1 引言与定位（含相关工作与贡献地图）

1.1 背景与动机

以仿射层（全连接/卷积/均值池化/推理态 BN/残差）与 ReLU/Leaky-ReLU/PReLU/Abs/Max 等门控为基本组件、且计算图为 DAG 的神经网络，其各输出分量在输入域上均为**连续分段线性（CPWL）**函数。这一事实使得诸多几何与形式化任务（线性区域、梯度/雅可比、决策边界、Lipschitz、鲁棒/等变/等价判定、干预/修复）可以在**片段几何**层面被精确表述与求解。

困难在于**表达爆炸**：若将网络逐层展开为由 `max/+` 复合构成的**符号树**，线性片段与门控条件在最坏情况下随门控数呈 $2^{\Theta(N)}$ 增长。先构造"完整符号表达式"，再将其编译为某种可计算结构（如自动机/图），在中等规模网络上即不可行。

1.2 问题陈述

我们关心如下目标：给定满足上述组件与 DAG 假设的网络 $F : \mathcal{D}_{\text{in}} \subseteq \mathbb{R}^n \to \mathbb{R}^m$，

1. **无损表示**：构造一个**可共享的有向无环图**，其在每个输入点 x 上与 $F(x)$ 完全一致；
2. **直接分析**：在该图上直接开展几何与验证问题，而不显式枚举全部线性区域；
3. **可扩展性**：在保持健全性的前提下，避免全局细分与全量比较面，令时间与空间开销与**访问到的子域与必要比较数**近似线性相关；
4. **可判定性**：等价、性质验证、最大因果影响等核心问题在该表示上应**可判定**，并能给出**证书**或**反例**。

1.3 核心思想与框架概述

(i) 函数权半环与带守卫的加权图（SWT）
我们采用按点热带半环

$$K_f = (\mathrm{CPWL}^{\pm\infty},\ \oplus = \max,\ \otimes = +)$$

作为**权重域**；边/结点权为 CPWL 函数，组合为按点 `max/+`。引入以 H-形式多面体表示的**守卫**，约束输入 x 在边上的可行性。按层编译得到的**符号加权变换器（SWT）**，以**共享守卫库**与**模板别名**避免重复子式复制；路径求值为沿路权的 $\otimes$ 累加，跨路径以 $\oplus$ 取最优，逐点与网络前向一致。

(ii) 动态按需细化（JIT-SWT）
为避免静态全展开带来的指数规模，我们提出**动态编译/按需细化**：
— 仅维护**全局守卫库**与**懒表达（Expr）**的共享 DAG，不预先枚举线性片段；
— 对 ReLU/Max/阈值等，仅在**访问到的 GuardSet**上、且**必要时才**插入比较/阈值超平面；
— 按需构造局部的**最小公共细分**与**赢家域**；
— 始终维护一对**上下包络** $(\underline{A}, \overline{A})$，确保 $\underline{A} \le F \le \overline{A}$；当相关子域已完全细化为单仿射时，$\underline{A} = \overline{A} = F$。

该框架统一了承载表示与求解过程：编译与分析同处一张**共享、可细化**的图上完成，指数爆炸被**查询/验证驱动的局部细化**所替代。

1.4 贡献与主结果（可检验标签）

A. CPWL 层演算与静态基线（§2）

- **AF-1…AF-5**：给出 CPWL 层演算的良定义性、同态求值、连续/凸的充分条件、a.e. 可微与组合性。
- **SWT-1**：从网络到 SWT 的**等价编译**（逐点一致，作为"真值语义"）。

- **SWT-3/4**：**等价可判定**与**差异区域自动机**（在共同细分上化为有限仿射比较/LP/SOCP）。
- **SWT-5**：在给定有限守卫库与仿射权基时的**最小实现复杂度存在性**与**NP-难性**。

B. 动态编译（JIT-SWT）的语义与保证（§3）

- **DYN-1（健全性）**：任何时刻维护 $\underline{A}(x) \le F(x) \le \overline{A}(x)$。
- **DYN-2（任意时精确性）**：在任意子域 C 上，若所有相关比较/阈值面已显式加入且懒表达在 C 内下沉为**单仿射**，则 $\underline{A} = \overline{A} = F$ 于 C 成立，与静态语义一致。
- **DYN-3（进度不回退）**：按需细化仅作用于被分裂子域，不破坏既有精确区域。
- **DYN-4（预算化复杂度上界）**：在切分预算 B 与守卫上限 G 下，图规模与求解次数对 (B, G) 呈线性上界；避免一次性 $\binom{k}{2}$ 全局比较。
- **DYN-5（支配剪枝正确性）**：若在子域 C 上 $\max(f_\pi - f_{\pi'}) \le 0$，则候选 π 在 C 非赢家，可安全剪除。
- **DYN-6（JIT-Decidability）**：在**有限细分策略**下，等价/性质验证**可判定**；无法在预算内决定时返回"当前不确定"并给出**最小差距子域**。

C. 函数几何与验证在 JIT 上的可判定性（§4）

- **GEO-1…GEO-5**：线性区域、决策复形、梯度/雅可比与**精确 Lipschitz**在 JIT 语义下的提取与终止条件；未完全细分时给**可证上下界**与**细化指引**。
- **VER-1…VER-3**：性质规格、鲁棒认证（ℓ_p 球上 LP/SOCP）、等变验证的**健全/可判定**流程；证书或反例由 JIT-B&B 产生。
- **CAU-1/2**：干预保持 CPWL；最大因果影响的精确解或界在 JIT 下计算。
- **SYN-1…SYN-3**：基于 JIT 验证器的 CEGIS 参数修复、由规范直接综合与最短结构编辑（A*/MILP）的可行性与证书化表述。

> 以上结论均为**构造性/可判定**陈述；完整证明置于附录。

1.5　定位与相关工作

表示层面　Max-of-Affine/热带代数侧重**凸** CPWL；加权有限自动机/树自动机多以**离散字母与标量权**为中心，难以直接承载**多面体守卫与函数权**。本工作中的 SWT 以"**函数权（CPWL）+多面体守卫**"构成共享 DAG，可**无损**表示**一般（含非凸）CPWL**；卷积/GNN 通过模板别名与滑窗/邻域守卫表达，避免数值复制。

验证与优化　MILP/几何/锥松弛方法多为"解题器驱动"的**端到端立式求解**；其缺点是缺乏可共享的**中间几何对象**与**增量式**可用性。本文将几何与验证统一到**同一 SWT/JIT-SWT 载体**上：在共同细分上将性质化为有限 LP/SOCP/仿射比较；JIT 细化策略与上/下包络保障了**健全性**与**预算可控**。

抽象解释与 CEGAR　程序分析中的抽象域与 CEGAR 提供了"**先粗后细**"的范式。JIT-SWT 将其移植到 CPWL 函数空间：上下包络相当于抽象元素，比较/阈值面作为**细化谓词**，以**证书驱动**的方式渐进逼近真值语义。

因果与可修复性　关于"干预/反事实"的现有工作多为经验/启发式。我们的 CAU-1/2 将**干预闭包**与**最大因果影响**转化为 CPWL/SWT 上的**精确可判定/可优化**问题，可在 JIT 框架下输出数值与见证。

1.6　作用范围与限制

适用范围：仿射层与 ReLU/Leaky-ReLU/PReLU/Abs/Max 门控的 DAG 网络；固定图上的 GNN（Sum/Mean/Max 聚合）；推理态 BN；输入域为盒/多面体/ℓ_p 球等凸域。
不纳入/需近似：注意力/乘法门（LSTM/GRU）、训练态 BN、随机算子、循环/动态图；函数间乘除（非常数）一般不闭合于 CPWL，本文以**分段线性上下界（如 McCormick）**或局部提升处理，保持验证**健全**。

1.7 术语约定与结构安排

- **守卫（guard）**：以 H-形式多面体 $C=\{x : Ax \le d\}$ 表示的约束；**守卫库**为其全局去重集合。
- **共同细分**：对若干守卫与比较面取交后得到的有限多面体族；在每个子域上，候选 CPWL 退化为单仿射。
- **懒表达（Expr）**：以 `Max/Sum/Scale/Compose` 组合的 e-graph 表达，不预先转为片段表。
- **上下包络**：JIT 中维护的 $(\underline{A}, \overline{A})$，满足 $\underline{A} \le F \le \overline{A}$。

文章结构：§2 给出设定与**静态 SWT 真值语义**；§3 引入 **JIT-SWT** 的对象、按需细化算子与 **DYN-1…6** 定理；§4 在 JIT 语义上重述 GEO/VER/CAU/SYN 并给出可判定与终止条件；§5 提供**最小而充分**的实验佐证（编译规模/切分次数/证书），完整证明与实现要点置于附录。

---

2 设定与静态基线

> 本章确立本文全部理论的**语义基础**与**静态参照物**。先给出统一组件与假设（A1–A6）、记号与函数代数；随后给出 CPWL 层演算（AF-1…AF-5）；最后定义**带多面体守卫的符号加权变换器（SWT）**的**静态语义与编译规则**，并给出等价性与可判定性等基线结论（SWT-1/3/4/5）。本章不包含任何实验细节。

2.1 组件、统一假设与数学习惯

2.1.1 输入域与数值域

- **输入域**：$\mathcal{D}_{\text{in}} \subseteq \mathbb{R}^n$ 为给定的**凸集合**（常见情形：盒、多面体、ℓ_p 球）；必要时可进一步限制在任务相关的凸子域 $\mathcal{D} \subseteq \mathcal{D}_{\text{in}}$ 上。
- **数值域**：所有权重、偏置与中间值均在 $\mathbb{R}$ 中取值（*推理态*），除非专门说明。
- **范数**：$\|\cdot\|_p$ 表示向量 p-范数；p^* 为对偶指数，满足 $1/p + 1/p^* = 1$。矩阵或线性算子范数 $\|J\|_{p\to r} = \sup_{\|x\|_p=1} \|Jx\|_r$。

2.1.2 组件覆盖与结构约束

- **仿射/线性子层**：全连接、卷积（含 padding/stride）、均值池化、加法残差、推理态 BN（均值/方差冻结）。
- **门控/激活**：ReLU、Leaky-ReLU（斜率 $\alpha \in [0,1]$）、PReLU（$\alpha \ge 0$）、Abs、按点 Max/MaxPool。
- **结构**：计算图为**有向无环图（DAG）**；GNN 情形下图 $G=(V,E)$ **固定**，聚合算子为 Sum/Mean/Max。
- **不纳入（需近似或不主讲）**：注意力/乘法门（LSTM/GRU）、训练态 BN（批统计与输入相关）、随机算子、循环/动态图、非线性乘除（函数×函数/÷函数）。

> 以上覆盖类的输出在输入域上均为**连续分段线性（CPWL）**，见 §2.2。

2.1.3 多面体与守卫表示

- **多面体（H-形式）**：$C=\{x\in\mathbb{R}^n : Ax \le d\}$，其中 $A \in \mathbb{R}^{k\times n}, d \in \mathbb{R}^k$。
- **多面复形**：有限个多面体的并，且两两交以面相容（相交亦为多面体，边界对齐）。
- **守卫（guard）**：指代某个 H-形式多面体。默认采用**闭集合**（$\ge, \le$）约定；涉及“tie=0”的阈值/比较，保留**双侧守卫**（≥ 0 与 ≤ 0）以覆盖等号情形。

2.2 CPWL 层演算与函数半环

2.2.1 CPWL 与函数半环

- **CPWL 函数类**：$\mathrm{CPWL} = \{f : \mathbb{R}^n \to \mathbb{R} \mid f\ \text{在有限多面复形上分段仿射且连续}\}$。
- **扩展类**：$\mathrm{CPWL}^{\pm\infty}$ 允许 $f \equiv -\infty$（记为 $\mathbf{0}$）。
- **函数半环**：

  $$K_f = \big(\mathrm{CPWL}^{\pm\infty},\ \oplus,\ \otimes,\ \mathbf{0},\ \mathbf{1}\big), \qquad (f \oplus g)(x) = \max\{f(x), g(x)\},\ (f \otimes g)(x) = f(x) + g(x),$$

  单位元 $\mathbf{0} \equiv -\infty,\ \mathbf{1} \equiv 0$。$\oplus$ 与 $\otimes$ 分别对应按点 max/加法。
- **非负子半环**：$S_+ = \{f \in K_f : f(x) \geq 0,\ \forall x\}$（供 ReLU/Max 的特例使用）。

2.2.2 预激活与门控原子

常用按点标量算子：

$$\begin{aligned}
&\mathrm{ReLU}(z) = \max\{0, z\}, \quad \mathrm{Abs}(z) = \max\{z, -z\}, \\
&\mathrm{LReLU}(z) = \max\{z, \alpha z\}\ (\alpha \in [0,1]), \quad \mathrm{PReLU}(z) = \max\{z, \alpha z\}\ (\alpha \geq 0), \\
&\max(z_1, \ldots, z_m) = \max_i z_i.
\end{aligned}$$

2.2.3 AF 系列结论（层演算基线）

AF-1（良定义性）
陈述：在 §2.1 的组件与 DAG 结构下，每层预激活属于 CPWL；施加任一上述门控后激活仍位于 K_f。
证明要点：仿射变换保持 CPWL；$\max$ 与非负线性组合保持 CPWL；ReLU/Leaky/PReLU/Abs/Max 可写为有限个仿射的 $\max$/线性组合。□

AF-2（同态求值）
陈述：对任一点 x_0，将层表达式按 $h_{x_0}(f) = f(x_0)$ 求值，等于数值前向结果。
证明要点：$\oplus, \otimes$ 为按点 $\max / +$；并行支路求和对应 $\otimes$，门控选择对应 $\oplus$。对层数归纳即可。□

AF-3（结构性质：连续；凸性的充分条件）
陈述：输出各分量连续且 CPWL。若每层进入激活前的**混合系数均**≥ 0，且激活**凸且单调非降**（ReLU/LReLU/PReLU/Max），则整体函数**凸**。若使用 Abs，仅当其**直接作用于仿射**时仍保凸。
证明要点：CPWL 在 $\max$/线性组合下闭合且连续；凸函数的非负线性组合与与单调非降函数的复合保持凸；Abs 复合非仿射不保证凸。□

AF-4（几乎处处可微）
陈述：CPWL 函数在有限多面复形上分段仿射，Lebesgue-a.e. 可微；区域 R_ρ 内 $F(x) = w_\rho^\top x + b_\rho$。不可微点的 Clarke 次微分为相邻区域梯度的凸包。□

AF-5（组合性）
陈述：有限次“仿射 + 上述门控”的复合仍为 CPWL。□

2.3 静态 SWT 基线：语义、编译与基线可判定性

本节将网络 F 编译到**带多面体守卫的符号加权变换器（SWT）**，并以此作为**真值语义**的静态参照。

2.3.1 SWA/SWT 的形式语义

守卫库与规范（共享约束）

- **C1（守卫库 $\mathcal{H}$）**：收录所有用到的线性不等式（含比较与阈值），经过**行归一化**与**tie 双侧化**后，每条不等式**仅注册一次**。
- **C2（边的守卫存储）**：图中每条边仅保存 $\mathcal{H}$ 的**索引集合**（GuardId 的有序集）。不在边上显式存“路径交集”。
- **C3（不以线性区域为状态）**：状态仅对应**结构位点/模板实例**。线性区域在判定阶段由守卫交得到。

符号加权自动机（SWA，标量输出）
一个 SWA 是七元组

$$A = (Q, q_{\text{init}}, F, E, \mathsf{G}, \mathsf{W}, K_f)$$

其中 Q 有限状态集，$q_{\text{init}} \in Q$ 初态，$F \subseteq Q$ 终态，$E \subseteq Q \times Q$ 有向边；
$\mathsf{G} : E \to \{\text{H - 形式多面体}\}$ 为守卫；$\mathsf{W} : E \cup Q \to K_f$ 为函数权。
对输入 x，可行路径 $\pi = e_1 \cdots e_T$ 满足 $x \in \bigcap_t \mathsf{G}(e_t)$。**路径值**

$$\mathsf{val}_A(\pi, x) = \mathsf{W}(q_{\text{init}})(x) \ \otimes \ \bigotimes_{t=1}^{T} \mathsf{W}(e_t)(x) \ \otimes \ \mathsf{W}(q_T)(x).$$

输出为

$$A(x) = \bigoplus_{\pi:\, q_{\text{init}} \to F,\ x \models \pi} \mathsf{val}_A(\pi, x).$$

向量输出 $F = (F_1, \ldots, F_m)$ 可视为 m 个 SWA 的并置，或采用分量化的权映射。

符号加权变换器（SWT）
SWT 是“**层到层**”的图算子：将上一层的“（守卫，函数权/仿射）片段表”经**守卫交/比较**与**权函数运算**映为下一层片段表，并与已有结构连接，得到新的 SWA。全网逐层编译实现**无环共享图**。

2.3.2 从网络到 SWT 的编译规则（静态基线）

下述规则在满足 C1–C3 的前提下逐层应用，所有由 ReLU/Max 等引入的比较/阈值面统一加入 $\mathcal{H}$。

- **（仿射/BN/残差）**
  对上一层片段 (C, w, b)，仿射 $y = Wx + b_0$ 生成

  $$(C,\ \tilde{w} = Ww,\ \tilde{b} = Wb + b_0).$$

  推理态 BN 并入仿射。残差为两支在交域上的权相加（$\otimes$）。
- **（ReLU / Abs / Leaky-/PReLU）**
  对 (C, w, b) 产生两片：

  $$\begin{cases} C^+ = C \cap \{w^\top x + b \geq 0\}, & (w, b) \\ C^- = \ C \cap \{w^\top x + b \leq 0\}, & (0, 0) \ \ (\text{ReLU}) \end{cases}$$

  Abs 的负支权替换为 $(-w, -b)$；Leaky/PReLU 的负支为 $(\alpha w, \alpha b)$。**tie**（=0）两侧并存，由 $\oplus$ 解决。
- **（按点 Max / MaxPool）**
  候选 $\{(C_i, w_i, b_i)\}_{i=1}^{k}$ 的赢家域

$$C_i^\star = \Big(\bigcap_{j=1}^{k} C_j\Big) \ \cap \ \bigcap_{j\neq i}\{(w_i - w_j)^\top x + (b_i - b_j) \ge 0\};$$

在 $C_i^\star$ 上取 (w_i, b_i)。所有比较面加入 $\mathcal{H}$。

- **（卷积/均值池化）**
  对每个输出位置复制**模板实例**，用**滑窗守卫**编码有效感受野/stride/padding；参数采用**模板别名**（不复制数值，只复制索引）。均值池化为无权仿射。
- **（GNN）**
  Sum/Mean 聚合为稀疏仿射；Max 聚合按比较守卫编码；节点更新 MLP 按上述仿射+门控规则。
- **（数值规范）**
  守卫统一行归一化；比较与阈值采用闭集合（$\ge, \le$）双侧保留；实现层面的判等阈值 τ 不影响理论语义（本章不涉数值阈值）。

2.3.3 静态等价与规模上界

SWT-1（等价编译；静态真值语义）
陈述：按 §2.3.2 逐层编译所得 SWA A_F 与原网络 F 满足

$$\forall x \in \mathcal{D}_{\text{in}}, \quad A_F(x) = F(x).$$

证明要点：对层数归纳。仿射层：在同一守卫内权以 $\otimes$ 累加等同并行求和；门控层：守卫分裂与赢家域构造精确实现 $\max$ /阈值逻辑；卷积/GNN：位置/节点模板展开保持逐点语义。路径求值与并行择优分别等同"求和/取最大"。□
标签：**构造性**、逐点一致。

SWT-2（无环与规模上界；概述）
陈述：若计算图为 DAG 且采用 C1–C3 的守卫库共享编译，则 A_F **无环**，且存在常数 $c_1, c_2 > 0$（与层类型相关）使

$$|Q| \ \le \ c_1\,(N_{\text{lin}} + T_{\text{conv}}), \qquad |E|,\ |\mathcal{H}| \ \le \ c_2\,(N_{\text{lin}} + T_{\text{conv}} + G_{\text{cmp}}),$$

其中 N_{lin} 为仿射子层数，T_{conv} 为卷积模板实例数，$G_{\text{cmp}} = \sum_{v\in\text{Max}} \binom{k_v}{2}$ 为比较面数（ReLU/Leaky/PReLU/Abs 视作 $k_v = 2$）。
要点：编译仅沿前向复制/分裂并做守卫交，不引回边；节点规模线性受"仿射子层 + 模板实例"约束；比较面主导 $|E|$ 与 $|\mathcal{H}|$，守卫库全局复用避免按路径复制。
证明与精确常数：置于附录。此处作为**规模上界基线**供后续与 JIT 对照。

2.3.4 等价判定与差异区域（静态基线可判定性）

SWT-3（等价可判定）
问题：给定两台无环 SWA A_1, A_2，判定 $\forall x \in \mathcal{D},\ A_1(x) \equiv A_2(x)$。
算法（共同细分）：将两侧所有守卫并入同一库，对候选仿射加入**两两比较面** $\{f_i \ge f_j\}$，得到有限多面体族 $\{R_\rho\}$。在每个 R_ρ 上两侧都退化为**单仿射** $w_{k,\rho}^\top x + b_{k,\rho}$（$k = 1, 2$），比较 $(w_{1,\rho}, b_{1,\rho}) \overset{?}{=} (w_{2,\rho}, b_{2,\rho})$。若不等，则在该区解一次 LP（或 SOCP 视域）即可产出反例点。
结论：**可判定**；最坏复杂度指数（细分规模），每次可行性为 LP/SOCP。□

SWT-4（差异区域自动机）
目标：构造识别集合 $\{x : \ |A_1(x) - A_2(x)| > \varepsilon\}$ 的自动机。
构造：令 $g = A_1 - A_2$；在共同细分上添加 $\{g \ge \varepsilon\}$ 与 $\{-g \ge \varepsilon\}$ 守卫，取并。输出为差异区域的多面体复形；可解一次 LP 取见证。□

2.3.5 最小实现复杂度与难度标签

SWT-5（最小守卫实现复杂度；NP-难）
设定：固定**有限**守卫库 $\mathcal{H}$ 与**有限**仿射权基 $\mathcal{B}$。若 F 可由 $(\mathcal{H},\mathcal{B})$ 表达，定义

$$\mathrm{MC_g}(F;\mathcal{H},\mathcal{B})=\min\{|\mathrm{guards}(A)|:\ A\ \text{为无环 SWA},\ \mathrm{guards}(A)\subseteq\mathcal{H},\ \mathrm{weights}(A)\subseteq\mathcal{B},\ A\equiv F\}.$$

结论：该最小值**存在**；判定 $\mathrm{MC_g}(F;\mathcal{H},\mathcal{B})\le k$ 一般**NP-难**（由 Set-Cover 多项式规约）。若 F 不可由 $(\mathcal{H},\mathcal{B})$ 表达，则 $\mathrm{MC_g}=+\infty$。
证明概要：以必须区分的输入子域族为"元素"，候选守卫为"子集"，最少守卫覆盖 $\Leftrightarrow$ 复杂度 $\le k$。完整规约见附录。□

2.4 几何对象与记号（供后续统一引用）

- **线性区域表**：有限集合 $\{(R_\rho,w_\rho,b_\rho)\}_\rho$，满足 $\mathcal{D}_{\mathrm{in}}=\bigcup_\rho R_\rho$、$x\in R_\rho\Rightarrow F(x)=w_\rho^\top x+b_\rho$，除边界外两两不交。
- **决策差分**：分类分量 $i\neq j$ 的差分 $g_{ij}=F_i-F_j$；零水平集 $DB_{ij}=\{x:g_{ij}(x)=0\}$ 是有限多面复形。
- **雅可比/梯度**：在 R_ρ 内梯度/雅可比常值，记为 w_ρ/J_ρ。
- **Lipschitz 常数**：标量 $L_p(F)=\max_\rho\|w_\rho\|_{p^*}$；向量 $L_{p\to r}(F)=\max_\rho\|J_\rho\|_{p\to r}$。
- **复杂度标签**：在各定理后统一标注"构造性/可判定/规模/难度"。

2.5 作用范围、边界情形与默认约定（理论层面）

- **默认闭集合**：阈值/比较用 $\geq,\leq$；"tie=0"在两侧守卫皆保留，由 $\oplus=\max$ 选择。
- **Abs 的凸性边界**：仅当 Abs 直接作用于仿射时保持全局凸性；一般复合不保凸。
- **PReLU/Leaky 的单调性**：要求负支斜率 $\alpha\geq 0$ 以保证激活单调非降（AF-3 的凸性充分条件用到）。
- **卷积边界**：padding/stride 通过滑窗守卫编码；"有效域"在 §4（理论）与实验中分别讨论（不在本章展开）。
- **非线性乘除**：函数×函数或 ÷函数一般不闭合于 CPWL，不属于本章语义范围；若需处理，将在后续 JIT 语义中以**上下界**或**局部提升**方式保持验证健全性。

---

3 动态编译（JIT-SWT）：语义、算法与理论保证（核心理论章）

> 本章在第 2 章的**静态 SWT 真值语义**之上，引入**动态按需细化（JIT-SWT）**。我们给出对象与不变式、按需细化原子算子、上下包络语义、分支定界（B&B）式驱动算法，以及一组可检验定理（DYN-1…DYN-6）与复杂度/内存上界。全章不包含任何实现或实验细节。

3.1 对象与不变式

3.1.1 守卫库与 GuardSet

- **全局守卫库** $\mathcal{H}=\{h_\ell(x): a_\ell^\top x \le d_\ell\}_{\ell=1}^M$。
  规范化：$\|a_\ell\|_2=1$；阈值/比较采用闭集合（$\ge,\le$）双侧保留；每个超平面**只注册一次**（C1）。
- **GuardSet**：守卫索引的有序有限集 $S\subseteq\{1,\dots,M\}$，表示多面体

$$C(S)=\bigcap_{\ell\in S}\{x:\ a_\ell^\top x\le d_\ell\}.$$

  边/节点仅保存**索引集合**（C2），不保存路径交集。
- **可行性记忆**：$\text{feas}(S)\in\{\text{unknown},\text{infeas},\text{feas}\}$，由一次 LP 可判定；结果缓存（后续用于剪枝）。

3.1.2 懒表达（Expr）与共享

- **Expr 语法（标量）**：

$$\texttt{Expr}\ ::=\ \texttt{Affine}(w,b)\mid\texttt{Sum}(\mathcal{E})\mid\texttt{Max}(\mathcal{E})\mid\texttt{Scale}(c,E)\mid\texttt{Bias}(b,E),$$

  其中 $\mathcal{E}$ 为有限 Expr 集，$c\in\mathbb{R}$，$\texttt{Affine}(w,b)(x)=w^\top x+b$。

  > 备注：线性层可在图级实现，也可等价为若干 `Scale` + `Sum` + `Bias` 的组合（后者便于统一边界证明）。

- **共享机制**：α-等价子式通过**结构哈希**与**并查集**统一（e-graph），同构子式只存一次；仿射原子 (w,b) 通过哈希驻留（interning）共享。
- **多输出**：向量表达 $\mathbf{E}=(E_1,\dots,E_m)$ 为分量级的标量 Expr 组（第 2 章向量输出的 SWA/SWT 并置语义）。

3.1.3 JIT-SWT 图与三条不变式

- **JIT-SWT 图**：与第 2 章 SWA 同构的**有向无环**结构（C3），但**权不再立即下沉为分段表**，而是引用 `Expr`。边携带 GuardSet S。
- **不变式 I（唯一守卫）**：$\mathcal{H}$ 中每条不等式规范化并仅出现一次；GuardSet 用索引集合表达。
- **不变式 II（按需细化）**：**仅在访问到的 GuardSet 上**插入新的比较/阈值面，将 S 划分为 $S\cup\{\ell\}$ 与 $S\cup\{\bar\ell\}$（$\bar\ell$ 表示对应的“反向”守卫）。全局不做预分割。
- **不变式 III（上下包络）**：任意时刻，JIT-SWT 图伴随一对函数 $(\underline{A},\overline{A})$，满足

$$\forall x\in\mathcal{D},\qquad \underline{A}(x)\ \le\ A(x)\ \le\ \overline{A}(x),$$

  其中 A 是图的**静态真值语义**（第 2 章），$\underline{A},\overline{A}$ 的构造见 §3.2.3。

3.2 按需细化算子与界推理

我们给出三类原子细化器（门控符号判定、Max 赢家判定、最小公共细分）与一套可替换的上下界推理规则。它们共同保证 DYN-1 ~ DYN-3。

3.2.1 门控符号按需细化（`ENSURE_SIGN`）

输入：预激活 $z = \mathtt{Expr}$，GuardSet S。
目标：在 $C(S)$ 上决定 ReLU/Leaky/PReLU/Abs 的**分支**；若无法整体决定，则仅在 S 上插入一次阈值面 $\{z \geq 0\}$ 进行**二分**。

步骤

1. 计算上下界 $[\mathrm{LB}(z,S), \mathrm{UB}(z,S)]$（§3.2.3）。
2. 若 $\mathrm{UB}(z,S) \leq 0$，则在 $C(S)$ 上采用"负支"替换：
   - ReLU：$\mathtt{Zero}$；Leaky/PReLU：$\mathtt{Scale}(\alpha, z)$；Abs：$\mathtt{Scale}(-1, z)$。
     若 $\mathrm{LB}(z,S) \geq 0$，则采用"正支"：$\mathtt{Id}(z)$。
3. 否则（区间跨 0），向 $\mathcal{H}$ 注册一次 $\{z \geq 0\}$ 的超平面（若不存在），将 S 二分为 $S^+ = S \cup \{\ell\}$ 与 $S^- = S \cup \{\bar{\ell}\}$，递归地在 $S^\pm$ 上判定。

> 该算子仅在**必要时**插入**一条**阈值面，满足不变式 II。

3.2.2 Max 赢家按需细化（`ENSURE_WINNER`）

输入：候选 $\mathcal{E} = \{E_1, \ldots, E_k\}$，GuardSet S。
目标：在 $C(S)$ 上确定赢家集合；若整体不可判定，则仅引入**一条**比较面进行二分。

步骤

1. 计算每个候选的界 $[\mathrm{LB}(E_i,S), \mathrm{UB}(E_i,S)]$。
2. **支配剪枝**：若存在 $i \neq j$，使 $\mathrm{UB}(E_i,S) \leq \mathrm{LB}(E_j,S)$，则 i 在 S 上永不胜出，可移除（保存在 e-graph，图上不再扩展）。
3. 若存在唯一 $i^\star$ 满足 $\mathrm{LB}(E_{i^\star},S) \geq \max_{j \neq i^\star} \mathrm{UB}(E_j,S)$，则确定赢家 $i^\star$ 于 $C(S)$。
4. 否则选择一对 (p,q)（策略见 §3.3.2），向 $\mathcal{H}$ 注册比较面 $\{E_p \geq E_q\}$，将 S 二分为 $S \cup \{\ell_{p \geq q}\}$ 与 $S \cup \{\ell_{q \geq p}\}$。

> 结合 §3.2.3 的 LP-支配检查可加强剪枝；正确性见 DYN-5。

3.2.3 上下界（LB/UB）推理规则

为保证 DYN-1，我们定义抽象**界预言机**：对任一 `Expr` 与 GuardSet S，产生 $[\mathrm{LB}(E,S), \mathrm{UB}(E,S)]$ 满足

$$\mathrm{LB}(E,S) \;\leq\; \inf_{x \in C(S)} E(x) \;\leq\; \sup_{x \in C(S)} E(x) \;\leq\; \mathrm{UB}(E,S).$$

允许多种实现，只要**健全**；常用两层级：

- **结构规则（常数时间）**

$$
\begin{aligned}
&\mathrm{LB}(\texttt{Affine}(w,b),S)=\min_{x\in C(S)} w^\top x+b \quad （\mathrm{LP}，\text{可选近似}），\\
&\mathrm{UB}(\texttt{Affine}(w,b),S)=\max_{x\in C(S)} w^\top x+b \quad （\mathrm{LP}，\text{可选近似}）；\\
&\mathrm{LB}(\texttt{Sum}(\mathcal{E}),S)=\sum_{E\in\mathcal{E}}\mathrm{LB}(E,S),\quad \mathrm{UB}(\texttt{Sum}(\mathcal{E}),S)=\sum_{E\in\mathcal{E}}\mathrm{UB}(E,S);\\
&\mathrm{LB}(\texttt{Scale}(c,E),S)=\begin{cases}c\,\mathrm{LB}(E,S), & c\ge 0,\\ c\,\mathrm{UB}(E,S), & c<0,\end{cases}\qquad \mathrm{UB}(\texttt{Scale}(c,E),S)=\begin{cases}c\,\mathrm{UB}(E,S), & c\ge 0,\\ c\,\mathrm{LB}(E,S), & c<0;\end{cases}\\
&\mathrm{LB}(\texttt{Bias}(b,E),S)=\mathrm{LB}(E,S)+b,\quad \mathrm{UB}(\texttt{Bias}(b,E),S)=\mathrm{UB}(E,S)+b;\\
&\mathrm{LB}(\texttt{Max}(\{E_i\}),S)=\max_i\mathrm{LB}(E_i,S),\quad \mathrm{UB}(\texttt{Max}(\{E_i\}),S)=\max_i\mathrm{UB}(E_i,S).
\end{aligned}
$$

- **提升规则（可选更紧）**
  对仿射原子采用 LP **精确**界；对复合 `Expr` 采用分离超平面或小规模 LP/SOCP 直接求界（当 `Expr` 已在 S 内单仿射时即为精确）。

> 任何时刻允许从结构界升级为 LP 精确界；DYN-1 与单调性（§3.3.1）不受影响。

3.2.4 最小公共细分（`ENSURE_COMMON_REFINE`）

当需要比较/求和两个来自不同 GuardSet 的表达式时，仅在**当前访问的 GuardSet**上引入必要超平面，形成最小公共细分。
定义：给定 S_1,S_2，在访问 GuardSet S（通常 $S\subseteq S_1\cup S_2$）时，最小公共细分为

$$\{\,S\cup T\ :\ T\subseteq(S_1\cup S_2)\setminus S,\ C(S\cup T)\neq\varnothing,\text{且不可再合并}\,\}.$$

算法上可按需引入 $S_1\triangle S_2$ 中的守卫，逐个二分，直到在每个子域上两侧表达式**可比/可加**而不再需要额外比较面。

> 这保证不变式 II，并为 DYN-2 提供“局部完全细化”的判定基元。

3.3 JIT 语义、正确性与驱动算法

3.3.1 上下包络语义与单调性

定义 3.1（上下包络）
对 JIT-SWT 当前图，$\underline{A},\overline{A}$ 按下述规则逐层定义：

- 仿射/和/缩放/偏置：用 §3.2.3 的和/缩放/平移规则组合上下界；
- ReLU/Leaky/PReLU/Abs：视作 `Max` / `Scale` 的组合，套用相同规则；
- Max/MaxPool：$\underline{A}=\max_i\underline{A}_i$、$\overline{A}=\max_i\overline{A}_i$。
  对每个 GuardSet S 上的输出，取相应表达式的 $[\mathrm{LB},\mathrm{UB}]$ 值。最终

$$\underline{A}(x)=\sup\{\gamma:\ \forall S\ni x,\ \gamma\le\mathrm{LB}(E_{\mathrm{out}},S)\},\quad \overline{A}(x)=\inf\{\eta:\ \forall S\ni x,\ \eta\ge\mathrm{UB}(E_{\mathrm{out}},S)\}.$$

引理 3.2（健全与单调）
对任意细化序列（插入新守卫/比较面、或用更紧界替换旧界），始终有

$$\underline{A}\ \nearrow,\qquad \overline{A}\ \searrow,\qquad \underline{A}\le A\le\overline{A}.$$

证明要点：每个构造子在 §3.2.3 下界/上界运算**单调且保序**；新增守卫只会缩小可行集，使下界不减、上界不增；组合沿 DAG 传播保持不等式。□

定理 DYN-1（健全性）
任意时刻 $\underline{A}(x) \le A(x) \le \overline{A}(x)$ 在 $\mathcal{D}$ 上成立。
证：由引理 3.2 逐层继承并对图拓扑归纳。□

3.3.2　按需细化驱动（B&B 核）

目标：判定/优化性质 ϕ（如：$\forall x \in D,\ g(x) \ge 0$）或计算精确值（如极值/Lipschitz），在**不完全细分**的前提下输出**证书/反例**或“当前不确定 + 最紧子域”。

核心循环（概念化伪代码）

```
B&B(A, D):
  Q ← {S0}   // 初始 GuardSet：表示域 D 的 H-形式
  while Q not empty and budget not exceeded:
      S ← argmax_{T∈Q} Gap(T)   // Gap(T) = UB(g,T) - LB(g,T)
      if LB(g,S) ≥ 0: mark S as SAFE; Q ← Q \ {S}; continue
      if UB(g,S) <  0: return COUNTEREX(S)   // 证反例：可解一条LP/SOCP取点
      // 不确定，挑选一次细化
      if can_decide_by_winner/ sign on S:
          ENSURE_WINNER/ENSURE_SIGN(..., S)
      else:
          ENSURE_COMMON_REFINE(S, ...)
      Q ← (Q \ {S}) ∪ {children of S}
  if all popped as SAFE: return PROOF (certificate: {LB(g,S)≥0})
  else: return UNKNOWN with argmax-gap S*
```

细化选择策略（不影响健全性，仅影响收敛速度）：

- **最大间隙**：优先细化 $\mathrm{UB} - \mathrm{LB}$ 最大的子域；
- **最强对比**：在 `ENSURE_WINNER` 中选择 (p, q) 使 $\mathrm{UB}(E_p - E_q, S) - \mathrm{LB}(E_p - E_q, S)$ 最大；
- **最“居中”的面**：选在 $C(S)$ 上距离中心最近的阈值/比较面，减少不平衡分割。

停机与证书

- 若所有活动 GuardSet S 满足 $\mathrm{LB}(g, S) \ge 0$，则给出**满足证书**（每个子域上的下界不等式集合）；
- 若某个 S 满足 $\mathrm{UB}(g, S) < 0$，则在 $C(S)$ 上解一次凸问题给出**反例点**；
- 若预算耗尽，则返回 `UNKNOWN` 与**最紧子域** $S^\star = \arg\max \mathrm{UB} - \mathrm{LB}$。

定理 DYN-6（JIT-Decidability）
对闭性质 ϕ（由有限线性/二阶锥约束组成），若允许任意多的有限细化，则 B&B 过程可判定 ϕ 的真值；否则，过程在任意时刻返回健全的三值答案（真/假/不确定）。
证明要点：当局部完全细化（§3.3.3）覆盖 D 时，每个子域上 g 单仿射，B&B 的 LB/UB 即为精确值；有限个子域下终止。预算受限时的“真/假/不确定”直接由 LB/UB 的健全性保证。□

3.3.3　任意时精确性与进度不回退

定义 3.3（局部完全细化）
对 GuardSet S，若满足：
(i) 所有涉及 S 的门控与 Max 候选对的比较面都已加入 $\mathcal{H}$，且
(ii) `Expr` 在 $C(S)$ 内退化为**单仿射**，
则称 S 已局部完全细化。

定理 DYN-2（任意时精确性）
若 S 局部完全细化，则在 $C(S)$ 上 $\underline{A} = \overline{A} = A$。
证明要点：在 $C(S)$ 内无任何门控/Max 的不确定性，所有 `Expr` 均为仿射，LB/UB 规则在仿射处取等，继而组合保持相等。□

定理 DYN-3（进度不回退）
细化某 GuardSet S 只可能：
(a) 保持 S 为叶并使之"更精确"（更紧 LB/UB），或
(b) 把 S 一分为二 S_1, S_2（加入一条新面），且以后对 S_1, S_2 的操作不影响 S 以外的任何 GuardSet 上的表达与界；
已达成的"$\underline{A} = \overline{A}$"区域不会被再次打回"不确定"。
证明要点：按需细化仅在当前 S 引入新守卫；组合子在 DAG 中向上单调传播，不会破坏其他 GuardSet 的 LB/UB 等式；e-graph 共享不影响语义。□

3.3.4 支配剪枝的正确性

命题 3.4（支配剪枝）
在 GuardSet S 上，若

$$\max_{x\in C(S)} \big(E_\pi(x) - E_{\pi'}(x)\big) \ \le\ 0,$$

则候选 π 在 $C(S)$ 上**不可能成为 Max/门控的赢家**，可从 S 的候选集中安全移除。
证明：对任意 $x \in C(S)$，有 $E_\pi(x) \le E_{\pi'}(x)$；故在 Max/门控比较时 π 从不被选择。□

> 该命题支持 `ENSURE_WINNER` 的第 2 步；若 $\max$ 使用 LP 得到的上界 ≤ 0，结论为**严格**支配；若仅使用结构上界，需要小心保证健全（宁可不剪）。

3.3.5 静态–动态逐点等价（DYN-7）

定义 3.5（完全细化覆盖）
给定域 $D \subseteq \mathcal{D}_{\text{in}}$。称 GuardSet 的有限集合 $\mathcal{S} = S_1, \dots, S_T$ 为 D 的**完全细化覆盖**，若满足：
(i) $D \subseteq \bigcup_{t=1}^{T} C(S_t)$；
(ii) 对每个 S_t，所有与之相关的门控/比较面均已加入守卫库，且输出表达在 $C(S_t)$ 内**单仿射**（即第 3.3.3 节的"局部完全细化"）。

> 注：在 `ENSURE_SIGN/ENSURE_WINNER` 中，我们采用"**先最小公共细分线性化，后加线性比较面**"的约定；只有当待比较表达在当前 S 上已单仿射时，才将比较/阈值的**线性**超平面纳入守卫库。

定理 DYN-7（静态 SWT 与 JIT-SWT 的全域逐点等价）
设网络 F 满足 §2.1 的组件与 DAG 假设。令 A_{stat} 为 §2.3 的静态编译结果，A_{JIT} 为 JIT-SWT 在某时刻的图。若存在 D 的**完全细化覆盖** $\mathcal{S}$，则有

$$\forall x \in D, \qquad A_{\text{JIT}}(x) \ =\ A_{\text{stat}}(x) \ =\ F(x).$$

证明要点：

1. **静态基线**：由 SWT-1，$\forall x$，$A_{\text{stat}}(x) = F(x)$。
2. **局部等式**：对任意 $S \in \mathcal{S}$，因在 $C(S)$ 内表达单仿射且比较面一致，$A_{\text{JIT}}(x) = A_{\text{stat}}(x)$ 于 $C(S)$ 成立；且仿射上 $\underline{A} = \overline{A} = A$（由 DYN-2）。
3. **覆盖合并**：$C(S)_{S\in\mathcal{S}}$ 覆盖 D，故全域上 $A_{\text{JIT}} \equiv A_{\text{stat}} \equiv F$ 于 D。□

推论（公平细化下的终止）
静态守卫库 $\mathcal{H}^*$ 有限（比较/阈值面有限）。若 JIT 采用**公平**策略（每个可行且未完全细化的 GuardSet 终会被选择）并允许有限多次细化，则必能在**有限步**上产生 D 的完全细化覆盖，继而由 DYN-7 得 $A_{\mathrm{JIT}} \equiv A_{\mathrm{stat}} \equiv F$ 于 D。
要点：可加入的线性比较面与 GuardSet 的裂分步骤皆来自有限集合；公平选择保证最终覆盖。

备注（比较数与工作量）
JIT 可通过**支配剪枝**省略静态中永不制胜的比较面；这不会改变最终函数，只影响达到完全细化的路径与工作量（与 §3.3.4 一致）。

3.4　复杂度与内存（预算化上界）

3.4.1　计数基元与度量

- B：**切分预算**——允许插入的新守卫（比较/阈值）条数；
- G：全局**守卫上限**——守卫库总规模；
- N_E：e-graph 节点（Expr）上限；
- N_{LP}：LP/SOCP 调用次数；
- $|Q|$：活动 GuardSet（B&B 队列）规模。

3.4.2　预算化规模上界

定理 DYN-4（预算化复杂度上界）
在 JIT-SWT 下，若切分预算 B 与守卫库上限 G 有界，则

$$\begin{aligned}
&\text{GuardSet 数} \ \le\ O(B) \quad (\text{二叉切分，常数因子与合并策略有关});\\
&|\mathcal{H}| \ \le\ \min\{G,\ |\mathcal{H}_0|+B\} \qquad (\mathcal{H}_0 \text{ 为初始守卫数});\\
&\text{图节点/边规模} \ \le\ O(N_{\mathrm{lin}}+T_{\mathrm{conv}}+B);\\
&N_{\mathrm{LP}} \ \le\ O\big(B+|Q|\big) \quad (\text{每次细化/判定至多触发常数次 LP/SOCP}).
\end{aligned}$$

证明要点：每次细化仅增加**一条**守卫并使一个 GuardSet 至多分裂为两个，因此 GuardSet 总数随 B 线性；守卫库与图规模在初始静态规模的基础上增量受 B 控制；B&B 每步对当前 GuardSet 做常数个界判断/支配判定/可行性检查。□

推论 3.5（避免全局 $\binom{k}{2}$ 比较）
`ENSURE_WINNER` 每次只引入**一条**比较面；因此总比较面数 $\le B$，远小于静态一次性加入的 $\sum \binom{k_v}{2}$。

3.4.3　内存共享与回收

- **守卫唯一化**确保 $|\mathcal{H}|$ 只随**新增面**增长；
- **e-graph 共享**使重复子式常数折扣；
- GuardSet 与 LP 结果可按 (S, query) 键缓存；
- 若需常数内存运行，可对不再访问的 GuardSet/Expr 采用引用计数回收（理论语义不受影响；本章不展开实现策略）。

3.5　JIT 上的等价、验证与最优化（理论语义）

虽然完整流程在第 4 章统一表述，这里给出与 JIT 语义直接相关的两个核心保证（便于在 §4 直接调用）。

3.5.1 等价判定（JIT 视角）

定理 3.6（JIT 等价判定的健全/完备性）
令 A_1, A_2 为两台静态 SWA 的 JIT 版本。对性质

$$\phi: \forall x \in D,\ \|A_1(x) - A_2(x)\|_\infty \le \varepsilon,$$

用 §3.3.2 的 B&B 在差分 $g = \max_i |A_{1,i} - A_{2,i}|$ 上运行：

- 若过程返回 `PROOF`，则 ϕ 成立（健全）；
- 若返回 `COUNTEREX`，则 ϕ 不成立，并给出见证点（健全）；
- 若允许任意多有限细化（覆盖 D），则过程**必定终止并给出真值**（完备）。
  证明要点：直接由 DYN-1、DYN-2、DYN-6。□

3.5.2 极值/Lipschitz 的精确与上界

命题 3.7（极值与 Lipschitz 的任意时界）
对标量 F 与域 D，JIT-B&B 维护

$$\underline{M} = \max_{S \subseteq D} \mathrm{LB}(F, S), \qquad \overline{M} = \max_{S \subseteq D} \mathrm{UB}(F, S),$$

满足 $\underline{M} \le \max_{x \in D} F(x) \le \overline{M}$，且随细化 $\underline{M} \nearrow, \overline{M} \searrow$。当覆盖的所有 S 上 F 单仿射时，$\underline{M} = \overline{M}$ 给出**精确极值**。
对 Lipschitz 常数同理：在每个 S 上读取局部雅可比（若单仿射）或使用上界算子，取子域最大即得任意时的下/上界，并在完全细化后达到精确值（第 4 章给出细节）。□

3.6 边界、可扩展方向与假设回顾（理论层面）

- **闭包边界**：JIT-SWT 的算子集合（和/缩放/偏置/Max/门控/仿射/卷积/GNN 聚合）均在 CPWL 内闭合。**函数×函数/除以函数**一般不闭合，若出现，将作为**扩展模块**用分段线性上下界近似或局部二阶提升处理（不影响 DYN-1）。
- **数值中立**：本章所有陈述不依赖具体数值阈值 τ 或数值实现；τ 只在实现层面用于处理 tie，理论上我们采用闭集约定并双侧保留。
- **DAG 假设**：无环是 JIT-SWT 良定义与 DYN-2 的必要条件。循环/动态图不在本章范围。
- **守卫生成的有限性**：所有比较/阈值面来自有限个门控与 Max 构造；因此在理论上存在一个**有限**的"完全细化"集合（虽未必实际枚举）。

3.7 本章小结（供后续引用）

- 定义了 JIT-SWT 的对象（$\mathcal{H}$、GuardSet、e-graph `Expr`）与三条不变式；
- 给出按需细化原子：`ENSURE_SIGN`、`ENSURE_WINNER`、`ENSURE_COMMON_REFINE`，以及健全的 LB/UB 推理；
- 证明了**健全性（DYN-1）**、**任意时精确性（DYN-2）**、**进度不回退（DYN-3）**、**预算化复杂度上界（DYN-4）**、**支配剪枝正确性（DYN-5）**与**JIT-Decidability（DYN-6）**；
- 给出 B&B 驱动的停机与证书化准则，为第 4 章的几何/验证/因果/综合提供可直接调用的理论基础。

> 由此，JIT-SWT 成为与第 2 章静态语义**等价且更可扩展**的运行语义：在**访问到的子域与必要比较数**上线性扩张，既支持**任意时的上下界**与**证书化**，又在**局部完全细化**后与静态 SWT **逐点一致。**

4 JIT-SWT 上的可判定分析与函数几何

> 目的：在第 2 章静态真值语义与第 3 章 JIT-SWT（按需细化、上下包络、B&B 驱动）的基础上，系统刻画**函数几何**（区域/边界/梯度/Lipschitz/极值）与**形式化分析**（验证/等变/因果/综合）在 JIT 语义下的**可判定性、精确性与收敛**。本章所有结论均不依赖实现细节；当需要数值求解时，默认使用 LP/SOCP 作为**理论原语**。

4.1 线性区域、决策边界与梯度（GEO 系列 in JIT）

4.1.1 按需线性区域提取（GEO-1 in JIT）

定义 4.1（活跃片段与局部完全细化）
给定 JIT-SWT 与 GuardSet S。称三元组 (S, w, b) 为**活跃片段**，若在 $C(S)$ 内输出分量 F 为单仿射 $F(x) = w^\top x + b$。若对 S 满足第 3 章定义的**局部完全细化**（所有相关门控/比较面已加入且 `Expr` 在 $C(S)$ 内退化为单仿射），则 (S, w, b) 为**确定的活跃片段。**

算法（增量构造“足够的区域”而非全域枚举）

- 输入：感兴趣的域 $D \subseteq \mathcal{D}_{\text{in}}$（H-形式）。
- 初始化：队列 $Q \leftarrow \{S_0\}$（$C(S_0) = D$），区域表 $\mathcal{R} \leftarrow \varnothing$。
- 循环：
    1. 取 $S \in Q$。若 $C(S) = \varnothing$（LP 不可行），跳过；
    2. 对 S 上所有门控/Max 调用 `ENSURE_SIGN/ENSURE_WINNER`；若仍不确定，则调用 `ENSURE_COMMON_REFINE` 按最小公共细分二分一次，放回分支；
    3. 若 S 已局部完全细化，读取 w, b（沿 DAG 汇总仿射原子），将 (S, w, b) 加入 $\mathcal{R}$；
    4. 重复直至队列耗尽或达到预算（§3.4 的 B, G）。

定理 4.2（健全性与任意时精确性）
在任何时刻，$\mathcal{R}$ 中的条目对应一组**两两内点不交**的多面体，其并覆盖 D 的一部分，并且在这些多面体内 F **精确为**相应仿射；若继续细化直至 D 被**有限个**确定活跃片段覆盖，则 $\mathcal{R}$ 为完整的**线性区域表。**
证明要点：由 DYN-2（局部完全细化⇒精确）与 `ENSURE_*` 的二分仅在当前 GuardSet 上发生，合并得不相交覆盖；可达面有限 ⇒ 存在有限完全细分。□

复杂度：可判定；最坏指数（门控数）；每次可行性/支配判定为 LP；预算化规模由 DYN-4 控制。

4.1.2 决策边界复形（GEO-3 in JIT）

设定：分类分量 $i \neq j$；差分 $g_{ij} = F_i - F_j$。
对象：零水平集 $DB_{ij} = \{x \in D : \ g_{ij}(x) = 0\}$。

命题 4.3（分片仿射描述）
当 D 被一组确定活跃片段 $\{(S_\rho, w_\rho, b_\rho)\}$ 覆盖时，

$$DB_{ij} = \bigcup_{\rho} \Big(C(S_\rho) \ \cap \ \{ w_{\rho,ij}^\top x + b_{\rho,ij} = 0 \} \Big),$$

其中 $w_{\rho,ij}, b_{\rho,ij}$ 是 g_{ij} 在 S_ρ 上的仿射参数。每一片是多面体与超平面相交得到的**多面体片**，并两两以面相容，构成有限**多面复形。**
证明要点：局部单仿射 ⇒ 零集为超平面；与多面体相交为多面体片；有限并。□

几何量（在片段 S_ρ 内）：法向 $\nu_\rho = w_{\rho,ij}/\|w_{\rho,ij}\|_2$；点 x 到边界的欧式距离

$$\operatorname{dist}(x, DB_{ij} \cap C(S_\rho)) = \frac{|w_{\rho,ij}^\top x + b_{\rho,ij}|}{\|w_{\rho,ij}\|_2}.$$

任意时版本
若尚未完全细化，可用 $\underline{g}_{ij}, \overline{g}_{ij}$ 的零水平集给出**内/外近似**：

$$\{x:\ \overline{g}_{ij}(x) \le 0\} \ \subseteq\ \{x:\ g_{ij}(x) \le 0\} \ \subseteq\ \{x:\ \underline{g}_{ij}(x) \le 0\},$$

由此得到**内包/外包复形**，并以最大间隙子域优先细化，保证复形逼近（DYN-1,2）。

4.1.3 梯度/雅可比自动机（GEO-4 in JIT）

定义 4.4（梯度/雅可比片段机）
当 D 被确定活跃片段 $\{(S_\rho, w_\rho, b_\rho)\}$ 覆盖时，定义与 JIT-SWT 同步的变换器 $T_{\nabla F}$（或 T_{J_F}）：在每个 S_ρ 上输出常向量 w_ρ（或矩阵 J_ρ）。在不可微集合（边界的有限复形）上，输出 Clarke 次微分的一个**选取规则**（如最小范数解，解一小型 QP）。

定理 4.5（a.e. 精确与边界健全）
Lebesgue-a.e. 的 $x \in D$ 落在某个 S_ρ 的相对内点，$T_{\nabla F}$ 输出 $\nabla F(x)$（或 $J_F(x)$）；若 x 在边界，T 输出的代表属于 Clarke 次微分。
证明要点：CPWL a.e. 可微（AF-4）；边界代表可通过相邻片段梯度凸包获得；QP 选取满足闭包性质。□

复杂度：与确定活跃片段数同阶；候选数的预算化由 DYN-4 控制。

4.2 极值与 Lipschitz（GEO-2/GEO-5 in JIT）

4.2.1 域内极值（GEO-2 in JIT）

问题：给定凸域 D，求 $\max_{x\in D} F(x)$ 与 $\min_{x\in D} F(x)$。

定理 4.6（任意时上下界与精确性）
在 B&B 过程中维护

$$\underline{M} = \max_{S\subseteq D} \operatorname{LB}(F,S), \qquad \overline{M} = \max_{S\subseteq D} \operatorname{UB}(F,S),$$

则 $\underline{M} \le \max_{x\in D} F(x) \le \overline{M}$，并随细化满足 $\underline{M} \nearrow, \overline{M} \searrow$。当覆盖 D 的所有 GuardSet S 上 F 单仿射时，

$$\max_{x\in D} F(x) = \max_S \max_{x\in C(S)\cap D} w_S^\top x + b_S,$$

内层是凸优化：多面体/盒/ℓ_∞/ℓ_1 为 LP；ℓ_2 球或其与多面体交为 SOCP；纯 ℓ_2 球有闭式 $w^\top x_0 + b + \epsilon\|w\|_2$ 。
证明要点：DYN-1,2；区域内仿射极值的凸性与闭式结论（第 2 章表述沿用）。□

复杂度：可判定；最坏指数；每次子问题为 LP/SOCP，多项式可解。

4.2.2 全局/局部 Lipschitz（GEO-5 in JIT）

定义 4.7（Lipschitz 常数）
标量 F：$L_p(F)=\sup_{x\neq y}\frac{|F(x)-F(y)|}{\|x-y\|_p}$。向量 $F:\ell_p\to\ell_r$：$L_{p\to r}(F)=\sup_{\|v\|_p=1}\|J_F(x)v\|_r$（a.e. 处雅可比存在；边界取 Clarke 上确界）。

定理 4.8（片段最大等于常数）
若 D 被确定活跃片段覆盖，则

- 标量：$L_p(F;D)=\max_{S:\,C(S)\cap D\neq\varnothing}\|w_S\|_{p^*}$。
- 向量：$L_{p\to r}(F;D)=\max_{S:\,C(S)\cap D\neq\varnothing}\|J_S\|_{p\to r}$。
  证明要点：CPWL 在各片段线性；边界 Clarke 广义雅可比为相邻雅可比的凸包，上确界由极点（片段雅可比）取得。□

任意时上下界

- 下界：$\underline{L}=\max_{S\text{ 已完全细化}}\|w_S\|_{p^*}$（或 $\|J_S\|_{p\to r}$）。
- 上界：未完全细化子域采用可证上界（如区间/线性松弛导出的雅可比上界、锥规划上界），取全域最大 $\overline{L}$。
- 收敛：细化覆盖 D 后 $\underline{L}=\overline{L}=L$。

复杂度注记

- 易解闭式：$\|\cdot\|_{1\to1}$、$\|\cdot\|_{\infty\to\infty}$、$\|\cdot\|_{1\to\infty}$（最大列/行和与最大绝对元）；
- $\|\cdot\|_{2\to2}$：谱范数（可用幂迭代作为理论原语）；
- **NP-难族**：$\infty\to1$，$\infty\to2$，$2\to1$。在 JIT 中作为上界/下界（不要求一次到精确），由细化收敛到等式（当目标范数可在各片段上精确求得时）。

4.3 验证、等变与因果（VER/CAU in JIT）

4.3.1 性质规格语言与产品构造（VER-1 in JIT）

性质语言（原子）

- **输入约束**：$x\in D$（盒/多面体/ℓ_p 球）；
- **输出阈值/区间**：$F_k(x)\le u$，$F_k(x)\ge\ell$；
- **分类正确/裕度**：$\arg\max_i F_i(x)=y\iff\bigwedge_{j\neq y}F_y-F_j\ge0$；或 $F_y-\max_{j\neq y}F_j\ge\gamma$；
- **关系型**：$|F(x)-F'(x)|\le\varepsilon$ 等。

产品构造
将反例条件编为**反例自动机** $A_{\neg\phi}$（差分/阈值写成守卫/比较），与 JIT-SWT 复合得到 A_{cex}。在 JIT 语义下运行 B&B：

- 若所有 GuardSet 上 $\mathrm{LB}(g,S)\ge0$，给出**满足证书**；
- 若某 GuardSet 上 $\mathrm{UB}(g,S)<0$，求**一个**见证点作为**反例**；
- 若预算内不确定，返回“未决 + 最紧子域”。

定理 4.9（健全性与可判定性）
保持第 3 章 DYN-1/2/6 的前提，产品构造 + JIT-B&B 对上述性质给出健全三值答案；允许任意多有限细化时**可判定**。□

4.3.2　鲁棒性认证（VER-2 in JIT）

问题：给定 x_0, ϵ, p 与标签 y，验证 $B_p(x_0, \epsilon) \subseteq D$ 内是否 F 预测不变（或裕度 $\geq \gamma$）。记

$$g(x) = F_y(x) - \max_{j \neq y} F_j(x).$$

方法 A（分区精确法 in JIT）

- 在 JIT 上同时对 F_y 与候选 $\{F_j\}$ 引入**必要**比较面，使在每个访问到的 GuardSet 上 g 单仿射；
- 在每个子域上解

$$\min_{x \in C(S) \cap B_p(x_0, \epsilon)} w_S^\top x + b_S$$

（$p \in \{1, \infty\}$ 为 LP；$p = 2$ 为 SOCP），取全局最小 $g_{\min}$。

- 若 $g_{\min} \geq \gamma$，则认证通过并给出**证书**（子域上的最小值下界）；若 $g_{\min} < \gamma$，则给出达到该值的点为**反例**。

方法 B（混合整数法 in JIT）

- 在 JIT 子域上仅对必要门控编码**指示约束/紧 big-M**（由局部界得 M），把问题转为单域 MIP；
- 得到全局最优反例或认证证书（在该编码域上）。

定理 4.10（健全性与完备条件）
方法 A 在完全细化后为**精确证书**；在未完全细化时给出**下界证书**（不可伪阳性）；方法 B 在所编码域上给出**全局正确**结论。允许任意多有限细化且域 $B_p(x_0, \epsilon)$ 有界时，方法 A/B 均可判定。□

4.3.3　等变性验证（VER-3 in JIT）

设定：输入变换 $\mathcal{T}_g$ 与输出变换 $\mathcal{T}_{g'}$（如 CNN 平移、GNN 置换）。二者都可编为 SWT。
目标：判定

$$A_F \circ \mathcal{T}_g \;\equiv\; \mathcal{T}_{g'} \circ A_F \;\text{ 于域 } D.$$

方法：构造差分 $H(x) = A_F(\mathcal{T}_g x) - \mathcal{T}_{g'}(A_F(x))$；对每个输出分量应用 §4.3.1 的产品构造与 JIT-B&B：

- 若对所有分量都有 $\mathrm{LB}(|H|, S) \geq 0$ 且上界 $< \varepsilon$（如数值容差），则给出**等价证书**（容差意义下）；
- 否则给出**差异子域/见证点**；
- 在 CNN 中需要在定义的**有效子域** D_{eff} 上判定（排除 padding/stride 引入的边界效应）。

定理 4.11（健全性与约束域）
在 D_{eff} 上，若 JIT-B&B 返回“等价”，则两侧在该域上逐点一致（或在容差 ε 内一致）；如返回反例，则必为真实差异。允许任意多有限细化时，可判定。□

4.4　综合与修复（SYN 系列 in JIT）

> 本节给出**方法性**（constructive but not necessarily complete）结论：JIT 作为验证-判定器（oracle）驱动 CEGIS/切面/A*，提供**健全**但不保证完备/全局最优的综合与修复流程；在可证条件下给出完备性保证。

4.4.1 参数修复（SYN-1 in JIT）

问题

$$\min_{\Delta W}\ \|\Delta W\|_p \quad \text{s.t.} \quad A_{W+\Delta W} \models \Phi \text{ 于域 } D.$$

CEGIS-JIT 流程（理论版）

1. **验证子程序**：调用 JIT-B&B 检查 Φ；若成立，返回修复解（$\Delta W = 0$ 或当前 ΔW）。
2. **反例提取**：若失败，返回一组**反例点/子域** $\{S_k\}$。
3. **参数更新子问题**：固定 $\{S_k\}$ 上的线性/锥约束（源自片段仿射）构造一个**凸**或 **MIP** 子问题，求得新的 ΔW。
4. 迭代直至满足或证实不可行（如由子问题返回不可行证书或 ΔW 违反上限）。

定理 4.12（健全不完备）
若流程终止并返回解，则该解**满足** Φ（JIT 验证器健全）；若返回“不可行”证书（来自子问题或 JIT 证明 Φ 不可满足），则报告真实不可行。一般情形下不保证终止；当 Φ 为线性规格且参数化在目标子域上诱导**凸约束**时，流程**终止**并找到可行解或不可行证书。□

4.4.2 由规范直接综合（SYN-2 in JIT）

问题

$$\min_{W}\ \Psi(W) \quad \text{s.t.} \quad A_{F_W} \models \Phi \text{ 于域 } D.$$

两阶段策略（理论刻画）

- **第一阶段（充分条件）**：施加便于求解的**充分**约束（如谱范数乘积上界 $\prod_l \|W_l\|_{p\to p} \le L_0$）以确保 Φ（如 Lipschitz 上界）；得到一个初始可行 $W^{(0)}$。
- **第二阶段（切面细化）**：用 JIT-B&B 生成**差异切面**（反例子域 $\{S_k\}$ 及其上线性/锥约束），在 W 的可行域上加入这些切面，解一个收紧的（但仍凸/可解的）子问题更新 W。

定理 4.13（健全性与收缩）
若第二阶段以**单调收缩**的方式加入切面（每次切面排除当前违反 Φ 的参数片段），则得到的可行域序列单调下降，并在有限步内达到“JIT-B&B 于预算内无法发现反例”的模型；该模型在完全细化时满足 Φ。□

> 完备性依赖于“充分条件→必要条件”的逼近是否能在有限切面内覆盖；一般不保证。

4.4.3 最短结构编辑（SYN-3 in JIT）

问题：在**有限**原子编辑集 $\mathcal{O}$（增/删层、Max↔Avg、stride/padding、剪枝）上，求最短编辑序列 S 使 $A_{S(F)} \models \Phi$；并给定步数/位置上限。

方法 A（有界 A*）

- **状态**：当前模型 F'；**动作**：$o \in \mathcal{O}$。
- **代价**：步数或加权步数；**启发** h：由 JIT-B&B 的**最大因果影响上界**（§4.3.4）或 Lipschitz 上界构造，使得 h **可采纳**（不高估剩余代价）且**一致**（三角不等式）。
- 若搜索图有限且 h 可采纳一致，则找到**全局最短编辑序列**。

方法 B（有限 MILP）

- 在预枚举的有限候选编辑上引入二元变量 z_i，编码"是否应用"；
- 用指示/凸包约束将 $\{z_i\}$ 与语义耦合；
- 目标 $\min\sum z_i$；JIT 作为验证器产出切面约束（如差异子域），逐步收紧。

定理 4.14（健全与最优条件）
方法 A 在可采纳一致启发与有界搜索图条件下返回**全局最短**编辑序列；方法 B 在**有限候选集**上返回**全局最优。** 两者均由 JIT-B&B 提供健全证书/切面以保证正确性。□

4.4.4 干预与最大因果影响（CAU-1/2 in JIT）

干预语义（CAU-1）
在 DAG 内将子表达式（节点/通道/共享维）替换为任意 CPWL P_c，得到 F_C。由于 CPWL 在和/Max 下闭合（AF-1,5），F_C 与差分 $g_C = F - F_C$ 仍为 CPWL，JIT-SWT 可直接编译与细化。

最大因果影响（CAU-2）

$$I_{\max}(C;D) = \sup_{x\in D} |F(x) - F_C(x)|.$$

JIT 计算：在 B&B 上以 g_C 为目标，维护

$$\underline{I} = \max_S \max\{\mathrm{LB}(g_C,S),\mathrm{LB}(-g_C,S)\},\ \overline{I} = \max_S \max\{\mathrm{UB}(g_C,S),\mathrm{UB}(-g_C,S)\},$$

并细化至单仿射后解两次仿射最大化（LP/SOCP）得精确值。
定理 4.15（健全与精确收敛）：$\underline{I} \le I_{\max} \le \overline{I}$，并随细化收敛；完全细化后 $\underline{I} = \overline{I} = I_{\max}$。□

4.5 统一的"任意时—精确"范式与复杂度小结

- **任意时**：所有任务（区域/边界/梯度/极值/Lipschitz/验证/等变/因果/综合）在 JIT 下均以**上下界**形式进行，随细化**单调**收敛（DYN-1,3）。
- **精确性**：当且仅当覆盖域被**局部完全细化**，所有量转为**片段仿射**或其组合，从而得到**精确**答案（DYN-2）。
- **可判定性**：性质语言由有限线性/二阶锥原子构成 ⇒ 在"允许有限多细化"的前提下**可判定**（DYN-6）。
- **复杂度**：最坏指数（与可能片段数同阶）；但在预算 B, G 下的**规模上界线性**于 B, G（DYN-4），避免静态的 $\sum\binom{k_v}{2}$ 全局比较。
- **证书化**：真（全域 LB 证书）、假（反例点/域）、未知（最紧子域）三值输出，确保结果**可核验。**

4.6 本章小结（面向引用）

- **GEO**：按需提取活跃片段（GEO-1），构造决策边界复形（GEO-3），输出梯度/雅可比自动机（GEO-4），计算极值与 Lipschitz 的任意时上下界与精确值（GEO-2/5）。
- **VER/CAU**：性质验证（VER-1）与鲁棒认证（VER-2）在 JIT 下健全/可判定；等变验证（VER-3）通过差分构造与有效域限制得到健全证书；干预与最大因果影响（CAU-1/2）以 JIT-B&B 方式精确可解。
- **SYN**：参数修复（SYN-1）、由规范综合（SYN-2）与最短结构编辑（SYN-3）以 JIT 作为健全的验证-判定器，给出可构造流程与相应的充分完备条件。

> 至此，JIT-SWT 为**几何—验证—因果—综合**提供了统一的"**按需细化、任意时上下界、完全细化即精确**"理论框架。第 5 章仅以最小实验展示该框架的可用性与伸缩性指标（时间/规模/证书），不再引入新理论假设。

5　实验验证（小而充分）

> 目标：以**最小但充分**的实验验证第 2–4 章的理论与 JIT-SWT 的可用性。我们仅报告**规模/时间/证书**，避免冗长对比。所有实验均可在单机完成。

5.1　统一设置

环境

- 硬件：单机 CPU（≥8 核）＋可选 GPU（训练用，验证不依赖 GPU）。
- 软件：Python 3.10；深度学习库 PyTorch 或 JAX（二选一）；线性/锥规划：Gurobi / CPLEX / MOSEK（任一）或 CVXOPT；数值线性代数（谱范数）使用 scipy/numpy。
- 浮点：FP32；等号/比较阈值 $\tau = 10^{-7}$；守卫行归一化 $\|a\|_2 = 1$。
- 随机：`seed=2025`（numpy/torch/random）。

实现与接口

- `Compile(F, JIT=False/True) → A_F`：静态或 JIT-SWT 编译器（§2.3, §3）。
- `ForwardEq(F, A_F; X)`：逐点一致性检查。
- `Regions(A_F; D)`：按需提取线性片段（JIT）或从静态图读出。
- `Lipschitz(A_F, p→r, D)`：GEO-5（精确或上下界）。
- `Verify(A_F, ϕ; D)`：VER-1/2/3（B&B，返回"真/假/不确定"与证书/反例）。
- `Intervene(A_F, C)` 与 `Imax(A_F, A_{F_C}, D)`：CAU-1/2。
- **JIT 预算**：切分上限 `B`、守卫库上限 `G`（默认 `B=2e4, G=1e5`，可调）。

计量（所有任务均报告）

- 编译：时间（s）、#states、#guards（唯一化后）、（静态基线）#comparators$_{\text{static}}$ 与（JIT 实际）#splits。
- B&B：总迭代、#LP/#SOCP 调用、命中率（缓存复用）、最终答案类型（证书/反例/未决）。
- 几何：#reachable regions、梯度/边界片段数。
- 额外：峰值内存（MB，选报）。

5.2　任务一：FFN（UCI Iris）

数据与域

- Iris（3 类，4 维），特征标准化为零均值单位方差。
- 训练/验证/测试：70%/15%/15%。
- $D_{\text{in}} = \prod_{k=1}^{4}[\mu_k - 3\sigma_k,\ \mu_k + 3\sigma_k]$。

模型与训练

- 结构：`Linear(4→16) → ReLU → Linear(16→16) → ReLU → Linear(16→3)`。
- 训练：交叉熵，Adam(lr=1e−3)，epochs=100，batch=32，选验证最佳权重。

评测流程

1. `Compile(F, JIT=False)` 与 `Compile(F, JIT=True)`；记录规模与时间。
2. `ForwardEq`：在 $D_{\rm in}$ 等距采样 1,000 点，报告 $\max \|F(x) - A_F(x)\|_\infty$。
3. `Regions(A_F; D_{\rm in})`（JIT）：按需提取可达线性片段，报告片段数。
4. `Lipschitz(A_F, 2→2, D_{\rm in})`：给出 $L^{\rm exact}$（GEO-5）与层谱范数乘积上界 $L^{\rm upper}$，报告比值 $L^{\rm exact}/L^{\rm upper}$。
5. **鲁棒认证**（VER-2）：随机取 10 个测试样本 x_0，半径 $\epsilon \in \{0.1, 0.2\}$（$\ell_2$ 球），判定 $g(x) = F_y(x) - \max_{j\neq y} F_j(x) \ge 0$。报告通过率与若干反例（若存在）及其 $\|x - x_0\|_2$。

报告表 A（FFN）

metric	value
compile time (static / JIT) [s]	
#states / #guards (static / JIT)	
#comparators_static / #splits_JIT	
forward max-err on 1k (∞-norm)	
#reachable regions in $D_{\rm in}$ (JIT)	
$L^{\rm exact}_{2\to2}$ / $L^{\rm upper}_{2\to2}$	
robustness pass @ $\epsilon = 0.1/0.2$	
#LP / #SOCP (total)	

5.3 任务二：轻量 CNN（CIFAR-10 子集）

数据与域

- 每类 1,000 张，共 10,000（train）/ 2,000（test），像素 $[0, 1]$。
- 平移集合 $\mathcal{S} = \{(\Delta x, \Delta y) : \Delta x, \Delta y \in \{-2, -1, 0, 1, 2\}\}$。
- **有效域**掩膜：对 stride=1, padding=1，去除边框 2 像素（等变性评测仅在有效域上）。

模型与训练

- 结构 A（等变友好，stride=1）：`Conv3x3(3→16,s=1,p=1) → ReLU → Conv3x3(16→32,s=1,p=1) → ReLU → GlobalAvgPool → Linear(32→10)`。
- 对照结构 B（含下采样）：将第一层改为 `s=2`。
- 训练：交叉熵，Adam(lr=1e−3)，epochs=20，batch=128。

评测流程

1. `Compile(F, JIT=True)`；记录规模与时间。
2. 对 100 张随机测试图像：对每个 $\Delta \in \mathcal{S}$，构造 `shift(x,Δ)`（零填充后裁剪）；比较

$$A_F(x) \quad \text{vs.} \quad A_F(\text{shift}(x, \Delta))$$

（GlobalAvgPool 后输出向量应等同）。

3. **结构 A**：统计全 Δ 的等变通过率；若失败，调用 `Verify` 的差异自动机（SWT-4）定位差异守卫（多为边界）。
4. **结构 B**：分别统计偶数/奇数平移的通过率；期望偶数⊃高通过、奇数⊃明显失败；记录差异守卫集中在 stride/padding 引入的边界。

报告表 B（CNN）

metric	value
compile time [s]	
#states / #guards	
#splits_JIT / #LP	
equivariance pass (A, all shifts)	
pass rate (B, even / odd shifts)	
#diff-regions linked to boundary/stride	

> **图 1（可选）**：差异守卫热图（像素坐标上累计触发频次）。

5.4 任务三：固定图 GNN（Zachary Karate）

图与特征

- $|V| = 34, \ |E| = 78$。
- 节点特征：度、聚类系数、谱嵌入前 4 维（共 6 维）；标签为 2 社团（仅为训练监督）。

模型与训练

- `GCNConv(6→16) → ReLU → GCNConv(16→16) → ReLU → Linear(16→2)`；聚合 Sum 或 Mean。
- 训练：epochs=200，Adam(lr=1e−2)。

评测流程

1. `Compile(F, JIT=True)`；记录规模与时间。
2. **置换等变**：采样 50 个随机节点置换 π，构造输入置换 $\mathcal{T}_\pi$ 与输出置换 $\mathcal{T}_\pi'$，调用 `Verify(A_F∘T_π = T'_π∘A_F)`；记录通过率与最早出现差异的层（若有）。
3. **干预与最大因果影响**：将第二层激活的方差最大通道 $k^\star$ 置零：$\texttt{do}(h^{(2)}_{v,k^\star} \leftarrow 0)$。
   令 $\mathcal{D} = \{\mathbf{X} : \ \|\mathbf{X} - \mathbf{X}_0\|_\infty \le 0.1\}$。
   调用 `Imax` 计算 $I_{\max} = \sup_{\mathbf{X} \in \mathcal{D}} \|F(\mathbf{X}) - F_C(\mathbf{X})\|_\infty$，并报告达到上界的节点/类别 margin 变化。

报告表 C（GNN）

metric	value
compile time [s]	
#states / #guards	

metric	value
permutation equivariance pass (50 perms)	
$I_{\max}$ (value) / arg-max node(s)	
#splits_JIT / #LP	

5.5 消融与可扩展性（小规模、可复现）

A. JIT 预算扫掠（与 DYN-4 对应）

- 固定一个任务（推荐 Iris/FFN），令 `B∈{1e3, 5e3, 1e4, 2e4}`；记录：#splits、#LP、用时、LB/UB 间隙、是否判定。
- 预期趋势：#splits 与判定率单调上升，LB/UB 间隙单调收敛；时间近似线性于 `B`。

B. 代价分解

- 报告时间占比：LP/SOCP、守卫管理、e-graph 重写/哈希、前端遍历。
- 目的：显示“解题器调用”是主要瓶颈，证明共享与按需细化的必要性。

C. 阈值敏感性

- $\tau \in \{10^{-6}, 10^{-7}, 10^{-8}\}$：比较等价/鲁棒判定的一致性；报告差异样本是否集中在“几何 tie”区域（支持闭集合约定的健全性）。

D. 规模外推（模板共享）

- 在 CNN 上线性放大通道数（如 16→32→64），记录 #guards 与用时随模板实例数的增长；预期随“模板实例数 + 必要比较数”线性增长（对比 §2.3 的静态上界）。

5.6 复现实务（一页即可）

- 所有脚本均以同一 CLI 入口：`train_<task>.py`（训练）→ `compile.py --jit {0,1}` → `eval_<task>.py`（ForwardEq/Regions/Lipschitz/Verify/Imax）。
- 默认超参：`seed=2025`, `tau=1e-7`, `B=2e4`, `G=1e5`, `solver_timelimit=600s`。
- 重要开关：`--jit-budget B`、`--guards-cap G`、`--solver exact|fast`（是否用 LP 精确界）。
- 产出：表 A/B/C（CSV）、差异守卫热图（PNG，可选）、证书/反例（JSON，含 GuardSet 与见证点）。