# 面向车辆可塑性的白盒神经网络集成：量化自适应非线性模型预测控制中的符号可审计性效率代价

Enzo Nicol´as Spotorno、Matheus Wagner 和 Antˆonio Augusto Fr¨ohlich巴西圣卡塔琳娜联邦大学（*UFSC*）弗洛里´亚诺波利斯，巴西电子邮箱：{enzoniko、wagner、guto}@lisha.ufsc.br

arXiv:2602.01516v1 [cs.LG] 2 Feb 2026

摘要——**我们提出了一种白盒自适应非线性模型预测控制架构，通过采用模块化主权范式，在冻结的、面向特定工况的神经网络专家之间进行仲裁，从而解决车辆可塑性问题（无需重新训练即可适应变化的运行工况）。该集成动力学在 CasADi 中作为完全可遍历的符号图进行维护，实现最大程度的运行时可审计性。同步仿真验证了其在复合工况转变（摩擦、质量、阻力）下的快速适应能力（∼7.3 毫秒）和近乎理想的跟踪保真度，而非自适应基线则无法实现这一点。实证基准测试量化了透明性代价：与编译型参数化物理模型相比，符号图维护使求解器延迟增加了 72–102×，确立了严格白盒实现所需付出的效率代价。**

索引词—**自适应模型预测控制、神经网络、自主车辆、符号可审计性、车辆可塑性。**

## I. 引言与相关工作

自主系统，尤其是在汽车稳定性控制和自主赛车等安全关键领域，在其控制与决策组件所采用的动态模型的可塑性和可验证性方面持续面临挑战。一方面，此类系统必须在无需重新训练的情况下展现可塑性，使其行为适应运行条件的变化和车队异质性，以保持高性能 [1]。另一方面，ISO 26262等标准下的认证保障流程更倾向于透明、可分析的白盒模型 [2]。当前最先进的部署工具（例如 *acados*、L4CasADi [3]）通过生成编译后的模型代码实现实时性能，从而有效避免运行时符号遍历，并将验证转移到代码生成溯源与可复现构建实践[4], ，借助工具资格认证满足ISO 26262。相比之下，我们研究在运行时保留显式符号表示（例如通过CasADi SX [5]）这一替代方案。该方法在透明度上提供了理论上的最大上界，允许直接检查导数图，但会带来尚未充分刻画的计算开销。

近期的基于学习的建模方法受到通用基础模型趋势的影响 [6], ，往往依赖于对大型单体模型进行微调。这类方法容易陷入稳定性—可塑性困境，可能损害闭环稳定性和形式化保证 [7], [8]。相比之下，混合专家模型和 HYDRA架构等基于学习的方法 [6], 为本研究采用的模块化主权范式提供了灵感。这些方法倡导构建这样的系统：通过在一组冻结且经过预先验证的专用模型中进行仲裁来实现适应，而非持续更新单个复杂的黑箱 [9]。这种模块化结构既能保持各个组件的完整性，又与符号实现兼容，从而同时支持适应和验证。

相关工作，例如隐式自适应方法（如 Neural-Fly [10] 以及基于 PDE 的函数逼近方法，如 $S^2$GPT-PINN [11]），通过表达能力强的函数逼近器调整行为；而显式参数自适应方法（如 Deep Dynamics [12]）则在固定结构内估计物理参数。实时方法包括 LPV-MPC [13], GP-MPC [14], 和分层自适应非线性模型预测控制 [15]（已在全尺寸车辆上实现 ∼35ms 的求解时间）。尽管单体基础模型可能具备广泛的泛化能力，但安全关键型应用通常更倾向于模块化，以便进行形式化验证并减轻灾难性遗忘 [6]。此外，单体网络存在频谱偏差，会优先拟合低频分量，因此可能掩盖对控制至关重要的突发工况变化 [16]。我们的方法与混合专家架构相似，但用基于优化的调节器 QP取代不透明的学习式门控，将冻结的、针对特定工况的专家进行融合。这种设计优先考虑工况分离，使突变能够被分析，而非被隐式平滑处理 [6]。

然而，对于这一范式的实际影响，尤其是在非线性模型预测控制求解器中强制采用符号化实现所产生的性能代价，我们仍缺乏深入理解。与以效率优化为目标的方法不同，本研究专门分离并量化了在模块化主权 架构 [6]中保持完整非线性符号保留所带来的具体效率代价。我们旨在评估将此类神经自适应控制器集成到白盒非线性模型预测控制框架中的权衡，优先考虑符号可检查性、可追溯性和完整可审计性，而非原始执行速度。我们的贡献有三方面：我们提出一种符号化非线性模型预测控制集成方案，将冻结的神经专家稀疏集成用于在严格可审计性约束下实现车辆可塑性；我们刻画符号透明性的计算成本，并量化其相对于参数化模型的效率差距；我们还通过功能验证，评估该架构应对突发工况转变（例如，

本研究部分由 FUNDEP 资助，资助项目编号为 Rota 2030 27192.02.INT01/2022.01-00、29271.02.01/2022.01-00 和 29271.03.01/2023.04-00。

摩擦变化）和车队异质性的能力。我们通过性能界分析证明，尽管存在已识别的计算成本，该方法仍能解决可塑性问题。

## II. 方法论

我们采用受 HYDRA 启发的模块化主权架构 [6]。我们不训练单体模型，也不显式估计物理参数，而是将车辆动力学构建为一组冻结的、针对特定工况的专家向量场的凸组合，其中每个向量场都对连续时间动力学模型的状态导数进行参数化。全局有效动力学通过向量场混合得到：$\hat{\mathbf{x}}(t) = \sum_{i=1}^{N} w_i \cdot \Psi_i(\mathbf{x}(t),\ \mathbf{u}(t))$, 其中$\mathbf{w} \in \mathbb{R}^N$ 是治理向量（$\sum_i w_i = 1,\ w_i \geq 0$），$\Psi_i$ 是冻结的专家网络，而$\mathbf{x}$，$\mathbf{u}$ 分别表示状态和输入。这样可将动力学约束在专家模型逐点构成的凸包内，避免超出模型族范围进行外推。这一几何特性对于处理车队异质性至关重要：凸组合通过覆盖不同平台之间的动力学空间，使控制器无需重新训练，就能为未见过的车辆配置插值出正确的动力学。自适应非线性模型预测控制共享运动学状态（位置和姿态），而动力学加速度（纵向、横向和横摆角速度导数）则通过专家输出的凸组合计算得出；组合权重由调节器 [6] 使用测量状态导数（$\dot{\boldsymbol{x}} \approx (\boldsymbol{x}_k - \boldsymbol{x}_{k-1})/T_s$）的有限差分近似估计，并通过指数移动平均（EMA）平滑。

为实现零样本部署，专家库采用贪心最坏情况选择策略构建，以激励对车辆动力学进行尽可能稀疏的覆盖 [6], [11]。我们采用标准的六状态动态单轨自行车模型，并以Pacejka轮胎力 [12]作为真实值生成器。通过改变参数集 $\Phi$ （例如摩擦、质量和阻力）来建模不同运行工况之间的差异，从而模拟环境变化和车队异质性。冻结神经网络库基于混合合成数据集进行训练。该数据集将均匀状态空间采样与针对性设计的“啁啾”轨迹相结合，以激励高侧滑动力学，确保专家模型能够捕捉随机探索通常遗漏的极限操控行为。

关于最优控制问题，控制器在时域 $H = 15$（$T_s = 0.02$ s）内求解离散时间优化问题。目标是最小化跟踪误差和控制力度：

$$J = \| \quad _H - \quad _{\text{ref}\,H}\|_P^2 + \mathbf{pp},$$
$$\sum_{k=0}^{H-1} \left( \| \quad _{k+1} - \quad _{\text{ref}\,k+1}\|_Q^2 + \|\Delta \quad _k\|_R^2 \right)$$

$\mathbf{pp}$, $\mathbf{u}$，同时满足集成动力学 $\mathbf{x}_{k+1} = \mathbf{x}_k + T_s \cdot f_{\text{ens}}(\mathbf{x}_k,\ \mathbf{u}_k,\ \mathbf{w}_{\text{gov}})$、初始状态 $\mathbf{x}_0 = \hat{\mathbf{x}}_0$，以及标准的执行器限制和变化率限制$\mathbf{u} \in [\mathbf{u}_{\min},\ \mathbf{u}_{\max}]$ [1]。此外，参考轨迹通过沿赛道中心线投影位置，以几何方式生成，并假设纵向速度恒定为$v_{\text{ref}} = 1.5$ m/s。该参考轨迹忽略了摩擦极限，因此非线性模型预测控制必须尽可能地逼近它。调节器模块在运行时估计混合权重 $\mathbf{w}_k$ 。为了解决在车辆系统中状态导数（$\dot{\mathbf{x}}$）很少被直接测量这一实际限制，我们使用最近的状态-输入测量值 $\mathcal{H}_k$，通过一阶前向欧拉离散化来构建回归，其中每个元素为 $h_k = (\mathbf{x}_k,\ \mathbf{x}_{k-1},\ \mathbf{u}_{k-1})$。调节器 最小化 $\min_{\mathbf{w}_k} \sum_{h_k \in \mathcal{H}_k} \left\| \mathbf{x}_k - \mathbf{x}_{k-1} - dt \sum_{i=1}^{N} w_k^i \Psi^i(\mathbf{x}_{k-1},\ \mathbf{u}_{k-1}) \right\|_2^2$，约束条件为 $\sum_{i=1}^{N} w_k^i = 1,\ w_k^i \geq 0$。单纯形约束确保所得动力学保持在专家模型的凸包内。这是一种隐式自适应方法，通过在固定模型库上进行系数混合来调整系统行为，使其能够适应专家模型集成中所表示的复合工况变化，而无需显式估计物理参数。

在注入非线性模型预测控制（NMPC）之前，对估计权重$\mathbf{w}_k$进行指数移动平均（EMA）平滑，衰减系数为 $\alpha = 0.1$ ，以抑制高频振荡，避免其在瞬态过程中 destabilize 闭环。回归使用最近 $W = 20$个状态-输入对的滑动窗口，在稳健估计与对突发工况转变的响应速度之间取得平衡。这些参数通过经验调优；正式的敏感性分析留待未来工作，以优化噪声抑制与适应延迟之间的权衡。选定的权重$\mathbf{w}_k^*$ 在一次非线性模型预测控制（NMPC）执行周期内被视为固定参数。在此假设下，有效模型雅可比矩阵是各专家模型雅可比矩阵的凸组合，$\mathbf{J}_{\text{eff}}(\mathbf{x}, \overline{\mathbf{u}}) = \sum_{i=1}^{N} w_i^* \frac{\partial \Psi_i}{\partial \mathbf{x}}(\mathbf{x}, \mathbf{u})$, 从而无需对权重选择机制求导即可提供解析梯度。这里我们区分结构透明性（可遍历的符号图）与语义可解释性。尽管求解器可以完全访问符号雅可比矩阵（结构层面），多层感知机权重在语义层面仍然不透明，即使物理信息机器学习技术能够提升其可解释性。尽管如此，我们着重量化结构图遍历成本。为保持这种结构可审计性，我们使用 CasADi SX 中完全符号化的表示来实现集成模型，而非采用不透明的编译代码。因此，计算约束雅可比矩阵和拉格朗日函数海森矩阵时，需要反复遍历由神经网络专家模型生成的大型符号计算图。

**专家模型训练**。我们训练八个冻结的物理信息神经网络（物理信息神经网络）模型，经经验选取，以在物理参数流形的覆盖范围与内存及计算成本之间取得平衡。每个专家模型针对不同的运行工况逼近连续时间动力学 $\dot{\mathbf{x}} = \Psi_i(\mathbf{x}, \mathbf{u})$。所有专家模型均实现为多层感知机（3个隐藏层、64个神经元、双曲正切激活函数），并对状态-控制输入进行Z分数归一化。训练最小化复合损失函数$L_{\text{total}} = L_{\text{data}} + \lambda L_{\text{phy}}$,

$\lambda = 0.1$, 其中 $L_{\text{phy}}$ 通过在原始物理状态上评估约束并将其归一化到网络输出分布来强制运动学一致性。优化遵循两阶段混合流程：Adam全局搜索（学习率 $= 10^{-3}$，在验证集上提前停止），随后以最佳Adam权重初始化进行L-BFGS精修。该流程将专家模型均方根误差从$\mathcal{O}(5 \times 10^{-2})$（仅Adam）降至 $\approx 4 \times 10^{-6}$，从而限制认知

[1]代价矩阵为对角矩阵，包含 $Q_p = 10$、$R_\delta = 1.0$、$R_D = 0.1$。需要注意的是，变化率约束专门适用于转向角 $\delta$（而非油门 $D$），以防止激进的转向操作，同时允许油门快速响应。

误差在NMPC预测时域上的累积。

我们分两个阶段进行评估 [2]:

**第一阶段计算基准测试：** 本阶段评估神经动力学模型与解析动力学模型的求解器墙钟时间和适应延迟。我们使用仿真的 1:10比例旅行车（F1TENTH）和 1:43比例遥控车（ORCA）模型[17]，预测时域为 $N = 15$，采样时间为 $dt = 0.02$ 秒。评估指标包括对 NLP 评估时间与线性求解时间的分解，以及在三类模型——基于QP的神经集成重加权、朴素/JIT物理模型重新编译和优化的参数化物理模型更新——下，突发摩擦变化（$\mu : 1.0 \rightarrow 1.25$）后的控制器更新延迟比较。

**第二阶段功能可塑性验证：** 本阶段仅在 ETHZ 1:43比例自主赛车赛道 [17]上评估闭环性能。赛道的狭窄几何形状会放大微小的预测误差，可用于压力测试，揭示认知不确定性在激进控制下如何传播。鉴于已识别出的求解器延迟目前使实时硬件部署无法实现，我们采用同步仿真，将功能正确性与计算开销分离。在此模式下，推理期间虚拟时间暂停，因此所有控制器的信息延迟均相同。这一概念验证评估将架构贡献与实时实施限制区分开来，为未来部署建立功能基线。本阶段遵循诊断层级：**(i)** 定义性能上限的理想 ODE 专家模型，**(ii)** 用于隔离偶然不确定性敏感性的含噪 ODE 专家模型（加性高斯噪声，$\sigma = 0.05$，与仅使用Adam的RMSE处于同一量级），以及 **(iii)** 代表性能下限的神经PINN专家模型。控制器在以下情形下接受评估：**(i)** 突发湿滑赛道状态转变（$\mu \rightarrow 0.5$），**(ii)** 复合车队异质性状态转变（$\mu \rightarrow 0.5$, $m \rightarrow 1.2m_{\text{nom}}$, $C_d \rightarrow 1.4C_{d,\text{nom}}$），以及 **(iii)** 标称稳定性情形，以验证调节器 不会引发虚假适应。

## III. 结果

表 I 综合比较了符号可审计性与速度之间的权衡。神经集成虽能实现可塑性，但与优化后的物理基线相比，会导致 72×–102× 的减速。详细性能分析揭示了这是结构性问题：对于 F1TENTH，NLP评估耗时 ∼588 毫秒（占总时间的 **96%** ），而线性求解器仅耗时 ∼9 毫秒（$p < 0.001$）。与解析模型不同，神经集成迫使求解器遍历大型计算图，以生成可验证雅可比矩阵。这造成了“计算零值的代价”：自动微分引擎 [5] 必须遍历稠密路径，以验证稀疏贡献（与 ∼3.6%的密度，涵盖两个平台）。这种跨不同车辆规模的一致性表明，透明性惩罚是神经网络架构固有的固定结构性成本，与车辆的物理质量无关。

尽管稳态开销较高，适应机制仍十分迅速（∼7.3 毫秒），与朴素的“即时”重新编译（延迟峰值为 ∼752 毫秒）形成对比。这一开销表明，对于低维车辆动力学而言，专家网络的参数过多（$v_x$，$v_y$，$\omega$），这也指出了未来采用基于敏感度的剪枝的机会。

此外，我们验证了所提出的架构能够解决车辆可塑性问题，处理突发工况转变和车队异质性，前提是通过同步仿真解除先前确定的计算瓶颈。性能在三个诊断层级上进行评估，汇总于表 I。性能以第 1 层转变前基线（$v_x = 0.3124$m/s，$v_y$ =0。0563m/s，位置=0.0602 m）为标准化基准，采用性能下降 $\delta = 100 \times$（后 $-$ 前$_{\text{base}}$）/|前$_{\text{base}}$| 和缓解 $\mu = 100 \times (\delta_{\text{base}} - \delta_{\text{adapt}})/|\delta_{\text{base}}|$.

首先，在理想化常微分方程设置下进行理论验证（第 1 层），预计调节器 能够恢复接近上限的性能。表 I 证实了这一点：在仅摩擦工况转变下，自适应控制器将位置性能下降控制在 +12.9%，相较于基线实现了 97.5% 的缓解。在第 2 层（$\sigma = 0.05$）中通过传感器噪声引入偶然不确定性，结果表明，尽管残差存在高频抖动，回归逻辑仍保持稳定。位置性能的缓解效果依然显著，权重轨迹也保持平滑，这证实偶然不确定性不会破坏调节器的估计机制，与指数移动平均平滑的预期一致。当采用白盒神经专家（第 3 层）时，性能完全受认知不确定性支配。对于使用仅使用 Adam 的训练进行朴素训练的物理信息神经网络（第 3a级），其绝对预测误差并不安全（位置漂移达到米级）。尽管如此，适应发挥着安全层的作用：如表 I 所示，调节器 缓解了主要失效模式，降低横向速度误差，并防止高曲率机动期间发生甩尾失控。这得益于专家重新加权，它纠正了系统性的横向滑移低估，并部分补偿了有偏的纵向阻力，但残余偏差会引发权重振荡。

然而，在第3b级采用混合训练方案后，认知不确定性降至最低，架构也缩小了与 ODE 性能上限之间的差距。如图 1所示，整个运行过程中，位置误差始终低于 0.1 m，与理想 ODE 情况相当。定量而言，与不安全的 Tier3a 基线相比，绝对跟踪误差降低了 35×。在所有参数异质性测试中，即使摩擦、质量和阻力同时发生变化，调节器 仍能恢复相当一部分性能。与仅改变摩擦的情况相比，缓解效果较弱，反映了库覆盖范围在应对多项参数同时偏移时的局限性；尽管如此，该系统仍展现出非自适应基线所不具备的显著鲁棒性。对所有层级进行零假设验证后确认

[2]所有闭环实验和计算实验均基于100个相互独立的随机种子进行评估。报告指标为均值，并附带95%自助法置信区间（1000次重采样）。确定性基线按构造具有零方差；在相关情况下，同时报告成对显著性（$p < 0.05$）和效应量。所有实验均在配备32 GB内存的 Intel Core i7-14700 CPU（2.10 GHz）上进行仿真，使用 CasADi 3.6.x 和 IPOPT 3.14.x，以及 MA57线性求解器。该概念验证实验的完整实现代码仓库将会公开，其中包含确保可复现性的所有细节。

表 I 综合实验结果。**（稳态）性能：**神经集成虽会导致减速，但适应延迟仅为 7.3 ms，优于即时编译（752 ms）。**（迁移后）移位均方根误差：**括号内为无移位指标；正向缓解表示相较基线有所改善（第 1 层基线：$v_x$=0.3124, $v_y$=0.0563, POS=0.0602 M）。

| 测试平台 | 模型 | 构建时间（毫秒） | 求解时间（毫秒） [95% 置信区间] | 减速 | 雅可比矩阵密度 | 适应延迟(ms) |
|---|---|---|---|---|---|---|
| **F1TENTH** (1:10 比例) | 物理（参数化） | 265 | 7.38 [7.20–7.56] | 1.0× | 3.54% | ∼0.01（显式）/ ∼752（即时编译） |
| | 神经集成 | 10,521 | 535.00 [518–552] | 72.5× | 3.64% | **7.30 [7.1–7.5]** |
| **ORCA**（遥控汽车） | 物理（参数化） | 285 | 5.35 [4.69–5.82] | 1.0× | 3.54% | — |
| | 神经集成 | 10,850 | 545.00 [530-572] | 101.8× | 3.64% | — |

| Tier | $v_x$ (m/s) 后测 B | $v_x$ (m/s) 后测 A | $v_x$ 中介效应 (%) | $v_y$ (m/s) 后测 B | $v_y$ (m/s) 后测 A | $v_y$ 中介效应 (%) | 位置（米） 后测 B | 位置（米） 后测 A | 位置 中介效应 (%) |
|---|---|---|---|---|---|---|---|---|---|
| **仅摩擦（严重）** | | | | | | | | | |
| 1 | 0.2374 (0.1617) | 0.2371 (0.1702) | +0.4 (-5.6) | 0.3579 (0.0646) | 0.2566 (0.0593) | +33.6（+63.9） | 0.1214 (0.0389) | 0.0617 (0.0333) | **+97.5 (+26.3)** |
| 2 | 0.2286 (0.1593) | 0.2352 (0.1742) | -7.9 (-9.7) | 0.3427 (0.0643) | 0.2609 (0.0593) | +28.6 (+62.5) | 0.1134 (0.0390) | 0.0653 (0.0338) | **+90.4 (+24.5)** |
| 3b | 0.2476 (0.2128) | 0.2547 (0.2137) | -11.0 (-0.9) | 0.3102 (0.0634) | 0.2942 (0.0705) | +6.3 (-100.0) | 0.0927 (0.0407) | 0.0762 (0.0386) | **+50.8 (+10.8)** |
| 3a | 1.62 (1.40) | 1.09 (1.05) | +40.5（+32.2） | 0.78 (0.40) | 0.23 (0.15) | +76.0 (+72.7) | 2.85 (2.00) | 1.12 (0.95) | **+62.0（+54.1）** |
| **所有参数（严重）** | | | | | | | | | |
| 1 | 0.3540 (0.1617) | 0.2052 (0.1702) | +357.7 (-5.6) | 0.5598 (0.0646) | 0.5459 (0.0593) | +2.8（+63.9） | 0.5777 (0.0389) | 0.2882 (0.0333) | **+55.9 (+26.3)** |
| 2 | 0.3512 (0.1597) | 0.2221 (0.1720) | +332.7 (-8.1) | 0.5596 (0.0657) | 0.5385 (0.0595) | +4.2 (+66.0) | 0.5769 (0.0394) | 0.3197 (0.0332) | **+49.8 (+29.8)** |
| 3b | 0.2887 (0.2128) | 0.2569 (0.2137) | +134.2 (-0.9) | 0.5132 (0.0634) | 0.5080 (0.0705) | +1.1 (-100.0) | 0.4870 (0.0407) | 0.3956 (0.0386) | **+21.4 (+10.8)** |
| 3a | 1.54 (1.35) | 0.93 (0.90) | +49.7 (+43.4) | 0.90 (0.45) | 0.28 (0.18) | +73.5 (+68.6) | 2.65 (1.90) | 0.98 (0.85) | **+64.5 (+57.1)** |

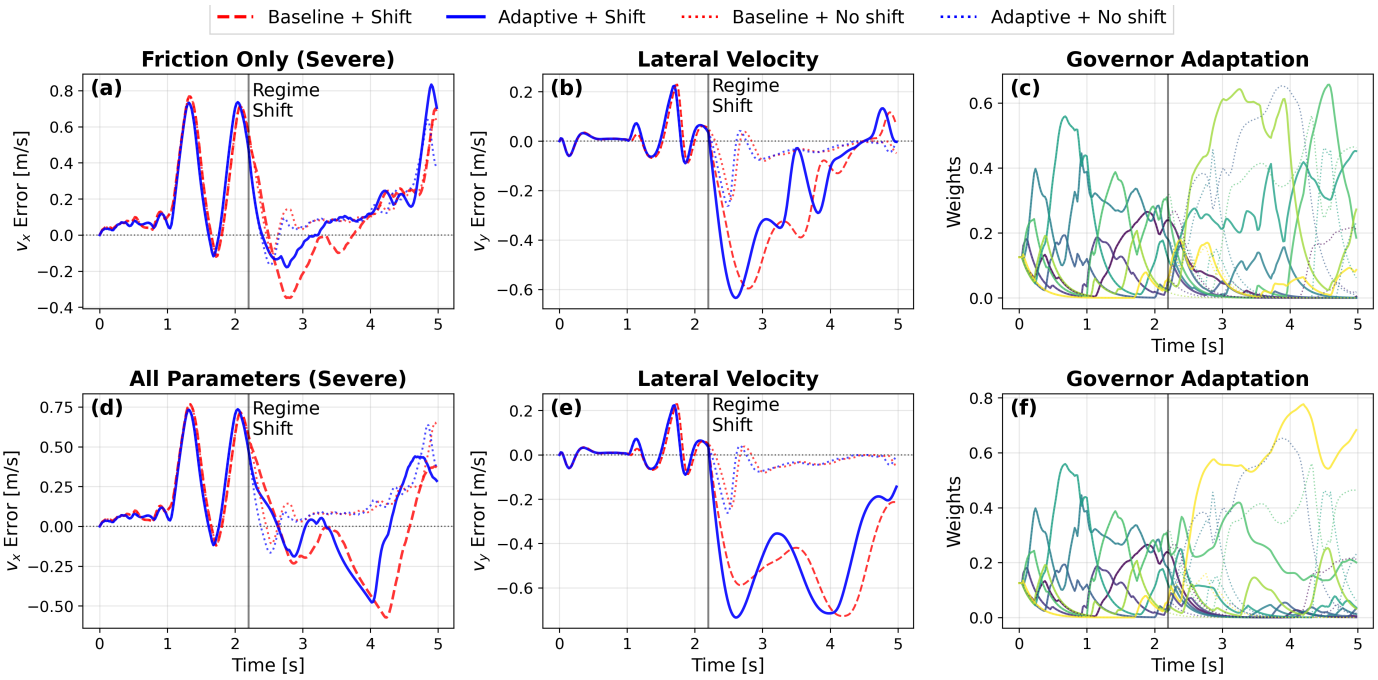



图1. 训练良好的物理信息神经网络表现，混合训练（均方根误差 $\approx 4 \times 10^{-6}$）缩小了与常微分方程上限的差距。位置误差 $< 0.1$ 米，在 0.8 内恢复 s.

在无变化条件下，性能退化有界或为负，位置误差往往会随时间推移而改善，这是凸混合产生的轻微正则化效应所致。尽管调节器会针对跟踪引起的残差持续进行细微的权重调整，但显著变化主要发生在真正的工况转变期间（图 1），这证实了适应过程稳定且非虚假，这是安全部署的关键前提。因此，从朴素的第3a级过渡到混合训练的第3b级，使安全差距缩小了一个数量级以上，并恢复了理想 ODE 专家模型的性能上限。这一功能提升足以证明相关计算开销是合理的：尽管符号图遍历会根据基准物理复杂度带来 72–102× 倍的减速，但它能够实现经验证的白盒控制器，使其具备自主以亚车道精度实现适应。功能验证证实，该架构成功解决了可塑性问题，从而推动未来工作优化计算实现，以使这一权衡在实时条件下可行。

## IV. 讨论与结论

本工作量化了在白盒自适应控制中优先考虑符号可审计性而非执行速度所付出的效率代价。结果表明，严格的同步可验证性目前阻碍了实时部署，但该架构在功能上解决了车辆可塑性问题。相较于参数化物理模型，观测到的 72–102× 倍减速确立了维持完整运行时自省所需付出的结构性代价和经验基线。不同于延迟优化方法

[14], [15], 我们的工作分离出了符号神经集成可审计性的结构性代价。代码生成框架（如 *acados* 或 L4CasADi）会将模型编译为不透明的二进制文件，而我们的方法迫使求解器在每次迭代中遍历神经集成的显式符号计算图。这确保每个雅可比矩阵条目都可追溯至特定的专家模型贡献，从而提供比标准工具资格认证更深入的内省。尽管如此，该方法目前引入了“计算零值的代价”，因为自动微分引擎的大部分求解器时间都耗费在遍历稀疏图路径上。

尽管存在这些计算开销，功能验证仍证实，所获得的可塑性在参数化模型失效时提供了关键的鲁棒性。经过优化的物理模型在预定义参数下表现出色，却容易受到未建模异质性的影响。我们的隐式适应能够应对摩擦、质量和阻力的复合工况转变，与非自适应基线相比，可降低跟踪误差。重要的是，这种可塑性并未带来在线反向传播的不稳定风险，因为调节器仅通过混合经过预验证且冻结的专家模型来运行。这证实，计算成本换来了安全裕度：能够应对认知不确定性，同时不越出模型库经验证的凸包。此外，在工况未发生转变的情形下观察到的性能提升表明，这种凸混合发挥了集成正则化器的作用，相较于单一参数化模型，它能更好地平滑细微的模型失配。

因此，这些发现并非意味着走入死胡同，而是为实现白盒自适应的实时可用性指明了路线图。不同尺度下雅可比矩阵密度始终较低（∼3.6%），这表明基于敏感度的剪枝可将符号图压缩一个数量级，同时不损失功能。此外，适应延迟（∼7.3ms）与较长的求解器延迟显著解耦，这意味着异步架构有望调和可塑性与速度之间的矛盾，尽管这可能需要以严格的同步可审计性换取性能。未来工作还必须解决本诊断研究揭示的理论和语义局限。尽管我们的实证结果验证了凸包的几何约束，但要实现形式化认证，仍需为调节器的切换逻辑推导驻留时间条件或李雅普诺夫界，以保证闭环稳定性。最后，为弥合结构透明性（可遍历图）与真正语义可解释性之间的差距，后续版本应以柯尔莫哥洛夫-阿诺德网络（KAN）取代不透明的多层感知机，使专家模型的物理含义与求解器的可检查性相一致。因此，本研究可作为概念验证和基线：尽管同步白盒集成目前受制于效率瓶颈，但它们为解决可塑性-稳定性困境提供了一条可验证且透明的途径。

## 参考文献


[1] M. Maiworm、D. Limon 和 R. Findeisen，“基于在线学习的模型预测控制：采用高斯过程模型并提供稳定性保证”，《国际鲁棒与非线性控制杂志》，第 31 卷，第 18 期，8785–8812 页，2021 年。

[2]R. Salay、R. Queiroz 和 K. Czarnecki，“ISO 26262 分析：机器学习与汽车软件安全”，SAE国际，SAE 技术论文 2018-01-1075，2018 年。 [在线]。获取地址：https://doi.org/10 4271 2018 01 1075 。/ -

[3] - T. Salzmann 、 J. Arrizabalaga 、 J. Andersson 、 M. Pavone 和 M. Ryll，“面向 CasADi 的学习：数值优化中的数据驱动模型”，载于第 6 届动力学与控制学习年度会议。PMLR，2024 年，第 541–553 页。[4] R. Verschueren、G. Frison、D. Kouzoupis、J. Frey、N. van Duijkeren、A. Zanelli、B. Novoselnik、T. Albin、R. Quirynen 和 M. Diehl，“acados——用于快速嵌入式最优控制的模块化开源框架”，数学规划计算，第 14 卷，第 2 期，第 147–183 页，2022 年。[5] J. A. Andersson、J. Gillis、G. Horn、J. B. Rawlings 和 M. Diehl，“CasADi：用于非线性优化和最优控制的软件框架”，数学规划计算，第 11 卷，第 1 期，第 1–36 页，2019 年。[6] E. N. Spotorno 和 A. A. M. Fr¨ ohlich，“立场：信息物理系统中的可认证状态完整性——模块化主权为何能解决可塑性-稳定性悖论”，2026 年。 [在线]。获取地址：https://arxiv.org/abs/2601 21249 。M. Maheshwari、J. C. Raisbeck 和 B. C.

[7] da Silva，“应对强化学习中的可塑性-稳定性困境”，2025 年。 [在线]。获取地址：https://arxiv.org/abs/2512 01034 。F. Wu、

[8] G. Wang、S. Zhuang、K. Wang 和 J. Zhang，“将模型预测控制与线性二次调节器及神经网络结合，实现摊销效率和稳定控制”，IEEE自动控制汇刊，2023 年。[9] L. Pan、H. Wang、Z. Chen、Y. Huang 和 Y. Niu，“用于多变量软测量的可控专家混合模型”，IEEE工业信息学汇刊，2025 年。[10] M. O’Connell、G. Shi、X. Shi、K. Azizzadenesheli、A. Anandkumar、Y. Yue 和 S.-J. Chung，“Neural-Fly 助力强风环境下敏捷飞行的快速学习”，科学机器人学，第 7 卷，6597，2022 年 66，第 p. eabm。[11] Y. Ji、Y. Chen 和 S. Koohy，“$S^2$ gpt-pinns：面向偏微分方程的稀疏小型模型”，arXiv 预印本 arXiv:2506.15687，2025 年。[12] J. Chrosniak、J. Ning 和 M. Behl，“Deep Dynamics：用于自主赛车的物理约束神经网络车辆动力学建模”，IEEE机器人与自动化快报，第 9 卷，第 6 期，第 5292–5297 页，2024 年。[13] M. M. Morato，“线性参数变化系统的预测控制方法”，博士论文，格勒诺布尔阿尔卑斯大学与圣卡塔琳娜联邦大学，2023 年 2 月，导师为 Julio Elias Normey-Rico 和 Olivier Sename。 [ 在线 ]。获取地址：https://theses.fr/2023 009 GRALT A. Scampicchio、E. Arcari、A.

[14] Lahr 和 M. N. Zeilinger，“模型预测控制中的动力学学习高斯过程”，控制年度评论，第 60 卷，文章编号 101034，2025 年。 [在线]。获取地址：https://www.sciencedirect.com/science/article/pii/S1367578825000483

[15] M. Thompson、J. Dallas、J. Y. M. Goh 和 A. Balachandran，“自适应非线性模型预测控制：在自动驾驶车辆中最大化轮胎力并规避障碍物”，IEEE现场机器人学汇刊，第 1 卷，第 318–331 页，2024 年。[16] N. Rahaman、A. Baratin、D. Arpit、F. Draxler、M. Lin、F. Hamprecht、Y. Bengio 和 A. Courville，“论神经网络的频谱偏差”，载于国际机器学习会议。PMLR，2019 年，第 5301–5310 页。[17] A. Jain、M. O’Kelly、P. Chaudhari 和 M. Morari，“BayesRace：利用先前经验学习自主赛车”，载于第 4 届机器人学习会议（CoRL）论文集，2020 年。