

# HardNet: Hard-Constrained Neural Networks with Universal Approximation Guarantees

**Youngjae Min**

*Massachusetts Institute of Technology*

YJM@MIT.EDU

**Navid Azizan**

*Massachusetts Institute of Technology*

AZIZAN@MIT.EDU

## Abstract

Incorporating prior knowledge or specifications of input-output relationships into machine learning models has attracted significant attention, as it enhances generalization from limited data and yields conforming outputs. However, most existing approaches use soft constraints by penalizing violations through regularization, which offers no guarantee of constraint satisfaction, especially on inputs far from the training distribution—an essential requirement in safety-critical applications. On the other hand, imposing hard constraints on neural networks may hinder their representational power, adversely affecting performance. To address this, we propose **HardNet**, a practical framework for constructing neural networks that inherently satisfy hard constraints without sacrificing model capacity. Unlike approaches that modify outputs only at inference time, **HardNet** enables end-to-end training with hard constraint guarantees, leading to improved performance. To the best of our knowledge, **HardNet** is the first method that enables efficient and differentiable enforcement of more than one *input-dependent* inequality constraint. It allows unconstrained optimization of the network parameters using standard algorithms by appending a differentiable *closed-form* enforcement layer to the network’s output. Furthermore, we show that **HardNet** retains neural networks’ universal approximation capabilities. We demonstrate its versatility and effectiveness across various applications: learning with piecewise constraints, learning optimization solvers with guaranteed feasibility, and optimizing control policies in safety-critical systems.<sup>1</sup>

**Keywords:** constrained neural networks, physics-constrained machine learning, safety-critical systems, control theory, optimization

## 1 Introduction

Neural networks are widely adopted for their generalization capabilities and their ability to model highly nonlinear functions in high-dimensional spaces. With their increasing proliferation, it has become more important to be able to impose constraints on neural networks in many applications. By incorporating domain knowledge about input-output relationships through constraints, we can enhance generalization, particularly when available data is limited (Pathak et al., 2015; Oktay et al., 2017; Raissi et al., 2019). These constraints introduce inductive biases that guide the model’s learning process toward plausible solutions that adhere to known properties of the problem domain, potentially reducing overfitting. Consequently, neural networks can more effectively capture underlying patterns and make accurate predictions on unseen data, despite scarce training samples.

---

1. The code is available at <https://github.com/azizanlab/hardnet>.

Moreover, adherence to specific requirements is critical in many practical applications. For instance, in robotics, this could translate to imposing collision avoidance or ensuring configurations remain within a valid motion manifold (Ding and Fan, 2014; Wang and Yan, 2023; Ryu et al., 2022; Huang et al., 2022). In geometric learning, this could mean imposing a manifold constraint (Lin and Zha, 2008; Simeonov et al., 2022). In financial risk management, violating constraints on the solvency of the portfolio can lead to large fines (McNeil et al., 2015). Enforcing neural network outputs to satisfy these non-negotiable rules (i.e., hard constraints) makes models more reliable, interpretable, and aligned with the underlying problem structure.

However, introducing hard constraints can potentially limit a neural network’s expressive power. To illustrate this point, consider a constraint that requires the model’s output to be less than 1. One could simply restrict the model to always output a constant value less than 1, which ensures the constraint satisfaction but obviously limits the model capacity drastically. This raises the question:

*Can we enforce hard constraints on neural networks without losing their expressive power?*

The model capacity of neural networks is often explained through the universal approximation theorem, which shows that a neural network can approximate any continuous function given a sufficiently wide/deep architecture. Demonstrating that this theorem still holds under hard constraints is essential to understanding the trade-off between constraint satisfaction and model capacity.

**Contributions** We tackle the problem of enforcing hard constraints on neural networks, namely:

- **We present a practical framework** called **HardNet** (short for hard-constrained neural network) for constructing neural networks that satisfy input-dependent constraints by construction. HardNet is, to the best of our knowledge, the first method that enables efficient and differentiable enforcement of more than one input-dependent inequality constraint. It allows for unconstrained optimization of the networks’ parameters with standard algorithms.
- **We prove universal approximation theorems** for our method, showing that despite enforcing the hard constraints, our construction retains the expressive power of neural networks, i.e., it provably does not overconstrain the model.
- **We demonstrate the utility** of our method on a variety of scenarios where it is critical to satisfy hard constraints—learning with piecewise constraints, learning optimization solvers with guaranteed feasibility, and optimizing control policies in safety-critical systems.
- **We provide the first systematic taxonomy** and comparative analysis of hard-constrained neural networks (Table 1)—aligning constraint type, input-dependence, guarantees, cost, and expressivity.

## 2 Related Work

**Neural Networks with Soft Constraints** Early approaches used data augmentation or domain randomization to structure the dataset to satisfy the necessary constraints before training the neural network. Other initial directions focused on introducing the constraints

Table 1: Comparison of methods enforcing hard constraints on neural networks for the target function  $y = f(x) \in \mathbb{R}^{n_{\text{out}}}$ . HardNet-Aff is the only method to enforce input-dependent constraints provably and efficiently with universal approximation guarantees. (Eq.: Equality, Ineq.: Inequality)

Method	Constraint	Input Depend.	Support Eq./Ineq.	Satisfaction Guarantee	Computation	Universal Approx.
Soft-Constrained Frerix et al. (2020)	Any	Yes	Both	No	Closed-Form	Yes
	$Ay \leq 0$	No	Both	Always	Closed-Form	Unknown
LinSATNet (Wang et al., 2023)	$A_1y \leq b_1, A_2y \geq b_2$ ( $y \in [0, 1]^{n_{\text{out}}}, A_*, b_* \geq 0$ )	No	Both	Asymptotic	Iterative	Unknown
C-DGM (Stoian et al., 2024)	$Ay \leq b$	No	Both	Always	Closed-Form	Unknown
RAYEN (Tordesillas et al., 2023)	$y \in \mathcal{C}$ ( $\mathcal{C}$ : linear, quadratic, SOC, LMI)	No	Both	Always	Closed-Form	Unknown
POLICE (Balestrieri and LeCun, 2023)	$y = Ax + b \quad \forall x \in R$	Yes	Eq. Only	Always	Closed-Form	Unknown
KKT-hPINN (Chen et al., 2024)	$Ax + By = b$ (# constraints $\leq n_{\text{out}}$ )	Yes	Eq. Only	Always	Closed-Form	Unknown
ACnet (Beucler et al., 2021)	$h_x(y) = 0$ (# constraints $\leq n_{\text{out}}$ )	Yes	Eq. Only	Always	Closed-Form	Unknown
DC3 (Donti et al., 2021b)	$g_x(y) \leq 0, h_x(y) = 0$	Yes	Both	Asymptotic for linear $g_x, h_x$	Iterative	Unknown
<b>HardNet-Aff (Ours)</b>	$b^l(x) \leq A(x)y \leq b^u(x)$ (# constraints $\leq 2n_{\text{out}}$ )	Yes	Both	Always	Closed-Form	Yes

as *soft* penalties (Márquez-Neila et al., 2017; Dener et al., 2020) into the cost function of the neural network along with penalty weights or Lagrange multipliers as hyperparameters. Raissi et al. (2019); Li et al. (2024) leveraged this idea in their work on physics-informed neural networks (PINNs) to enforce that the output satisfies a given differential equation. In parallel to these penalty-based and augmented Lagrangian methods, Chamon and Ribeiro (2020) Chamon et al. (2023) proposed rigorous methods that optimize over both primal and dual variables with distributional guarantees based on the PAC-learning framework. Hounie et al. (2023) extended this approach by adaptively relaxing constraints to find a better compromise between the objective and the constraints. While soft-constraint methods are useful for incentivizing the desirable behavior in the model, their main limitation is that they do not ensure constraint satisfaction for arbitrary inputs, especially those far from the training distribution.

**Neural Networks with Hard Constraints** Some conventional neural network components can already enforce specific types of hard constraints. For instance, sigmoids can impose lower and upper bounds, softmax layers enforce simplex constraints, and ReLU layers are projections onto the positive orthant. The convolution layer in ConvNets encodes a translational equivariance constraint, which led to significant improvements in empirical performance. Learning new equivariances and inductive biases that accelerate learning for specific tasks is an active research area.

Recent work has explored new architectures to (asymptotically) impose various hard constraints by either finding certain parameterizations of feasible sets or incorporating

differentiable projections into neural networks, as summarized in Table 1. Frerix et al. (2020) addressed homogeneous linear inequality constraints by embedding a parameterization of the feasible set in a neural network layer. Huang et al. (2021) and LinSATNet (Wang et al., 2023) introduced differentiable projection methods that iteratively refine outputs to satisfy linear constraints. However, these iterative approaches do not guarantee constraint satisfaction within a fixed number of iterations, limiting their reliability in practice. C-DGM (Stoian et al., 2024) enforces linear inequality constraints in generative models for tabular data by incrementally adjusting each output component in a finite number of iterations. However, its application to input-dependent constraints is limited as it cannot efficiently handle batched data. When constraints are input-dependent, the method requires recomputing the reduced constraint sets for each input, making it computationally prohibitive. In the context of optimal power flow, Chen et al. (2023) enforces feasibility for learning optimization proxies through closed-form differentiable repair layers. While effective, this approach is restricted to specific affine constraints.

Beyond affine constraints, RAYEN (Tordesillas et al., 2023) and Konstantinov and Utkin (2023) enforce certain convex constraints by parameterizing the feasible set such that the neural network output represents a translation from an interior point of the convex feasible region. However, these methods are limited to constraints dependent only on the output, and not the input. Extending these methods to input-dependent constraints is challenging because it requires finding different parameterizations for each input, such as determining a new interior point for every feasible set.

Another line of work considers hard constraints that depend on both input and output. POLICE (Balestriero and LeCun, 2023) enforces the output to be an affine function of the input in specific regions by reformulating the neural networks as continuous piecewise affine mappings. KKT-hPINN (Chen et al., 2024) handles more general affine equality constraints by projecting the output to the feasible set where the projection is computed using KKT conditions. ACnet (Beucler et al., 2021) enforces nonlinear equality constraints by transforming them into affine constraints for redefined inputs and outputs. However, these methods are restricted to equality constraints. DC3 (Donti et al., 2021b) tackles more general nonlinear constraints by reducing inequality constraints violations via gradient-based methods over the manifold where equality constraints are satisfied. However, it does not guarantee constraint satisfaction in general and is sensitive to the number of gradient steps and the step size, which require fine-tuning.

More closely related to our framework, methods to enforce a single affine inequality constraint have been proposed in the control literature: Kolter and Manek (2019) presented a framework for learning a stable dynamical model that satisfies a Lyapunov stability constraint. Based on this method, Min et al. (2023) presented the CoILS framework to learn a stabilizing control policy for an unknown control system by enforcing a control Lyapunov stability constraint. Our work generalizes the ideas used in these works to impose more general affine/convex constraints while proving universal approximation guarantees that are absent in prior works; On the theoretical front, Kratsios et al. (2021) presented a constrained universal approximation theorem for *probabilistic* transformers whose outputs are constrained to be in a feasible set. However, their contribution is primarily theoretical, and they do not present a method for learning such a probabilistic transformer.

**Formal Verification of Neural Networks** Verifying whether a provided neural network (after training) always satisfies a set of constraints for a certain set of inputs is a well-studied subject. Albargouthi et al. (2021) provide a comprehensive summary of the constraint-based and abstraction-based approaches to verification. Constraint-based verifiers are often both sound and complete but they have not scaled to practical neural networks, whereas abstraction-based techniques are approximate verifiers which are sound but often incomplete (Bunel et al., 2018; Elboher et al., 2020; Brown et al., 2022; Tjeng et al., 2019; Liu et al., 2021; Fazlyab et al., 2020; Qin et al., 2019; Ehlers, 2017). Other approaches have focused on formally verified exploration and policy learning for reinforcement learning (Bastani et al., 2018; Anderson et al., 2020; Wabersich et al., 2022). Contrary to most formal verification methods, which take a pre-trained network and verify that its output always satisfies the desired constraints, our method guarantees constraint satisfaction *by construction* throughout the training.

To address constraint violations in trained models after verification, some safe reinforcement learning methods use shielding mechanisms by overriding unsafe decisions using a backup policy based on reachability analysis (Shao et al., 2021; Bastani et al., 2021). While effective, this setup introduces a hard separation between learning and enforcement, often sacrificing performance and limiting joint optimization. Shielding is typically not differentiable and cannot be integrated into training. Similarly, editing methods modify trained networks post hoc to enforce output constraints by solving relaxed optimization problems over the model parameters (Sotoudeh and Thakur, 2021; Tao and Thakur, 2024). Though recent works demonstrate their application during training, these techniques generally target input-independent constraints and are architecture-dependent.

**Neuro-Symbolic AI** HardNet also aligns with the objectives of Neuro-symbolic AI, a field that has gained significant attention in recent years for its ability to integrate complex background knowledge into deep learning models. Unlike HardNet, which focuses on algebraic constraints, the neuro-symbolic AI literature primarily addresses logical constraints. A common approach in this field is to *softly* impose constraints during training by introducing penalty terms into the loss function to discourage constraint violations (Xu et al., 2018; Fischer et al., 2019; Badreddine et al., 2022; Stoian et al., 2023). While these methods are straightforward to implement, they do not guarantee constraint satisfaction. In contrast, works such as Giunchiglia and Lukasiewicz (2020); Ahmed et al. (2022); Giunchiglia et al. (2024) ensure constraints are satisfied by embedding them into the predictive layer, thus guaranteeing compliance by construction. Another line of research maps neural network outputs into logical predicates, ensuring constraint satisfaction through reasoning on these predicates (Manhaeve et al., 2018; Pryor et al., 2023; van Krieken et al., 2023).

### 3 Preliminaries

#### 3.1 Notation

For  $p \in [1, \infty)$ ,  $\|v\|_p$  denotes the  $\ell^p$ -norm for a vector  $v \in \mathbb{R}^m$ , and  $\|A\|_p$  denotes the operator norm for a matrix  $A \in \mathbb{R}^{k \times m}$  induced by the  $\ell^p$ -norm, *i.e.*,  $\|A\|_p = \sup_{w \neq 0} \|Aw\|_p / \|w\|_p$ .  $v_{(i)} \in \mathbb{R}$  denotes the  $i$ -th component of  $v$ .  $[A; B]$  denotes the row-wise concatenation of the matrices  $A$  and  $B$ .

For a domain  $\mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$  and a codomain  $\mathcal{Y} \subset \mathbb{R}^{n_{\text{out}}}$ , let  $\mathcal{C}(\mathcal{X}, \mathcal{Y})$  be the class of continuous functions from  $\mathcal{X}$  to  $\mathcal{Y}$  endowed with the sup-norm:  $\|f\|_\infty := \sup_{x \in \mathcal{X}} \|f(x)\|_\infty$ . Similarly,  $L^p(\mathcal{X}, \mathcal{Y})$  denotes the class of  $L^p$  functions from  $\mathcal{X}$  to  $\mathcal{Y}$  with the  $L^p$ -norm:  $\|f\|_p := (\int_{\mathcal{X}} \|f(x)\|_p^p dx)^{\frac{1}{p}}$ . For function classes  $\mathcal{F}_1, \mathcal{F}_2 \subset \mathcal{C}(\mathcal{X}, \mathcal{Y})$  (respectively,  $\mathcal{F}_1, \mathcal{F}_2 \subset L^p(\mathcal{X}, \mathcal{Y})$ ), we say  $\mathcal{F}_1$  *universally approximates* (or *is dense in*)  $\mathcal{F}_2$  if for any  $f_2 \in \mathcal{F}_2$  and  $\epsilon > 0$ , there exists  $f_1 \in \mathcal{F}_1$  such that  $\|f_2 - f_1\|_\infty \leq \epsilon$  (respectively,  $\|f_2 - f_1\|_p \leq \epsilon$ ). For a neural network, its depth and width are defined as the total number of layers and the maximum number of neurons in any single layer, respectively.

### 3.2 Universal Approximation Theorem

The universal approximation property is a foundational concept in understanding the capabilities of neural networks in various applications. Classical results reveal that shallow neural networks with arbitrary width can approximate any continuous function defined on a compact set as formalized in the following theorem (Cybenko, 1989; Hornik et al., 1989; Leshno et al., 1993; Pinkus, 1999):

**Theorem 1 (Universal Approximation Theorem for Shallow Networks)** *Let  $\rho \in \mathcal{C}(\mathbb{R}, \mathbb{R})$  and  $\mathcal{K} \in \mathbb{R}$  be a compact set. Then, depth-two neural networks with  $\rho$  activation function universally approximate  $\mathcal{C}(\mathcal{K}, \mathbb{R})$  if and only if  $\rho$  is nonpolynomial.*

To further understand the success of deep learning, the universal approximation property for deep and narrow neural networks has also been studied in the literature (Lu et al., 2017; Hanin and Sellke, 2017; Kidger and Lyons, 2020; Park et al., 2021). Interesting results show that a critical threshold exists on the width of deep networks that attain the universal approximation property. For instance, deep networks with ReLU activation function with a certain minimum width can approximate any  $L^p$  function as described in the following theorem (Park et al., 2021, Thm. 1):

**Theorem 2 (Universal Approximation Theorem for Deep Networks)** *For any  $p \in [1, \infty)$ ,  $w$ -width neural networks with ReLU activation function universally approximate  $L^p(\mathbb{R}^{n_{\text{in}}}, \mathbb{R}^{n_{\text{out}}})$  if and only if  $w \geq \max\{n_{\text{in}} + 1, n_{\text{out}}\}$ .*

Despite these powerful approximation guarantees, they fall short when neural networks are required to satisfy hard constraints, such as physical laws or safety requirements. These theorems ensure that a neural network can approximate a target function arbitrarily closely but do not guarantee adherence to necessary constraints. Consequently, even if the target function satisfies specific hard constraints, the neural network approximator might violate them—especially in regions where the target function barely meets the constraints. This shortcoming is particularly problematic for applications that demand strict compliance with non-negotiable domain-specific rules. Therefore, ensuring that neural networks can both approximate target functions accurately and rigorously satisfy hard constraints remains a critical challenge for their deployment in practical applications.

## 4 HardNet: Hard-Constrained Neural Network

In this section, we present a practical framework, HardNet, shown in Figure 1, for enforcing input-dependent hard constraints on neural networks while retaining their universal

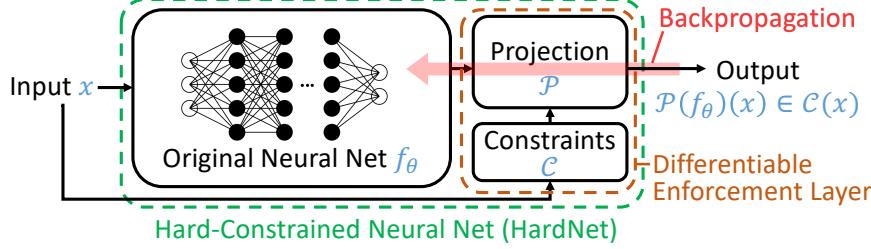


Figure 1: Schematic of HardNet. Its differentiable enforcement layer allows unconstrained end-to-end optimization of the network parameters using standard algorithms while guaranteeing satisfaction with input-dependent constraints by construction. The layer can be applied to any neural networks.

approximation properties. In a nutshell, for a parameterized (neural network) function  $f_\theta : \mathcal{X} \subset \mathbb{R}^{n_{\text{in}}} \rightarrow \mathbb{R}^{n_{\text{out}}}$ , we ensure the satisfaction of given constraints by appending a differentiable enforcement layer with a projection  $\mathcal{P}$  to  $f_\theta$ . This results in the projected function  $\mathcal{P}(f_\theta) : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}}}$  meeting the required constraints while allowing its output to be backpropagated through to train the model via gradient-based algorithms. Importantly, we show that the proposed architecture has universal approximation guarantees, i.e., it universally approximates the class of functions that satisfy the constraints.

A key challenge in this approach is devising a differentiable projection that has efficient forward and backward passes. For instance, consider affine constraints  $A(x)f(x) \leq b(x) \forall x \in \mathcal{X}$  for a function  $f : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}}}$  with  $A(x) \in \mathbb{R}^{n_c \times n_{\text{out}}}$  and  $b(x) \in \mathbb{R}^{n_c}$ , one would have

$$\mathcal{P}(f_\theta)(x) = \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z - f_\theta(x)\|_2 \text{ s.t. } A(x)z \leq b(x). \quad (1)$$

Although the constraints are affine, this optimization *does not admit a closed-form solution* in general for more than one constraint, making it computationally expensive—especially as it needs to be computed for every sample  $x$  (during training/inference) and every parameter  $\theta$  (during training).

In case of a single constraint  $a(x)^\top f(x) \leq b(x) \forall x \in \mathcal{X}$  with  $a(x) \in \mathbb{R}^{n_{\text{out}}}$  and  $b(x) \in \mathbb{R}$ , recent work in the control literature—for instance, Kolter and Manek (2019) for learning stable dynamics and Donti et al. (2021a); Min et al. (2023) for learning stabilizing controllers—has adopted the following closed-form solution, which is differentiable almost everywhere:

$$\mathcal{P}(f_\theta)(x) = \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z - f_\theta(x)\|_2 \text{ s.t. } a(x)^\top z \leq b(x) \quad (2)$$

$$= f_\theta(x) - \frac{a(x)}{\|a(x)\|^2} \text{ReLU}(a(x)^\top f_\theta(x) - b(x)). \quad (3)$$

**Example 1**  $a(x) = [-1; x]$  and  $b(x) = 0$  encode the constraint  $(f(x))_{(0)} \geq x(f(x))_{(1)}$  on  $f : \mathbb{R} \rightarrow \mathbb{R}^2$ . Then, a sample  $f_\theta(1) = [3; 5]$  is projected to  $\mathcal{P}(f_\theta)(1) = [4; 4]$ , satisfying the constraint.

Nonetheless, the formulation is limited to enforcing *only a single* inequality constraint. Moreover, its empirical success in learning the desired functions has not been theoretically

understood. To that end, we propose HardNet-Aff, *the first method, to the best of our knowledge, that enables efficient (closed-form) and differentiable enforcement of more than one input-dependent inequality constraint*. In addition, we provide a rigorous explanation for its expressivity through universal approximation guarantees. Then, we discuss HardNet-Cvx as a conceptual framework to satisfy general input-dependent convex constraints exploiting differentiable convex optimization solvers.

#### 4.1 HardNet-Aff: Imposing Input-Dependent Affine Constraints

Suppose we have multiple input-dependent affine constraints in an aggregated form:

$$b^l(x) \leq A(x)f(x) \leq b^u(x) \quad \forall x \in \mathcal{X}, \quad (4)$$

where  $A(x) \in \mathbb{R}^{n_c \times n_{\text{out}}}$  and  $b^l(x), b^u(x) \in \mathbb{R}^{n_c}$  for  $2n_c$  inequality constraints.

**Remark 3** *The constraint form in (4) is general and includes equality constraints by setting  $b^l = b^u$ . Another approach to enforcing equality constraints is to have the neural network predict only a subset of the outputs, with the remaining components computed to satisfy the equality constraints, as in Beucler et al. (2021) and Donti et al. (2021b). However, that method may fail if the chosen subset is invalid for certain inputs. For example, the constraint  $[x \ x-1]f(x)=1$  on  $f: \mathbb{R} \rightarrow \mathbb{R}^2$  prevents either component from being a free variable at both  $x=0$  and 1. See Appendix B for incorporating this approach into our method.*

**Remark 4** *One-sided inequality constraints can be represented by setting  $b^l = -\infty$  or  $b^u = \infty$ . In addition, different types of constraints (inequality and equality) can be combined by specifying  $b^l$  and  $b^u$  component-wise.*

**Assumption 5** *For each  $x \in \mathcal{X}$ , i) there exists  $y \in \mathbb{R}^{n_{\text{out}}}$  that satisfies the constraints in (4), and ii)  $A(x)$  has full row rank.*

The first assumption says that the constraints (4) are feasible, while the second one requires  $n_c \leq n_{\text{out}}$ . Under the assumptions, we propose HardNet-Aff by developing a novel closed-form projection that enforces the constraints (4) as below:

$$\text{HardNet-Aff: } \mathcal{P}(f_\theta)(x) = f_\theta(x) + A(x)^+ [\text{ReLU}(b^l(x) - A(x)f_\theta(x)) - \text{ReLU}(A(x)f_\theta(x) - b^u(x))], \quad (5)$$

for all  $x \in \mathcal{X}$  where  $M^+ := M^\top (MM^\top)^{-1}$  denotes the pseudoinverse of a matrix  $M$ . Note that the projection in (5) generalizes the single-constraint case in (3) with  $n_c = 1$  and  $b^l = -\infty$ . However, unlike (3), HardNet-Aff in general does not perform the minimum  $\ell^2$ -norm projection as in (2). Instead, we can characterize its projection through the following optimization problem; see Appendix A.1 for a proof.

**Proposition 6** *Under Assumption 5, for any parameterized function  $f_\theta : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}}}$ , HardNet-Aff in (5) satisfies*

$$\begin{aligned} \mathcal{P}(f_\theta)(x) &= \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z - f_\theta(x)\|_2 \\ &\text{s.t. } z \in \left\{ \arg \min_{y \in \mathbb{R}^{n_{\text{out}}}} \|A(x)(y - f_\theta(x))\|_2 \text{ s.t. } b^l(x) \leq A(x)y \leq b^u(x) \right\}. \end{aligned} \quad (6)$$

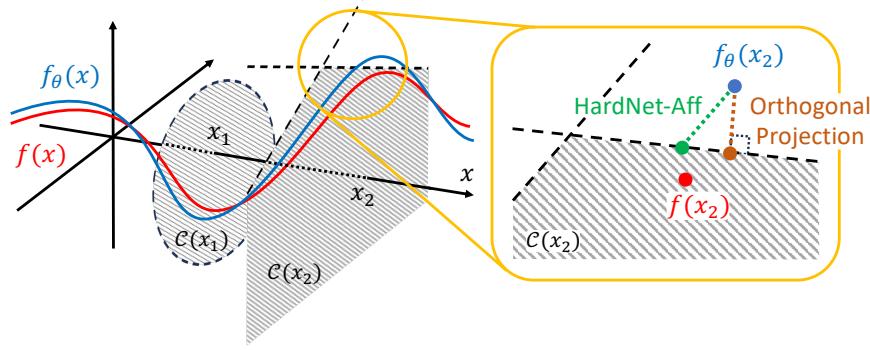


Figure 2: Illustration of input-dependent constraints and projections performed by HardNet. A target function  $f: \mathbb{R} \rightarrow \mathbb{R}^2$  satisfies hard constraints  $f(x) \in \mathcal{C}(x)$  for each  $x \in \mathbb{R}$ . The feasible set  $\mathcal{C}(x)$  is visualized as the gray area for two sample inputs  $x_1$  and  $x_2$ . While the function  $f_\theta$  closely approximates  $f$ , it violates the constraints. HardNet-Aff projects the violated output onto the feasible set in parallel to the boundaries of the satisfied constraints. In contrast, the minimum  $\ell^2$ -norm optimization in (1) projects the output orthogonally to the closest boundary.

Thus, HardNet-Aff satisfies the constraint (4) while minimally altering the output from the plain output  $f_\theta(x)$  in the sense of (6). We note that the inner optimization in (6) has infinitely many solutions when  $A(x)$  has a non-zero null space (i.e.,  $n_c < n_{\text{out}}$ ). In such cases, HardNet-Aff chooses the solution that is closest (in Euclidean distance) to the plain output  $f_\theta(x)$ . On the other hand, for a square matrix  $A(x)$ , the inner optimization has a unique solution while the square of its objective function is the Bregman divergence generated from the function  $\psi_x(y) = \|A(x)y\|_2^2$ .

In addition to the optimization formulation, HardNet-Aff can also be understood geometrically through the following property; see Appendix A.2 for a proof.

**Proposition 7 (Parallel Projection)** *Under Assumption 5, for any parameterized function  $f_\theta: \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}}}$ , for each  $i$ -th row  $a_i \in \mathbb{R}^{n_c}$  of  $A(x)$ , HardNet-Aff in (5) satisfies*

$$a_i^\top \mathcal{P}(f_\theta)(x) = \begin{cases} b_{(i)}^l(x) & \text{if } a_i^\top f_\theta(x) < b_{(i)}^l(x) \\ b_{(i)}^u(x) & \text{if } a_i^\top f_\theta(x) > b_{(i)}^u(x) \\ a_i^\top f_\theta(x) & \text{o.w.} \end{cases} \quad \text{for all } x \in \mathcal{X}. \quad (7)$$

If  $f_\theta(x)$  violates any constraints, it is projected onto the boundary of the feasible set ( $a_i^\top \mathcal{P}(f_\theta)(x) = b_{(i)}^l(x)$  or  $b_{(i)}^u(x)$ ). Notably, the projection alters the output in a direction parallel to the boundary of each satisfied constraint's feasible set ( $a_i^\top \mathcal{P}(f_\theta)(x) = a_i^\top f_\theta(x)$ ). This parallel projection is illustrated in Fig. 2.

While HardNet-Aff guarantees the satisfaction of the hard constraints (4), it should not lose the neural networks' expressivity for practical deployment. To that end, we rigorously show that HardNet-Aff preserves the neural networks' expressivity by the following theorem; see Appendix A.3 for a proof.

**Theorem 8** Consider input-dependent constraints (4) that satisfy assumption 5. Suppose  $\mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$  is compact, and  $A(x)$  is continuous over  $\mathcal{X}$ . Then, for any function classes  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset \mathcal{C}(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$  (or  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$  for any  $p \in [1, \infty)$ ) and the projection  $\mathcal{P}$  of HardNet-Aff in (5), if  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ ,  $\mathcal{F}_{\text{HardNet-Aff}} := \{\mathcal{P}(f_{\text{NN}}) | f_{\text{NN}} \in \mathcal{F}_{\text{NN}}\}$  universally approximates  $\mathcal{F}_{\text{target}} := \{f_t \in \mathcal{F} | f_t \text{ satisfies (4)}\}$ .

Considering  $\mathcal{F}_{\text{NN}}$  as the function class of plain neural networks, this theorem shows that HardNet-Aff preserves their expressivity over  $\mathcal{F}$  under the constraints (4). The main idea behind this theorem is that for HardNet-Aff in (5),  $\|f - \mathcal{P}(f_{\theta})\|$  could be bounded in terms of  $\|f - f_{\theta}\|$ . By selecting  $f_{\theta}$  such that  $\|f - f_{\theta}\|$  is arbitrarily small, we can make  $\mathcal{P}(f_{\theta})$  approach the target function  $f$  as closely as desired. The existence of such an  $f_{\theta}$  can be guaranteed by existing universal approximation theorems on plain neural networks. For instance, if we utilize Theorem 2 in Theorem 8, we can obtain the following universal approximation theorem for HardNet-Aff.

**Corollary 9** Suppose the assumptions of Theorem 8 hold. Then, for any  $p \in [1, \infty)$ , HardNet-Aff with  $w$ -width ReLU neural networks defined in (5) universally approximates  $\mathcal{F}_{\text{target}} := \{f_t \in L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}}) | f_t \text{ satisfies (4)}\}$  if  $w \geq \max\{n_{\text{in}} + 1, n_{\text{out}}\}$ .

#### 4.2 HardNet-Cvx: Imposing Input-Dependent Convex Constraints

Going beyond affine constraints, we discuss HardNet-Cvx as a conceptual framework for enforcing general input-dependent convex constraints  $f(x) \in \mathcal{C}(x) \forall x \in \mathcal{X}$  where  $\mathcal{C}(x) \subset \mathbb{R}^{n_{\text{out}}}$  is a convex set. Unlike the affine case, the closed-form projection from the single-constraint case in (3) does not extend to general convex constraints. Thus, we present HardNet-Cvx by generalizing the optimization-based projection in (2) as below:

$$\text{HardNet-Cvx} : \mathcal{P}(f_{\theta})(x) = \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z - f_{\theta}(x)\|_2 \text{ s.t. } z \in \mathcal{C}(x), \quad (8)$$

for all  $x \in \mathcal{X}$ . While no general closed-form solution for this optimization problem exists, we can employ differentiable convex optimization solvers for an implementation of HardNet-Cvx such as Amos and Kolter (2017) for affine constraints (when HardNet-Aff cannot be applied) and Agrawal et al. (2019) for more general convex constraints. This idea was briefly mentioned by Donti et al. (2021b) and used as a baseline (for input-independent constraints) by Tordesillas et al. (2023). We present HardNet-Cvx as a general framework, independent of specific implementation methods, to complement HardNet-Aff and provide a unified solution for various constraint types.

As in Section 4.1, we demonstrate that HardNet-Cvx preserves the expressive power of neural networks by proving the following universal approximation theorem; see Appendix A.4 for a proof.

**Theorem 10** Consider input-dependent sets  $\mathcal{C}(x) \subset \mathbb{R}^{n_{\text{out}}}$  that are convex for all  $x \in \mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$ . Then, for any  $p \in [1, \infty)$ , HardNet-Cvx with  $w$ -width ReLU neural networks defined in (8) universally approximates  $\mathcal{F}_{\text{target}} := \{f_t \in L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}}) | f_t(x) \in \mathcal{C}(x) \forall x \in \mathcal{X}\}$  if  $w \geq \max\{n_{\text{in}} + 1, n_{\text{out}}\}$ .

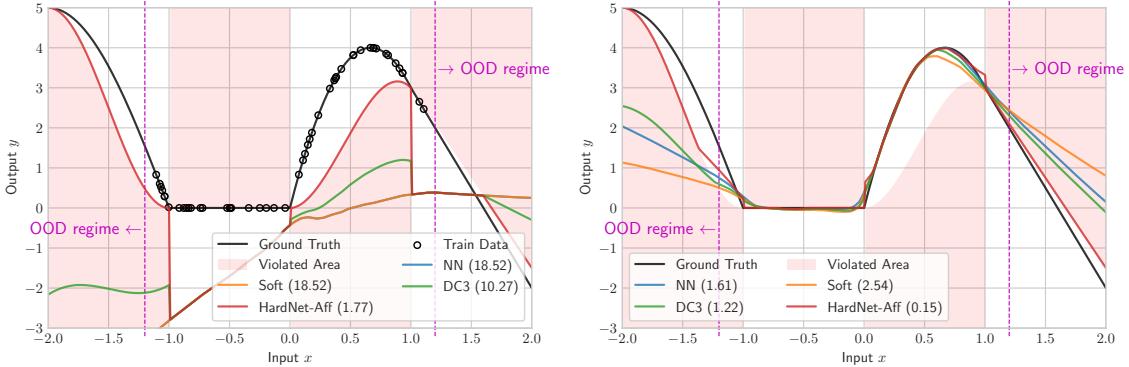


Figure 3: Learned functions at the initial (left) and final (right) epochs with the piecewise constraints. The models are trained on the samples indicated with circles, with their MSE from the true function shown in parentheses. HardNet-Aff adheres to the constraints from the start of the training and generalizes better than the baselines as it enforces constraints even in the out-of-distribution (OOD) regime. On the other hand, the baselines violate the constraints throughout the training.

## 5 Experiments

In this section, we demonstrate the versatility and effectiveness of HardNet-Aff over three constrained scenarios: learning with piecewise constraints, learning optimization solvers with guaranteed feasibility, and optimizing control policies in safety-critical systems.

As evaluation metrics, we measure the violation of constraints in addition to the application-specific performance metrics. For a test sample  $x \in \mathcal{X}$  and  $n_{\text{ineq}}$  inequality constraints  $g_x(f(x)) \leq 0 \in \mathbb{R}^{n_{\text{ineq}}}$ , their violation is measured with the maximum ( $\leq \max$ ) and mean ( $\leq \text{mean}$ ) of  $\text{ReLU}(g_x(f(x)))$  and the number of violated constraints ( $\leq \#\right)$ . Similar quantities of  $|h_x(f(x))|$  are measured for  $n_{\text{eq}}$  equality constraints  $h_x(f(x)) = 0 \in \mathbb{R}^{n_{\text{eq}}}$ . Then, they are averaged over all test samples. The inference time ( $T_{\text{test}}$ ) for the test set and the training time ( $T_{\text{train}}$ ) are also compared.

We compare HardNet with the following baselines: (i) **NN**: Plain neural networks, (ii) **Soft**: Soft-constrained neural networks, where constraint violations are penalized by adding regularization terms  $\lambda \|\text{ReLU}(g_x(f(x_s)))\|_2^2 + \lambda \|h_x(f(x_s))\|_2^2$  to the loss function for each sample  $x_s \in \mathcal{X}$ , (iii) **DC3** (Donti et al., 2021b): Similarly to HardNet-Aff, DC3 approximates part of the target function with a neural network. It first augments the output to satisfy equality constraints, then corrects it using gradient descent to minimize inequality violations. DC3 backpropagates through this iterative correction procedure to train the model. All methods use 3-layer fully connected neural networks with 200 neurons per hidden layer and ReLU activation. The results are produced with Intel Xeon Gold 6248 and NVidia Volta V100.

Table 2: Results for learning with the piecewise constraints. **HardNet-Aff** generalizes better than the baselines with the smallest MSE from the true function without any constraint violation. The max and mean of constraint violations are computed over 401 test samples. Better (resp. worse) values are colored greener (resp. redder). Standard deviations over 5 runs are shown in parentheses.

	MSE	max violation	mean violation	$T_{\text{test}}$ (ms)	$T_{\text{train}}$ (s)
NN	1.85 (0.19)	3.16 (0.29)	0.60 (0.04)	0.14 (0.00)	2.24 (0.09)
Soft	2.36 (0.22)	3.70 (0.25)	0.69 (0.03)	0.15 (0.02)	3.86 (0.03)
DC3	1.15 (0.10)	2.31 (0.23)	0.43 (0.02)	6.02 (0.07)	15.67 (0.82)
<b>HardNet-Aff</b>	0.16 (0.01)	0.00 (0.00)	0.00 (0.00)	0.88 (0.05)	5.62 (0.06)

Table 3: Results for learning solvers of nonconvex optimization problems with 100 variables, 50 equality constraints, and 50 inequality constraints. **HardNet-Aff** attain feasible solutions with the smallest suboptimality gap among the feasible methods. The max, mean, and the number of violations are computed out of the 50 constraints. Better (resp. worse) values are colored greener (resp. redder). Standard deviations over 5 runs are shown in parentheses.

	Obj. val	$\not\leq$ max/mean/#	$\neq$ max/mean/#	$T_{\text{test}}$ (ms)	$T_{\text{train}}$ (s)
Optimizer	-14.28 (0.00)	0.0/0.0/0.0 (0.0/0.0/0.0)	0.0/0.0/0.0 (0.0/0.0/0.0)	1182.0 (3.49)	-
NN	-27.43 (0.00)	12.1/1.1/12.0 (0.0/0.0/0.0)	15.1/6.4/50.0 (0.0/0.0/0.0)	0.32 (0.06)	78.10 (2.36)
Soft	-13.13 (0.01)	0.0/0.0/0.0 (0.0/0.0/0.0)	0.4/0.1/50.0 (0.0/0.0/0.0)	0.37 (0.07)	77.58 (0.97)
DC3	-12.57 (0.04)	0.0/0.0/0.0 (0.0/0.0/0.0)	0.0/0.0/0.0 (0.0/0.0/0.0)	9.61 (0.47)	3606.74 (2.45)
<b>HardNet-Aff</b>	-14.10 (0.01)	0.0/0.0/0.0 (0.0/0.0/0.0)	0.0/0.0/0.0 (0.0/0.0/0.0)	6.69 (0.06)	1343.80 (1.39)

### 5.1 Learning with Piecewise Constraints

In this experiment, we demonstrate the efficacy of **HardNet-Aff** and the expressive power of input-dependent constraints on a problem involving learning a function  $f : [-2, 2] \rightarrow \mathbb{R}$  with piecewise constraints shown in Fig. 3. The function outputs are required to avoid specific regions defined over separate subsets of the domain  $[-2, 2]$ . An arbitrary number of such piecewise constraints can be captured by a single input-dependent affine constraint. The models are trained on 50 labeled data points randomly sampled from  $[-1.2, 1.2]$ ; see Appendix D.1 for details. Additionally, we assess **HardNet-Aff** with more complex constraints in which each regime is governed by both upper and lower bounds (or, in the degenerate case, an equality) in Appendix D.2.

As shown in Fig. 3 and Table 2, **HardNet-Aff** consistently satisfies the hard constraints throughout training and achieves better generalization than the baselines, which violate these constraints. Especially at the boundaries  $x = -1$  and  $x = 1$  in the initial epoch results, the jumps in DC3’s output value, caused by DC3’s correction process, insufficiently reduce the constraint violations. The performance of its iterative correction process heavily depends on the number of gradient descent steps and the step size. DC3 requires careful hyperparameter tuning unlike **HardNet-Aff**.

Table 4: Results for optimizing safe control policies. HardNet-Aff generates trajectories without constraint violation and has the smallest costs among the methods with zero violation. The max and mean constraint violations are computed for the violations accumulated throughout the trajectories. Better values are colored greener. Standard deviations over 5 runs are shown in parentheses.

	Cost	max violation	mean violation	$T_{\text{test}}$ (ms)	$T_{\text{train}}$ (min)
CBF-QP	948.32 (0.00)	0.00 (0.00)	0.00 (0.00)	579.29 (4.60)	-
NN	421.92 (0.15)	157.62 (0.90)	118.92 (0.55)	0.23 (0.01)	256.34 (4.01)
Soft	480.10 (0.54)	6.92 (0.05)	3.95 (0.10)	0.22 (0.00)	255.07 (0.77)
DC3	480.21 (0.71)	6.86 (0.13)	3.88 (0.12)	15.71 (0.29)	637.69 (6.71)
HardNet-Aff	518.85 (8.71)	0.00 (0.00)	0.00 (0.00)	2.71 (0.06)	370.05 (3.42)

## 5.2 Learning Optimization Solvers with Guaranteed Feasibility

We consider learning optimization solvers with the following nonconvex optimization as in (Donti et al., 2021b):

$$f(x) = \arg \min_y \frac{1}{2} y^\top Q y + p^\top \sin y \quad \text{s.t. } Ay \leq b, Cy = x,$$

where  $Q \in \mathbb{R}^{n_{\text{out}} \times n_{\text{out}}} \succeq 0$ ,  $p \in \mathbb{R}^{n_{\text{out}}}$ ,  $A \in \mathbb{R}^{n_{\text{ineq}} \times n_{\text{out}}}$ ,  $b \in \mathbb{R}^{n_{\text{ineq}}}$ ,  $C \in \mathbb{R}^{n_{\text{eq}} \times n_{\text{out}}}$  are constants and  $\sin$  is the element-wise sine function. The target function  $f$  outputs the solution of each optimization problem instance determined by the input  $x \in [-1, 1]^{n_{\text{eq}}}$ . The main benefit of learning this nonconvex optimization solver with neural networks is their faster inference time than optimizers based on iterative methods. To ensure that the learned neural networks provide feasible solutions, the constraints of the optimization problems are set as hard constraints.

In this experiment, we guarantee that the given constraints are feasible for all  $x \in [-1, 1]^{n_{\text{eq}}}$  by computing a proper  $b$  for randomly generated  $A, C$  as described in (Donti et al., 2021b). Then the models are trained on 10000 unlabeled data points uniformly sampled from  $[-1, 1]^{n_{\text{eq}}}$ . For this unsupervised learning task, the loss function for each sample  $x_s$  is set as  $\frac{1}{2} f_\theta(x_s)^\top Q f_\theta(x_s) + p^\top \sin f_\theta(x_s)$ . To reproduce similar results as in (Donti et al., 2021b), the models are equipped with additional batch normalization and dropout layers in this experiment. As shown in Table 3, HardNet-Aff consistently finds feasible solutions with a small suboptimality gap from the optimizer (IPOPT) with a much shorter inference time.

## 5.3 Optimizing Control Policies in Safety-Critical Systems

In this experiment, we apply HardNet-Aff to enforce safety constraints in control systems. Consider a control-affine system with its known dynamics  $f$  and  $g$ :  $\dot{x}(t) = f(x(t)) + g(x(t))u(t)$ , where  $x(t) \in \mathbb{R}^{n_{\text{in}}}$  is the system state, and  $u(t) \in \mathbb{R}^{n_{\text{out}}}$  is the control input at time  $t$ . For safety reasons (e.g., avoiding obstacles), the system requires  $x(t) \in \mathcal{X}_{\text{safe}} \subset \mathbb{R}^{n_{\text{in}}}$  for all  $t$ . We translate this safety condition into a state-dependent affine constraint on the control input using a control barrier function (CBF)  $h : \mathbb{R}^{n_{\text{in}}} \rightarrow \mathbb{R}$  (Ames et al., 2019). Suppose its super-level set  $\{x \in \mathbb{R}^{n_{\text{in}}} | h(x) \geq 0\} \subset \mathcal{X}_{\text{safe}}$  and  $h(x(0)) \geq 0$ . Then, we can ensure

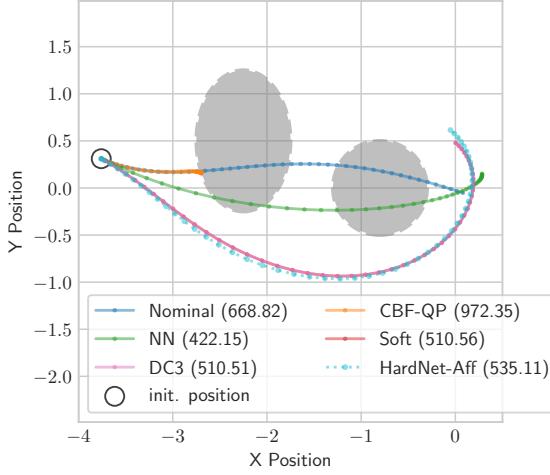


Figure 4: Simulated trajectories from a random initial state, with costs shown in parentheses. HardNet-Aff avoids the obstacles while obtaining a low cost value. Even though the soft-constrained method and DC3 appear to avoid obstacles and achieve smaller costs than the other collision-free trajectories, they violate the safety constraints (which are more conservative than hitting the obstacles).

$h(x(t)) \geq 0 \forall t \geq 0$  by guaranteeing

$$\dot{h}(x) = \nabla h(x)^\top (f(x) + g(x)\pi(x)) \geq -\alpha h(x) \quad (9)$$

at each  $x(t)$  for a state-feedback control policy  $\pi : \mathbb{R}^{n_{\text{in}}} \rightarrow \mathbb{R}^{n_{\text{out}}}$  with some  $\alpha > 0$ . Enforcing (9) for multiple CBFs ensures the trajectory remains within the intersection of the corresponding safe sets.

We consider controlling a unicycle system to minimize the cost over trajectories while avoiding collisions with two elliptical obstacles, each presented with a CBF (see Appendix D.3 for details). Then, we can formulate the problem as an optimization problem with its objective function being the expected cost over the trajectory  $x(t)$  generated by a parameterized state feedback policy  $\pi_\theta : \mathbb{R}^{n_{\text{in}}} \rightarrow \mathbb{R}^{n_{\text{out}}}$  from random initial point  $x(0) \sim \mathcal{D}$ :

$$\arg \min_{\theta} \mathbb{E}_{x(0) \sim \mathcal{D}} \int_{t=0}^T [x^\top Q x + \pi_\theta(x)^\top R \pi_\theta(x)] dt \quad \text{s.t. (9) holds for all CBFs } \forall t \in [0, T] \forall i \quad (10)$$

where  $Q$  is the state cost matrix and  $R$  is the control cost matrix.

Given a nominal controller  $\pi_{\text{nom}} : \mathbb{R}^{n_{\text{in}}} \rightarrow \mathbb{R}^{n_{\text{out}}}$  designed without considering obstacles, a conventional approach to find a safe controller is to solve the following quadratic program at each  $x(t)$ :

$$\text{CBF-QP} : \pi_{\text{CBF-QP}}(x) = \arg \min_u \|u - \pi_{\text{nom}}(x)\|_2 \quad \text{s.t. (9) holds for all CBFs.}$$

The downside of this method is that the controller cannot optimize a cost/reward over trajectories, as it only stays close to the nominal controller. Instead, we can do so by training

neural network policies  $\pi_\theta(x) := \pi_{\text{nom}}(x) + f_\theta(x)$  with neural networks  $f_\theta$ . For computation, we approximate (10) by minimizing the costs of rolled-out trajectories from randomly sampled initial states. As shown in Fig. 4 and Table 4, HardNet-Aff consistently guarantees safe trajectories with low costs.

## 6 Conclusion

In this paper, we presented HardNet, a practical framework for constructing neural networks that inherently satisfy input–output constraints. We proved that imposing these hard constraints does not limit the expressive power of these neural networks by providing universal approximation guarantees. We demonstrated the utility and versatility of our method across several applications, such as learning with piecewise constraints, learning optimization solvers with guaranteed feasibility, and optimizing control policies in safety-critical systems. Using HardNet in other application domains that benefit from incorporating domain-specific knowledge is a promising direction for future work. One such example is in Tang et al. (2024). Also, we aim to explore developing methods for performing fast projections for problems with more general constraints. Lastly, extending our approach to support other forms of inductive biases, such as equivariances and invariances, would potentially be of great interest.

### ACKNOWLEDGMENTS

The authors thank Anoopkumar Sonar for his help during the early development of this manuscript. The authors acknowledge the MIT SuperCloud and Lincoln Laboratory Supercomputing Center for providing computing resources that have contributed to the results reported within this paper. This work was supported in part by MathWorks, the MIT-IBM Watson AI Lab, the MIT-Amazon Science Hub, and the MIT-Google Program for Computing Innovation.

## References

- A. Agrawal, B. Amos, S. Barratt, S. Boyd, S. Diamond, and J. Z. Kolter. Differentiable convex optimization layers. *Advances in neural information processing systems*, 32, 2019.
- K. Ahmed, S. Teso, K.-W. Chang, G. Van den Broeck, and A. Vergari. Semantic probabilistic layers for neuro-symbolic learning. *Advances in Neural Information Processing Systems*, 35:29944–29959, 2022.
- A. Albarghouthi et al. Introduction to neural network verification. *Foundations and Trends® in Programming Languages*, 7(1–2):1–157, 2021.
- A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada. Control barrier functions: Theory and applications. In *2019 18th European control conference (ECC)*, pages 3420–3431. IEEE, 2019.
- B. Amos and J. Z. Kolter. Optnet: Differentiable optimization as a layer in neural networks. In *International Conference on Machine Learning*, pages 136–145. PMLR, 2017.

- G. Anderson, A. Verma, I. Dillig, and S. Chaudhuri. Neurosymbolic reinforcement learning with formally verified exploration. *Advances in neural information processing systems*, 33: 6172–6183, 2020.
- S. Badreddine, A. d. Garcez, L. Serafini, and M. Spranger. Logic tensor networks. *Artificial Intelligence*, 303:103649, 2022.
- R. Balestriero and Y. LeCun. Police: Provably optimal linear constraint enforcement for deep neural networks. In *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1–5. IEEE, 2023.
- O. Bastani, Y. Pu, and A. Solar-Lezama. Verifiable reinforcement learning via policy extraction. *Advances in neural information processing systems*, 31, 2018.
- O. Bastani, S. Li, and A. Xu. Safe reinforcement learning via statistical model predictive shielding. In *Robotics: Science and Systems*, pages 1–13, 2021.
- T. Beucler, M. Pritchard, S. Rasp, J. Ott, P. Baldi, and P. Gentine. Enforcing analytic constraints in neural networks emulating physical systems. *Physical review letters*, 126(9): 098302, 2021.
- R. A. Brown, E. Schmerling, N. Azizan, and M. Pavone. A unified view of sdp-based neural network verification through completely positive programming. In *International conference on artificial intelligence and statistics*, pages 9334–9355. PMLR, 2022.
- R. Bunel, I. Turkaslan, P. H. Torr, P. Kohli, and M. P. Kumar. A unified view of piecewise linear neural network verification. In *Proceedings of the 32nd International Conference on Neural Information Processing Systems*, NIPS’18, page 4795–4804. Curran Associates Inc., 2018.
- L. Chamon and A. Ribeiro. Probably approximately correct constrained learning. *Advances in Neural Information Processing Systems*, 33:16722–16735, 2020.
- L. F. Chamon, S. Paternain, M. Calvo-Fullana, and A. Ribeiro. Constrained learning with non-convex losses. *IEEE Transactions on Information Theory*, 69(3):1739–1760, 2023.
- H. Chen, G. E. C. Flores, and C. Li. Physics-informed neural networks with hard linear equality constraints. *Computers & Chemical Engineering*, 189:108764, 2024.
- W. Chen, M. Tanneau, and P. Van Hentenryck. End-to-end feasible optimization proxies for large-scale economic dispatch. *IEEE Transactions on Power Systems*, 39(2):4723–4734, 2023.
- G. Cybenko. Approximation by superpositions of a sigmoidal function. *Mathematics of control, signals and systems*, 2(4):303–314, 1989.
- A. Dener, M. A. Miller, R. M. Churchill, T. Munson, and C.-S. Chang. Training neural networks under physical constraints using a stochastic augmented lagrangian approach. *arXiv preprint arXiv:2009.07330*, 2020.

- M. Ding and G. Fan. Multilayer joint gait-pose manifolds for human gait motion modeling. *IEEE Transactions on Cybernetics*, 45(11):2413–2424, 2014.
- P. L. Donti, M. Roderick, M. Fazlyab, and J. Z. Kolter. Enforcing robust control guarantees within neural network policies. In *International Conference on Learning Representations*, 2021a.
- P. L. Donti, D. Rolnick, and J. Z. Kolter. DC3: A learning method for optimization with hard constraints. In *International Conference on Learning Representations*, 2021b.
- R. Ehlers. Formal verification of piece-wise linear feed-forward neural networks. In *Automated Technology for Verification and Analysis: 15th International Symposium, ATVA 2017, Pune, India, October 3–6, 2017, Proceedings 15*, pages 269–286. Springer, 2017.
- Y. Y. Elboher, J. Gottschlich, and G. Katz. An abstraction-based framework for neural network verification. In *Computer Aided Verification: 32nd International Conference, CAV 2020, Los Angeles, CA, USA, July 21–24, 2020, Proceedings, Part I*, page 43–65. Springer-Verlag, 2020. ISBN 978-3-030-53287-1. doi: 10.1007/978-3-030-53288-8\_3.
- M. Fazlyab, M. Morari, and G. J. Pappas. Safety verification and robustness analysis of neural networks via quadratic constraints and semidefinite programming. *IEEE Transactions on Automatic Control*, 67(1):1–15, 2020.
- M. Fischer, M. Balunovic, D. Drachsler-Cohen, T. Gehr, C. Zhang, and M. Vechev. Dl2: training and querying neural networks with logic. In *International Conference on Machine Learning*, pages 1931–1941. PMLR, 2019.
- T. Frerix, M. Nießner, and D. Cremers. Homogeneous linear inequality constraints for neural network activations. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pages 748–749, 2020.
- E. Giunchiglia and T. Lukasiewicz. Coherent hierarchical multi-label classification networks. *Advances in neural information processing systems*, 33:9662–9673, 2020.
- E. Giunchiglia, A. Tatmir, M. C. Stoian, and T. Lukasiewicz. Ccn+: A neuro-symbolic framework for deep learning with requirements. *International Journal of Approximate Reasoning*, page 109124, 2024.
- B. Hanin and M. Sellke. Approximating continuous functions by relu nets of minimal width. *arXiv preprint arXiv:1710.11278*, 2017.
- K. Hornik, M. Stinchcombe, and H. White. Multilayer feedforward networks are universal approximators. *Neural networks*, 2(5):359–366, 1989.
- I. Hounie, A. Ribeiro, and L. F. Chamon. Resilient constrained learning. *Advances in Neural Information Processing Systems*, 36:71767–71798, 2023.
- D. Huang, H. Zhang, X. Song, and R. Shibasaki. Differentiable projection for constrained deep learning. *arXiv preprint arXiv:2111.10785*, 2021.

- H. Huang, D. Wang, R. Walters, and R. Platt. Equivariant transporter network. *arXiv preprint arXiv:2202.09400*, 2022.
- P. Kidger and T. Lyons. Universal approximation with deep narrow networks. In *Conference on learning theory*, pages 2306–2327. PMLR, 2020.
- J. Z. Kolter and G. Manek. Learning stable deep dynamics models. *Advances in neural information processing systems*, 32, 2019.
- A. V. Konstantinov and L. V. Utkin. A new computationally simple approach for implementing neural networks with output hard constraints. In *Doklady Mathematics*, volume 108, pages S233–S241. Springer, 2023.
- A. Kratsios, B. Zamanlooy, T. Liu, and I. Dokmanić. Universal approximation under constraints is possible with transformers. *arXiv preprint arXiv:2110.03303*, 2021.
- M. Leshno, V. Y. Lin, A. Pinkus, and S. Schocken. Multilayer feedforward networks with a nonpolynomial activation function can approximate any function. *Neural networks*, 6(6):861–867, 1993.
- X. Li, J. Deng, J. Wu, S. Zhang, W. Li, and Y.-G. Wang. Physical informed neural networks with soft and hard boundary constraints for solving advection-diffusion equations using fourier expansions. *Computers & Mathematics with Applications*, 159:60–75, 2024. ISSN 0898-1221. doi: <https://doi.org/10.1016/j.camwa.2024.01.021>.
- T. Lin and H. Zha. Riemannian manifold learning. *IEEE transactions on pattern analysis and machine intelligence*, 30(5):796–809, 2008.
- C. Liu, T. Arnon, C. Lazarus, C. Strong, C. Barrett, and M. J. Kochenderfer. Algorithms for verifying deep neural networks. *Foundations and Trends® in Optimization*, 4(3-4):244–404, 2021. ISSN 2167-3888. doi: 10.1561/2400000035.
- Z. Lu, H. Pu, F. Wang, Z. Hu, and L. Wang. The expressive power of neural networks: A view from the width. *Advances in neural information processing systems*, 30, 2017.
- R. Manhaeve, S. Dumancic, A. Kimmig, T. Demeester, and L. De Raedt. Deepproblog: Neural probabilistic logic programming. *Advances in neural information processing systems*, 31, 2018.
- P. Márquez-Neila, M. Salzmann, and P. Fua. Imposing hard constraints on deep networks: Promises and limitations. *arXiv preprint arXiv:1706.02025*, 2017.
- A. J. McNeil, R. Frey, and P. Embrechts. *Quantitative risk management: concepts, techniques and tools-revised edition*. Princeton university press, 2015.
- Y. Min, S. M. Richards, and N. Azizan. Data-driven control with inherent lyapunov stability. In *2023 62nd IEEE Conference on Decision and Control (CDC)*, pages 6032–6037. IEEE, 2023.

- O. Oktay, E. Ferrante, K. Kamnitsas, M. Heinrich, W. Bai, J. Caballero, S. A. Cook, A. De Marvao, T. Dawes, D. P. O'Regan, et al. Anatomically constrained neural networks (acnnns): application to cardiac image enhancement and segmentation. *IEEE transactions on medical imaging*, 37(2):384–395, 2017.
- S. Park, C. Yun, J. Lee, and J. Shin. Minimum width for universal approximation. In *International Conference on Learning Representations*, 2021.
- D. Pathak, P. Krahenbuhl, and T. Darrell. Constrained convolutional neural networks for weakly supervised segmentation. In *Proceedings of the IEEE international conference on computer vision*, pages 1796–1804, 2015.
- A. Pinkus. Approximation theory of the MLP model in neural networks. *Acta numerica*, 8: 143–195, 1999.
- C. Pryor, C. Dickens, E. Augustine, A. Albalak, W. Y. Wang, and L. Getoor. Neupsl: neural probabilistic soft logic. In *Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence*, pages 4145–4153, 2023.
- C. Qin, K. D. Djivjotham, B. O'Donoghue, R. Bunel, R. Stanforth, S. Gowal, J. Uesato, G. Swirszcz, and P. Kohli. Verification of non-linear specifications for neural networks. In *International Conference on Learning Representations*, 2019.
- M. Raissi, P. Perdikaris, and G. E. Karniadakis. Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. *Journal of Computational physics*, 378:686–707, 2019.
- H. Ryu, H.-i. Lee, J.-H. Lee, and J. Choi. Equivariant descriptor fields: Se (3)-equivariant energy-based models for end-to-end visual robotic manipulation learning. *arXiv preprint arXiv:2206.08321*, 2022.
- Y. S. Shao, C. Chen, S. Kousik, and R. Vasudevan. Reachability-based trajectory safeguard (rts): A safe and fast reinforcement learning safety layer for continuous control. *IEEE Robotics and Automation Letters*, 6(2):3663–3670, 2021.
- A. Simeonov, Y. Du, A. Tagliasacchi, J. B. Tenenbaum, A. Rodriguez, P. Agrawal, and V. Sitzmann. Neural descriptor fields: Se (3)-equivariant object representations for manipulation. In *2022 International Conference on Robotics and Automation (ICRA)*, pages 6394–6400. IEEE, 2022.
- M. Sotoudeh and A. V. Thakur. Provable repair of deep neural networks. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, pages 588–603, 2021.
- M. C. Stoian, E. Giunchiglia, and T. Lukasiewicz. Exploiting t-norms for deep learning in autonomous driving. In *International Workshop on NeuralSymbolic Learning and Reasoning*, 2023.

- M. C. Stoian, S. Dyrmishi, M. Cordy, T. Lukasiewicz, and E. Giunchiglia. How realistic is your synthetic data? constraining deep generative models for tabular data. In *The Twelfth International Conference on Learning Representations*, 2024.
- S. Tang, T. Sapsis, and N. Azizan. Learning chaotic dynamics with embedded dissipativity. *arXiv preprint arXiv:2410.00976*, 2024.
- Z. Tao and A. Thakur. Provable editing of deep neural networks using parametric linear relaxation. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*, 2024.
- M. Tayal, B. G. Goswami, K. Rajgopal, R. Singh, T. Rao, J. Keshavan, P. Jagtap, and S. Kolathaya. A collision cone approach for control barrier functions. *arXiv preprint arXiv:2403.07043*, 2024.
- V. Tjeng, K. Y. Xiao, and R. Tedrake. Evaluating robustness of neural networks with mixed integer programming. In *International Conference on Learning Representations*, 2019.
- J. Tordesillas, J. P. How, and M. Hutter. Rayen: Imposition of hard convex constraints on neural networks. *arXiv preprint arXiv:2307.08336*, 2023.
- E. van Krieken, T. Thanapalasingam, J. Tomczak, F. Van Harmelen, and A. Ten Teije. A-nesi: A scalable approximate method for probabilistic neurosymbolic inference. *Advances in Neural Information Processing Systems*, 36:24586–24609, 2023.
- K. P. Wabersich, L. Hewing, A. Carron, and M. N. Zeilinger. Probabilistic model predictive safety certification for learning-based control. *IEEE Transactions on Automatic Control*, 67(1):176–188, 2022. doi: 10.1109/TAC.2021.3049335.
- R. Wang, Y. Zhang, Z. Guo, T. Chen, X. Yang, and J. Yan. Linsatnet: the positive linear satisfiability neural networks. In *International Conference on Machine Learning*, pages 36605–36625. PMLR, 2023.
- X. Wang and W. Q. Yan. Human identification based on gait manifold. *Applied Intelligence*, 53(5):6062–6073, 2023.
- J. Xu, Z. Zhang, T. Friedman, Y. Liang, and G. Broeck. A semantic loss function for deep learning with symbolic knowledge. In *International conference on machine learning*, pages 5502–5511. PMLR, 2018.

## Appendix A. Proofs

### A.1 Proof of Proposition 6

**Proposition 6** Under Assumption 5, for any parameterized function  $f_\theta : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}}}$ , HardNet-Aff in (5) satisfies

$$\begin{aligned} \mathcal{P}(f_\theta)(x) &= \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z - f_\theta(x)\|_2 \\ \text{s.t. } z &\in \left\{ \arg \min_{y \in \mathbb{R}^{n_{\text{out}}}} \|A(x)(y - f_\theta(x))\|_2 \text{ s.t. } b^l(x) \leq A(x)y \leq b^u(x) \right\}. \end{aligned} \quad (6)$$

**Proof** We first construct a minimum  $\ell^2$ -norm optimization that characterizes HardNet-Aff based on a property of the pseudoinverse. Then, we show the optimization is equivalent to (6). We drop the input dependency on  $x$  when it is evident to simplify the presentation. Rewriting the closed-form projection of HardNet-Aff in (5),

$$\mathcal{P}(f_\theta)(x) - f_\theta(x) = A^+ [\text{ReLU}(b^l - Af_\theta(x)) - \text{ReLU}(Af_\theta(x) - b^u)].$$

Based on the property of the pseudoinverse  $A^+$  of a full row rank matrix  $A$  that  $z^* = A^+y$  finds the minimum  $\ell^2$ -norm solution among all solutions of the (under-determined) linear system  $y = Az$ , we have

$$\mathcal{P}(f_\theta)(x) - f_\theta(x) = \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z\|_2 \text{ s.t. } Az = \text{ReLU}(b^l - Af_\theta(x)) - \text{ReLU}(Af_\theta(x) - b^u),$$

which implies

$$\mathcal{P}(f_\theta)(x) = \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|z - f_\theta(x)\|_2 \text{ s.t. } z \in \mathcal{Z}_{\text{eq}}$$

with the feasible set  $\mathcal{Z}_{\text{eq}} := \{z \in \mathbb{R}^{n_{\text{out}}} | Az = Af_\theta(x) + \text{ReLU}(b^l - Af_\theta(x)) - \text{ReLU}(Af_\theta(x) - b^u)\}$ .

Now, we prove the equation (6) by showing that the feasible set  $\mathcal{Z}_{\text{eq}}$  is the same as that of the outer optimization in (6), denoted by  $\mathcal{Z}_{\text{opt}} := \left\{ \arg \min_{z \in \mathbb{R}^{n_{\text{out}}}} \|A(z - f_\theta(x))\|_2 \text{ s.t. } b^l \leq Az \leq b^u \right\}$ . Let  $a_i \in \mathbb{R}^{n_c}$  denote the  $i$ -th row of  $A$ . We first observe that, for any  $z \in \mathcal{Z}_{\text{opt}}$ ,

$$\|A(z - f_\theta(x))\|_2^2 = \sum_{i=1}^{n_c} (a_i^\top (z - f_\theta(x)))^2 \quad (11)$$

$$\geq \sum_{i=1}^{n_c} \left( \text{ReLU}(b_{(i)}^l - a_i^\top f_\theta(x)) - \text{ReLU}(a_i^\top f_\theta(x) - b_{(i)}^u) \right)^2 \quad (12)$$

$$= \|\text{ReLU}(b^l - Af_\theta(x)) - \text{ReLU}(Af_\theta(x) - b^u)\|_2^2, \quad (13)$$

where the inequality (12) holds for each summand. It can be easily verified by considering the component-wise constraint  $b_{(i)}^l \leq a_i^\top z \leq b_{(i)}^u$  in three cases: i)  $a_i^\top f_\theta(x) < b_{(i)}^l$ , ii)  $b_{(i)}^l \leq a_i^\top f_\theta(x) \leq b_{(i)}^u$ , and iii)  $a_i^\top f_\theta(x) > b_{(i)}^u$ . With this observation, we show  $\mathcal{Z}_{\text{eq}} = \mathcal{Z}_{\text{opt}}$ :

i) ( $\mathcal{Z}_{\text{eq}} \subset \mathcal{Z}_{\text{opt}}$ ) Suppose  $z' \in \mathcal{Z}_{\text{eq}}$ . Then, following the same proof of Proposition 7 in Appendix A.2 with replacing  $\mathcal{P}(f_\theta)(x)$  as  $z'$ , we can show  $b^l \leq Az' \leq b^u$ . In other words,  $z'$  satisfies the constraints of  $\mathcal{Z}_{\text{opt}}$ . Also,  $z'$  attains the lower bound of the objective of  $\mathcal{Z}_{\text{opt}}$

in (12) since  $A(z' - f_\theta(x)) = \text{ReLU}(b^l - Af_\theta(x)) - \text{ReLU}(Af_\theta(x) - b^u)$ . This implies  $z' \in \mathcal{Z}_{\text{opt}}$ . Thus,  $\mathcal{Z}_{\text{eq}} \subset \mathcal{Z}_{\text{opt}}$ .

ii) ( $\mathcal{Z}_{\text{opt}} \subset \mathcal{Z}_{\text{eq}}$ ) Suppose  $z' \in \mathcal{Z}_{\text{opt}}$ . Since  $\mathcal{P}(f_\theta)(x) \in \mathcal{Z}_{\text{eq}} \subset \mathcal{Z}_{\text{opt}}$  attains the lower bound (13), the inequality (12) should hold with equality for each summand for any  $z \in \mathcal{Z}_{\text{opt}}$ . In addition to the equality, if we consider the component-wise constraint  $b_{(i)}^l \leq a_i^\top z \leq b_{(i)}^u$  in three cases: i)  $a_i^\top f_\theta(x) < b_{(i)}^l$ , ii)  $b_{(i)}^l \leq a_i^\top f_\theta(x) \leq b_{(i)}^u$ , and iii)  $a_i^\top f_\theta(x) > b_{(i)}^u$ , we can show

$$A(z' - f_\theta(x)) = \text{ReLU}(b^l - Af_\theta(x)) - \text{ReLU}(Af_\theta(x) - b^u).$$

This implies  $z' \in \mathcal{Z}_{\text{eq}}$ . Thus,  $\mathcal{Z}_{\text{opt}} \subset \mathcal{Z}_{\text{eq}}$ . ■

## A.2 Proof of Proposition 7

**Proposition 7 (Parallel Projection)** *Under Assumption 5, for any parameterized function  $f_\theta : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}}}$ , for each  $i$ -th row  $a_i \in \mathbb{R}^{n_c}$  of  $A(x)$ , HardNet-Aff in (5) satisfies*

$$a_i^\top \mathcal{P}(f_\theta)(x) = \begin{cases} b_{(i)}^l(x) & \text{if } a_i^\top f_\theta(x) < b_{(i)}^l(x) \\ b_{(i)}^u(x) & \text{if } a_i^\top f_\theta(x) > b_{(i)}^u(x) \\ a_i^\top f_\theta(x) & \text{o.w.} \end{cases} \quad \text{for all } x \in \mathcal{X}. \quad (7)$$

**Proof** Given row index  $i \in \{1, \dots, n_c\}$  and input  $x \in \mathcal{X}$ , for the plain neural network  $f_\theta$ , we can consider three cases: i)  $b_{(i)}^l(x) \leq a_i^\top f_\theta(x) \leq b_{(i)}^u(x)$ , ii)  $a_i^\top f_\theta(x) < b_{(i)}^l(x)$ , and iii)  $a_i^\top f_\theta(x) > b_{(i)}^u(x)$ . In each case, we show that the projected output  $\mathcal{P}(f_\theta)(x)$  satisfies the corresponding equality in Proposition 7.

i) Suppose  $b_{(i)}^l(x) \leq A(x)f_\theta(x) \leq b_{(i)}^u(x)$ . From (5),

$$A(x)\mathcal{P}(f_\theta)(x) = A(x)f_\theta(x) + \text{ReLU}(b^l(x) - A(x)f_\theta(x)) - \text{ReLU}(A(x)f_\theta(x) - b^u(x)).$$

Then, for the  $i$ -th component,

$$a_i^\top \mathcal{P}(f_\theta)(x) = a_i^\top f_\theta(x) + \text{ReLU}(b_{(i)}^l(x) - a_i^\top f_\theta(x)) - \text{ReLU}(a_i^\top f_\theta(x) - b_{(i)}^u(x)) = a_i^\top f_\theta(x)$$

as  $b_{(i)}^l(x) - a_i^\top f_\theta(x) \leq 0$  and  $a_i^\top f_\theta(x) - b_{(i)}^u(x) \leq 0$ .

ii) Suppose  $a_i^\top f_\theta(x) < b_{(i)}^l(x)$ . Then,

$$\begin{aligned} a_i^\top \mathcal{P}(f_\theta)(x) &= a_i^\top f_\theta(x) + \text{ReLU}(b_{(i)}^l(x) - a_i^\top f_\theta(x)) - \text{ReLU}(a_i^\top f_\theta(x) - b_{(i)}^u(x)) \\ &= a_i^\top f_\theta(x) + (b_{(i)}^l(x) - a_i^\top f_\theta(x)) = b_{(i)}^l(x) \end{aligned}$$

as  $b_{(i)}^l(x) - a_i^\top f_\theta(x) > 0$  and  $a_i^\top f_\theta(x) - b_{(i)}^u(x) < 0$ .

iii) Suppose  $a_i^\top f_\theta(x) > b_{(i)}^u(x)$ . Then,

$$\begin{aligned} a_i^\top \mathcal{P}(f_\theta)(x) &= a_i^\top f_\theta(x) + \text{ReLU}(b_{(i)}^l(x) - a_i^\top f_\theta(x)) - \text{ReLU}(a_i^\top f_\theta(x) - b_{(i)}^u(x)) \\ &= a_i^\top f_\theta(x) - (a_i^\top f_\theta(x) - b_{(i)}^u(x)) = b_{(i)}^u(x) \end{aligned}$$

as  $b_{(i)}^l(x) - a_i^\top f_\theta(x) < 0$  and  $a_i^\top f_\theta(x) - b_{(i)}^u(x) > 0$ . This shows Proposition 7 holds. ■

### A.3 Proof of Theorem 8

**Theorem 8** Consider input-dependent constraints (4) that satisfy assumption 5. Suppose  $\mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$  is compact, and  $A(x)$  is continuous over  $\mathcal{X}$ . Then, for any function classes  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset \mathcal{C}(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$  (or  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$  for any  $p \in [1, \infty)$ ) and the projection  $\mathcal{P}$  of HardNet-Aff in (5), if  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ ,  $\mathcal{F}_{\text{HardNet-Aff}} := \{\mathcal{P}(f_{\text{NN}}) | f_{\text{NN}} \in \mathcal{F}_{\text{NN}}\}$  universally approximates  $\mathcal{F}_{\text{target}} := \{f_t \in \mathcal{F} | f_t \text{ satisfies (4)}\}$ .

**Proof** For any functions  $f_{\text{NN}} \in \mathcal{F}_{\text{NN}}$  and  $f_t \in \mathcal{F}_{\text{target}}$ , we first show that  $\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2$  can be bounded by some constant times  $\|f_t(x) - f_{\text{NN}}(x)\|_2$  for all  $x \in \mathcal{X}$ . We drop the input dependency on  $x$  when it is evident to simplify the presentation. From HardNet-Aff in (5),

$$\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 = \|f_t(x) - f_{\text{NN}}(x) - A^+ [\text{ReLU}(b^l - Af_{\text{NN}}(x)) - \text{ReLU}(Af_{\text{NN}}(x) - b^u)]\|_2 \quad (14)$$

$$\leq \|f_t(x) - f_{\text{NN}}(x)\|_2 + \|A^+ \text{ReLU}(b^l - Af_{\text{NN}}(x))\|_2 + \|A^+ \text{ReLU}(Af_{\text{NN}}(x) - b^u)\|_2, \quad (15)$$

by the triangle inequalities. Then, for the second term of RHS,

$$\|A^+ \text{ReLU}(b^l - Af_{\text{NN}}(x))\|_2 = \|A^+ \text{ReLU}(b^l - Af_t(x) + A(f_t(x) - f_{\text{NN}}(x)))\|_2 \quad (16)$$

$$\leq \|A^+\|_2 \|\text{ReLU}(b^l - Af_t(x) + A(f_t(x) - f_{\text{NN}}(x)))\|_2 \quad (17)$$

$$\leq \|A^+\|_2 \|A(f_t(x) - f_{\text{NN}}(x))\|_2 \quad (18)$$

$$\leq \|A^+\|_2 \|A\|_2 \|f_t(x) - f_{\text{NN}}(x)\|_2, \quad (19)$$

where we use the following lemma for (18):

**Lemma 11** For any  $v, w \in \mathbb{R}^{n_c}$ , if  $v \leq 0$ ,  $\|\text{ReLU}(v + w)\|_2 \leq \|w\|_2$ .

For its proof, we consider a simpler case first. For  $v, w \in \mathbb{R}$ , if  $v \leq 0$ , then  $|\text{ReLU}(v + w)| \leq |w|$ . This is because if  $w \leq -v \leq 0$ ,  $|\text{ReLU}(v + w)| = 0 \leq |w|$ , else  $w > -v \geq 0$  so that  $|\text{ReLU}(v + w)| = v + w \leq w = |w|$ . Then, for  $v, w \in \mathbb{R}^{n_c}$ , if  $v \leq 0$ ,

$$\|\text{ReLU}(v + w)\|_2^2 = \sum_{i=1}^{n_c} |\text{ReLU}(v_{(i)} + w_{(i)})|^2 \leq \sum_{i=1}^{n_c} |w_{(i)}|^2 = \|w\|_2^2.$$

Thus, the lemma holds. This lemma implies (18) as  $b^l - Af_t(x) \leq 0$  since  $f_t \in \mathcal{F}_{\text{target}}$  satisfies the constraints (4). Similarly,

$$\|A^+ \text{ReLU}(Af_{\text{NN}}(x) - b^u)\|_2 \leq \|A^+\|_2 \|A\|_2 \|f_{\text{NN}}(x) - f_t(x)\|_2.$$

Then, putting them together in (15), we obtain

$$\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \leq (1 + 2\|A^+\|_2 \|A\|_2) \|f_t(x) - f_{\text{NN}}(x)\|_2.$$

Since  $A(x)$  is continuous over the compact domain  $\mathcal{X}$ , there exists some constant  $K > 0$  such that

$$(1 + 2\|A^+\|_2 \|A\|_2) \leq K,$$

for all  $x \in \mathcal{X}$ . Thus,

$$\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \leq K \|f_t(x) - f_{\text{NN}}(x)\|_2.$$

Now, we extend this inequality to the general  $\ell^p$ -norm and  $\ell^\infty$ -norm by using the inequalities  $\|v\|_q \leq \|v\|_r \leq m^{\frac{1}{r} - \frac{1}{q}} \|v\|_q$  for any  $v \in \mathbb{R}^m$  and  $q \geq r \geq 1$ . If  $p \leq 2$ ,

$$\begin{aligned} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_p &\leq n_{\text{out}}^{\frac{1}{p} - \frac{1}{2}} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \\ &\leq n_{\text{out}}^{\frac{1}{p} - \frac{1}{2}} K \|f_t(x) - f_{\text{NN}}(x)\|_2 \leq n_{\text{out}}^{\frac{1}{p} - \frac{1}{2}} K \|f_t(x) - f_{\text{NN}}(x)\|_p. \end{aligned}$$

If  $p > 2$ ,

$$\begin{aligned} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_p &\leq \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \\ &\leq K \|f_t(x) - f_{\text{NN}}(x)\|_2 \leq K n_{\text{out}}^{\frac{1}{2} - \frac{1}{p}} \|f_t(x) - f_{\text{NN}}(x)\|_p. \end{aligned}$$

Thus, for any  $p \in [1, \infty)$ ,

$$\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_p \leq n_{\text{out}}^{\left|\frac{1}{p} - \frac{1}{2}\right|} K \|f_t(x) - f_{\text{NN}}(x)\|_p. \quad (20)$$

Then, with  $p \rightarrow \infty$ ,

$$\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_\infty \leq n_{\text{out}}^{\frac{1}{2}} K \|f_t(x) - f_{\text{NN}}(x)\|_\infty. \quad (21)$$

Now, we prove the theorem. Suppose  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset \mathcal{C}(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$ . For any  $f_t \in \mathcal{F}_{\text{target}} \subset \mathcal{F}$  and  $\epsilon > 0$ , we have a function  $f_{\text{NN}} \in \mathcal{F}_{\text{NN}}$  such that

$$\|f_t - f_{\text{NN}}\|_\infty \leq \frac{\epsilon}{n_{\text{out}}^{\frac{1}{2}} K}, \quad (22)$$

since  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ . For such  $f_{\text{NN}}$ ,

$$\begin{aligned} \|f_t - \mathcal{P}(f_{\text{NN}})\|_\infty &= \sup_{x \in \mathcal{X}} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_\infty \\ &\leq \sup_{x \in \mathcal{X}} n_{\text{out}}^{\frac{1}{2}} K \|f_t(x) - f_{\text{NN}}(x)\|_\infty \\ &= n_{\text{out}}^{\frac{1}{2}} K \sup_{x \in \mathcal{X}} \|f_t(x) - f_{\text{NN}}(x)\|_\infty = n_{\text{out}}^{\frac{1}{2}} K \|f_t - f_{\text{NN}}\|_\infty \leq \epsilon, \end{aligned}$$

where the first and last inequalities are from (21) and (22), respectively. Since  $\mathcal{P}(f_{\text{NN}}) \in \mathcal{F}_{\text{HardNet-Aff}}$ ,  $\mathcal{F}_{\text{HardNet-Aff}}$  universally approximates  $\mathcal{F}_{\text{target}}$ .

Similarly, suppose  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$ . For any  $f_t \in \mathcal{F}_{\text{target}} \subset \mathcal{F}$  and  $\epsilon > 0$ , we have a function  $f_{\text{NN}} \in \mathcal{F}_{\text{NN}}$  such that

$$\|f_t - f_{\text{NN}}\|_p \leq \frac{\epsilon}{n_{\text{out}}^{\left|\frac{1}{p} - \frac{1}{2}\right|} K}, \quad (23)$$

since  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ . For such  $f_{\text{NN}}$ ,

$$\begin{aligned}\|f_t - \mathcal{P}(f_{\text{NN}})\|_p &= \left( \int_{\mathcal{X}} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_p^p dx \right)^{1/p} \\ &\leq \left( \int_{\mathcal{X}} (n_{\text{out}}^{\frac{1}{p}-\frac{1}{2}} K)^p \|f_t(x) - f_{\text{NN}}(x)\|_p^p dx \right)^{1/p} \\ &= n_{\text{out}}^{\frac{1}{p}-\frac{1}{2}} K \left( \int_{\mathcal{X}} \|f_t(x) - f_{\text{NN}}(x)\|_p^p dx \right)^{1/p} = n_{\text{out}}^{\frac{1}{p}-\frac{1}{2}} K \|f_t - f_{\text{NN}}\|_p \leq \epsilon,\end{aligned}$$

where the first and last inequalities are from (20) and (23), respectively. Since  $\mathcal{P}(f_{\text{NN}}) \in \mathcal{F}_{\text{HardNet-Aff}}$ ,  $\mathcal{F}_{\text{HardNet-Aff}}$  universally approximates  $\mathcal{F}_{\text{target}}$ .  $\blacksquare$

#### A.4 Proof of Theorem 10

**Theorem 10** Consider input-dependent sets  $\mathcal{C}(x) \subset \mathbb{R}^{n_{\text{out}}}$  that are convex for all  $x \in \mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$ . Then, for any  $p \in [1, \infty)$ , HardNet-Cvx with  $w$ -width ReLU neural networks defined in (8) universally approximates  $\mathcal{F}_{\text{target}} := \{f_t \in L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}}) | f_t(x) \in \mathcal{C}(x) \forall x \in \mathcal{X}\}$  if  $w \geq \max\{n_{\text{in}} + 1, n_{\text{out}}\}$ .

As for HardNet-Aff, we prove this theorem as a corollary of the following theorem:

**Theorem 12** Consider input-dependent sets  $\mathcal{C}(x) \subset \mathbb{R}^{n_{\text{out}}}$  that are convex for all  $x \in \mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$ . Then, for any function classes  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset \mathcal{C}(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$  (or  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$  for any  $p \in [1, \infty)$ ) and the projection  $\mathcal{P}$  of HardNet-Cvx in (8), if  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ ,  $\mathcal{F}_{\text{HardNet-Cvx}} := \{\mathcal{P}(f_{\text{NN}}) | f_{\text{NN}} \in \mathcal{F}_{\text{NN}}\}$  universally approximates  $\mathcal{F}_{\text{target}} := \{f_t \in \mathcal{F} | f_t(x) \in \mathcal{C}(x) \forall x \in \mathcal{X}\}$ .

**Proof** Similarly to the proof of Theorem 8 in Appendix A.3, for any functions  $f_{\text{NN}} \in \mathcal{F}_{\text{NN}}$  and  $f_t \in \mathcal{F}_{\text{target}}$ , we first prove the following inequality:

$$\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \leq \|f(x) - f_{\text{NN}}(x)\|_2 \quad \forall x \in \mathcal{X}.$$

Given  $x \in \mathcal{X}$ , consider the simple case  $f_{\text{NN}}(x) \in \mathcal{C}(x)$  first. Then,  $\mathcal{P}(f_{\text{NN}})(x) = f_{\text{NN}}(x)$  from the projection in (8) which satisfies  $\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \leq \|f_t(x) - f_{\text{NN}}(x)\|_2$ .

On the other hand, if  $f_{\text{NN}}(x) \notin \mathcal{C}(x)$ , consider the triangle connecting  $f_{\text{NN}}(x)$ ,  $\mathcal{P}(f_{\text{NN}})(x)$  and  $f_t(x)$ . Then, the side between  $f_{\text{NN}}(x)$  and  $\mathcal{P}(f_{\text{NN}})(x)$  is orthogonal to the tangent hyperplane of the convex set  $\mathcal{C}(x)$  at  $\mathcal{P}(f_{\text{NN}})(x)$ . For the two half-spaces separated by the tangent hyperplane,  $f_t(x)$  belongs to the other half-space than the one that contains  $f_{\text{NN}}(x)$  since  $\mathcal{C}(x)$  is convex. Thus, the vertex angle at  $\mathcal{P}(f_{\text{NN}})(x)$  is larger than  $\pi/2$ . This implies that the side between  $f_{\text{NN}}(x)$  and  $f_t(x)$  is the longest side of the triangle, so  $\|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_2 \leq \|f_t(x) - f_{\text{NN}}(x)\|_2$ .

Then, We can extend this  $\ell^2$ -norm result to general  $\ell^p$ -norm and  $\ell^\infty$ -norm as in Appendix A.3:

$$\|f(x) - \mathcal{P}(f_{\text{NN}})(x)\|_p \leq n_{\text{out}}^{\frac{1}{p}-\frac{1}{2}} \|f(x) - f_{\text{NN}}(x)\|_p. \quad (24)$$

With  $p \rightarrow \infty$ ,

$$\|f(x) - \mathcal{P}(f_{\text{NN}})(x)\|_\infty \leq n_{\text{out}}^{\frac{1}{2}} \|f(x) - f_{\text{NN}}(x)\|_\infty. \quad (25)$$

Now, we prove the theorem. Suppose  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset \mathcal{C}(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$ . For any  $f_t \in \mathcal{F}_{\text{target}} \subset \mathcal{F}$  and  $\epsilon > 0$ , we have a function  $f_{\text{NN}} \in \mathcal{F}_{\text{NN}}$  such that

$$\|f_t - f_{\text{NN}}\|_{\infty} \leq \frac{\epsilon}{n_{\text{out}}^{\frac{1}{2}}}, \quad (26)$$

since  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ . For such  $f_{\text{NN}}$ ,

$$\begin{aligned} \|f_t - \mathcal{P}(f_{\text{NN}})\|_{\infty} &= \sup_{x \in \mathcal{X}} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_{\infty} \\ &\leq \sup_{x \in \mathcal{X}} n_{\text{out}}^{\frac{1}{2}} \|f_t(x) - f_{\text{NN}}(x)\|_{\infty} \\ &= n_{\text{out}}^{\frac{1}{2}} \sup_{x \in \mathcal{X}} \|f_t(x) - f_{\text{NN}}(x)\|_{\infty} = n_{\text{out}}^{\frac{1}{2}} \|f_t - f_{\text{NN}}\|_{\infty} \leq \epsilon, \end{aligned}$$

where the first and last inequalities are from (25) and (26), respectively. Since  $\mathcal{P}(f_{\text{NN}}) \in \mathcal{F}_{\text{HardNet-Cvx}}$ ,  $\mathcal{F}_{\text{HardNet-Cvx}}$  universally approximates  $\mathcal{F}_{\text{target}}$ .

Similarly, suppose  $\mathcal{F}_{\text{NN}}, \mathcal{F} \subset L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$ . For any  $f_t \in \mathcal{F}_{\text{target}} \subset \mathcal{F}$  and  $\epsilon > 0$ , we have a function  $f_{\text{NN}} \in \mathcal{F}_{\text{NN}}$  such that

$$\|f_t - f_{\text{NN}}\|_p \leq \frac{\epsilon}{n_{\text{out}}^{| \frac{1}{p} - \frac{1}{2} |}}, \quad (27)$$

since  $\mathcal{F}_{\text{NN}}$  universally approximates  $\mathcal{F}$ . For such  $f_{\text{NN}}$ ,

$$\begin{aligned} \|f_t - \mathcal{P}(f_{\text{NN}})\|_p &= \left( \int_{\mathcal{X}} \|f_t(x) - \mathcal{P}(f_{\text{NN}})(x)\|_p^p dx \right)^{1/p} \\ &\leq \left( \int_{\mathcal{X}} (n_{\text{out}}^{| \frac{1}{p} - \frac{1}{2} |})^p \|f_t(x) - f_{\text{NN}}(x)\|_p^p dx \right)^{1/p} \\ &= n_{\text{out}}^{| \frac{1}{p} - \frac{1}{2} |} \left( \int_{\mathcal{X}} \|f_t(x) - f_{\text{NN}}(x)\|_p^p dx \right)^{1/p} = n_{\text{out}}^{| \frac{1}{p} - \frac{1}{2} |} \|f_t - f_{\text{NN}}\|_p \leq \epsilon, \end{aligned}$$

where the first and last inequalities are from (24) and (27), respectively. Since  $\mathcal{P}(f_{\text{NN}}) \in \mathcal{F}_{\text{HardNet-Cvx}}$ ,  $\mathcal{F}_{\text{HardNet-Cvx}}$  universally approximates  $\mathcal{F}_{\text{target}}$ .  $\blacksquare$

Thus, by utilizing Theorem 2 in this theorem, we have Theorem 10 as a corollary.

## Appendix B. An Alternative Approach to Handle Equality Constraints Separately

In this section, we propose an alternative approach to handle equality constraints separately, rather than setting  $b^l = b^u$  in (4). We first define some additional notation:

**Additional notation**  $v_{(i)} \in \mathbb{R}$ ,  $v_{(:,i)} \in \mathbb{R}^i$ , and  $v_{(i,:)} \in \mathbb{R}^{m-i}$  denote the  $i$ -th component, the first  $i$  and the last  $m - i$  components of  $v$ , respectively. Similarly,  $A_{(:,i)} \in \mathbb{R}^{k \times i}$  and  $A_{(i,:)} \in \mathbb{R}^{k \times (m-i)}$  denote the first  $i$  and the last  $m - i$  columns of  $A$ , respectively.

Now, suppose we have multiple input-dependent affine constraints in an aggregated form:

$$A(x)f(x) \leq b(x), \quad C(x)f(x) = d(x) \quad \forall x \in \mathcal{X}, \quad (28)$$

where  $A(x) \in \mathbb{R}^{n_{\text{ineq}} \times n_{\text{out}}}$ ,  $b(x) \in \mathbb{R}^{n_{\text{ineq}}}$ ,  $C(x) \in \mathbb{R}^{n_{\text{eq}} \times n_{\text{out}}}$ ,  $d(x) \in \mathbb{R}^{n_{\text{eq}}}$  for  $n_{\text{ineq}}$  inequality and  $n_{\text{eq}}$  equality constraints. For partitions  $A(x) = [A_{(n_{\text{eq}})} A_{(n_{\text{eq}},:)})]$  and  $C(x) = [C_{(n_{\text{eq}})} C_{(n_{\text{eq}},:)})]$ , we make the following assumptions about the constraints:

**Assumption 13** *For each  $x \in \mathcal{X}$ , i) there exists  $y \in \mathbb{R}^{n_{\text{out}}}$  that satisfies the constraints in (28), ii)  $C_{(n_{\text{eq}})}$  is invertible, and iii)  $\tilde{A}(x) := A_{(n_{\text{eq}})} - A_{(n_{\text{eq}})} C_{(n_{\text{eq}})}^{-1} C_{(n_{\text{eq}},:)}$  has full row rank.*

Given  $x \in \mathcal{X}$ , when  $C(x)$  has full row rank (i.e., no redundant constraints), there exists an invertible submatrix of  $C(x)$  with its  $n_{\text{eq}}$  columns. Without loss of generality, we can assume  $C_{(n_{\text{eq}})}$  is such submatrix by considering a proper permutation of the components of  $f$ . Then, the second assumption holds when the same permutation lets  $C_{(n_{\text{eq}})}$  invertible for all  $x \in \mathcal{X}$ . The last assumption requires the total number of the constraints  $n_{\text{ineq}} + n_{\text{eq}}$  to be less than or equal to the output dimension  $n_{\text{out}}$  and  $A(x)$  to have full row rank.

Under the assumptions, we first efficiently reduce the  $n_{\text{ineq}} + n_{\text{eq}}$  constraints to  $n_{\text{ineq}}$  equivalent inequality constraints on partial outputs  $f_{(n_{\text{eq}},:)}$  for a partition of the function  $f(x) = [f_{(n_{\text{eq}},:)}; f_{(n_{\text{eq}},:)})]$ . Consider the hyperplane in the codomain  $\mathcal{Y}$  over which the equality constraints are satisfied. Then, for the function output  $f(x)$  to be on the hyperplane, the first part  $f_{(n_{\text{eq}},:)}$  is determined by  $f_{(n_{\text{eq}},:)}$ :

$$f_{(n_{\text{eq}},:)}(x) = C_{(n_{\text{eq}})}^{-1} (d(x) - C_{(n_{\text{eq}},:)}) f_{(n_{\text{eq}},:)}(x). \quad (29)$$

Substituting this  $f_{(n_{\text{eq}},:)}$  into the inequality constraints, the constraints in (28) is equivalent to the following inequality constraints with (29):

$$\underbrace{(A_{(n_{\text{eq}},:)}) - A_{(n_{\text{eq}})} C_{(n_{\text{eq}})}^{-1} C_{(n_{\text{eq}},:)})}_{=: \tilde{A}(x)} f_{(n_{\text{eq}},:)}(x) \leq \underbrace{b(x) - A_{(n_{\text{eq}})} C_{(n_{\text{eq}})}^{-1} d(x)}_{=: \tilde{b}(x)} \quad \forall x \in \mathcal{X}.$$

We propose a closed-form projection to enforce this  $n_{\text{ineq}}$  equivalent inequality constraints on  $f_{(n_{\text{eq}},:)}$ , while the first part  $f_{(n_{\text{eq}},:)}$  of the function is completely determined by the second part  $f_{(n_{\text{eq}},:)}$  as in (29). We let the parameterized function  $f_\theta : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}} - n_{\text{eq}}}$  approximate only the second part (or disregard the first  $n_{\text{eq}}$  outputs if  $f_\theta(x) \in \mathbb{R}^{n_{\text{out}}}$  is given). Then, we project  $f_\theta$  to satisfy the constraints in (28) as below:

$$\mathcal{P}(f_\theta)(x) = \left[ C_{(n_{\text{eq}})}^{-1} (d(x) - C_{(n_{\text{eq}},:)}) f_\theta^*(x); f_\theta^*(x) \right], \quad (30)$$

where  $f_\theta^*(x) := f_\theta(x) - \tilde{A}(x)^+ \text{ReLU}(\tilde{A}(x)f_\theta(x) - \tilde{b}(x))$  for all  $x \in \mathcal{X}$  with  $M^+ := M^\top (MM^\top)^{-1}$  denoting the pseudoinverse of a matrix  $M$ . This novel projection satisfies the following properties.

**Proposition 14** *Under Assumption 13, for any parameterized (neural network) function  $f_\theta : \mathcal{X} \rightarrow \mathbb{R}^{n_{\text{out}} - n_{\text{eq}}}$  and for all  $x \in \mathcal{X}$ , the projection  $\mathcal{P}(f_\theta)$  in (30) satisfies*

i)  $A(x)\mathcal{P}(f_\theta)(x) \leq b(x)$ ,    ii)  $C(x)\mathcal{P}(f_\theta)(x) = d(x)$ ,

iii) For each  $i$ -th row  $a_i \in \mathbb{R}^{n_{\text{out}}}$  of  $A(x)$ ,  $a_i^\top \mathcal{P}(f_\theta)(x) = \begin{cases} a_i^\top \bar{f}_\theta(x) & \text{if } a_i^\top \bar{f}_\theta(x) \leq b_{(i)}(x) \\ b_{(i)}(x) & \text{o.w.} \end{cases}$ ,

where  $\bar{f}_\theta(x) := [[C_{(n_{\text{eq}})}^{-1} (d(x) - C_{(n_{\text{eq}},:)}) f_\theta(x)]; f_\theta(x)] \in \mathbb{R}^{n_{\text{out}}}$ .

**Proof** We simplify the notation of the partition by  $(\cdot)_1 := (\cdot)_{(n_{\text{eq}})}$  and  $(\cdot)_2 := (\cdot)_{(n_{\text{eq}})}$ . Also, we drop the input dependency on  $x$  when it is evident. Then,

$$\begin{aligned} A(x)\mathcal{P}(f_\theta)(x) &= A_1\mathcal{P}(f_\theta)_1 + A_2\mathcal{P}(f_\theta)_2 \\ &= A_1C_1^{-1}(d - C_2f_\theta^*) + A_2f_\theta^* \\ &= (A_2 - A_1C_1^{-1}C_2)f_\theta^* + A_1C_1^{-1}d \\ &= \tilde{A}f_\theta^* - \tilde{b} + b = \tilde{A}f_\theta - \text{ReLU}(\tilde{A}f_\theta - \tilde{b}) - \tilde{b} + b \leq \tilde{b} - \tilde{b} + b = b(x). \end{aligned}$$

This shows (i). For (ii),

$$C(x)\mathcal{P}(f_\theta)(x) = C_1\mathcal{P}(f_\theta)_1 + C_2\mathcal{P}(f_\theta)_2 = (d - C_2f_\theta^*) + C_2f_\theta^* = d(x).$$

For (iii), we first observe that

$$a_i^\top \bar{f}_\theta(x) \leq b_{(i)}(x) \iff a_{i1}^\top f_\theta + a_{i2}^\top C_2^{-1}(d - C_1f_\theta) \leq b_{(i)} \iff \tilde{a}_i^\top f_\theta \leq \tilde{b}_{(i)}.$$

Then, if  $a_i^\top \bar{f}_\theta(x) \leq b_{(i)}(x)$ ,

$$\begin{aligned} a_i^\top \mathcal{P}(f_\theta)(x) &= a_{i1}^\top \mathcal{P}(f_\theta)_1 + a_{i2}^\top \mathcal{P}(f_\theta)_2 \\ &= (a_{i2}^\top - a_{i1}^\top C_1^{-1}C_2)f_\theta^* + a_{i1}^\top C_1^{-1}d = (a_{i2}^\top - a_{i1}^\top C_1^{-1}C_2)f_\theta + a_{i1}^\top C_1^{-1}d = a_i^\top \bar{f}_\theta(x), \end{aligned}$$

where the second last equality is from  $\tilde{A}f_\theta^* = \tilde{A}f_\theta - \text{ReLU}(\tilde{A}f_\theta - \tilde{b})$  and  $\tilde{a}_i^\top f_\theta \leq \tilde{b}_{(i)}$ . Similarly, if  $a_i^\top \bar{f}_\theta(x) > b_{(i)}(x)$ ,

$$a_i^\top \mathcal{P}(f_\theta)(x) = (a_{i2}^\top - a_{i1}^\top C_1^{-1}C_2)f_\theta^* + a_{i1}^\top C_1^{-1}d = \tilde{b}_{(i)} + a_{i1}^\top C_1^{-1}d = b_{(i)}(x)$$

■

While the projection (30) guarantees the satisfaction of the hard constraints (28), we can also rigorously show that it preserves the neural network's expressive power by the following universal approximation theorem, as in Appendix A.3.

**Theorem 15** Consider input-dependent constraints (28) that satisfy assumption 13. Suppose  $\mathcal{X} \subset \mathbb{R}^{n_{\text{in}}}$  is compact, and  $A(x), C(x)$  are continuous over  $\mathcal{X}$ . For any  $p \in [1, \infty)$ , let  $\mathcal{F} = \{f \in L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}}) | f \text{ satisfies (4)}\}$ . Then, the projection with  $w$ -width ReLU neural networks defined in (30) universally approximates  $\mathcal{F}$  if  $w \geq \max\{n_{\text{in}} + 1, n_{\text{out}} - n_{\text{eq}}\}$ .

**Proof** We first show that  $\|f(x) - \mathcal{P}(f_\theta)(x)\|_2$  can be bounded by some constant times  $\|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2$ . From (30),

$$\begin{aligned} \|f(x) - \mathcal{P}(f_\theta)(x)\|_2^2 &= \|f_{(n_{\text{eq}})}(x) - \mathcal{P}(f_\theta)_{(n_{\text{eq}})}(x)\|_2^2 + \|f_{(n_{\text{eq}})}(x) - \mathcal{P}(f_\theta)_{(n_{\text{eq}})}(x)\|_2^2 \\ &= \|C_{(n_{\text{eq}})}^{-1}C_{(n_{\text{eq}})}(f_{(n_{\text{eq}})}(x) - f_\theta^*(x))\|_2^2 + \|f_{(n_{\text{eq}})}(x) - f_\theta^*(x)\|_2^2 \\ &\leq (1 + \|C_{(n_{\text{eq}})}^{-1}C_{(n_{\text{eq}})}\|_2^2)\|f_{(n_{\text{eq}})}(x) - f_\theta^*(x)\|_2^2, \end{aligned}$$

where the second equality holds by substituting  $f_{(n_{\text{eq}})}(x)$  in (29). Meanwhile,

$$\begin{aligned} \|f_{(n_{\text{eq}})}(x) - f_\theta^*(x)\|_2 &\leq \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2 + \|\tilde{A}^+ \text{ReLU}(\tilde{A}f_\theta(x) - \tilde{b})\|_2 \\ &\leq \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2 + \|\tilde{A}^+\|_2 \|\text{ReLU}(\tilde{A}f_{(n_{\text{eq}})}(x) - \tilde{b} + \tilde{A}(f_\theta - f_{(n_{\text{eq}})}))\|_2 \\ &\leq \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2 + \|\tilde{A}^+\|_2 \|\tilde{A}(f_\theta(x) - f_{(n_{\text{eq}})}(x))\|_2 \\ &\leq (1 + \|\tilde{A}^+\|_2 \|\tilde{A}\|_2) \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2. \end{aligned}$$

Then, putting them together, we obtain

$$\|f(x) - \mathcal{P}(f_\theta)(x)\|_2 \leq (1 + \|\tilde{A}^+\|_2 \|\tilde{A}\|_2) \sqrt{(1 + \|C_{(n_{\text{eq}})}^{-1} C_{(n_{\text{eq}})}\|_2^2)} \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2.$$

Since  $A(x), C(x)$  are continuous over the compact domain  $\mathcal{X}$ , there exists some constant  $K > 0$  s.t.

$$(1 + \|\tilde{A}^+\|_2 \|\tilde{A}\|_2) \sqrt{(1 + \|C_{(n_{\text{eq}})}^{-1} C_{(n_{\text{eq}})}\|_2^2)} \leq K$$

for all  $x \in \mathcal{X}$ . Thus,

$$\|f(x) - \mathcal{P}(f_\theta)(x)\|_2 \leq K \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_2$$

Extending the inequalities to general  $\ell^p$ -norm for  $p \geq 1$  by using the inequalities  $\|v\|_q \leq \|v\|_r \leq m^{\frac{1}{r} - \frac{1}{q}} \|v\|_q$  for any  $v \in \mathbb{R}^m$  and  $q \geq r \geq 1$ ,

$$\|f(x) - \mathcal{P}(f_\theta)(x)\|_p \leq (n_{\text{out}} - n_{\text{eq}})^{\frac{1}{p} - \frac{1}{2}} K \|f_{(n_{\text{eq}})}(x) - f_\theta(x)\|_p$$

Then,  $f_\theta$  being dense in  $L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}} - n_{\text{eq}}})$  implies  $\mathcal{P}(f_\theta)$  being dense in  $L^p(\mathcal{X}, \mathbb{R}^{n_{\text{out}}})$ . Thus, we can employ any universal approximation theorem for  $f_\theta$  and convert it to that for  $\mathcal{P}(f_\theta)$ . While we utilize Theorem 2 in this theorem, other universal approximation theorems on plain neural networks, such as Theorem 1, can also be employed. ■

## Appendix C. Gradient Properties of HardNet-Aff

This section investigates how the enforcement layer in HardNet-Aff affects gradient computation. For simplicity, we focus on the case where the constraints are  $A(x)f(x) \leq b(x) \forall x \in \mathcal{X}$ . For a datapoint  $(x, y)$ , consider the loss function  $\ell(\mathcal{P}(f_\theta(x)), y)$ . Using the chain rule, the gradient is given by:

$$\nabla_\theta \ell(\mathcal{P}(f_\theta(x)), y)^\top = \frac{\partial \ell(\mathcal{P}(f_\theta(x)), y)}{\partial \mathcal{P}(f_\theta(x))} \frac{\partial \mathcal{P}(f_\theta(x))}{\partial f_\theta(x)} \frac{\partial f_\theta(x)}{\partial \theta}. \quad (31)$$

Here, the Jacobian of the enforcement layer  $\frac{\partial \mathcal{P}(f_\theta(x))}{\partial f_\theta(x)} \in \mathbb{R}^{n_{\text{out}} \times n_{\text{out}}}$  plays a key role. Let  $v_i := \mathbb{1}\{a_i(x)^\top f_\theta(x) > b_{(i)}(x)\}$  indicate whether the  $i$ -th constraint is violated by  $f_\theta(x)$ . Then,

$$\frac{\partial \mathcal{P}(f_\theta(x))}{\partial f_\theta(x)} = I - A^+ \begin{bmatrix} v_1 a_1^\top \\ \vdots \\ v_{n_c} a_{n_c}^\top \end{bmatrix}.$$

Two critical properties of this Jacobian can lead to zero gradient in (31). First, if the number of constraints equals the output dimension ( $n_c = n_{\text{out}}$ ) and all constraints are violated ( $v_i = 1 \forall i$ ), then the Jacobian becomes zero, causing the gradient (31) to vanish. Note that this issue never happens when  $n_c < n_{\text{out}}$ . Second, for each  $i \in \{1, 2, \dots, n_c\}$ , the following holds:

$$a_i^\top \frac{\partial \mathcal{P}(f_\theta(x))}{\partial f_\theta(x)} = a_i^\top - a_i^\top A^+ \begin{bmatrix} v_1 a_1^\top \\ \vdots \\ v_{n_c} a_{n_c}^\top \end{bmatrix} = a_i^\top - e_i^\top \begin{bmatrix} v_1 a_1^\top \\ \vdots \\ v_{n_c} a_{n_c}^\top \end{bmatrix} = a_i^\top - v_i a_i^\top.$$

This implies that if the loss gradient with respect to the projected output,  $(\frac{\partial \ell(\mathcal{P}(f_\theta(x)), y)}{\partial \mathcal{P}(f_\theta(x))})^\top \in \mathbb{R}^{n_{\text{out}}}$ , lies in the span of  $\{a_i | i \in \{1, \dots, n_c\}, v_i = 1\}$ , then the overall gradient (31) becomes zero. This case in fact subsumes the first case, as when  $n_c = n_{\text{out}}$  and  $v_i = 1 \forall i$ , the constraint vectors set spans the entire output space  $\mathbb{R}^{n_{\text{out}}}$ .

However, such special cases are rare in practical settings, particularly when the model is trained on batched data. Even when zero gradients occur for certain datapoints, they can be offset by nonzero gradients from the other datapoints within the batch. This averaging effect allows the model to update in a direction that decreases the overall loss function. Thus, **HardNet-Aff** allows training the projected function to achieve values (strictly) within the feasible set using conventional gradient-based algorithms. Additionally, one can promote the model  $f_\theta$  to be initialized within the feasible set using the warm-start scheme outlined in Appendix C.1, which involves training the model without the enforcement layer for a few initial epochs while regularizing with constraint violations.

We demonstrate the gradient behaviors discussed earlier using simple simulations of training **HardNet-Aff** with the conventional gradient-descent algorithm. Consider two datapoints:  $d_1 = (-1, [-0.5, 0.5]^\top)$  and  $d_2 = (1, [0.5, 0]^\top)$ , and a neural network  $f_\theta : \mathbb{R} \rightarrow \mathbb{R}^2$  with two hidden layers, each containing 10 neurons with ReLU activations. The model enforces the input-independent constraint  $[0, 1]\mathcal{P}(f_\theta)(x) \leq 0.9$  using **HardNet-Aff**. Starting from the same initialization, the model is trained to minimize the squared error loss, first on  $d_1$  alone and then on both datapoints, using two different learning rates (0.01 and 0.1), as shown in Fig. 5.

Initially,  $f_\theta$  violates the constraint on both datapoints. When trained on  $d_1$  alone with a learning rate of 0.01, the optimization path converges to a point where the loss gradient with respect to the projected output is orthogonal to the gradient boundary, causing the overall gradient (31) to vanish. However, when the model is trained on both datapoints, the vanishing gradient for  $d_1$  is mitigated by the nonzero gradient for  $d_2$ , enabling the model to achieve target values strictly within the feasible set. Furthermore, using a larger learning rate (0.1) allows the model to avoid the vanishing gradient issue and reach the target value even when trained solely on  $d_1$ .

### C.1 Learning with Warm Start

In addition to the **HardNet** architecture shown in Figure 1 that consists of a neural network  $f_\theta$  and a differentiable enforcement layer with a projection  $\mathcal{P}$  appended at the end, we propose a training scheme that can potentially result in better-optimized models. For the first  $k$  epochs of training, we disable the enforcement layer and train the plain neural network  $f_\theta$ . Then,

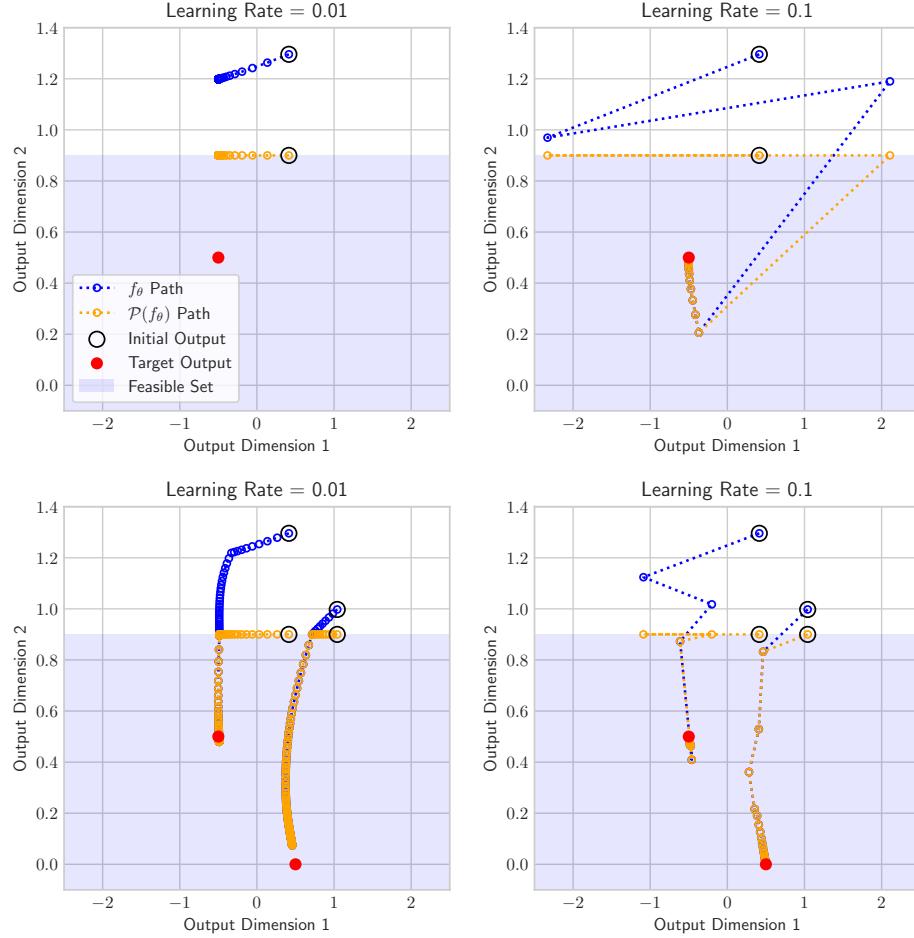


Figure 5: Visualization of 100 gradient descent steps for training a HardNet-Aff model on a single datapoint (first row) and two datapoints (second row) from the same initialization, using two different learning rates (0.01 and 0.1). With the smaller learning rate, training on a single datapoint results in a zero gradient due to the enforcement layer (top left). However, when training on both datapoints, the vanishing gradient for the first datapoint is mitigated by the nonzero gradient from the second datapoint (bottom left). Also, using the larger learning rate enables the model to avoid the vanishing gradient issue, even when trained on the single datapoint (top right).

Table 5: Results for learning with the piecewise constraints. **HardNet-Aff** attains a comparable MSE distance from the true function as other methods without any constraint violation. The max and mean of constraint violations are computed over 401 test samples. Better (resp. worse) values are colored greener (resp. redder). Standard deviations over 5 runs are shown in parentheses.

	MSE	max violation	mean violation	$T_{\text{test}}$ (ms)	$T_{\text{train}}$ (s)
NN	0.04 (0.01)	0.73 (0.07)	0.02 (0.01)	0.14 (0.00)	2.07 (0.11)
Soft	0.05 (0.01)	0.69 (0.04)	0.02 (0.00)	0.15 (0.01)	4.00 (0.07)
DC3	0.04 (0.01)	0.48 (0.03)	0.01 (0.00)	6.05 (0.05)	15.09 (0.68)
<b>HardNet-Aff</b>	0.06 (0.01)	0.00 (0.00)	0.00 (0.00)	0.86 (0.00)	5.50 (0.18)

from the  $(k+1)$ -th epoch, we train on the projected model  $\mathcal{P}(f_\theta)$ . During the  $k$  epochs of warm start, the neural network  $f_\theta$  can be trained in a soft-constrained manner by regularizing the violations of constraints. In this paper, we train the **HardNet-Aff** models without the warm-start scheme for simplicity, except in Section 5.2 where we use the warm-start for the initial 100 epochs.

## Appendix D. Experimental Details

### D.1 Details for the Learning with Piecewise Constraints Experiment

The target function and constraints are as below:

$$f(x) = \begin{cases} -5 \sin \frac{\pi}{2}(x+1) & \text{if } x \leq -1 \\ 0 & \text{if } x \in (-1, 0] \\ 4 - 9(x - \frac{2}{3})^2 & \text{if } x \in (0, 1] \\ 5(1-x) + 3 & \text{if } x > 1 \end{cases}, \text{Constraints: } \begin{cases} f(x) \geq 5 \sin^2 \frac{\pi}{2}(x+1) & \text{if } x \leq -1 \\ f(x) \leq 0 & \text{if } x \in (-1, 0] \\ f(x) \geq (4 - 9(x - \frac{2}{3})^2)x & \text{if } x \in (0, 1] \\ f(x) \leq 4.5(1-x) + 3 & \text{if } x > 1 \end{cases}.$$

These four constraints can be aggregated into the following single affine constraint:

$$a(x)f(x) \leq b(x) : \begin{cases} a(x) = -1, b(x) = -5 \sin^2 \frac{\pi}{2}(x+1) & \text{if } x \leq -1 \\ a(x) = 1, b(x) = 0 & \text{if } x \in (-1, 0] \\ a(x) = -1, b(x) = (9(x - \frac{2}{3})^2 - 4)x & \text{if } x \in (0, 1] \\ a(x) = 1, b(x) = 4.5(1-x) + 3 & \text{if } x > 1 \end{cases}.$$

The results in Section 5.1 show **HardNet-Aff** can help generalization on unseen regimes by enforcing constraints. In this section, we provide additional results that train the models on data spanning the entire domain of interest  $[-2, 2]$ . As shown in Figure 6 and Table 5, the models exhibit similar generalization performances while **HardNet-Aff** satisfies the constraints throughout the training.

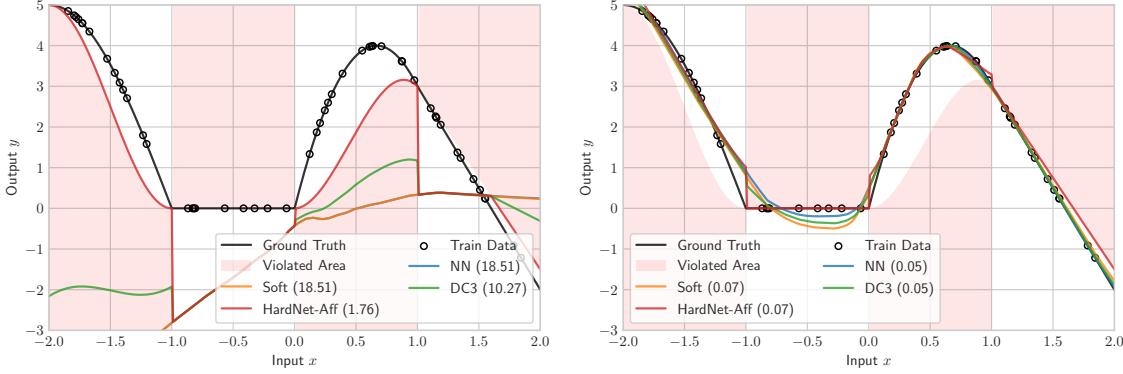


Figure 6: Learned functions at the initial (left) and final (right) epochs with the piecewise constraints. The models are trained on the samples indicated with circles, with their MSE distances from the true function shown in parentheses. HardNet-Aff adheres to the constraints from the start of the training. On the other hand, the baselines violate the constraints throughout the training.

## D.2 Additional Experiment: Learning with Piecewise Constraints for Both Upper and Lower Bounds

Building on the piecewise-constraint study in Section 5.1, we next assess HardNet-Aff with more complex constraints in which each regime is governed by both upper and lower bounds (or, in the degenerate case, an equality).

We adopt the following ground-truth function:

$$f(x) = \begin{cases} -5 \sin \frac{\pi}{2}(x+1) - 2 & \text{if } x \leq -1 \\ -2 & \text{if } x \in (-1, 0] \\ 2 - 9(x - \frac{2}{3})^2 & \text{if } x \in (0, 1] \\ \frac{3}{x^2} - 2 & \text{if } x > 1 \end{cases}$$

subject to the following piecewise box constraints:

$$\text{Constraints: } \begin{cases} 5 \sin^2 \frac{\pi}{2}(x+1) - 2 \leq f(x) \leq -3 \sin \frac{\pi}{2}(x+1) & \text{if } x \leq -1 \\ f(x) = -2 & \text{if } x \in (-1, 0] \\ (4 - 9(x - \frac{2}{3})^2)x \leq f(x) \leq 3 - 4(x - 0.5)^2 & \text{if } x \in (0, 1] \\ \frac{3}{x^3} - 2 \leq f(x) \leq 2 & \text{if } x > 1 \end{cases}.$$

These piecewise constraints can be aggregated compactly into a boxed input-dependent affine constraint  $b^\ell(x) \leq a(x)f(x) \leq b^u(x)$  with

$$a(x) = 1, \quad (b^\ell(x), b^u(x)) = \begin{cases} \left(5 \sin^2 \frac{\pi}{2}(x+1) - 2, -3 \sin \frac{\pi}{2}(x+1)\right), & x \leq -1, \\ (-2, -2), & x \in (-1, 0], \\ \left((4 - 9(x - \frac{2}{3})^2)x, 3 - 4(x - 0.5)^2\right), & x \in (0, 1], \\ \left(\frac{3}{x^3} - 2, 2\right), & x > 1. \end{cases}$$

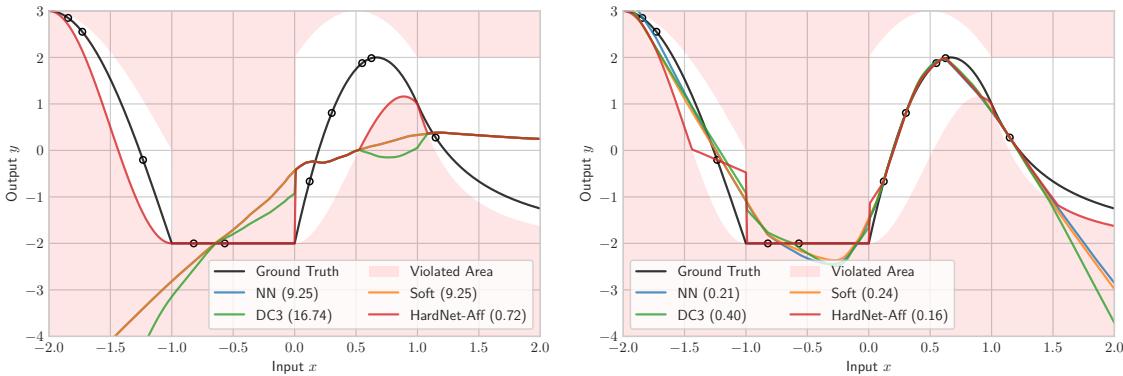


Figure 7: Learned functions at the initial (left) and final (right) epochs with the piecewise box constraints. The models are trained on the samples indicated with circles, with their MSE distances from the true function shown in parentheses. HardNet-Aff adheres to the constraints from the start of the training. On the other hand, the baselines violate the constraints throughout the training.

Table 6: Results for learning with the piecewise constraints. HardNet-Aff attains a comparable MSE distance from the true function as other methods without any constraint violation. The max and mean of constraint violations are computed over 401 test samples. Better (resp. worse) values are colored greener (resp. redder). Standard deviations over 5 runs are shown in parentheses.

	MSE	max violation	mean violation	$T_{\text{test}}$ (ms)	$T_{\text{train}}$ (s)
NN	0.14 (0.04)	0.92 (0.15)	0.12 (0.02)	0.14 (0.00)	2.52 (0.09)
Soft	0.15 (0.05)	0.99 (0.18)	0.11 (0.02)	0.16 (0.03)	2.56 (0.07)
DC3	0.20 (0.10)	1.27 (0.43)	0.12 (0.05)	6.84 (0.04)	16.61 (0.16)
HardNet-Aff	0.15 (0.01)	0.00 (0.00)	0.00 (0.00)	0.93 (0.01)	5.29 (0.15)

In this experiment, all models are trained on ten randomly sampled points in the domain  $[-2, 2]$ . Figure 7 contrasts the learned functions at epoch 0 and epoch 1000. Despite this extreme sparsity, HardNet-Aff satisfies the box constraints from the very first epoch and retains feasibility throughout training. While the baselines breach the constraints at many inputs, HardNet-Aff respects them everywhere and typically tracks the true function more closely in regions with no data. Quantitative metrics averaged over five runs appear in Table 6. HardNet-Aff attains competitive mean-squared error (MSE) while incurring *zero* violation, at the cost of only a modest increase in training time.

### D.3 Details for the Safe Control Experiment

In this experiment, we consider controlling a unicycle system with system state  $x = [x_p, y_p, \theta, v, w]^\top$  which represents the pose, linear velocity, and angular velocity. The dynamics

of the unicycle system is given by

$$\begin{bmatrix} \dot{x}_p \\ \dot{y}_p \\ \dot{\theta} \\ \dot{v} \\ \dot{w} \end{bmatrix} = \begin{bmatrix} v \cos \theta \\ v \sin \theta \\ w \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{\text{lin}} \\ a_{\text{ang}} \end{bmatrix},$$

with the linear and angular accelerations  $a_{\text{lin}}, a_{\text{ang}}$  as the control inputs.

To avoid an elliptical obstacle centered at  $(c_x, c_y)$  with its radii  $r_x, r_y$ , one could consider the following CBF candidate:

$$h_{\text{ellipse}}(x) = \left( \frac{c_x - (x_p + l \cos \theta)}{r_x} \right)^2 + \left( \frac{c_y - (y_p + l \sin \theta)}{r_y} \right)^2 - 1,$$

where  $l$  is the distance of the body center from the differential drive axis of the unicycle system. However, it is not a valid CBF since the safety condition (9) does not depend on the control input (i.e.,  $\nabla h_{\text{ellipse}}(x)^\top g(x) = 0 \ \forall x$ ). Instead, we can exploit a higher-order CBF (HOCBF) given by

$$h(x) = \dot{h}_{\text{ellipse}}(x) + \kappa h_{\text{ellipse}}(x),$$

for some  $\kappa > 0$ . Then, ensuring  $h \geq 0$  implies  $\dot{h} \geq 0$  given  $h(x(0)) \geq 0$ , and the safety condition (9) for this  $h$  depends on both control inputs  $a_{\text{lin}}, a_{\text{ang}}$ . Refer to Tayal et al. (2024) for a detailed explanation.

The goal of this problem is to optimize the neural network policy  $\pi_\theta(x) = \pi_{\text{nom}}(x) + f_\theta(x)$  to minimize the expected cost over the trajectories from random initial points within the range from  $[-4, 0, -\pi/4, 0, 0]$  to  $[-3.5, 0.5, -\pi/8, 0, 0]$ . For an initial state sample  $x_s$ , we consider the cost of the rolled-out trajectory through discretization with time step  $\Delta t = 0.02$  and  $n_{\text{step}} = 50$  as

$$\Delta t \sum_{i=0}^{n_{\text{step}}-1} x_i^\top Q x_i + \pi_\theta(x_i)^\top R \pi_\theta(x_i), \quad (32)$$

where  $x_i$  is the state after  $i$  steps, and  $Q = \text{diag}(100, 100, 0, 0.1, 0.1)$  and  $R = \text{diag}(0.1, 0.1)$  are diagonal matrices. The neural network policies are optimized to reduce (32) summed over 1000 randomly sampled initial points.