系统）。考虑一种语言 $\mathcal{L}$，其中包含有限个一元谓词符号、有限个一元函数符号以及一个常量 ε。交替下推系统是一种推理系统，其规则与图 1 所示的规则类似，其中每条规则的所有前提彼此不同。

图 1左栏中的规则——引入规则、任意规则和空规则——是引入规则，而右栏中的规则——消去规则和中性规则——则不是。消去规则有一个主要前提，即最左侧的前提；而中性规则的所有前提都是主要前提。

例 1 中介绍的系统 $\mathcal{I}$ 是一个交替下推系统。为了将定理 1、2 和 3 应用于交替下推系统，我们需要证明的是。

–对于每个交替下推系统 $\mathcal{I}$，存在一个有限的饱和系-统 $\mathcal{I}'$ 使得 $\mathcal{I}$ 被包含于且等价于 $\mathcal{I}'$，– 每个交替下推系统 $\mathcal{I}$ 都有一个补 $\mathcal{I}_{\mathcal{J}}$。

为了构建饱和系统 $\mathcal{I}'$，我们引入以下始终会终止的饱和过程 [8]。

定义 13（饱和）。每当我们有一个具有 n 个前提的非引入规则 g，其中最左侧的 m 个前提是主要前提，并且有 m 个引入规则 f_1、.....、 f_m 时，就将通过复合 g 与 f_1、.....、 f_m 以及 $n - m$ 次恒等函数所得到的可导出规则进行简化，并将其加入。

为了证明每个交替下推系统 $\mathcal{I}$ 都有补 $\mathcal{I}_{\mathcal{J}}$，我们从以下引理开始。

引理5. 对于每个交替下推系统 $\mathcal{I}$，都存在一个等价的 ˆ 推理系统 $\mathcal{I}$ 和一个有限集 $\mathcal{C}$，使得

ˆ – $\mathcal{I}$ 的规则的结论属于 $\mathcal{C}$，– 对于每个闭命题 A，在 $\mathcal{C}$ 中都存在唯一的命题 B，使得 A 是 B的一个实例。

证明。我们以 $\mathcal{C}$为例，取包含所有形如 $P(\varepsilon)$和 $P(ax)$的原子命题的集合。然后，我们将每条以 $P(x)$为结论的中性规则和消去规则，替换为一条以 $P(\varepsilon)$为结论的实例，并且对于每个函数符号 a，替换为一条以 $P(ax)$为结论的实例。

ˆ例 6. 令 $\mathcal{I}$ 为 例 1 中引入的系统。系统 I 是

$$\frac{U(x)}{Q(ax)} \qquad \frac{V(x)}{Q(ax)} \qquad \frac{T(x)}{R(ax)} \qquad \frac{}{T(\varepsilon)} \qquad \frac{}{T(ax)}$$

$$\frac{Q(\varepsilon)\ \ R(\varepsilon)}{P(\varepsilon)} \qquad \frac{Q(ax)\ \ R(ax)}{P(ax)} \qquad \frac{S(\varepsilon)}{P(\varepsilon)} \qquad \frac{S(ax)}{P(ax)} \qquad \frac{P(a)}{Q(\varepsilon)}$$

$$\frac{P(aax)}{Q(ax)}$$

定义14（补）。设 $\mathcal{I}$ 是一个交替下推系统，ˆ$\mathcal{I}$是引理 5 中构造的系统，且 $\mathcal{C}$ 是原子命题的有限集，使得

ˆ – $\mathcal{I}$ 的规则的结论都属于集合 $\mathcal{C}$，– 对于每个闭命题 A，在 $\mathcal{C}$ 中存在唯一一个命题 B，使得 A 是 B的一个实例。

ˆ 接下来，我们如下定义系统 $\mathcal{J}$：对于 $\mathcal{C}$中的每个 B，如果系统 $\mathcal{I}$ 包含n 条规则 r_1^B,...,r_n^B，其结论为 B,

$$\frac{A_1^1\ \ldots\ A_{m_1}^1}{B}$$

$$\ldots$$

$$\frac{A_1^n\ \ldots\ A_{m_n}^n}{B}$$

其中 n 可以为零，并且每个 m_i $(1 \leq i \leq n)$ 也可以为零，那么系统 $\mathcal{J}$包含这些 $m_1 \times \ldots \times m_n$ 规则

$$\frac{A_{j_1}^1\ \ldots\ A_{j_n}^n}{B}$$

ˆ 命题 10。系统 $\mathcal{J}$ 是 $\mathcal{I}$ 的补：对于每个命题 B，如果 $\langle A_1^1$、...、$A_{n_1}^1\rangle$、...、$\langle A_1^p$、...、$A_{n_p}^p\rangle$ 都是从中 Bˇ 在 $\mathcal{I}$ 中可导出的前提序列，那么从中 B 在 $\mathcal{J}$ 中可导出的前提序列都是形如 $\langle A_{j_1}^1$、...、$A_{j_p}^p\rangle$ 的序列，其中 j_i 是某个序列。

证明。考虑一个闭命题 B。存在唯一的命题 C in $\mathcal{C}$，使得 $B = \sigma C$。考虑所有结论为 C 的规则，并令 $\langle D_1^1, ..., D_{n_1}^1 \rangle, ..., \langle D_1^p, ..., D_{n_p}^p \rangle$ 为这些规则的所有前提。从中可在 $\hat{\mathcal{I}}$ 中导出 B 的前提序列为 $\langle \sigma D_1^1, ..., \sigma D_{n_1}^1 \rangle, ..., \langle \sigma D_1^p, ..., \sigma D_{n_p}^p \rangle$。根据构造，$\mathcal{J}$ 包含所有形如的规则。

$$\frac{D_{j_1}^1 \ \ldots \ D_{j_n}^n}{C}$$

因此，在 $\mathcal{J}$ 中可导出 B 的序列，都是形如 $\langle \sigma D_{j_1}^1$、...、$\sigma D_{j_p}^p \rangle$ 的序列，其中 j_i 是某个序列。

$\hat{}$ 例7。考虑例 6 中的系统 $\mathcal{I}$。按照定义14构造的补 $\mathcal{J}$ 包含以下推理规则。

$$\frac{Q(\varepsilon) \quad S(\varepsilon)}{P(\varepsilon)} \qquad \frac{R(\varepsilon) \quad S(\varepsilon)}{P(\varepsilon)} \qquad \frac{Q(ax) \quad S(ax)}{P(ax)} \qquad \frac{R(ax) \quad S(ax)}{P(ax)} \qquad \frac{P(a)}{Q(\varepsilon)}$$

$$\frac{P(aax) \quad U(x) \quad V(x)}{Q(ax)} \qquad \frac{}{R(\varepsilon)} \qquad \frac{T(x)}{R(ax)} \qquad \frac{}{S(x)} \qquad \frac{}{U(x)}$$

$$\frac{}{V(x)}$$

注意，该系统与例1中介绍的补等价，但由于集合 $\mathcal{C}$ 的系统化定义，存在细微差异。

7 结论

我们介绍了一种通用方法，用于在命题无法在推理系统 $\mathcal{I}$中得到证明时构造反证。首先，我们证明了，如果推理系统 $\mathcal{I}$ 具有补 $\mathcal{J}$，那么可以将其扩展为完备系统 $\mathcal{I}_{\mathcal{J}}$，从而能够使用（可能是）无限证明证明形如 $\vdash A$ 和 $\nvdash A$的序列式（定理1）。然后，我们证明了，如果推理系统 $\mathcal{I}$ 等价于自动机 $\mathcal{A}$，且该自动机也具有补 $\mathcal{B}$，那么 $\mathcal{I}_{\mathcal{J}}$ 中的（可能是）无限证明总能作为 $\mathcal{A}_{\mathcal{B}}$ 中的证明而具有有限表示（定理2）。最后，我们介绍了一种有效且高效的方法，将系统 $\mathcal{A}_{\mathcal{B}}$ 中序列式 $\nvdash A$ 的有限证明转换为系统$\mathcal{I}_{\mathcal{J}}$中该序列式的（可能是）无限证明，并逐步解释不可证性的原因（定理3）。这些结果通过应用于交替下推系统进行了说明，在该应用中，它们产生了有限的不可达性证书。它们也可以顺利应用于其他推理系统，例如下推系统的动态网络 [2,11]。

致谢

作者感谢 Ahmed Bouajjani 富有启发性的讨论。本研究得到 ANR-NSFC 项目 LOCALI（NSFC 61161130530and ANR 11 IS02 002 01）和中国国家基础研究计划（973）项目（编号：2014CB340302）的资助。

参考文献

1.A. Bouajjani,J.Esparza,andO.Maler, 下推自动机的可达性分析：应用于模型检验 A.W.Mazurkiewicz, J.Winkowski（编）*Concurrency theory*, 《计算机科学讲义》, 1243, 1997, 135-150。 2.A.Bouajjani,M. M¨uller-Olm, T. Touili, 下推系统动态网络的正则符号分析 M. Abadi, L.deAlfaro,L.（编）CONCUR 2005, 《计算机科学讲义》, 3653, 2005, 473-487。3. C. Baier, J.-P. Katoen, *Principles of model checking*, MITPress, 2008。 4. K. Clark, 失败即否定, H.Gallaire andJ.Minker, （编）, *Logic and Databases* 1978 ,

Plenum Press, 。 5. E. Clarke, O. Grumberg,K.McMillan,X.Zhao, 符号模型检验中反例和见证的高效生成, *Design Automation Conference* 1995 427 432 , , -。

6. E. Clarke, O. Grumberg,D. Peled, *Model checking*, MIT Press, 2001。 7.N. Dershowitz andZ.Manna, 使用多重集序证明终止性, *Communications of the ACM* 22 8 1979, 465 476 , （）,

第–页。8. G. Dowek andY. Jiang,可判定性、引入规则和自动机, *International Conferences on Logic for Programming Artificial Intelligence and Reasoning* 2015 , , 。

9. C. Hewitt,PLANNER的描述与理论分析（使用模式）：一种用于证明定理和操作机器人模型的语言, A.I. Memo No.251, MIT Project MAC, 1972。10.B.Jacobsand J. Rutten, （余）代数与（余）归纳法导论, D. Sangiorgiand J.Rutten（编） *Advanced topics in bisimulation and coinduction*, 《理论计算机科学剑桥论丛》, 52, Cambridge University Press, 2011, 第38-99页。 11. P. Lammich, M.M¨uller-Olm, A.Wenner, 具有树正则约束的动态下推网络的前驱集合《计算机辅助验证》：第21届国际会议, CAV2009。 12. P.Roussel, PROLOG：使用手册, 内部报告, G.I.A., LUMINY UER, Universit´e d'Aix-Marseille, 1975。 13. D. Sangiorgi, *Introduction to Bisimulation and Coinduction*, Cambridge University Press, 2011。