星空下的学习基础

FeliceCardone
LucaPaolini意大利都灵大学计算机系
{felice.cardone,luca.paolini}@unito.it

计算机科学基础是理论研究中的一个重要领域，Stefano 在这一领域作出了重要贡献，尤其是从逻辑和证明论视角出发。最近，我们与他一起教授一门关于这一主题的入门课程，课程秉持这样一种理念：理解并撰写普通的论述性证明，是未来程序员应掌握的一项宝贵技能。这段共同经历启发了本文所采用的教学方法。

计算机科学中的具体基础主题背后蕴含着一些核心技巧，而这些技巧最适合通过实例来讲授。然而，标准教科书往往没有充分强调这些无处不在的技巧，也常常缺乏与信息学直接相关的实例。我们认为，与其只专注于具体的基础主题，不如突出这些基本技巧，这将为入门课程带来显著的教学益处。

本文提出将关系的传递闭包作为一个案例研究，以支持我们的方法。尽管所有证明都很基础，我们认为这是一个合适的主题，可以用来运用一些范式性概念——这些概念与计算思维内在相关——并将其作为计算机科学基础课程的结构锚点。具体而言，我们着重介绍证明中采用的技巧，这些技巧全面概括了入门逻辑课程通常教授的内容；同时也介绍抽象结构，它们使我们能够将传递闭包与克莱尼星号（通过量子格）以及闭包算子（定义在完备格上）联系起来。随后，我们概述了一系列可供进一步探讨的例子；正如我们关于星号的案例研究所示，这些例子可以作为一种动手实践的方法，帮助学生掌握计算基础课程中需要学习的基本分析技能。

谨以此文献给 Stefano Berardi，祝贺他生日。

1 引言

本文旨在介绍若干基本概念中的一种可能选择，它们可构成面向一年级学生（大学一年级学生）的计算机科学基础课程的骨干。本文采用相对叙述性的风格，是因为我们关注所选内容的教学价值；因此，我们优先讨论这些概念与其他主题和技巧之间的联系，而非其形式细节——顺便一提，这些概念早已广为人知。

我们的整体提议是改变此类课程的传统组织方式，调整其侧重点。计算机科学基础课程通常按章节展开，分别纵向讲解自动机、形式语言、可计算性和复杂性等基本概念；而我们认为，通过开展一个或多个横向项目，以连贯的叙述串联相关主题、形成横截面，可以增强学生对这门学科方法论连贯性的认识。

本文阐述了此类项目的核心内容，主要围绕迭代这一概念的两种关键表现形式展开：自反传递闭包和克莱尼迭代，它们是本文的主角。在最后一节，我们还提出了其他一些例子，可用于实现与本文相同的教学目的。

T. Altenkirch、F.Barbanera、F. Damiani 和 U. de'Liguoro（编）：《逻辑与类型理论：献给 Stefano Berardi 的论文集》，值其 64 岁生日之际出版，EPTCS 441，2026 年，第 83–95 页，
doi:10.4204/EPTCS.441.5

© Cardone, Paolini 本作品采用知识共享署名许可协议授权。

不过，在展开叙述之前，有必要先用几句话明确我们对将计算机科学基础作为一门教学学科的看法，尤其是考虑到我们所设想的这门课程具体实例的目标受众。

在整 个论述中，我们假定一年级学生已经接触过基础的 f:

1. 证明技巧（直接证明、反证法与逆否证明，以及简单形式的归纳法）。在此，我们假定证明规则被描述为自然演绎规则，特别是作为引入规则或消去规则。我们通常非正式地采用 Fitch [9], 所运用的子证明方法；关于此方法，已有大量面向多个课程体系一年级学生的优秀教科书，并附有许多详解习题；

2. 基本的集合论构造，如幂集、笛卡尔积、关系及其性质；

3. 各类代数结构，如格与幺半群，以及这些类别中自由结构的例子，特别是集合上的自由幺半群。我们还假定学生能够轻松地将在特定运算下封闭的元素集合识别为某种代数结构的实例：至少对于幂集（作为完备格概念或完备布尔代数的实例）以及字母表上的词集（作为该字母表上的自由幺半群），需要做到这一点。

按照对“基础”的主流理解，该学科的核心主题至少应包括：形式语言、自动机、一阶逻辑及其模型的基本内容。从这一角度看，基础可能会变得百科全书式，往往涵盖不适合入门课程的高级主题。我们主张一种不同的观点：基础最好被理解为一种面对问题求解的普遍态度。这种态度始于将自然语言谨慎地用作分析工具，并逐渐发展为对证明及其底层技巧、不同概念之间关系，以及在证明构造中利用这些概念之间差异所获优势的认识。在这一框架下，我们的方案可以被视为设计一个工作坊，旨在将这一思想背景的全部潜力应用于一组具有相关性的具体案例。

我们论述的出发点是集合上一个二元关系的传递闭包 这一概念，以及该概念的若干变体。需要特别指出的是，本文绝不应被理解为一篇技术性主题综述；对于这一主题，已有许多优秀论文从诸多不同的普遍性层次提供了介绍（相关参考文献见本文最后一节）。下文由一系列讲座的教学笔记组成，这些讲座在一个具体案例中体现了我们总体的教学方法；该案例的技术细节大多已经确立。

我们唯一的主张是，所选主题构成了一个连贯项目的主题，旨在学习本课程预期教授的基本技巧；我们希望这能有所助益，甚至能激发人们进一步讨论：对于我们所探讨的这类基础课程，哪些内容值得纳入。我们常常加入一些旁论，以激发读者兴趣并解释所引入的概念和构造：我们将它们置于本文的教学语境这一主线之中，同时也勾勒其历史背景；在许多情况下，这些背景与数学基础的发展密不可分。

我们的方法可以概括为横向的，即一种精心选择主题的做法，从而使这些证明能够在重要的启发性背景中提供主要的方法论示例。这应与更为传统的纵向 方法相对照，后者从固定范围中选取每个主题，并探究至预期深度。当然，此类示例很多，即便在这种情况下，也存在一些我们尚未走过、或仅仅略作提示并留待品味

授课者自行定夺的路径。其中一例是对闭包算子及相关闭包系统的简要提及，这或许可以用来说明“传递闭包”中的闭包所对应的含义。

2 传递闭包

设 $R \subseteq X \times X$ 是集合 X 上的一个二元关系。可能出现如下情形：对某些 $x,y,z \in X$，虽然有 xRy 且 yRz，但 xRz 并不成立；也就是说，关系 R 可能不是传递的。然而，在某些情况下，人们希望扩展 R，使之包含所有这样的对 (x,z)：存在 $y \in X$，使得 xRy 且 yRz。

例如，xRy 可能表示如下事实：从内存状态 x 出发，执行程序的一条指令后会到达状态 y。在这种情况下，为了描述整个程序的执行，我们自然会去研究序列

$$x = x_1 R x_2 R \dots R x_n = y$$

这些序列由有限多个（可能为 0 个）中间步骤组成，从输入 x 通向输出 y。这一新关系记作 R^*，它由 R 生成，其含义是：它是 R 的最小自反且传递扩张，即 R 的自反传递闭包。

题外话 1。 一般闭包概念的历史——自反传递闭包正是其中一个实例——可以追溯到抽象代数的起源，以及 Cantor、Dedekind 和稍晚一些的 E. H. Moore 在集合论方面的早期工作。完整的历史可在优秀综述的第 1 节中重构 [8]；它也与伽罗瓦连接的历史以及范畴论中的 伴随 概念有关（因此也与 单子概念有关；后者在研究编程语言的类型系统时变得十分重要）。同一作者还撰写了另一篇很不错的综述[7]。闭包概念的基础情形所蕴含的非正式思想是：有一个集合 $A \subseteq X$，需要根据定义在 X 的子集上的某种性质，通过添加点来完成。于是，将这一完成过程视为 X 上的一个算子，即一个函数 $c\colon \mathscr{P}X \to \mathscr{P}X$，它定义在 X 的子集上，便是很自然的；满足

- c 是膨胀的，也就是说 $X \subseteq cX$；
- c 是幂等的，$c \circ c = c$；
- c 是单调的，即 $cX \subseteq cY$ 当 $X \subseteq Y$ 时。

第一条性质表示点的（可能）增加，而幂等性则对应一种有趣的语言现象：闭合这一动词与填满等其他动词具有相同的现象。闭集的形式为 cX，对闭集进行闭合不会改变该集合：闭集是 c 的不动点。我们可以将闭包算子的序论性质推广到偏序集上的函数，但本文只需要算子表述；这已足以将自反传递闭包与另一种星号运算——克林闭包进行比较。

闭包算子 $c : \mathscr{P}X \to \mathscr{P}X$ 与摩尔族一一对应。摩尔族定义为 $\mathscr{C}$ 由 X 的子集组成的集合族，其中 $\mathscr{C}$ 中任意一组元素的交仍是 $\mathscr{C}$ 中的一个元素。例如，某个集合上的传递关系 τ 构成了此意义下的摩尔族（证明一组传递关系的交仍是传递关系，是一个简单的直接证明练习）。因此，传递闭包可以视为一种闭包算子，它将集合上的每个二元关系 R 映射为 τ 中所有包含 R 的元素的交。自最初的参考文献 [14] 以来，这种对应关系如今已成为广为人知的结论。

定义 2.1（自反传递闭包）**.** 令 1 表示 X 上的恒等关系，并令 $\circ$ 表示关系复合[1]。若 R 是集合 X 上的二元关系，则其传递闭包 $R^* \subseteq X \times X$ 是满足以下条件的最小关系 $S \subseteq X \times X$：

- $R \subseteq S$,
- $1 \subseteq S$，以及
  - $S \circ S \subseteq S$。显然，$R^* \subseteq X \times X$ 具有以下性质：$R \subseteq R^*$；$1 \subseteq R^*$；$R^* \circ R^* \subseteq R^*$。

练习 2.2。• 证明：二元关系 S 是传递的，当且仅当 $S \circ S \subseteq S$。当然，使用传递性的通常定义，即对于所有 x、y、z，当 xSz 且 zSy 时，S 传递当且仅当 xSy。

- 回顾一下，如果集合 X 上的关系满足：对于所有 x、$y \in X$，只要 xRy，就存在 $z \in X$ 使得 xRz 且 zRy，则称该关系是稠密的。包含关系[2] $S \subseteq S \circ S$ 是稠密关系的一个特征：证明存在不是稠密关系的传递关系。

现在的问题是如何构造 R^*。至少有四种等价的方法，每种方法都体现了构造传递闭包的不同视角。我们的主张是，证明这些方法等价的过程涉及学生在课程结束时应能熟练运用的大多数证明技巧。在下一节中，我们将用完备格相关的其他技巧来补充这些技巧，这也将说明为何我们选择（自反）传递闭包作为一个重要的案例研究。根据这些方法分别构造出的关系将记作 $R^{\Cap}, R^{\Cup}, R^{\triangledown}, R^{\triangle}$。它们各自都有自己的历史和个性。

定义 2.3. 设 R 是集合 X 上的一个二元关系。

1. 我们定义 $R^{\Cap} := \bigcap_{n\in\omega} S$。$1 \cup R \cup (S \circ S) \subseteq S$
2. 我们定义 $R^{\Cup} := \bigcup R^n$，其中 $R^0 := 1$ 且 $R^{n+1} := R \circ R^n$。
3. 以下规则中，$x, y, z \in X$，定义了一个形式系统，其定理恰好刻画了所有属于 $R^{\triangledown}$ 的有序对：

$$\frac{}{xR^{\triangledown}x}\ (\mathrm{id}) \qquad \frac{xRy}{xR^{\triangledown}y}\ (\mathrm{in}) \qquad \frac{xRy \quad yR^{\triangledown}z}{xR^{\triangledown}z}\ (\mathrm{tx})$$

（第二条规则是多余的，见下方练习 2.4。）

4. 设 $R[A] := \{b \mid \exists a \in A, aRb\}$，则我们定义

$$R^{\triangle} := \{(x,y) \mid \forall A \subseteq X\big(\text{ if } (R[A] \subseteq A \text{ and } x \in A) \text{ then } y \in A\big)\}.$$

补充说明 2. R 的定义$^{\triangle}$ 基本上与弗雷格在 1879 年最初定义的祖先关系相同，罗素和怀特海在《数学原理》[29], 中使用了这一关系，之后蒯因在其 1940 年的教科书 [19] 以及后来在其集合论专著中也使用了这一关系 [20]。在最初对祖先关系的论述中，使用的是逆关系 R^{-1}，而不是 R：从这个意义上说，传递闭包与祖先关系互为对偶，前者指向后代，后者回溯至祖先。子句 $R[A] \subseteq A$ 表达了这样一个事实：A 是 X 的遗传子集：这意味着，对任意 $a \in A$,

[1] 若 R, S 是关系，则 $R \circ S := \{(x,z) \mid xRy \text{ 且 } ySz$，对某个 $y\}$，其中 $:=$ 表示定义。[2] 注意，本练习的这一部分涉及对量化命题之否定的操作性理解。

它的 R-后继都属于 A，a 的 R-后继的 R-后继也都属于 A，依此类推；因此，直观地说，A 中任意元素的 R-后代也都属于 A。整个定义的意思是：只要 y 属于每个包含 x 的 X 的遗传子集，x 就与 y 具有传递闭包 R 下的关系。

练习 2.4. 证明定义$R^{\triangledown}$ 的第二条规则是多余的。

例 2.5. 设 $X = \{a、b、c\}$，并设 $R = \{(a、b)、(b、c)\}$ 是 X 上的一个二元关系。

- 包含 a 的 X 的子集有四个：$A_0 = \{a\}$、$A_1 = \{a, b\}$、$A_2 = \{a, c\}$ 和 $A_3 = \{a, b,c\}$。我们有 $R[A_0] = \{b\}$、$R[A_1] = \{b, c\}$、$R[A_2] = \{b\}$ 和 $R[A_3] = \{b, c\}$（见定义 2.3.4）。由于满足 R[Ai] ⊆Ai 的 Ai 只有 A3，因此很容易看出 $\{(a, a), (a, b), (a, c)\} \subseteq R^{\triangle}$。
- 包含 b 的 X 的子集有四个：$B_0 = \{b\}$、$B_1 = \{a, b\}$、$B_2 = \{b, c\}$ 和 $B_3 = \{a, b,c\}$。我们有 $R[B_0] = \{c\}$、$R[B_1] = \{b, c\}$、$R[B_2] = \{c\}$ 和 $R[B_3] = \{b, c\}$。由于只有 B2 和 B3 满足 R[Bi] ⊆Bi，因此很容易看出 $\{(b, b), (b, c)\} \subseteq R^{\triangle}$。
- 关于c 的同样推理留作练习。

现在我们可以陈述主定理。

定理 2.1。$R^* = R^{\Cap} = R^{\Cup} = R^{\triangledown} = R^{\triangle}$。

定理的证明分为几个引理。

引理 2.2。$R^{\Cap} \subseteq R^{\Cup}$

证明。 只需证明 $\mathbb{1} \cup R \cup (R^{\Cup} \circ R^{\Cup}) \subseteq R^{\Cup}$。显然 $\mathbb{1} \subseteq R^{\Cup}$ 且 $R \subseteq R^{\Cup}$，因为 $R^0 = \mathbb{1}$和 $R^1 = R \circ R^0 = R \circ \mathbb{1} = R$ 都由定义 2.3.2 得出。此外，我们还注意到：

- $xR^{\Cup}y$ 意味着存在$n \in \omega$，使得xR_ny，
- $yR^{\Cup}z$ 意味着存在$m \in \omega$，使得yR_mz，

因此$xR^{\Cup}z$，因为$xR^{n+m}z$。 □

插论 3. 证明的第一部分可由以下事实推出：传递闭包R 是最小的传递扩张R，且该扩张具有传递性。这里的“最小”是相对于集合论包含而言的，因此要对所有R 的传递扩张取交（非谓述的）。从历史角度看，这一点对于理解庞加莱对非谓述定义的批评十分重要；这些定义正是他反对弗雷格—怀特海—罗素的祖先关系定义的核心原因。从技术角度看，$R^{\Cap}$ 的定义促使我们思考性质闭包这一概念，以及闭包系统与闭包算子之间的关系，例如 [6]中所述。我们将在第5节回到这个主题。

引理2.3. $R^{\Cup} \subseteq R^{\triangledown}$

证明。 用归纳法我们证明，对所有 $n \in \omega$，我们有 $R^n \subseteq R^{\triangledown}$。显然，$R^0 = \mathbb{1} \subseteq R^{\triangledown}$ 由第一条规则得出。$R^{n+1} = R \circ R^n$，根据归纳假设，$R^n \subseteq R^{\triangledown}$，因此 $R^{n+1} \subseteq R^{\triangledown}$ 由第三条规则得出。 □

严格来说，下面的引理本可由前面两条引理推出，但直接给出一个证明颇具启发性。

引理2.4。$R^{\Cap} \subseteq R^{\triangledown}$

证明。 由规则 (id) 和 (in) 可轻易推出 $\mathbb{1} \subseteq S$ 以及 $R \subseteq S$。接下来只需推出 $S \circ S \subseteq S$。这是因为我们可以证明该规则

$$\frac{xR^{\triangledown}y \qquad yR^{\triangledown}z}{xR^{\triangledown}z}\ (\text{trx})$$

是可容许的，也就是说，可以将它添加到形式系统中，而不增加定理集合（见插论4）。特别地，我们证明，对于每个形如

$$\mathfrak{D}_{trx} = \dfrac{\begin{array}{cc}\vdots\,\mathfrak{D}_L & \vdots\,\mathfrak{D}_R \\ xR^{\triangledown}y & yR^{\triangledown}z\end{array}}{xR^{\triangledown}z}\ (\text{trx})$$

其中 $\mathfrak{D}_L$，$\mathfrak{D}_R$ 中没有出现 (trx) 的推导，我们都可以通过对 $\mathfrak{D}_L$子推导的高度进行归纳，构造出一个结论相同且不使用 (trx) 的推导。
根据 $\mathfrak{D}_L$中应用的最后一条规则，分为三种情况。

- 如果 $\mathfrak{D}_L$ 中的最后一条规则是 (id)，那么所需的推导就是 $\mathfrak{D}_R$；根据假设，它不包含 (trx) 的应用。
- 如果 $\mathfrak{D}_L$ 中的最后一条规则是 (in)，那么该推导的形式为 $\dfrac{\dfrac{xRy}{xR^{\triangledown}y}\ (\text{in}) \qquad \vdots\,\mathfrak{D}_R^0}{xR^{\triangledown}z}\ (\text{trx})$。我们可以通过将证明树替换为 $\dfrac{xRy \qquad \vdots\,\mathfrak{D}_R^0}{xR^{\triangledown}z}\ (\text{tx})$。
- 如果 $\mathfrak{D}_L$ 中的最后一条规则是 (tx)，那么推导的形式为

$$\dfrac{\dfrac{xRu \qquad \vdots\,uR^{\triangledown}y}{xR^{\triangledown}y}\ (\text{tx}) \qquad \vdots\,\mathfrak{D}_R^0}{xR^{\triangledown}z}\ (\text{trx}) \tag{1}$$

因此，我们可以构造推导

$$\dfrac{xRu \qquad \dfrac{\vdots \qquad \vdots\,\mathfrak{D}_R^0}{uR^{\triangledown}z}\ (\text{trx})}{xR^{\triangledown}z}\ (\text{tx})$$

但归纳假设适用于$uR^{\triangledown}y$的推导，因此存在一个证明

$$\dfrac{\vdots \qquad \vdots\,\mathfrak{D}_R^0}{uR^{\triangledown}z}\ (\text{trx})$$

不使用 (trx)，这表明可以消除第 1 步中 (trx) 的应用。

□

插论4。 此处，我们本可以就形式系统和可容许规则的概念展开一段插论。Lorenzen 在其 1955 年关于逻辑与数学的操作性基础的论著中引入了这一概念[13]。可容许性是比可推导性更精细的性质。要确立某条规则在形式系统中是可容许的，通常需要进行分析：在对推导高度作归纳证明的过程中，考察结论可能通过哪些方式得出。这使得可容许性的证明成为理想的练习，能让学生熟悉这种归纳证明的思路。

引理2.5。 $R^{\triangledown} \subseteq R^{\Cap}$

证明。 我们需要证明：如果 $xR^{\triangledown}y$，那么对于满足 $\mathbb{1} \cup R \cup (S \circ S) \subseteq S$ 的每个 S，都有 xSy。证明对推导 $xR^{\triangledown}y$ 的高度进行归纳（见插论5）。只需考虑推导 $xR^{\triangledown}y$ 中最后一条规则为（tx）时的归纳步骤：

$$\frac{xRu \qquad uR^{\triangledown}y}{xR^{\triangledown}y}$$

$uR^{\triangledown}y$ 的推导比当前考察的推导更短，因此归纳假设适用。于是，对于每个满足 S 条件的 uSy，都有

$$\mathbb{1} \cup R \cup (S \circ S) \subseteq S .$$

此外，对于每个这样的 S，都有 $R \subseteq S$，因此我们可以得出 xSu。由于 $S \circ S \subseteq S$，我们可以得出 $R^{\triangledown} \subseteq R^{\Cap}$。 □

插论5。 请注意，在证明（简单）形式系统中推导的性质时，通常会采用对形式推导的高度进行归纳的证明技巧 $R^{\triangledown}$。

引理2.6. $R^{\triangledown} \subseteq R^{\Cup}$

证明。 我们对证明 $xR^{\triangledown}y$ 的高度进行归纳，并证明对于某个 $n \in \omega$，有 $xR^{n}y$。当推导以第一条规则结束时，有 $x = y$ 且 $xR^{0}y$。否则，若 $xR^{\triangledown}y$，由于 xRy，则有 $xR^{1}y$。最后，若 $xR^{\triangledown}y$ 是由第三条规则推出的，根据归纳假设，对于某个 n，有 $yR^{n}z$，因此 $xR^{n+1}z$。 □

现在我们知道，R 的传递闭包的前三种刻画是等价的，还需要证明它们也与 $R^{\triangle}$ 的传递闭包一致。考虑按上述方式定义的 R^{*}，对于 $x \in X$，令 $\mathrm{desc}(x) = \{y \mid xR^{\Cup}y\}$。

引理2.7. $R^{\triangle} = R^{\Cup}$

证明。显然，R[desc(x)] ⊆desc(x) 且 x ∈ desc(x)，因此 $R^{\triangle} \subseteq R^{\Cup}$。反过来，任取满足 x ∈ A 且 R[A] ⊆ A 的 A ⊆ X，并对 n 进行归纳，证明 $xR^{n}y$ 蕴含 y ∈ A。基础情形显然，因为根据假设 x ∈ A。假设 $xRuR^{n}y$，则有 x ∈A、u ∈R[A]，进而 u ∈A。根据 A 的假设以及归纳假设，有 y ∈A。因此，我们得出结论：R 的祖先关系与 R 的传递闭包相同。 □

定理 2.1 的证明到此结束，该定理给出了（自反）传递闭包的四种等价刻画。

3 量子格

现在，我们以稍微更抽象的视角来看待 R^* 的刻画。到目前为止，我们一直在结构中进行研究

$$\mathscr{P}(X \times X)$$

二元关系在 X 上的结构，其中以关系复合作为幺半运算，以任意并和交作为格运算。这种结构是量子格 [21]的一个实例。

定义 3.1 （含幺量子格）。基本上，量子格是一个完备[3] 格（$L \leq$），配备了一个内部运算 $\cdot$: $L \times L \to L$，该运算满足结合律，并且对所有 X、$Y \subseteq L$，都有：

$$x \cdot (\bigvee Y) = \bigvee \{x \cdot y \mid y \in Y\} \qquad \text{and} \qquad (\bigvee X) \cdot x = \bigvee \{y \cdot x \mid y \in X\}.$$

如果量子格具有乘法的单位元 1，则称其为含幺：

$$x \cdot 1 = x = 1 \cdot x$$

对所有 $x \in L$。（此时，量子格自然构成一个幺半群。）

定义2.3.1中的R^* 可以很容易地写入任意含幺量子格中。含幺量子格是推广（自反）传递闭包定义的恰当结构，值得特别一提，因为它在我们关于基础的（并不那么）假想课程主题中发挥着统一作用。

Let R 是X上的一个关系。在含幺量子格中，我们可以写作$f(S) := 1 \vee (R \cdot S)$，并定义：

$$R^* = \bigwedge_{f(S) \leq S} S$$

并且我们可以证明，只要$f(S) \leq S$，就有$R^* \leq S$；此外，

$$f(R^*) = R^*, \tag{2}$$

因此R^* 是f的最小不动点。

旁论 6。R* 的构造是完备格上的单调函数到自身的最小不动点构造的一个特例，而这正是塔斯基 [26]著名定理的部分内容。该定理的证明只涉及完备格最基本的性质，因此适合我们讲座面向的公众理解，也可以作为一项扩展练习。另一个可供思考的主题可能稍微进阶一些：首先注意到，上述定义将 R* 刻画为某个（退化）范畴中的初始 f-代数，随后不动点性质便可由兰贝克引理[1]推出。展开范畴论术语来说，给定一个范畴 $\mathscr{C}$ 和一个 F 的自函子，F-代数是一个带有态射 a : FX $\to$ X 的对象 X，其中该态射属于范畴 $\mathscr{C}$。若对于任意其他 F-代数 b : FY $\to$ Y，都恰好存在一个范畴 $\mathscr{C}$ 中的态射 f : X $\to$ Y，使得 b ∘F f = f ∘a，则称该代数为初始代数。兰贝克引理指出，若 X , a 是一个初始 F-代数，则 a 是一个同构。若将其特化到偏序，F-代数就是一个不等式 FX ≤X；它是初始的，并且此时 FX =X，若对于任意 F-代数 Y 都有 X ≤Y。特别地，R* 是 F(S) := 𝟙 ∪(R ∘S) 的初始 F-代数。

[3]完备格是一个偏序集（$L \leq$），满足：L 的每个子集A 在L中都有最大下界（又称下确界或交）$\bigwedge A$，以及最小上界（又称上确界或并）$\bigvee A$。当A为空集时，A的交是L的最大元。同样，空集的并是L的最小元。

从我们当前的角度来看，一个重要的观察是，通过推广到量子格，我们可以适当地改变底层量子格，从而引入故事中的第二个星号。考虑字母表A上的形式语言所构成的量子格，定义如下：

$$\mathscr{P}(A^*)$$

其中A^* 定义为并集$\bigcup_{n\in\omega}A^n$，并且

$$A^0=\{\varepsilon\},\qquad A^{n+1}=\{aw\mid w\in A^n \text{ and } a\in A\}.$$

那么，幺结构由下式给出

$$LM:=\{uv\mid u\in L,v\in M\}$$

对于$L,M\subseteq A^*$。

旁注 7. 当然 A^* 与 A 上的列表集合同构，它是集合自函子 $X\mapsto 1+(A\times X)$ 的初始代数，其中空串 ε对应于 $\langle\rangle$，而形如 au 的字符串对应于有序对 $\langle a,u\rangle$。

语言理论中的星运算由不动点方程定义：

$$L^*=1\cup LL^*$$

that 给出了语言量子格 $\mathscr{P}(A^*)$ 中方程 (2) 的值，其中 $1=\{\varepsilon\}$.

插曲 8。

- 上文介绍的结构应该已经让学生熟悉这样一种观念：代数不一定与数字有关。关于语言的代数结构，一个自然的问题是正规 语言是否满足代数律。人们提出了各种类型的结构，始于 [5]：其中，Kleene 代数得到了广泛研究，但所采用的技术超出了大一学生可能理解的范围。

- 一个值得进一步探讨的有趣之处，是其中的范畴论主题。观察到量子格是完备且余完备的幺半范畴的一个特例后，我们便可以定义这类范畴中的幺半对象。接着，将自由对象的定义调整到这一受限的语境中，就会发现，在关系量子格中，R 上的自由幺半对象恰好是 R 的自反传递闭包；而在语言量子格中进行相同的构造，则得到克林星。事实上，在这些量子格中，a^*满足 $1\vee a\vee(a^*a^*)\leq a^*$，这蕴含了三个不等式，它们表明 a^* 是一个扩张 a 的幺半对象，即 $1\leq a^*$、$a\leq a^*$ 以及 $a^*a^*\leq a^*$。在这两种情况下，a^* 的自由性体现为这样一种性质：若 $1\vee a\vee bb\leq b$，则 $a^*\leq b$；这可由 [17, 定理 1]推出。

4 算法学

我们赋予这一论述的逻辑与代数视角，使我们得以与（自反）传递闭包的算法层面建立直接联系；显然，这并非计算机科学家培训中的陌生主题。诚然，我们的论述相当粗略，唯一的辩解是，算法学领域的许多教科书中已经详述了相关细节，例如 [2]。

考虑布尔代数

$$\mathbf{B} = (\{T,F\}, \vee, \wedge, \overline{\ }),$$

然后考虑一个有限集合 X，其元素按固定顺序枚举为 $X = \{x1,\ldots,x_n\}$，以及 $n \times n$ 阶 $\mathbf{B}$ 上的矩阵结构，它与 X 上的二元关系集合一一对应。要说明的基本思想是，关系复合与矩阵乘积相一致；只需考察定义关系积的标准逻辑公式，便可轻易看出这一点

$$(R \cdot S)(x,y) =_{\text{def}} \exists u \in X(R(x,u) \& S(u,y))$$

并按照代数逻辑的方式，将右侧解释为矩阵乘积的通常公式

$$\bigvee_{u \in X} R_{xu} \wedge S_{uy}$$

注意到$\bigvee_{u \in X}$ 是一个有限析取。然后，我们可以调整定义 2.3(2) 中给出的自反传递闭包概念

$$\bigvee_{0 \leq i \leq \#X} R^i$$

并得出结论：将后一个公式直接转换为三重嵌套for循环 [2, 4]，便可得到（效率不太高的）用于求布尔矩阵传递闭包的沃舍尔算法。

旁注 9。 从培养计算机科学家的角度来看，上述解释只是一个简单的编程练习。从基础的角度来看，上述论述引入了一种算法设计风格，有助于提炼出一种可专门化为若干著名算法（例如最短路径算法）的抽象算法。尽管算法学的这一领域已成为标准教科书中的一章，我们认为，这种解释所依据的方法论基础应当作为一项独立见解加以研究，从而深入理解代数结构和逻辑结构在计算机科学中的应用。实现这一点有多种方式，我们这里只指出一些参考资料，它们或许有助于读者了解可用于此目的的各种代数结构。一个基本概念是 路径代数 [4, 第 3]，，其中真值的布尔代数 $\mathbf{B}$ 就是一个例子。取 $n \times n$ 个布尔矩阵 X、Y，其元素取自 $\mathbf{B}$，便可定义 [4, §3.2。5]加法和乘法运算

$$(X + Y)_{ij} := X_{ij} \vee Y_{ij}$$

$$(X \cdot Y)_{ij} := \bigvee_{k=1}^{n} (X_{ik} \wedge Y_{kj})$$

它们给出了$n \times n$ 矩阵的集合，同样具有路径代数的结构。通常会采用更强的闭半环 结构 [2, §5.6] 。量子格也是能够进行同类代数处理的结构。超越计算布尔矩阵的自反传递闭包这一具体问题，

我们还可以纳入范围更广的代数结构，详见 [17,§2]中的讨论。

5 更多主题

我们已经介绍了一个章节，它看起来很像传统方法，但实际上并非如此。

我们讨论的主题或许可以纳入一种“纵向”方法，即列出基础课程教学大纲中的各个小节；但我们实际上强调的是一种互补的“横向”方法，试图分离出技术基础（而非基础理论），让学生能够通过前几节所建议的实践活动加以掌握。诚然，我们的讲述偏重代数结构：我们尝试提供一些例子，使之能够与假定同步进行的离散数学课程相协调。我们希望在讲座中纳入的一系列例子，可以取自关系代数、抽象重写系统，也可能取自经典递归论中最抽象的部分，例如 Owing 对对角化的处理 [15, II.2，第 154] 页。

最后，我们建议探讨一个与本书整体论述框架十分契合的主题 .

余归纳对传递闭包的论述，自然可以由余归纳作为补充。余归纳不仅在证明可能无限展开的结构（如流和标记迁移系统）的性质时发挥核心作用，也提供了与我们此前采用的方法相对偶的思路。在定义传递闭包时，我们寻找的是满足某些性质的最小对象；而余归纳关注的则是最大对象。用集合论表述时，余归纳（以及双模拟这一基本概念）所需的不过是包含关系下的二元关系完备格，因此，这一主题也适合采用与传递闭包相同的方式来论述。

部分文献

- 祖先关系首次出现于 [10]。 [29],的 E 节也讨论了祖先关系，该节的主题是归纳关系。另请参见 [19]中的 §39。
- 关于传递闭包的一些历史信息，以及从基础理论出发的研究动机，见 [18]。Vaughan Pratt 还在 [16] 中对用于求关系传递闭包（=布尔矩阵）的 Floyd-Warshall 算法进行了抽象化重述。Floyd-Warshall 算法本身的历史也很有意思：在 [27] 最初发表之后，经典著作 [3] 中出现了一个正确性证明。这个证明在 [28] 中得到了讨论和改进，并在 [11] 中受到进一步研究。
- 关于 Kleene 代数及相关结构的文献十分丰富：主要参考资料是 [5]。这个名称源自 Dexter Kozen：他的个人网页（https://www.cs.cornell.edu/~kozen/）提供了讲座和许多 Kozen 撰写的相关论文链接。尽管 [17] 并非专门讨论 Kleene 代数，却是了解整个领域的极佳入门读物。
- Sangiorgi 在一篇精彩的论文中研究了余归纳的起源 [23]。余归纳（及其对偶）是 [12], 的主题。整个领域的内容都涵盖在两卷本 [24, 25] 中。即使是一年级学生也能欣赏的余代数概念应用，是 [22] 以及该作者其他几篇论文的主题。

参考文献

[1] Jiˇrí Adámek、Stefan Milius 和 Lawrence S. Moss（2025）：初始代数与终余代数：函子不动点理论。剑桥理论计算机科学丛书，剑桥大学出版社，doi:10.1017/9781108884112。[2] Alfred V. Aho 和 John E. Hopcroft（1974）：计算机算法的设计与分析。Addison-Wesley Longman Publishing Co., Inc.，美国。[3] Alfred V. Aho 和 Jeffrey D. Ullman（1972）：语法分析、翻译与编译理论。Prentice-Hall, Inc.。[4] Bernard Carré（1979）：图与网络。牛津应用数学与计算机科学丛书，Clarendon Press。[5] John H. Conway（1971）：正则代数与有限状态机。Chapman and Hall 数学丛书，Chapman and Hall。[6] Brian A. Davey 和 Hilary A. Priestley（1990）：格与序导论。剑桥大学出版社，剑桥。[7] Marcel Erné（2004）：伴随与伽罗瓦连接：起源、历史与发展。载于 K. Denecke、M. Erné 和 S. L. Wismath 编：《伽罗瓦连接及其应用》，施普林格荷兰，多德雷赫特，第 1–138 页。[8]Marcel Erné（2009）：闭包。载于 Mynard Frederic 和 Elliott Pearl 编：《超越拓扑学》，《当代数学》第 486 卷，美国数学会，罗得岛州普罗维登斯，第 163–238 页，doi:10.1090/conm/486/09510。[9] Frederic Brenton Fitch（1952）：符号逻辑：导论。Ronald Press Company。[10] 戈特洛布·弗雷格（1879）：《概念文字：一种仿照算术构造的纯思维形式语言》。Louis Nebert，萨勒河畔哈雷。施普林格再版，参见 https://doi.org/10.1007/978-3-662-45011-6。[11] Joseph Goguen、James Thatcher、Eric G. Wagner 和 Jesse B. Wright（1976）：计算机科学与范畴论的交汇：I. 基本概念与示例。技术报告 RC5908，IBM。[12] Bart Jacobs 和 Jan Rutten（2011）：（余）代数与（余）归纳导论，第 38–99 页。剑桥理论计算机科学丛书，剑桥大学出版社。[13] Paul Lorenzen（1955）：《操作逻辑与数学导论》。施普林格，柏林。[14] Eliakim Hastings Moore（1910）：一般分析形式导论。耶鲁大学出版社。[15] Piergiorgio Odifreddi（1989）：经典递归论。《逻辑与数学基础研究》第 125 卷，North-Holland 出版公司，阿姆斯特丹。自然数函数与集合理论，附 G. E. Sacks 的序言。[16] Vaughan Pratt（1989）：富化范畴与弗洛伊德–沃舍尔联系。载于《第一届代数方法论与软件技术国际会议论文集》，艾奥瓦城，第 177–180 页。[17] Vaughan Pratt（1991）：动作逻辑与纯归纳。载于 J. van Eijck 编：《人工智能中的逻辑》，施普林格柏林海德堡，柏林、海德堡，第 97–120 页，doi:10.1007/BFb0018436。[18] Vaughan Pratt（1992）：二元关系演算的起源。载于《第七届 IEEE 计算机科学逻辑年会论文集》，第 248–254 页，doi:10.1109/LICS.1992.185537。[19] Willard Van Orman Quine（1940）：数理逻辑。哈佛大学出版社。[20] Willard Van Orman Quine（1963）：集合论及其逻辑，修订版。哈佛大学出版社，马萨诸塞州剑桥。[21] Kimmo I. Rosenthal（1990）：量子格及其应用。Pitman 数学研究笔记丛书第 234 卷，Longman Scientific & Technical。

[22] Jan Rutten（2003）：行为微分方程：流、自动机和幂级数的余归纳演算。《style id='4'>理论计算机科学308(1)，第 1–53 页，doi:10.1016/S0304-3975(02)00895-2。[23] Davide Sangiorgi（2009）：双模拟与余归纳的起源。《style id='9'>ACM 程序设计语言与系统汇刊31(4)，doi:10.1145/1516507.1516510。[24] Davide Sangiorgi（2011）：双模拟与余归纳导论。剑桥大学出版社，doi:10.1017/CBO9780511777110。[25] Davide Sangiorgi 和 Jan Rutten 编（2011）：双模拟与余归纳高级主题。剑桥大学出版社，美国，doi:10.1017/CBO9780511792588。[26]Alfred Tarski（1955）：格论不动点定理及其应用。太平洋数学杂志5(2)，第 285–309 页。网址：
h
t
t
p
s://
p
r
o
j
e
c
t
e
ucli
d.org/journals/pacific-journal-of-mathematics/volume-5/issue-2/A-lattice-theoretical-fixpoint-theorem-and-its-applications/pjm/1103044538.full。[27] Stephen Warshall（1962）：关于布尔矩阵的一个定理。《美国计算机协会杂志》9(1)，第 11–12 页，doi:10.1145/321105.3211。[28] Peter Wegner（1974）：对 *Aho* 和 *Ullman* 的 *Warshall* 算法正确性证明的修改。《SIGACT 新闻》6(1)，第 32–35 页，doi:10.1145/1811129.1811134。[29] Alfred North Whitehead 和 Bertrand Russell（1910）：《数学原理》。第 1 卷，剑桥大学出版社。