arXiv:2603.16274v1 [math.CT] 17 Mar 2026

从托orsors到拓扑斯：面向密码学中 Σ-协议的导论

Takao Inoué

大和大学信息学院，日本大阪*

2026年3月17日

摘要

本文为层与拓扑斯提供一篇预备性导论，作为作者此前关于托orsors的介绍在概念上的延续，并为作者在 arXiv 上发表的论文《格罗滕迪克拓扑与密码学安全的层论基础：攻击者模型与 Σ-协议作为第一步》[2] 做准备。本文并不试图对拓扑斯理论的所有内容进行百科全书式的综述，而是着重阐述从基于托orsor的局部到整体推理转向层论与拓扑斯论推理时最相关的部分：格罗滕迪克拓扑、层、位点上的托orsor、下降、层拓扑斯、初等拓扑斯、笛卡尔闭结构、子对象分类器以及内部逻辑。我们的目标不仅仅是提供动机，也力求充分讲解真正的拓扑斯理论，使读者不仅能从启发式角度，也能从结构上理解，后续密码学框架 [2] 为何使用格罗滕迪克拓扑与层论语言。为使本文更为自足，我们还加入了若干重要附录，涵盖范畴论基础、Yoneda 引理、极限与余极限、等化子与余等化子、Kan 延拓、内部逻辑与直觉主义逻辑之间的关系，以及附有解答的习题。在最后一部分，我们将说明这些思想如何为概念性地理解 Σ-协议奠定基础，尤其是其与局部一致性、可模拟性，以及从相容局部数据过渡到整体结构之间的联系。

关键词：拓扑斯理论、层论、Grothendieck 拓扑、扭子、下降、内部逻辑、直觉主义逻辑、范畴论、米田引理、 Σ-协议、密码学安全、可模拟性、局部到整体原理

2020年数学主题分类：18F10、18F20、18N10、03G30、94A60

目录

1 引言 **3**

*电子邮件：inoue.takao@yamato-u.ac.jp；个人邮箱：takaoapple@gmail.com[通信时我更愿意使用个人邮箱。]

2 位点、格罗滕迪克拓扑与层 43 位点上的扭子、余循环与下降 54 从层范畴到拓扑斯 65 初等拓扑斯 66 子对象分类器与内部逻辑 77 练习：使用层、拓扑斯与内部逻辑 98 拓扑斯中的挠子与局部对称性 109 面向 Σ-协议与密码学安全 11

10 展望 **12**

11 结论 **12**

A 范畴论简明介绍 13

A.1 范畴、态射与交换图 .13A.2 函子与自然变换 .14A.3 泛性质 .15A.4 极限与余极限 .15A.5 极限与余极限练习 .17A.6 Kan 延拓 .18A.7 可表函子与米田观点 .19A.8 笛卡尔闭范畴.21A.9 为什么这些概念对正文很重要 .21

B 内部逻辑与直觉主义逻辑 **21**

C 习题解答 **22**

D 一个可能的讲课计划 25D.1 建议的总时长 .25D.2 标准的 10 讲计划.25D.3 一种扩展为 12 讲的方案 .27

D.4 教学评注 .27

1 引言

本文旨在作为一组三步论述中的中间篇章。第一步是作者早先关于扭子的札记 [1], ，其中着重讨论了自由传递群作用、传输、局部平凡性和基于余循环的粘合。第三步是作者后来发表的论文 [2], ，该文提出了一种基于格罗滕迪克拓扑、攻击者模型和 Σ-协议的密码学安全层论方法。本文旨在填补这两部作品之间的概念空白。本文的目的是以严谨的数学方式阐明，从扭子到拓扑斯这一路径为何自然而然，以及为什么希望理解 [2] 的读者应当先了解拓扑斯理论的基本架构。

之所以仅建立一座表面的桥梁是不够的，有两个原因。首先，扭子理论本身已经包含了局部到整体哲学：扭子在局部上与作用群无法区分，但在整体上却可能不存在任何特定原点。这自然引出了局部平凡化、过渡函数、交叠上的相容性以及下降。其次， [2] 的密码学框架并非仅仅将层的语言作为一种隐喻来借用。它把格罗滕迪克拓扑、局部可观测性和信息粘合视为结构性要素。因此，读者不仅必须理解什么是层，还必须理解什么是拓扑斯、内部逻辑如何运作，以及为什么这样的环境能够支持严谨的局部推理。

正因如此，本文比一篇简短的概念性桥接文章更加充实。本文的风格仍然是入门性的，但旨在提供足够扎实的拓扑斯理论，使读者能够从内部理解后续的密码学应用。因此，我们不仅讨论位点上的层和扭子，还讨论从层范畴到拓扑斯的过渡、拓扑斯的初等定义、指数对象和子对象分类器的作用，以及内部逻辑的基本思想。本文的讨论有所取舍，并非百科全书式的全面介绍，但力求在数学上真实可靠。

贯穿本文的一条指导原则是，从扭子到拓扑斯并非转换研究主题，而是对托orsor 理论中已有结构的概念性拓展。扭子中缺乏典范原点、从局部平凡化中恢复扭子，以及交叠处的余循环关系，都指向这样一种框架：局部数据与粘合在其中居于首要地位。层论是系统描述此类现象的第一种语言。拓扑斯理论则进一步扩展了这种语言，将其拓展为一个完整的数学宇宙，拥有自身内部的真理、存在与函数概念。从这一视角看，理解拓扑斯也是理解扭子原本所要表达的内容。

本文的组织如下。第2 节回顾格罗滕迪克拓扑与层。第3节重新审视作为层论的和位点论的对象的扭子，重点讨论余循环与下降。第4节解释层范畴为何自然地导向拓扑斯。第5 节介绍初等拓扑斯。第6 节更详细地讨论子对象分类器与内部逻辑。第8节将扭子置于拓扑斯之中。第7 节在转向密码学之前安排一个练习部分。第9 节随后解释，为何这一完整的发展过程对于 Σ-协议以及 [2] 的概念性研究具有重要意义。第11 节总结从扭子到拓扑斯的发展历程及其对后续密码学框架的意义，从而结束全文。附录提供了大量辅助材料：范畴论简介、Yoneda 引理、笛卡尔闭范畴、极限与余极限、等化子与余等化子、Kan 延拓、内部逻辑与直觉主义逻辑之间的关系，以及习题解答。

2 位点、格罗滕迪克拓扑与层

从扭子到拓扑斯的第一个重要步骤，是从通常的开覆盖转向格罗滕迪克拓扑。这样一来，我们不仅可以在拓扑空间上讨论局部性与粘合，也可以在更为一般的范畴中进行讨论。

定义 2.1。 设 $\mathcal{C}$ 是一个范畴。对象 $U \in \mathrm{Ob}(\mathcal{C})$ 上的一个筛 S 是一个以 U 为余域的态射集合，并且对前复合封闭：如果 $f\colon V \to U$ 属于 S，且 $g\colon W \to V$ 是任意态射，那么 $f \circ g\colon W \to U$ 也属于 S。

定义 2.2。 范畴 $\mathcal{C}$ 上的Grothendieck 拓扑 J 为每个对象 U 指定一个由 U上的筛构成的集合$J(U)$，称为覆盖筛，并满足：

(i) 极大筛属于 $J(U)$；

(ii) 若 $S \in J(U)$，且 $f\colon V \to U$是任意态射，则拉回筛 f^*S属于 $J(V)$；

(iii) 若 S是 U上的一个筛，且存在 $R \in J(U)$，使得对每个 $f\colon V \to U$属于 R，拉回筛 f^*S都属于 $J(V)$，那么 $S \in J(U)$。

这对 $(\mathcal{C},\ J)$ 称为一个位点。

这些公理抽象了开覆盖的熟悉性质。条件 (ii) 表示覆盖可以拉回。条件 (iii) 是传递性条件：如果一个族经过覆盖的细化后成为覆盖，那么它本身已经是覆盖。

例 2.3. 设 X 是一个拓扑空间，令 $\mathcal{O}(X)$ 为其开集范畴，态射由包含映射给出。若 $U = \bigcup_i U_i$，则族 $\{U_i \subseteq U\}$ 是覆盖。由这类族生成的筛定义了 $\mathcal{O}(X)$上的一个 *Grothendieck* 拓扑。相应的层论就是 X上的通常层论。

定义 2.4. 设$(\mathcal{C},\ J)$ 为一个位点。$\mathcal{C}$ 上的集合预层是一个逆变函子 $\mathcal{F}:\mathcal{C}^{\mathrm{op}} \to$ **集合范畴**。若对于每个对象 U和每个覆盖筛 $S \in J(U)$，自然映射

$$\mathcal{F}(U) \longrightarrow \mathrm{Hom}(S, \mathcal{F})$$

是一个双射。等价地， U 上的截面由 U的每个覆盖上的相容截面唯一确定。

通俗地说，层是一种预层，其中局部相容数据能够唯一地粘合。定义的现代形式之所以重要，是因为它表明，“局部性”只取决于所选的 Grothendieck 拓扑，而不取决于任何预先给定的点集空间概念。这种灵活性恰恰是密码学应用中将发挥作用的特点：其中的“局部”部分并非字面意义上的拓扑空间开子集，而是由覆盖关系组织起来的信息状态 [2]。

命题 2.5。 设 $(\mathcal{C},\ J)$ 是一个位点。若 $\mathcal{F}$ 是一个层，且 $\{U_i \to U\}$ 是一个覆盖族，那么任何一族在所有交叠 $U_i \times_U U_j$ 上都相合的局部截面 $s_i \in \mathcal{F}(U_i)$ 都能粘合为唯一的全局截面 $s \in \mathcal{F}(U)$。

证明概要。族 $\{U_i \to U\}$在 U 上生成一个覆盖筛。拉回交叠上的相容性，恰好意味着从该筛到$\mathcal{F}$的诱导映射是自然的。根据层条件，这样的自然变换来自$\mathcal{F}(U)$ 的唯一一个截面。

□

因此，层论并非只是一个技术性的附加内容。它是这样一条原则的形式化表达：只要局部信息彼此相容，就应当能够重构整体信息。这正是托orsor 理论已经指向的方向。

3 位点上的扭子、余循环与下降

在较早的扭子笔记中， [1], 扭子是通过自由传递群作用引入的。在位点上，这一思想依然成立，但局部平凡性取代了存在真正整体基点的要求。

定义 3.1. 设$(C\ \ J)$ 是一个位点，G 是其上的群层。一个 G-扭子 是一个带有 G 右作用的层 P，满足：

(i) P 局部非空：存在一个覆盖族 $\{U_i \to U\}$，使得每个 $P(U_i)$ 都非空；*(ii)* 该作用局部自由且传递：对于每个对象 U 以及每个 $p, q \in P(U)$，都存在唯一的 $g \in G(U)$ 使得 $q = p \cdot g$。

这个定义体现了与经典情形相同的几何学。选定一个局部截面后，扭子看起来就像作用群，但整体上并不存在这样的规范选择。由此产生的整体不平凡性由余循环刻画。

命题 3.2。 设 P 是一个 G-扭子，且 $\{U_i \to U\}$ 是一个覆盖族，并选取局部截面 $s_i \in P(U_i)$。那么在每个交叠 $U_{ij} := U_i \times_U U_j$ 上都存在唯一的元素

$$g_{ij} \in \mathcal{G}(U_{ij})$$

使得

$$s_j = s_i \cdot g_{ij} \quad on\ U_{ij},$$

并且这些元素满足余循环条件

$$g_{ij} g_{jk} = g_{ik} \quad on\ U_i \times_U U_j \times_U U_k.$$

证明略。 每个 g_{ij} 的唯一性和存在性都来自自由传递性。通过 s_i 直接计算 s_k，或经由 s_j 计算，都可在三重交叠上得到余循环恒等式。 □

备注 3.3。 命题 *3.2*中的余循环，从绝对意义上说并不依赖于所选取的局部平凡化，而只是在预期的平凡化变换关系下保持不变。因此，扭子是由下降数据而非某个首选的全局点编码的。

这是下降变得不可避免的第一个地方。下降数据大致来说，是由局部数据连同交叠上的相容性组成的，并且在多个交叠上满足高阶相干性。扭子是这一原理最简洁的初等例子之一。

定义 3.4。设 $\{U_i \to U\}$ 是位点中的一个覆盖族。覆盖上的预层或结构化对象的下降数据 由每个 U_i 上的局部对象，以及交叠上的同构组成，并且这些同构在三重交叠上满足余循环条件。

定理 3.5 （扭子下降原理，非正式表述）。 U 上的一个 G-扭子，可以由 U 的一个覆盖上的局部平凡扭子，以及一个在三重交叠上满足相容条件的余循环重构得到。

证明思路。 首先取平凡扭子$\mathcal{G}|_{U_i}$，并利用余循环在交叠上将它们识别起来。层条件确保粘合后的对象存在，而余循环恒等式则保证粘合的结合律。

□

从这个意义上说，托orsor 理论已经自然地存在于一个位点上。后来转向拓扑斯并未摒弃这一视角；它为这一视角提供了一个更大的环境宇宙。

4 从层范畴到拓扑斯

对于一个位点（$\mathcal{C}$ J），集合范畴层的范畴 $\mathbf{Sh}(\mathcal{C}$ $J)$ 不仅是容纳粘合数据的便利场所。它本身就是一个高度结构化的数学世界。这是“拓扑斯”一词首次出现。

定义 4.1。 一个格罗滕迪克托扑斯是一个与某个站点 $\mathbf{Sh}(\mathcal{C}$ $J)$ ($\mathcal{C}$ J 上的层范畴等价的范畴).

典型例子是拓扑空间 X上的 $\mathbf{Sh}(X)$。但该定义更为宽泛：格罗滕迪克托扑斯是某种广义空间概念上的层范畴。因此，它应当同时被理解为

(a) 一个由局部变化的集合构成的范畴，以及

(b) 一个由这些集合的变化与粘合方式编码的广义空间。

命题 4.2。 对于任意位点 ($\mathcal{C}$ J)，范畴 $\mathbf{Sh}(\mathcal{C}$ $J)$ 具有有限极限。此外，包含映射 $\mathbf{Sh}(\mathcal{C}$ $J)$ $\to$ **集合范畴** $\mathcal{C}^{\mathrm{op}}$ 保有限极限。

证明略述。 预层的有限极限逐点计算。层条件在有限极限下保持稳定，因此层的逐点有限极限仍然是层。 □

这已经带来了丰富的结构。积、等化子、终对象以及许多熟悉的类集合构造都可在内部存在。但拓扑斯还具备更多结构：粗略地说，它还具有函数对象和一个内部真值对象。这正是它能够真正取代集合的宇宙的原因。

注 4.3。 从空间 X 到拓扑斯$\mathbf{Sh}(X)$ 的过程可以从两个相反的角度来理解。一种说法是，$\mathbf{Sh}(X)$ 只是 X上的层范畴。另一种说法则是，$\mathbf{Sh}(X)$是 X在数学上有意义的化身，因为它记载了对象如何在 X上局部变化并如何粘合。第二种观点是现代拓扑斯理论的概念来源之一。

5 初等拓扑斯

格罗滕迪克托扑斯源自位点，但拓扑斯也有一种内在的公理化定义。这就是初等托扑斯的概念。它提炼出使一个范畴类似于**集合范畴**的结构特征。

定义 5.1. 一个初等托扑斯 是一个具有以下性质的范畴 E:

(i) 有限极限，

(ii) 指数对象，以及

(iii) 一个子对象分类器。

我们简要回顾这些要素。有限极限提供终对象、积和等化子。指数对象意味着，对于对象 A，$B \in \mathcal{E}$，存在一个对象 B^A 表示从A 到 B的态射。因此，我们可以谈论内部函数对象。第三个要素——子对象分类器——是拓扑斯理论最具特色的特征之一。

定义 5.2。 具有有限极限的范畴 E 中的子对象分类器 是一个对象Ω，并配有一个态射

$$\text{true} : 1 \to \Omega$$

从终对象出发，使得对于每个单态射 $m\colon A \rightarrowtail X$，都存在唯一的态射

$$\chi_m : X \to \Omega$$

使得这个方块

$$\begin{array}{ccc} A & \longrightarrow & 1 \\ m \downarrow & & \downarrow \text{true} \\ X & \xrightarrow{\chi_m} & \Omega \end{array}$$

是一个拉回。

在**集合范畴**中，子对象分类器是二元素集合$\{0, 1\}$。子集 $A \subseteq X$ 由其特征函数 χ_A 分类：$X \to \{0, 1\}$。在一般的拓扑斯中，Ω 扮演真值对象的角色，但其中的真值不必只是布尔值，也不必是全局的。这正是局部逻辑发挥作用之处。

例 5.3. 对于拓扑空间 X，拓扑斯$\mathbf{Sh}(X)$ 是一个初等托扑斯。其子对象分类器Ω 是开子集层：对于每个开集 $U \subseteq X$，$\Omega(U)$ 是U的开子集集合。因此，U 上的真值并非由单个全局比特表示，而是由 U 中命题成立的一个开区域表示。

命题 5.4. 每个格罗滕迪克托扑斯都是初等托扑斯。

证明概要。 对于 $\mathbf{Sh}(\mathcal{C}\ J)$，有限极限继承自预层范畴；指数对象之所以存在，是因为层化保留了所需的结构；而子对象分类器则可以通过对局部覆盖筛的预层进行层化来构造。完整证明可参见标准参考文献 [3, 4]。

□

因此，从位点到层的过渡，不仅让我们来到了一个由粘合对象构成的范畴，也让我们进入了一个具有自身内部结构、类似集合的宇宙。

6 子对象分类器与内在逻辑

拓扑斯理论最深刻的洞见之一是，拓扑斯拥有自身的内部逻辑。这种逻辑并非从外部强加，而是源自范畴的结构特征，尤其是子对象分类器。

在普通集合论中，集合 X 上的谓词由 X的一个子集表示，或者等价地，由特征函数 $X \to \{0, 1\}$表示。在拓扑斯中，对象 X 上的谓词由 X的一个子对象表示，因此也可由分类箭头 $X \to \Omega$表示。因此，Ω充当真值对象。不同之处在于，这些真值可能随局部而变化。

注 6.1。 在 $\mathbf{Sh}(X)$中，关于开集 U 上命题的真值通常并非简单的“真”或“假”。它是命题成立的 U 的一个开子集。因此，真理具有局部性和几何性。这正是拓扑斯非常适合进行局部到整体推理的核心原因之一。

“拓扑斯具有内部逻辑”这一说法至少包含三层含义。首先，子对象的行为类似于谓词。其次，Ω 的行为类似于真值的内部代数。第三，量词可以通过范畴伴随来诠释，因此关于存在和全称性的陈述可以在内部表达。即使不对所有内容进行形式化，这三点也已经赋予“在拓扑斯内部推理”这一说法切实的数学内涵。

例 6.2 （层托扑斯中的真值）。 设 X 是一个拓扑空间，并设 $\Omega \in \mathbf{Sh}(X)$ 为子对象分类器。对于一个开集 $U \subseteq X$，集合 $\Omega(U)$ 是 U 的开子集所成的集合。若 $A \hookrightarrow F$ 是层 F 的一个子对象，则分类映射 $\chi_A : F \to \Omega$ 将截面$s \in F(U)$映射到 U 的最大开子集，在该子集上 s 属于 A。因此，谓词返回的并非一个全局比特值，而是一个有效区域。

例 6.3 （一个具体的局部谓词）。 取空间 X 上连续实值函数构成的层 $C^0(-, \mathbb{R})$。令 $P \hookrightarrow C^0(-, \mathbb{R})$ 为由严格正函数组成的子对象。那么对于 $f \in C^0(U, \mathbb{R})$，真值 $\chi_P(f) \in \Omega(U)$ 就是开子集

$$\{x \in U \mid f(x) > 0\}.$$

因此，内在陈述“$f > 0$”在 U 上并非简单地非真即假；它恰恰在正性成立的开区域上为真。这是局部真理的一个初等却极具启发性的模型。

我们还可以进一步推广。在初等托扑斯中，可以解释合取、蕴涵、量化、等词和存在。由此便得到一种内在于托扑斯的高阶直觉主义逻辑。对于本文而言，无须采用完整的形式体系，但以下启发式观点不可或缺：

> 托扑斯中的陈述是相对于局部语境来评估的，而存在性断言意味着存在相容的局部数据。

这在 Kripke–Joyal 语义中尤为 सूपष्ट。在层托扑斯中，说某个开集 U 迫使一个存在陈述，意味着 U 可以被较小的开集覆盖，并且在这些开集上存在见证，且满足预期的相容性条件。因此，存在的逻辑含义本身已经是层论的。

命题 6.4 （Kripke–Joyal 存在性启发式）。设 $\mathbf{Sh}(X)$ 为一个层托扑斯，且设 $\varphi(x)$ 为一个内在陈述。那么，断言“$U \Vdash \exists x\, \varphi(x)$”应理解如下：存在一个开覆盖 $U = \bigcup_i U_i$ 以及定义在 U_i 上的截面 x_i，使得每个 U_i 都迫使 $\varphi(x_i)$，并在需要时满足交叠上的相容性。

命题 6.5 （Kripke–Joyal 全称陈述启发式）。 设 $\mathbf{Sh}(X)$ 是一个层托扑斯，并设 $\varphi(x)$ 是关于层 F 的截面的一个内在陈述。那么，“$U \Vdash \forall x\, \varphi(x)$”表示：对于每个开子集 $V \subseteq U$ 以及每个截面 $x \in F(V)$，都有 $V \Vdash \varphi(x)$。因此，全称真值在限制到更小的开集时保持不变。

注 6.6。 存在陈述与全称陈述之间的这种差异至关重要。存在真值可能只有在经过某个覆盖之后才能确立，而全称真值则必须在每一次进一步局部化后仍然成立。这种不对称性是直觉主义推理和几何推理的特征之一。

例 6.7 （局部存在性与整体存在性）。 令 $X = S^1$ ，并令 F 为连续实值函数层。考虑陈述

$$\exists g \in F\,(g^2 = f)$$

对于固定截面 $f \in F(X)$ 。如果 f 处处为正，则该陈述在整体上为真。如果 f变号，则该陈述在整体上为假。但即使不存在整体平方根，仍可能在某个适当的开覆盖上存在局部平方根。在内部语言中，这意味着存在陈述可以在局部被迫成立，却不能在整体上被迫成立。

例 6.8 （蕴涵作为局部稳定性）。 对于拓扑斯中的子对象 A、B 、$\to F$ ，蕴涵$A \Rightarrow B$ 是 F的另一个子对象，其内部特征是：一个截面恰好在 A 中的成员关系局部蕴涵其属于 B的地方属于该子对象。在层托扑斯中，蕴涵因此并非纯粹的逐点运算；它记录了蕴涵的局部稳定性。

注 6.9。 初等托扑斯中的真值在内部构成海廷代数，而通常并不构成布尔代数。因此，排中律未必成立。这一事实的逻辑含义将在附录 B中讨论。现在需要注意的要点是，局部真理通常比经典二值真理更加微妙。

命题 6.10 （内部逻辑即有条理的局部推理）。 设 E 是一个格罗滕迪克托扑斯。那么，通过子对象解释谓词、通过Ω解释真值，并通过托扑斯的内部伴随结构解释量词，这种解释方式组织推理，使得局部相容性数据能够在内部表达和处理。

证明概要。 谓词由单态射表示，因而也由指向 Ω 的分类箭头表示。积和指数对象支持合取与函数空间。沿投影的拉回具有适当伴随函子，这为量化提供了范畴论层面的内容。在格罗滕迪克托扑斯中，Kripke–Joyal 语义使这些构造明确地呈现出局部性。 □

注 6.11。 这并不意味着托扑斯中的所有推理都只是局部拼凑。相反，这意味着全局真理由局部真理和粘合所中介。重点不在于否认整体结构，而在于从局部数据有条理地重构整体结构。

这一视角对于预期的密码学应用至关重要。后续论文 [2] 使用格罗滕迪克拓扑和类似层的组织方式，正是因为攻击者知识、可观测性和信息相容性并非简单的全局是/否问题。因此，拓扑斯的内部逻辑并非装饰性的抽象，而是对受控粘合的局部推理的一种建模。

7 实践：运用层、拓扑斯与内部逻辑

以下练习旨在帮助读者在转向明确的密码学讨论之前，巩固本文的主要思想。虽然这些练习在逻辑上并非后续章节所必需，但在教学上颇有帮助。答案汇集于附录 C。

练习 1. 设 X 是一个拓扑空间，且 $\Omega \in \mathbf{Sh}(X)$ 是子对象分类器。证明对于每个开集 $U \subseteq X$，集合 $\Omega(U)$ 可以视为 U 的开子集所成的集合。解释为什么这意味着 $\mathbf{Sh}(X)$ 中的真值具有局部性。

练习 2。 设 $\mathcal{G}$ 是位点 $(\mathcal{C}, J)$ 上的一个群层，$\mathcal{P}$ 是一个 $\mathcal{G}$-挠子。选取一个覆盖族上的局部截面，并导出相应的余循环 g_{ij}。形式化地验证，三重交叠上的余循环条件表达了传输的相容性。

练习 3。 在一个层托扑斯中，用文字说明以下两种含义之间的区别：

$$U \Vdash \exists x\, \varphi(x) \quad \text{and} \quad U \Vdash \forall x\, \varphi(x).$$

为什么第一个陈述可以传递到一个覆盖，而第二个陈述必须在每一次限制之后都成立？

练习 4。 设 $F = C^0(-, \mathbb{R})$ 是拓扑空间 X 上的，并设 $P, \to F$ 为正函数的子对象。对于一个截面 $f \in F(U)$，具体描述分类映射 $\chi_P(f) \in \Omega(U)$。这说明谓词“$f > 0$”的内在含义是什么？

练习 5。 设 $\mathcal{E}$ 是一个初等托扑斯。说明为什么有限极限、指数对象和一个子对象分类器这些数据使 $\mathcal{E}$ 看起来像一个集合宇宙。这些要素中，哪一个最直接地负责内在真值？

8 拓扑斯中的扭子与局部对称性

现在我们回到扭子，但采用拓扑斯理论提供的更成熟视角。一旦在拓扑斯 $\mathcal{E}$ 中工作，讨论内群、内作用，进而讨论内扭子，便顺理成章。

定义 8.1。 有限积范畴中的内部群 是一个对象 G，配备乘法、单位元和取逆态射，并在内部满足通常的群图表。

定义 8.2。 设 G 是拓扑斯 E 中的一个内部群。E 中的 G-扭子是一个对象 P，带有一个右 G-作用，且在内部满足：

(i) P 在局部有元素，
(ii) 该作用是自由的，*(iii)*
该作用是传递的。

等价地，典范映射

$$P \times G \longrightarrow P \times P, \qquad (p, g) \mapsto (p, p \cdot g),$$

是一个同构，且 $P \to 1$ 是一个满态射。

这个定义清楚地表明，扭子属于拓扑斯的范畴。缺少全局原点并非缺陷，而是一种正当的内部对称形式。重要的不是优选点的存在，而是局部点的存在以及在它们之间进行传输的能力。

命题 8.3。 设$(C\ \ J)$是一个位点，G是一个群层。那么，该位点上的G-挠子恰好是拓扑斯$\mathbf{Sh}(C\ \ J)$中内部群G的扭子。

证明概要。$\mathcal{G}$-扭子的站点论定义，恰好是局部可居性与自由传递作用的层论版本。在拓扑斯内部，它们分别成为内部满态射条件和同构 $P \times G \cong P \times P$。这两种定义可以直接相互转换。

□

注释 8.4。本命题说明了本文所采取的路径为何在概念上是一致的。第一篇扭子笔记 *[1]* 从外部引入了扭子。本文展示了同一思想如何自然地在拓扑斯中被内部化。这已足以表明，为何后续对密码学安全的层论阐述 *[2]* 应当以结构性的方式而非临时拼凑的方式处理局部知识和相容性。

9 迈向 Σ-协议与密码学安全

我们现在从概念层面说明，为何从扭子到拓扑斯的进展与Σ-协议相关。要点并不是说，标准的协议记录在任何朴素意义上确实是一个层或一个扭子。要点在于，理解局部一致性、可模拟性和全局知识所需的数学，已经在层论和拓扑斯理论中拥有一种自然的语言。

在挠子笔记 [1]，中，一个反复出现的主题是：即使没有特定原点，也可能进行协调传输。在 [2]，中，相应的密码学主题是，局部视图、攻击者观察和模拟证据片段都可以承载结构，而不必存在一个处处可见的单一朴素全局见证。因此，相关数学研究的不仅是全局对象的数学，更是局部可得相容对象的数学。

这正是格罗滕迪克拓扑发挥作用之处。Grothendieck 拓扑将何谓覆盖族形式化，从而也将何谓足以进行粘合的局部视图形式化。在 [2]，的密码学语境中，人们通过攻击者模型以及由可访问观察生成的覆盖来研究信息。层则编码了跨这些局部观察的信息一致性。拓扑斯理论的作用，是提供一种环境逻辑，使得人们能够在其中连贯地进行此类局部推理。

注 9.1. 可以启发式地将模拟器视为提供局部平凡化，不过它平凡化的不是几何丛，而是信息结构。模拟成功意味着某些局部可观测量能够以相容的方式生成。从这些局部片段过渡到有意义的全局陈述，自然会让人联想到下降。这本身并非协议理论的定理，但这种结构类比恰恰使层论和拓扑斯理论的语言富有成效。

作者的论文 [2] 应当置于这一背景下理解。该论文并非突然从普通的基于集合的协议记号中产生，而是源于一种持续贯彻的局部到整体观点：先是扭子，然后是层与拓扑斯，最后才是密码学安全。因此，本文与早先的挠子笔记旨在作为真正的铺垫，而非彼此无关的说明性旁述。其预期脉络是

$$\begin{aligned}&\text{torsors and cocycles} \longrightarrow \text{sheaves and descent}\\ &\quad\longrightarrow \text{topoi and internal logic} \longrightarrow \text{cryptographic local reasoning.}\end{aligned}$$

10 展望

仍有若干方向有待探索。首先，可以通过更全面地阐述几何态射、定义位点以及内在与外在观点之间的关系，来深化本文目前的导论性讨论。其次，可以不只在普通层拓扑斯中研究扭子，还可以将研究拓展到涉及叠或高阶拓扑斯的更精细情形。第三，也是与作者当前研究计划最相关的一点，可以尝试通过明确与攻击者模型和协议类别相对应的精确层论结构，使第9节中的密码学启发式更加精确。

不过，目前本文的目标是为后续工作做准备。本文与此前的扭子笔记 [1], 旨在让读者能够从概念上理解后续论文 [2] 。如果本文的讨论达到了目的，读者应当能够认识到，拓扑斯理论并非可有可无的抽象上层结构，而是对扭子中已有的局部到整体数学的一种自然扩展，因此也可作为结构性研究密码学安全的严肃候选语言。

11 结论

我们认为，从扭子到拓扑斯并非偶然的语言转换，而是对托orsor 理论中已有思想的结构性扩展。局部平凡性、交叠上的相容性、余循环数据和下降，早已指向这样一个世界：局部信息及其粘合居于首要地位。层论系统地组织了这一视角，而拓扑斯理论则将其进一步扩展到一个拥有自身关于真、存在与函数的内在概念的框架中。

因此，本文同时追求两个目标。一方面，本文介绍位点、层、拓扑斯、内部逻辑及相关范畴论工具。另一方面，本文也明确作为作者的密码学论文 [2], 的准备工作；该论文将格罗滕迪克拓扑和层论推理作为真正的结构性要素加以运用。此前的扭子笔记 [1] 为这一思路迈出了第一步；本文则通过更充分地阐明拓扑斯理论背景，进一步迈出了第二步。

附录的加入是出于教学上的考虑。尚未完全熟悉范畴论、内部逻辑或极限与余极限的读者，也应能将本文作为后续学习的实用准备。就此而言，本文不仅旨在搭建概念上的桥梁，也是一份实用的伴读材料。若本文达到了这一目的，读者便能以更清晰的认识来研读 [2]，理解为何局部推理、粘合和层论结构会自然而然地融入密码学安全与 Σ-协议的数学研究。

参考文献

[1] T. Inoué，《密码学中扭子的数学导论：兼论 Σ-协议》，预印本，arXiv，2026年。[2] T. Inoué，《格罗滕迪克拓扑与密码学安全的层论基础：攻击者模型与作为第一步的 Σ-协议》，预印本，arXiv，2026年。[3] S. Mac Lane 和 I. Moerdijk，《几何与逻辑中的层：拓扑斯理论初步导论》，施普林格，1992年。

[4] P. T. Johnstone，《大象素描：拓扑斯理论纲要》第 1 卷，牛津大学出版社，2002 年。[5] P. T. Johnstone，《大象素描：拓扑斯理论纲要》第 2 卷，牛津大学出版社，2002 年。[6] M. Artin、A. Grothendieck 和 J. L. Verdier，《托扑斯理论与概形的 étale 上同调》（SGA 4），《数学讲义》269、270、305 卷，施普林格，1972–1973 年。[7] S. Goldwasser、S. Micali 和 C. Rackoff，《交互式证明系统的知识复杂度》，《SIAM 计算杂志》18（1989），186–208。[8] I. Damgård，《关于》 Σ《-协议》，讲义，奥胡斯大学，2002 年。[9] C. P. Schnorr，《智能卡的高效身份识别与签名》，载于：《密码学进展——CRYPTO '89》，《计算机科学讲义》435 卷，施普林格，1990 年，第 239–252 页。

Takao Inoué

信息学院

大和大学

日本大阪府吹田市片山町 2-5-1，邮编 564-0082

inoue.takao@yamato-u.ac.jp

（个人）takaoapple@gmail.com（我更喜欢使用个人邮箱）

范畴论简要导论

本附录是为尚不熟悉范畴论、但仍希望读懂正文的读者编写的。它并非旨在取代一门完整的课程，而是希望提供足够的语言和技巧，以便开展有关层、拓扑斯和内部逻辑的基础工作。具体来说，我们将回顾范畴、函子、自然变换、泛构造、米田引理以及笛卡尔闭范畴。

A.1 范畴、态射与交换图

一个范畴 $\mathcal{C}$ 由以下部分组成：

(i) 一个对象类 A，B，C，……；(ii) 对每一对对象 A，B，都有一个由态射 $A \to B$ 构成的集合 态射集$_{\mathcal{C}}(A,\ B)$；(iii) 对每一组三个对象 A，B，C，都有一个复合律

$$\mathrm{Hom}_{\mathcal{C}}(B,C) \times \mathrm{Hom}_{\mathcal{C}}(A,B) \to \mathrm{Hom}_{\mathcal{C}}(A,C), \qquad (g,f) \mapsto g \circ f;$$

(iv) 对每个对象 A，一个恒等态射 $\mathrm{id}_A\colon\ A \to A$。

这些数据满足结合律

$$(h \circ g) \circ f = h \circ (g \circ f)$$

以及单位律

$$\mathrm{id}_B \circ f = f, \qquad f \circ \mathrm{id}_A = f.$$

典型例子包括集合范畴 **Set** 、群范畴**Grp** ，以及空间 X上的层范畴 **Sh(**X**)**。在所有这些范畴中，研究的不仅是孤立的对象，还包括对象之间的映射，以及各种构造呈现函子性地变化的方式。

如果范畴中的图表满足：任意一对具有相同源和目标的态射复合都相等，则称该图表可交换。例如，

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow{\scriptstyle h} & \downarrow{\scriptstyle g} \\ & & C \end{array}$$

当且仅当 $g \circ f = h$ 时可交换。许多范畴论定义无非是在陈述某个图表可交换，并且在所有此类图表中具有泛性质。

A.2 函子与自然变换

函子 *functor* $F\colon \mathcal{C} \to \mathcal{D}$ 将 $\mathcal{C}$ 中的每个对象 A 映射到 $\mathcal{D}$ 中的一个对象 $F(A)$，并将每个态射 $f\colon A \to B$ 映射到一个态射

$$F(f)\colon F(A) \to F(B)$$

以这样的方式

$$F(g \circ f) = F(g) \circ F(f), \qquad F(\mathrm{id}_A) = \mathrm{id}_{F(A)}.$$

因此，函子保留范畴结构。例如，幂集构造 $X \mapsto \mathcal{P}(X)$ 是一个函子 **集合范畴** $\to$**集合范畴**，而对于层 $\mathcal{F}$，赋值 $U \mapsto \mathcal{F}(U)$ 是一个从开集到集合范畴的逆变函子。

如果 $F, G\colon \mathcal{C} \to \mathcal{D}$ 是函子，那么一个自然变换 自然变换 $\eta\colon F \Rightarrow G$ 是一个由态射组成的族

$$\eta_A\colon F(A) \to G(A)$$

i由 $\mathcal{C}$ 的对象 A 索引，使得对于每个态射 $f\colon A \to B$，方块

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ \downarrow F(f) & & \downarrow G(f) \\ F(B) & \xrightarrow{\eta_B} & G(B) \end{array}$$

可交换。自然性体现了这样的思想：映射 η_A 与所有相关的结构映射相容。这是范畴论将“在所有情境中进行相同构造”形式化的基本方式之一。

A.3 泛性质

范畴论很大一部分内容是研究由泛性质定义的对象。关键在于，对象的特征并非取决于构造它的材料，而是取决于映入或映出它的映射。

例如 ，对象 A 和 B 的积是一个对象 $A \times B$，并配有投影 s

$$\pi_1 \colon A \times B \to A, \qquad \pi_2 \colon A \times B \to B,$$

使得对于每个对象 T 以及每一对映射

$$f \colon T \to A, \qquad g \colon T \to B,$$

都存在唯一的映射

$$\langle f, g \rangle \colon T \to A \times B$$

满足 $\pi_1 \circ \langle f, g \rangle = f$ 以及 $\pi_2 \circ \langle f, g \rangle = g$。相关图表为

$$\begin{array}{ccccc} & & T & & \\ & \swarrow f & \downarrow \langle f,g \rangle & \searrow g & \\ A & \xleftarrow{\pi_1} & A \times B & \xrightarrow{\pi_2} & B \end{array}$$

虚线箭头由泛性质唯一确定。这种唯一性往往比任何显式公式都更为重要。

另一个基本的泛构造是拉回。给定 $f \colon A \to C$ 和 $g \colon B \to C$，拉回是一个对象 $A \times_C B$，它适合放入一个交换方块中

$$\begin{array}{ccc} A \times_C B & \longrightarrow & B \\ \downarrow & & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

并且在所有此类方块中具有泛性质。拉回在层论中无处不在，例如将局部数据限制到交叠上时就会出现拉回。

A.4 极限与余极限

两类最基本的泛构造是极限 和余极限。极限是从外部对象向图表接收相容映射的一种泛性质方式，而余极限则是从图表向外发送相容映射的一种泛性质方式。积、拉回和等化子都是极限的例子。余积、推出和余等化子都是余极限的例子。

与其直接给出完整的抽象定义，不如先从例子开始。我们已经看到，积 $A \times B$ 由指向 A 和 B的映射刻画。这使它成为由 A 和 B组成的离散图的极限。同样，拉回

$$A \times_C B$$

是该余跨的极限

$$A \xrightarrow{f} C \xleftarrow{g} B.$$

拉回是施加相容性条件最基本的方式。在几何学和层论中，当两个数据片段被限制到公共交叠部分时，就会出现拉回。

另一个重要的极限是两个平行箭头的等化子

$$A \rightrightarrows_{g}^{f} B.$$

等化子是一个对象 E，带有一个映射 $e\colon E \to A$，使得

$$f \circ e = g \circ e,$$

并且它关于这一性质具有泛性质。在**集合范畴**中，可以将它具体地看作子集

$$E = \{a \in A : f(a) = g(a)\}.$$

因此，等化子是使两个映射相等的泛性质对象。它是一个极限，因为它从每个满足 f 和 g 已经相等的对象接收映射。

对偶地，余积 $A \amalg B$ 由包含映射刻画

$$A \to A \amalg B, \qquad B \to A \amalg B,$$

从 $A \amalg B$ 出发的映射恰好是从 A 和 B 出发的映射对。同样，推出是一个跨度的余极限

$$A \xleftarrow{f} C \xrightarrow{g} B,$$

并且可以将其视为沿着公共部分 C粘合 A 和 B 的泛性质方式。

与等化子对偶的是，两个平行箭头的余等化子

$$A \rightrightarrows_{g}^{f} B.$$

余等化子是一个对象 $q\colon B \to Q$，满足

$$q \circ f = q \circ g,$$

并且在具有这一性质的对象中具有泛性质。在**集合范畴**中，可以将其视为通过强制使.....相等而得到的 B 的商对象

$$f(a) \sim g(a) \qquad \text{for all } a \in A.$$

因此，余等化子是一个泛性质对象：在其中，两个映射经过商化后变得相等。它是一个余极限，因为任何来自 B、且已将 f（a）与 g（a）等同起来的映射，都唯一地经由 Q分解。

更一般地，设 $D\colon \mathcal{J} \to \mathcal{C}$ 是一个图表。从对象 L 到 D 的一个锥 是一个映射族 s

$$L \to D(j)$$

它与$\mathcal{J}$中的所有箭头相容。D 的一个极限 是到 D 的一个泛锥。对偶地，从 D 到对象 M 的一个余锥 是一个映射族

$$D(j) \to M$$

它与$\mathcal{J}$中的所有箭头相容，而 D 的一个余极限 是一个泛余锥。

在实践中，无须一开始就掌握完整的抽象定义。关键在于理解泛问题的逻辑。要构造一个极限，可以这样问：“哪个对象以最泛的方式接收来自其他所有对象的相容映射

？”要构造一个余极限，可以这样问：“哪个对象是以最泛的方式强制相容的出射映射而得到的？”这种思维方式是范畴论的核心，并且在层论、下降和拓扑斯理论中屡见不鲜。

停下来想一想传统名称也很有帮助：射影极限 （也称为逆极限）和归纳极限 （也称为正向极限）。逆系统通常是一个图表

$$X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \cdots$$

其中信息沿着过渡映射向后传递。它的极限是由所有相容族组成的对象

$$(x_0, x_1, x_2, \dots)$$

其中每个 x_n 都与 x_{n+1}的像相匹配。因此，逆极限表达了这样一种思想：在每个阶段跟踪数据，同时确保所有阶段之间完全相容。可以将其看作由相干逼近构成的对象。

对偶地，正向系统通常是一个图表

$$X_0 \to X_1 \to X_2 \to \cdots$$

其中信息向前传递。它的余极限将那些在某个较后阶段变得相等的元素等同起来。因此，正向极限表达了这样一种思想：通过反复添加数据，并施加由过渡映射生成的等同关系，构造出一个更大的对象。可以将其看作通过累积过程最终得到的对象。

例如，在**集合范畴**中，商映射序列的逆极限记录了在每个阶段都保持相容的序列，而包含链的正向极限就是所有阶段的并集。这些都是值得牢记的绝佳直观图像：逆极限刻画相容族，正向极限则刻画最终等同与累积。

A.5 极限与余极限练习

极限与余极限在初学时往往在概念上较难理解，因此在具体情境中练习很有帮助。

练习 C1. 设 $\mathcal{C}$ 是一个具有拉回的范畴。给定箭头

$$A \xrightarrow{f} C \xleftarrow{g} B,$$

证明一个态射 $X \to A \times_C B$ 等价于以下态射数据

$$u\colon X \to A, \qquad v\colon X \to B$$

使得 $f \circ u = g \circ v$。解释为什么这说明了“拉回是相容对的对象”这一说法是合理的。

练习 C2. 在集合范畴中，设

$$A = \{1, 2\}, \qquad B = \{a, b\}, \qquad C = \{*\}$$

由唯一的映射 $A \to C$ 和 $B \to C$给出。显式计算拉回 $A \times_C B$。然后计算该跨度的推出

$$A \xleftarrow{\mathrm{id}_A} A \xrightarrow{h} B$$

对于映射 $h\colon\ A \to B$ 满足 $h(1) = a$ 以及 $h(2) = b$。

习题 C3. 设 $D\colon \mathcal{J} \to \mathcal{C}$ 是一个图表，并设 $K\colon \mathcal{J} \to \mathbf{1}$ 是到终对象范畴的唯一函子。解释为什么左 Kan 延拓 $\mathrm{Lan}_K D$ 等同于 D 的余极限，以及为什么右 Kan 延拓 $\mathrm{Ran}_K D$ 等同于 D 的极限。你不必形式化地证明最一般的定理；只需仔细展开相应的泛性质即可。

习题 C4. 考虑 **集合范畴**中的逆系统

$$\cdots \xrightarrow{\pi_4} \mathbb{Z}/16\mathbb{Z} \xrightarrow{\pi_3} \mathbb{Z}/8\mathbb{Z} \xrightarrow{\pi_2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}/2\mathbb{Z},$$

其中每个映射都是模约化到较小的 2 的幂。具体描述这个系统的逆极限中的一个元素是什么。解释为什么应当把这个逆极限看作相容的逼近系统，而不是模某个固定的 2 的幂的单个剩余类。

习题 C5. 考虑 **集合范畴**中的正向系统

$$\{1,\dots,n\} \hookrightarrow \{1,\dots,n+1\} \hookrightarrow \{1,\dots,n+2\} \hookrightarrow \cdots,$$

其中每个映射都是显然的包含映射。求它的余极限。然后用文字解释，为什么这个例子体现了正向极限作为各阶段“最终并集”的直观含义。

A.6 Kan 延拓

Kan 延拓是范畴论中最重要的一般构造之一。确切地说，它们是沿另一个函子延拓某个函子的泛性质方式。许多熟悉的构造都是 Kan 延拓的特例，包括若干极限、余极限、层化类过程以及伴随函子。

假设给定范畴 $\mathcal{A}$、$\mathcal{B}$和$\mathcal{C}$，以及一个函子

$$K\colon \mathcal{A} \to \mathcal{B},$$

以及另一个函子

$$F\colon \mathcal{A} \to \mathcal{C}.$$

我们希望用一个定义在 $\mathcal{B}$ 上的函子替换 F。换言之，我们要寻找一个函子

$$G\colon \mathcal{B} \to \mathcal{C}$$

它以某种泛性质的意义，尽可能贴近这样的想法：

$$G \circ K \approx F.$$

这个问题有两个版本。

A沿着 K 对 F 的左 *Kan* 延拓，记作 F 沿着 K，记作

$$\mathrm{Lan}_K F,$$

是一个函子 $\mathcal{B} \to \mathcal{C}$，并配备了一个自然变换

$$\eta\colon F \Rightarrow (\mathrm{Lan}_K F) \circ K$$

它在所有此类对中具有泛性质。这意味着，如果 $H\colon \mathcal{B} \to \mathcal{C}$ 是另一个函子，并且$\alpha\colon F \Rightarrow H \circ K$ 是任意自然变换，那么存在唯一的自然变换

$$\overline{\alpha}\colon \operatorname{Lan}_K F \Rightarrow H$$

使得

$$\alpha = (\overline{\alpha} K) \circ \eta.$$

对偶地，沿 K 的 F 的右 *Kan* 延拓 记作

$$\operatorname{Ran}_K F,$$

是一个函子 $\mathcal{B} \to \mathcal{C}$，配备了一个自然变换

$$\epsilon\colon (\operatorname{Ran}_K F) \circ K \Rightarrow F$$

它在所有此类对中具有泛性质。因此，右 Kan 延拓解决了极限侧上最佳的泛性质延拓问题，而左 Kan 延拓则在余极限侧上解决这一问题。

Kan 延拓之所以重要，一个原因是它们统一了许多定义。例如，如果 $K\colon \mathcal{A} \to \mathbf{1}$ 是到终对象范畴的唯一函子，那么

$$\operatorname{Lan}_K F$$

本质上是 F 的余极限，而

$$\operatorname{Ran}_K F$$

本质上就是 F 的极限，前提是这些极限存在。因此，极限与余极限本身也可以视为到一点的 Kan 延拓。

第二个原因是，伴随函子可以用 Kan 延拓来刻画。如果 $K\colon \mathcal{A} \to \mathcal{B}$ 有左伴随，那么该左伴随可以描述为恒等函子的一个适当的 Kan 延拓。因此，Kan 延拓处于范畴论的核心地带：它们编码了以泛性质方式延拓结构的一般模式。

对于初学者，可以这样概括：

> Kan 延拓是在原本定义函子的范畴之外延续该函子的泛性质最优方式。

这句概括并非定义，但抓住了正确的直觉。左 Kan 延拓由余极限类型的信息构造，右 Kan 延拓则由极限类型的信息构造。因此，它们构成了一座桥梁，连接函子性与上文讨论的泛构造。

A.7 可表函子与米田观点

固定一个范畴 $\mathcal{C}$。对于任意对象 A，都可以得到一个逆变函子

$$h_A := \operatorname{Hom}_{\mathcal{C}}(-, A)\colon \mathcal{C}^{\mathrm{op}} \to \mathbf{Set},$$

称为由 A 表示的函子。它将对象 X 映射到态射的集合 $X \to A$。因此，指向 A 的态射定义了一个函子性的“侧写”，展现了从范畴其余部分的视角看 A的情况。

米田理论的基本见解是，一个对象完全由其轮廓所确定。也就是说，要理解 A，通常只需理解所有映射到 A的映射。这一原理十分重要，值得完整陈述。

定理 A.1 (米田引理**)**。 设 $\mathcal{C}$ 是一个局部小范畴， A 是 $\mathcal{C}$ 中的一个对象，且$F\colon \mathcal{C}^{\mathrm{op}} \to$ **集合范畴** 是一个预层。那么存在一个自然双射

$$\mathrm{Nat}(h_A, F) \cong F(A).$$

这里$\mathrm{Nat}(h_A, F)$ 表示从 h_A 到 F的自然变换集合。

证明。 给定一个自然变换 $\eta\colon\ h_A \Rightarrow F$，考虑元素

$$\eta_A(\mathrm{id}_A) \in F(A).$$

这定义了一个函数

$$\Phi\colon\ \mathrm{Nat}(h_A, F) \to F(A), \qquad \Phi(\eta) = \eta_A(\mathrm{id}_A).$$

反过来，给定 $x \in F(A)$，对每个对象 X 定义一个映射

$$\eta^x_X\colon h_A(X) = \mathrm{Hom}_{\mathcal{C}}(X, A) \to F(X)$$

by

$$\eta^x_X(f) = F(f)(x).$$

我们必须验证 η^x 是自然的。若 $u\colon\ Y \to X$，则对任意 $f\colon\ X \to A$，有

$$\eta^x_Y(f \circ u) = F(f \circ u)(x) = F(u)(F(f)(x)) = F(u)(\eta^x_X(f)),$$

因此自然性方块可交换。于是 x 确定了一个自然变换 η^x。这给出了一个函数

$$\Psi\colon F(A) \to \mathrm{Nat}(h_A, F), \qquad \Psi(x) = \eta^x.$$

Now

$$\Phi(\Psi(x)) = \eta^x_A(\mathrm{id}_A) = F(\mathrm{id}_A)(x) = x,$$

因此 $\Phi \circ \Psi = \mathrm{id}_{F(A)}$。反过来，若 $\eta\colon\ h_A \Rightarrow F$，则对每个 $f\colon\ X \to A$，将自然性应用于 f可得

$$\eta_X(f) = F(f)(\eta_A(\mathrm{id}_A)) = \left(\eta^{\eta_A(\mathrm{id}_A)}\right)_X(f).$$

因此 $\Psi(\Phi(\eta)) = \eta$。所以 Φ 和 Ψ 互为逆双射。 □

一个特别重要的推论是米田嵌入

$$\mathcal{C} \hookrightarrow [\mathcal{C}^{\mathrm{op}}, \mathbf{Set}], \qquad A \mapsto h_A,$$

它是全忠实的。因此，可以将每个范畴都视为存在于一个集合值函子范畴之中。这一观点是层论和拓扑斯理论的背景，因为层恰好是满足额外粘合条件的预层。

A.8 笛卡尔闭范畴

如果范畴 $\mathcal{C}$ 具有有限积，并且对于每一对对象 A，B，都存在一个指数对象 B^A，则称其为笛卡尔闭的。指数对象由一个自然双射刻画：

$$\mathrm{Hom}_{\mathcal{C}}(X \times A, B) \cong \mathrm{Hom}_{\mathcal{C}}(X, B^A)$$

对所有对象 X 都成立。等价地，从 $X \times A$ 到 B 的映射可由从 X 到 B^A 的映射表示。这就是柯里化的范畴形式。
在范畴 **集合范畴** 中，指数对象 B^A 是从 A 到 B 的函数集合。上述伴随恰好表明，一个函数

$$X \times A \to B$$

与一个函数是同一回事

$$X \to B^A.$$

因此，笛卡尔闭范畴是存在内部函数对象的范畴。

笛卡尔闭范畴之所以在这里重要，是因为初等拓扑斯按定义是具有有限极限、笛卡尔闭且拥有子对象分类器的范畴。因此，若要理解拓扑斯，就必须熟悉积与指数对象的逻辑。指数对象使蕴涵和函数类型能够在内部表示。这是从范畴结构通往内部逻辑的桥梁之一。

A.9 这些概念为何对正文至关重要

本文正文运用了以上所有思想。位点与层是在范畴中定义的。位点上的扭子是由局部泛性质定义的函子性对象。拓扑斯是具有足够内部结构、能够支持逻辑的范畴。从对象到预层的转换背后，始终隐含着米田引理；内部函数对象和蕴涵则以笛卡尔闭性为基础。因此，范畴论在这里并非仅仅是背景符号，而是使扭子、层与拓扑斯的局部到整体结构变得清晰易懂且便于处理的语言。

B 内部逻辑与直觉主义逻辑

初等拓扑斯的内部逻辑通常不是经典逻辑，而是直觉主义逻辑。这一说法值得仔细解释，因为它是拓扑斯理论中最重要的概念性启示之一。

在经典逻辑中，每个命题非真即假，而且排中律

$$P \vee \neg P$$

始终成立。等价地说，真值由布尔代数组织起来。在范畴**集合范畴**中，这体现为子对象分类器是二元素集合$\{0, 1\}$，而集合的子对象对应于取布尔值的特征函数。

在一般的拓扑斯中，真值对象是 Ω。其全局或局部真值的集合通常并非布尔的，而是具有海廷代数的结构。海廷代数

仍然支持合取、析取、蕴涵以及否定这一概念，但否定弱于布尔逻辑中的否定。公式 $P \vee \neg P$ 不一定成立。因此，内部逻辑通常是直觉主义的。

这并非缺陷或遗漏，而是如实反映了拓扑斯中的真理可能具有局部性这一事实。在层托扑斯 $\mathbf{Sh}(X)$ 中，关于开集 U 的命题可能在 U 的一部分成立，而在另一部分不成立。因此，它的真值由 U 的一个开子集表示。这类局部真值自然构成一个开集的海廷代数，而通常并不构成布尔代数。因此，直觉主义逻辑之所以出现，是因为局部性的几何学本身就不是布尔的。

记住二者区别的一个实用方法是：经典逻辑关注一个命题是否已经在全局上得到判定，而直觉主义逻辑关注能否在现有语境中构造或验证它。在拓扑斯中，现有语境往往是局部的。因此，直觉主义逻辑是构造性局部推理的自然逻辑。

Kripke–Joyal 语义与此的关系，让这一点尤为清楚。说 $U \Vdash \exists x\, \varphi(x)$，意味着可以转到 U 的一个覆盖，并在那里找到局部见证。说 $U \Vdash \forall x\, \varphi(x)$，意味着该陈述在对更小开集进行每一次限制后都必须继续成立。这些恰恰是直觉主义语义中所预期的规则：真理在细化下保持稳定，但可能需要通过局部构造来确立。

因此，可以如下概括这一情况。拓扑斯理论提供了一个环境性的范畴论框架，在其中，几何局部性、层论粘合与直觉主义推理彼此融为一体。拓扑斯的内部逻辑之所以是直觉主义的，是因为真值是通过语境、限制与相容性来调节的，而不是由单一的全局布尔判定过程决定的。

这一观察对于本文更为广泛的目标具有重要意义。本文后续的密码学应用 [2] 涉及局部可观测性、局部一致性、受控的信息粘合，以及从部分数据有条理地过渡到整体结构。就这些目的而言，直觉主义逻辑不仅在哲学上颇有趣味；它在结构上也是恰当的。它提供了一种逻辑语言，能够表达全局知识与局部强制信息之间的差异，而不会将二者混为一谈。

C 练习解答

练习 1 的解答。 对于层拓扑斯$\mathbf{Sh}(X)$，子对象分类器 Ω 为每个开集 U 赋予 U的开子集集合。事实上，终对象层在 U 上的限制的一个子对象，由其具有元素的开区域决定，因此，Ω(U)可以自然地识别为 U的开集格。因此， U 上的一个真值并不只是一个比特，而是 U 上某个命题成立的区域。这正是为什么真值具有局部性。

练习 2 的解答。 选取局部截面 $s_i \in \mathcal{P}(U_i)$。在每个交叠 $U_{ij} = U_i \times_U U_j$ 上，自由传递性保证存在唯一的元素 $g_{ij} \in \mathcal{G}(U_{ij})$，使得

$$s_j = s_i \cdot g_{ij}.$$

在三重交叠 U_{ijk} 上，可以直接比较 s_k 与 s_i ，也可以通过 s_j 比较：

$$s_k = s_i \cdot g_{ik} = s_j \cdot g_{jk} = s_i \cdot g_{ij} g_{jk}.$$

根据传输的唯一性，$g_{ik} = g_{ij} g_{jk}$。这就是余循环条件。

练习 3 的解答。 $U \Vdash \exists x\, \varphi(x)$ 表示，在通过覆盖细化 U 后，可以在各个部分上找到局部见证。因此，存在性可以是局部的。相比之下，$U \Vdash \forall x\, \varphi(x)$ 表示，每个较小开集 $V \subseteq U$ 上的每个截面都满足 φ。全称真值因此必须在每次进一步局部化后仍然成立。这一区别反映了量词的直觉主义含义。

练习 4 的解答。 对于 $f \in C^0(U,\ \mathbb{R})$，分类映射将 f 映射到开子集

$$\chi_P(f) = \{x \in U \mid f(x) > 0\}.$$

因此，内部谓词“$f > 0$”被解释为其中正性成立的开区域。这是层拓扑斯中真值的一个具体模型。

练习 5 的解答。 有限极限提供积、终对象、拉回和等化子，因此可以构造许多熟悉的类集合结构。指数对象提供内部函数对象。子对象分类器提供一个内在真值对象，并允许以范畴论方式表示谓词。在这些要素中，子对象分类器最直接地负责内在真值，尽管其他要素对于支撑更广泛的逻辑和范畴结构也是必需的。

练习 C1 的解答。 根据拉回的泛性质，给出一个映射

$$\phi\colon X \to A \times_C B$$

等价于给出映射

$$u = \pi_A \circ \phi\colon X \to A, \qquad v = \pi_B \circ \phi\colon X \to B$$

使得

$$f \circ u = g \circ v.$$

反过来，任意这样的相容对（$u,\ v$）都会唯一地诱导出一个映射

$$X \to A \times_C B.$$

因此，拉回恰好是一个泛性质对象，用来参数化到 A和 B 上的相容映射对，且它们在 C 上相合。

练习 C2 的解答。 由于映射 $A \to C$ 和 $B \to C$ 都是唯一的，且 C 只有一个元素，因此相容条件自动成立。因此

$$A \times_C B \cong A \times B$$

作为集合，因此具体地

$$A \times_C B = \{(1,a),(1,b),(2,a),(2,b)\}.$$

对于.....的推出

$$A \xleftarrow{\mathrm{id}_A} A \xrightarrow{h} B,$$

从不交并 $A \amalg B$开始，并将左侧的每个元素 $x \in A$与其在右侧的像$h(x) \in B$ 等同。由于 $h(1) = a$ 和 $h(2) = b$，这些关系将 1 与 a 等同，并将 2 与 b等同。施加这些等同关系后，除了由 a 和 b代表的两个等价类外，不会剩下其他点。因此，该推出与 B典范同构。

习题 C3 的解答。 从终对象范畴 $\mathbf{1}$ 到$\mathcal{C}$ 的函子，只需选择 $\mathcal{C}$中的一个对象。因此，一个函子

$$\operatorname{Lan}_K D\colon \mathbf{1} \to \mathcal{C}$$

恰好是 $\mathcal{C}$ 中的一个对象 L 。自然变换

$$D \Rightarrow (\operatorname{Lan}_K D) \circ K$$

于是恰好是从图表 D 到对象 L的一个余锥。左 Kan 延拓的泛性质表明，这个余锥在所有从 D出发的余锥中具有泛性质。但这恰好就是余极限的定义。

对偶地，右 Kan 延拓

$$\operatorname{Ran}_K D\colon \mathbf{1} \to \mathcal{C}$$

相当于一个对象 R 以及一个自然变换

$$(\operatorname{Ran}_K D) \circ K \Rightarrow D,$$

它恰好是从 R 指向图表 D的一个锥。其泛性质表明，这个锥在所有指向 D的锥中具有泛性质。这恰好就是极限的定义。

习题 C4 的解答。 逆极限中的一个元素是一个序列

$$(x_1, x_2, x_3, \dots), \qquad x_n \in \mathbb{Z}/2^n\mathbb{Z},$$

使得每个 x_{n+1} 模 2^n都化为 x_n 。因此，我们并不是从一开始就选定一个剩余类，而是分别选取模 2、模 4、模 8 等的一个剩余类，并确保它们彼此相容。这就是为什么最好将逆极限视为相容的逼近族。每个阶段都提供有限的信息，而极限则同时保留所有阶段的信息。这正是后来引出诸如 2 进整数这类对象的模式。

习题 C5 的解答。由于系统中的每个映射都是包含映射，因此除了集合自身已有的等同关系外，不会施加新的等同关系。因此，余极限就是所有阶段的并集：

$$\varinjlim_n \{1, \dots, n\} \cong \mathbb{N}_{>0}.$$

这很好地说明了正向极限的直观含义。我们从一个通过添加新元素而逐渐扩大的对象序列开始，而余极限就是最终包含所有曾在某个阶段出现过的元素的对象。在这个例子中，每个正整数都会在有限步之后出现，因此正向极限就是所有正整数构成的集合。

因此，极限与余极限是到终对象范畴的 Kan 延拓：

$$\operatorname{colim} D \simeq \operatorname{Lan}_K D, \qquad \lim D \simeq \operatorname{Ran}_K D.$$

D 可能的课程计划

根据听众的背景知识，这份讲义可以采用多种方式讲授。如果目标是为尚未完全熟悉范畴论的学生开设一门严谨但仍属入门性质的课程，那么一种自然的安排是**10–12 讲**，每讲**90 分钟**。如果将部分附录作为课外阅读材料，课程可以缩短为 8 讲；而较为从容的 14 讲版本则可以加入更多例子和练习。不过，在大多数情况下，10–12 讲的安排似乎最为现实。

本课程的指导原则是从具体的局部到整体直觉出发，逐步过渡到层、拓扑斯和内部逻辑这一更抽象的语言，然后再解释这为何与密码学安全的层论方法以及 Σ-协议相关。从这个意义上说，本课程不仅是对各个主题的概览，也是为论文《格罗滕迪克拓扑与密码学安全的层论基础：攻击者模型与 Σ-协议作为第一步》所做的系统准备。

D.1 建议的总体长度

以下是一项合理的建议。

- **最低版本：** 8 次、每次 90 分钟的讲座，前提是将附录安排为自学内容。
- **标准版本：** 10 次、每次 90 分钟的讲座，适用于均衡的入门课程。
- **扩展版：** 12 次讲座，每次 90 分钟；如果希望花些时间做练习、讨论例子以及拓扑斯的逻辑方面，可以采用此安排。

其中，**10 次讲座的安排** 可能是最合适的默认选择。它的时长足以让人理解这套理论，同时又足够精简，可用于聚焦式阅读课程或研究生研讨班。

D.2 标准的 10 次讲座安排

现在我们来介绍一套具体的 10 次讲座安排。

第 1 次讲座：从扭子到局部到整体思维。 回顾扭子的基本概念：自由传递作用、缺少优选原点、点与点之间的传输，以及局部平凡性的作用。再次说明扭子为何自然地引出余循环数据与粘合。本次讲座旨在阐明，转向层与拓扑斯并非改变研究主题，而是延续同一种局部到整体哲学。

讲座 2. 位点、格罗滕迪克拓扑与层。将范畴介绍为广义的索引世界，随后定义筛和格罗滕迪克拓扑。给出具体示例：拓扑空间上的开覆盖，以及简单的小站点示例。接着解释预层和层，着重说明粘合与局部性。教学目标是让层条件显得自然，而非只是一种形式化概念。

讲座 3. 位点上的扭子、余循环与下降。回到扭子，并以群层的语言来讨论。解释位点上的局部平凡性、切赫余循环和下降数据。这一讲尤为重要，因为它将前文的扭子笔记与当前文本联系起来，并准确说明扭子本就自然地存在于层论世界中的含义。

第 4 讲：层范畴与格罗滕迪克托扑斯。说明为什么层范畴不仅仅是方便的容器，而是真正的数学宇宙。介绍这样一句箴言：格罗滕迪克托扑斯是通过其层来观察的广义空间。比较**集合范畴**与 $\mathbf{Sh}(X)$，并解释为什么后者的表现如同前者的可变版本。

第 5 讲：初等拓扑斯。介绍有限极限、指数对象和子对象分类器。给出初等托扑斯的定义，并说明这一概念为何抽象出了层范畴的关键结构特征。在这里，将这些概念与**集合范畴**中的熟悉构造进行比较会很有帮助。

第 6 讲：子对象分类器与内部逻辑。阐述拓扑斯中的真值可能在局部发生变化这一观点。解释 Ω、特征态射以及谓词的解释。介绍内部逻辑的基本直觉及其局部特性。如果时间允许，可以用一个层的例子来说明局部真理与全局真理的差异。

第 7 讲：直觉主义逻辑与局部推理。承接上一讲，解释为什么拓扑斯的内部逻辑通常是直觉主义逻辑。以非正式但严谨的数学方式讨论合取、蕴涵和量词。通过这一讲，学生开始认识到，逻辑结构并非外在的装饰，而是拓扑斯自身几何结构的一部分。

第 8 讲：范畴论工具的实践应用。选取附录中的部分内容：米田引理、极限与余极限、等化子与余等化子、拉回与推出，以及笛卡尔闭性的含义。课堂上至少完成一道练习。目标不是把这门课变成一门通用范畴论课程，而是让学生掌握足够的实际运用能力，使前几讲的内容能够派上用场。

第 9 讲：拓扑斯中的挠子与局部对称性。解释如何在拓扑斯内部谈论群对象、扭子和局部对称性。本讲应阐明，进入拓扑斯理论后，扭子并未被抛在一边；相反，它们的概念变得更加清晰。借此从内部视角重新探讨下降与局部平凡性。

第 10 讲：迈向密码学安全与 Σ-协议。最后，解释通往密码学论文的概念桥梁。讨论为何层论和拓扑斯论推理能自然地阐明局部一致性、可模拟性、见证数据和粘合。此处的目标还不是重现密码学论文的完整技术论证，而是让学生能够有意义地读懂这篇论文。

D.3 一个可能的 12 讲扩展方案

如果还能安排两讲，一个有用的扩展方案如下。

- 增加一讲，专门通过习题讲解极限、余极限、米田引理和内部逻辑。
- 增加一讲，结合本文共同阅读密码学论文的精选段落，从而充分明确本导论的准备性。

这个 12 讲版　　特别适合研究生研讨班或指导阅读课程　　.

D.4 教学评注

对初学者而言，最困难的概念跃迁通常发生在两个方面。首先，他们可能将层理解为一种技术性工具，却没有看到层为何会自然地引出拓扑斯。其次，他们可能理解拓扑斯的形式定义，却没有看到内部逻辑为何重要。因此，应当反复回到少数几个核心主题：

- 局部数据与粘合，
- 缺乏首选的全局选择，
- 下降与相容性，
- 局部真理与全局真理的对比，
- 这些思想在结构性理解密码学安全中的作用。

简而言之，这些材料对于非常短的迷你课程来说可能过于丰富，但很适合**每讲 90 分钟、共 10–12 讲的课程**。这样的课程不仅能让学生初步了解层和拓扑斯，还能为他们日后学习 Σ-协议打下扎实的概念基础。