Abstract

Deep equilibrium models are based on implicitly defined functional relations and have shown competitive performance compared with the traditional deep networks. Monotone operator equilibrium networks (monDEQ) retain interesting performance with additional theoretical guaranties. Existing certification tools for classical deep networks cannot directly be applied to monDEQs for which much fewer tools exist. We introduce a semialgebraic representation for ReLU based monDEQs which allows to approximate the corresponding input output relation by semidefinite programming (SDP). We present several applications to network certification and obtain SDP models for the following problems: robustness certification, Lipschitz constant estimation, ellipsoidal uncertainty propagation. We use these models to certify robustness of monDEQs w.r.t. a general $L_q$ norm. Experimental results show that the proposed models outperform existing approaches for monDEQ certification. Furthermore, our investigations suggest that monDEQs are much more robust to $L_2$ perturbations than $L_\infty$ perturbations.

1 Introduction

With the increasing success of Deep Neural Networks (DNN) (e.g. computer vision, natural language processing), one witnesses a significant increase in size and complexity (topology and activation functions). This generates difficulties for theoretical analysis and a posteriori performance evaluation. This is problematic for applications where robustness issues are crucial, for example inverse problems (IP) in scientific computing. Indeed such IPs are notoriously ill-posed and as stressed in the March 2021 issue of SIAM News [1], “Yet DL has an Achilles' heel. Current implementations can be highly unstable, meaning that a certain small perturbation to the input of a trained neural network can cause substantial change in its output. This phenomenon is both a nuisance and a major concern for the safety and robustness of DL-based systems in critical applications—like healthcare—where reliable computations are essential”. Indeed, the Instability Theorem [1] predicts unavoidable lower bound on Lipschitz constants, which may explain the lack of stability of some DNNs, over-performing on training sets. This underlines the need to evaluate precisely a posteriori critical indicators, such as Lipschitz constants of DNNs. However, obtaining an accurate upper bounds on the Lipschitz constant of a DNN is a hard problem, it reduces to prove a global inequality $\Psi(x) \geq 0$ for all $x$ in a domain”,
i.e., to provide a \textit{proof of positivity} for a function $\Psi$, which has no simple explicit expression. Even for modest size DNNs this task is practically challenging, previous successful attempts \cite{8, 28} were restricted in practice to no more than two hidden layers with less than a hundred nodes. More broadly existing attempts to DNN certification rely either on zonotope calculus, linear programming (LP) or hierarchies of SDP based on positivity certificates from algebraic geometry \cite{34}, which may suffer from the curse of dimensionality.

Recently, implicit deep learning \cite{12} arises as a generalization of the recursive rules of traditional feedforward neural networks. Specifically, \textit{Deep Equilibrium Models (DEQ)} \cite{2} have emerged as a potential alternative to classical DNNs. With their much simpler layer structure, they provide competitive results on machine learning benchmarks \cite{2, 3}. Training DEQs involves solving fixed-point equations, which requires further conditions to make the iteration converge. Fortunately, \textit{Monotone operator equilibrium network (monDEQ)} introduced in \cite{45} satisfies such conditions. Moreover, the authors in \cite{33} provide explicit bounds on global Lipschitz constant of monDEQs (w.r.t. the $L_2$-norm) which can be used for robustness certification.

From a certification point of view, DEQs have the definite advantage of having only one implicit layer compared to DNNs and therefore is potentially more amenable to sophisticated techniques (e.g. algebraic certificates of positivity) which rapidly face their limit even for classical DNNs with modest size (but long depth). Therefore monDEQs constitute a class of DNNs for which robustness certification, uncertainty propagation or Lipschicity could potentially be investigated in a more satisfactory way than classical networks. Contrary to DNNs, for which a variety of tools have been developed, certification of DEQ models is relatively open, the only available tool is the Lipschitz bound in \cite{33}.

\textbf{Contribution}

We present three general semialgebraic models of ReLU monDEQ for certification ($p \in \mathbb{Z}_+ \cup \{+\infty\}$):

- \textit{Robustness Model} for network $L_p$ robustness certification.
- \textit{Lipschitz Model} for network Lipschitz constant estimation with respect to any $L_p$ norm.
- \textit{Ellipsoid Model} for ellipsoidal outer-approximation of the image by the network of a polyhedra or an ellipsoid.

All these models can be used for robustness certification, a common task which we consider experimentally. And the main originality of this work is to successfully apply the proposed techniques to monDEQ networks (especially for the Ellipsoid model which is a novel form of reachability analysis), which was not proposed before. Both Lipschitz and Ellipsoid models can in addition be used for further a posteriori analyses. Interestingly, all three models are given by solutions of semidefinite programs (SDP), obtained by Shor relaxation of a common semialgebraic representation of ReLU monDEQs. Our models are all evaluated to simple ReLU monDEQs on MNIST dataset similar as \cite{45, 33} on the task of robustness certification. We demonstrate that all three models outperform the approach of \cite{33} and the Robustness Model being the most efficient. Our experiments also suggest that DEQs are much less robust to $L_\infty$ perturbations than $L^2$ perturbations, in contrast with classical DNNs \cite{36} which have been shown to be robust on MNIST dataset to the level we are considering ($\varepsilon = 0.1$).

\textbf{Related works}

Neural network certification is a challenging topic in machine learning, contributions include:

\textbf{Robustness certification of DNNs} Even with high test accuracy, DNNs are very sensitive to tiny input perturbations, see e.g. \cite{42, 16}. Robustness to input perturbation has been investigated in many different works with various techniques, including SDP relaxation in SDP-cert \cite{36}, first-order dual SDP method \cite{10}, abstract interpretation with ERAN \cite{15, 31}, multi-neuron convex relaxations with PRIMA \cite{31}, GPU-based method GPUPoly \cite{30} which can scale to large networks with one million neurons and 34 layers, scalable quantitative verification framework with PROVERBO \cite{4}, LP relaxation in Reluplex \cite{25}, analytical certification with Fast-lin \cite{44} and CROWN \cite{47}, and their extension to convolutional neural networks with CNN-Cert \cite{7}. All these methods are restricted to DNNs or CNNs and do not directly apply to DEQs.
Lipschitz constant estimation of DNNs  
Lipschitz constant of DNNs can be used for robustness certification \[22\] \[18\]. Existing contributions include naive layer-wise product bound \[22\] \[43\], controlled ordinary differential equations (ODE) method \[20\], zonotope-based method \[24\] which can be further extended to generative models, Mixed-Integer Programming (MIP) \[23\] for exactly computing the local Lipschitz constant of ReLU networks, the LP relaxations for CNNs \[43\] and DNNs \[28\], as well as SDP relaxations \[35\] \[14\] \[8\].

Lipschitz constant estimation of DEQs  
The authors in \[45\] provide an optimization-free upper bound of the Lipschitz constant of monDEQs depending on network weights. This bound is valid for \(L^2\) norm and we present a general model for arbitrary \(L^p\) norm. Based on the works of \[43\], the authors in \[38\] introduced new parameterizations of DEQs that admit a Lipschitz bound during training via unconstrained optimization.

2 Preliminary Background and Notations

We consider the \(\text{ReLU}()\) function, which is simply defined as \(\text{ReLU}(x) = \max\{0, x\}\), and the output of the monDEQs can be written as

\[
F(x_0) = Cz + c, z = \text{ReLU}(Wz + Ux_0 + u), \tag{monDEQ}
\]

where \(W \in \mathbb{R}^{p \times p}, U \in \mathbb{R}^{p \times m}, u \in \mathbb{R}^{p}, C \in \mathbb{R}^{K \times p}, c \in \mathbb{R}^K\) are parameters of the network. The vector-valued function \(F(x_0)\) provides a score for each label \(i \in \{1, \ldots, K\}\) associated to the input \(x_0\), the prediction corresponds to the highest score, i.e., \(y_{x_0} = \arg \max_{i=1,\ldots,K} F(x_0)_i\). As in \[45\], the matrix \(I_p - W\) is strongly monotone: there is a known \(m > 0\) such that \(I_p - W \geq mI_p\), this constraint can be enforced by specific parametrization of the matrix \(W\). With the monotonicity assumption, the solution to equation \(z = \text{ReLU}(Wz + Ux_0 + u)\) is unique and can be evaluated using convergent algorithms, see \[45\] for more details.

Robustness of monDEQs: Given an input \(x_0 \in \mathbb{R}^p\), a norm \(\|\cdot\|\), and a network \(F : \mathbb{R}^p \to \mathbb{R}^K\), let \(y_0\) be the label of input \(x_0\), i.e., \(y_0 = \arg \max_{i=1,\ldots,K} F(x_0)_i\). For \(\varepsilon > 0\), denote by \(E = B(x_0, \varepsilon, \|\cdot\|)\) the ball centered at \(x_0\) with radius \(\varepsilon\) for norm \(\|\cdot\|\). If for all inputs \(x \in E\), the label of \(x\) equals \(y_0\), i.e., \(y = \arg \max_{i=1,\ldots,K} F(x)_i = y_0\), then we say that the network \(F\) is \(\varepsilon\)-robust at input \(x_0\) for norm \(\|\cdot\|\). An equivalent way to verify whether the network \(F\) is \(\varepsilon\)-robust is to check that for all labels \(i \neq y_0\), \(F(x)_i - F(x)_{y_0} < 0\).

Semialgebraicity of ReLU function: The key reason why neural networks with ReLU activation function can be tackled using polynomial optimization techniques is semialgebraicity of the ReLU function, i.e., it can be expressed with a system of polynomial (in)equalities. For \(x, y \in \mathbb{R}\), we have \(y = \text{ReLU}(x) = \max\{0, x\}\) if and only if \(y(y - x) = 0, y \geq x, y \geq 0\). For \(x, y \in \mathbb{R}^n\), we denote by \(\text{ReLU}(x)\) the coordinate-wise evaluation of \(\text{ReLU}\) function, and by \(xy\) the coordinate-wise product of \(x\) and \(y\). A subset of \(\mathbb{R}^n\) defined by a finite conjunction of polynomial (in)equalities is called a basic closed semialgebraic set. The graph of the \(\text{ReLU}\) function is a basic closed semialgebraic set.

Going back to equation \(\text{monDEQ}\), we have the following equivalence:

\[
z = \text{ReLU}(Wz + Ux_0 + u) \iff z(z - Wz - Ux_0 - u) = 0, z \geq Wz + Ux_0 + u, z \geq 0, \tag{1}
\]

where the right hand side is a system of polynomial (in)equalities. For the rest of the paper, mention of the \(\text{ReLU}\) function will refer to the equivalent polynomial system in \(1\).

POP and Putinar’s positivity certificate: In general, a polynomial optimization problem (POP) has the form

\[
\rho = \max_{x \in \mathbb{R}^n} \{ f(x) : g_i(x) \geq 0, i = 1, \ldots, p \}, \tag{POP_0}
\]
where \( f \) and \( g_i \) are polynomials whose degree is denoted by \( \text{deg} \). The robustness certification model (3.1), Lipischitz constant model (3.2) and ellipsoid model (3.3) are all POPs.

In most cases, the POPs are non-linear and non-convex problems, which makes them NP-hard. A typical approach to reduce the complexity of these problems is replacing the positivity constraints by Putinar’s positivity certificate [34]. The problem (POP) is equivalent to

\[
\rho = \min_{\lambda \in \mathbb{R}} \{ \lambda : \lambda - f(x) \geq 0, g_i(x) \geq 0, i = 1, \ldots, p, \forall x \in \mathbb{R}^n \}. \quad \text{(POP)}
\]

In order to reduce the size of the feasible set of problem (POP), we replace the positivity constraint \( \lambda - f(x) \geq 0 \) by a weighted sum-of-square (SOS) polynomial decomposition, involving the polynomials \( g_i \). Let \( d \) be a non-negative integer. Denote by \( \sigma_0^d(x) \), \( \sigma_i^d(x) \) some SOS polynomials of degree at most \( 2d \), for each \( i = 1, \ldots, p \). Note that if \( d = 0 \), such polynomials are non-negative real numbers.

Then the positivity of \( \lambda - f(x) \) is implied by the following decomposition

\[
\lambda - f(x) = \sigma_0^d(x) + \sum_{i=1}^p \sigma_i^{d-\omega_i}(x)g_i(x), \quad \omega_i = \lceil \text{deg } g_i/2 \rceil, \forall x \in \mathbb{R}^n, \quad (2)
\]

for any \( d \geq \max_i \omega_i \). Equation (2) is called the order-\( d \) Putinar’s certificate. By replacing the positivity constraint \( f(x) - \lambda \geq 0 \) in problem (POP) by Putinar’s certificate (2), we have for \( d \geq \max_i \omega_i \),

\[
\rho_d = \min_{\lambda \in \mathbb{R}} \{ \lambda : \lambda - f(x) = \sigma_0^d(x) + \sum_{i=1}^p \sigma_i^{d-\omega_i}(x)g_i(x), \omega_i = \lceil \text{deg } g_i/2 \rceil, \forall x \in \mathbb{R}^n \}. \quad \text{(POP-d)}
\]

It is obvious that \( \rho_d \geq \rho \) for all \( d \geq \max_i \omega_i \). Under certain conditions (slightly stronger than compactness of the set of constraints), it is shown that \( \lim_{d \to \infty} \rho_d = \rho \) [27]. The main advantage of relaxing problem (POP) to (POP-d) is that problem (POP-d) can be efficiently solved by semidefinite programming (SDP). Indeed a polynomial \( f \) of degree at most \( 2d \) is SOS if and only if there exists a positive semidefinite (PSD) matrix \( M \) (called a Gram matrix) such that \( f(x) = v(x)^T M v(x) \), for all \( x \in \mathbb{R}^p \), where \( v(x) \) is the vector of monomials of degree at most \( d \).

Problem (POP-d) is also called the order-\( d \) Lasserre’s relaxation. When the input polynomials are quadratic, the order-1 Lasserre’s relaxation is also known as Shor’s relaxation [40]. All our models are obtained using variations of Shor’s relaxation applied to different POPs, see Section 3.3 for more details.

### 3 Semialgebraic Models for Certifying Robustness of Neural Networks

In this section, we introduce several models for certification of monDEQs. All the models are based on semialgebraicity of ReLU and \( \partial \)ReLU (the subgradient of ReLU, see Section 3.2) to translate our targeted problems to POPs. Then we use Putinar’s certificates, defined in Section 3.2 to relax the non-convex problems to convex SDPs which can be solved efficiently using modern solvers.

**Notation:** Throughout this section, we consider a monDEQ for classification, denoted by \( F \), with fixed, given parameters, \( W \in \mathbb{R}^{p \times p}, U \in \mathbb{R}^{p \times p_0}, u \in \mathbb{R}^p, C \in \mathbb{R}^{K \times p}, c \in \mathbb{R}^K \), where \( p_0 \) is the number of input neurons, \( p \) is the number of hidden neurons, and \( K \) is the number of labels. For \( q \in \mathbb{Z}_+ \cup \{ +\infty \}, \| \cdot \|_q \) is the \( L_q \) norm defined by \( \| x \|_q := (\sum_{i=1}^{p_0} |x_i^q|^q)^{1/q} \) for all \( x \in \mathbb{R}^{p_0} \). Throughout this section \( \epsilon > 0 \) and \( x_0 \in \mathbb{R}^{p_0} \) are fixed, we denote by \( \mathcal{E} := \mathbb{B}(x_0, \epsilon, \| \cdot \|_q) = \{ x \in \mathbb{R}^{p_0} : \| x - x_0 \|_q \leq \epsilon \} \) the ball centered at \( x_0 \) with radius \( \epsilon \) for \( L_q \) norm, a perturbation region. If \( q < +\infty \), i.e., \( q \) is a positive integer, \( \| x - x_0 \|_q \leq \epsilon \) is equivalent to the polynomial inequality \( \| x - x_0 \|_q \leq \epsilon^q \); if \( q = \infty \), \( \| x - x_0 \|_\infty \leq \epsilon \) is equivalent to \( \| x - x_0 \|_2 \leq \epsilon^2 \) (where \( |x| \) denotes the vector of absolute values of coordinates of \( x \) which is a system of \( p_0 \) polynomial inequalities. Hence the input set \( \mathcal{E} \) is a semialgebraic set for all considered \( L_q \) norms. For a matrix \( A \in \mathbb{R}^{m \times n} \), its operator norm induced by the norm \( \| \cdot \| \) is given by \( \| A \| := \inf \{ \lambda : \| Ax \| \leq \lambda \| x \|, \forall x \in \mathbb{R}^n \} \).

#### 3.1 Robustness Model

Let \( y_0 \) be the label of \( x_0 \) and let \( z \in \mathbb{R}^p \) be the variables in the monDEQ implicit layer. The proposed model directly estimates upper bounds on the gap between the score of label \( y_0 \) and the score of labels
different from \(y_0\). Precisely, for \(i \in \{1, \ldots, K\}\) such that \(i \neq y_0\), denote by \(\xi_i = (C_{i*} - C_{y_0*})^T\). For \(x \in \mathcal{E}\), the gap between its score of label \(i\) and label \(y_0\) is \(F(x)_i - F(x)_{y_0} = \xi_i^T z\). The Robustness Model for monDEQ reads:

\[
\delta_i := \max_{x \in \mathbb{R}^n, z \in \mathbb{R}^r} \{\xi_i^T z : z = \text{ReLU}(Wz + Ux + u), x \in \mathcal{E}\}. \tag{CertMON-i}
\]

Using the semialgebraicity of both ReLU in \([1]\), and set \(\mathcal{E}\), problem (CertMON-i) is a POP for all \(i\). As discussed in Section 2, one is able to derive a sequence of SDPs (Lasserre’s relaxation) to obtain a converging serie of upper bounds of the optimal solution of (CertMON-i). For Robustness Model, we consider only the order-1 Lasserre’s relaxation (Shor’s relaxation), and denote by \(\delta_i\) the upper bound of \(\delta_i\) by Shor’s relaxation, i.e., \(\delta_i \leq \hat{\delta}_i\). Recall that if for all label \(i\) different from \(y_0\), we have \(F(x)_i < F(x)_{y_0}\), then the label of \(x\) is still \(y_0\). This justifies the following claim:

**Certification criterion:** If \(\hat{\delta}_i < 0\) for all \(i \neq y_0\), then the network \(F\) is \(\varepsilon\)-robust at \(x_0\).

Robustness Model for DNNs has already been investigated in \([36]\), where the authors also use Shor’s relaxation as we do. Different from DNNs, we only have one implicit layer in monDEQ. Therefore, the number of variables in problem (CertMON-i) only depends on the number of input neurons \(p_0\) and hidden neurons \(p\).

### 3.2 Lipschitz Model

We bound the Lipschitz constant of monDEQ with respect to input perturbation. Recall that the *Lipschitz constant* of the vector-valued function \(F\) (resp. \(z\)) w.r.t. the \(L_q\) norm and input ball \(\mathcal{S} \supset \mathcal{E}\), denoted by \(L^q_{F,\mathcal{S}}\) (resp. \(L^q_{z,\mathcal{S}}\)), is the smallest value of \(L\) such that \(\|F(x) - F(y)\|_q \leq L \|x - y\|_q\) (resp. \(\|z(x) - z(y)\|_q \leq L \|x - y\|_q\)) for all \(x, y \in \mathcal{S}\). For \(x, x_0 \in \mathcal{S}\), with \(\|x - x_0\|_q \leq \varepsilon\), we can estimate the perturbation of the output as follows:

\[
\begin{align*}
\|F(x) - F(x_0)\|_q & \leq L^q_{F,\mathcal{S}} \cdot \|x - x_0\|_q \leq \varepsilon L^q_{F,\mathcal{S}}, \quad \text{(3)}
\|F(x) - F(x_0)\|_q & \leq \|C\|_q \cdot L^q_{z,\mathcal{S}} \cdot \|x - x_0\|_q \leq \varepsilon \|C\|_q \cdot L^q_{z,\mathcal{S}}, \quad \text{(4)}
\end{align*}
\]

The authors in \([33]\) use inequality (4) with \(q = 2\), as they provide an upper bound of \(L^2_{z,\mathcal{S}}\). In contrast, our model provides upper bounds on Lipschitz constants of \(F\) or \(z\) for arbitrary \(L_q\) norms. We directly focus on estimating the value of \(L^q_{F,\mathcal{S}}\) instead of \(L^q_{z,\mathcal{S}}\).

Since the ReLU function is not smooth, we define its *subgradient*, denoted by \(\partial \text{ReLU}\), as the set-valued map \(\partial \text{ReLU}(x) = 0\) for \(x < 0\), \(\partial \text{ReLU}(x) = 1\) for \(x > 0\), and \(\partial \text{ReLU}(x) = [0, 1]\) for \(x = 0\). Similar to ReLU function, \(\partial \text{ReLU}\) is also semialgebraic.

**Semialgebraicity of \(\partial \text{ReLU}\):** If \(x, y \in \mathbb{R}\), we have \(y \in \partial \text{ReLU}(x)\), if and only if \(y(y - 1) \leq 0, xy \geq 0, x(y - 1) \geq 0\). If \(x, y \in \mathbb{R}^n\), then \(\partial \text{ReLU}(x)\) denotes the coordinate-wise evaluation of \(\partial \text{ReLU}\). Going back to monDEQ, let \(s\) be any subgradient of the implicit variable: \(s \in \partial \text{ReLU}(Wz + Ux + u)\). We can write equivalently a system of polynomial inequalities:

\[
s(s - 1) \leq 0, s(Wz + Ux + u) \geq 0, (s - 1)(Wz + Ux + u) \geq 0. \tag{5}
\]

For the following discussion, \(\partial \text{ReLU}\) will refer to the equivalent polynomial systems (5).

With the semialgebraicity of ReLU in \([1]\) and \(\partial \text{ReLU}\) in \([5]\), one is able to compute upper bounds of the Lipschitz constant of \(F\) via POPs. The proof of the next Lemma is postponed to Appendix [A.1]

**Lemma 1** Define

\[
\hat{L}^q_{F,\mathcal{S}} = \max \{t^T U^T y : t, x \in \mathbb{R}^{p_0}, s, z, y, r, v, w \in \mathbb{R}^K, x \in \mathcal{S}, \|t\|_q \leq 1, w^T v \leq 1, \|w\|_q \leq 1, r - W^T y = C^T v, y = \text{diag}(s) \cdot r; s \in \partial \text{ReLU}(Wz + Ux + u), z = \text{ReLU}(Wz + Ux + u)\} \quad \text{(LipMON)}
\]

Then \(\hat{L}^q_{F,\mathcal{S}}\) is an upper bound of the Lipschitz constant of \(F\) w.r.t. the \(L_q\) norm, i.e., \(L^q_{F,\mathcal{S}} \leq \hat{L}^q_{F,\mathcal{S}}\).

Since problem (LipMON) is a POP, we also consider Shor’s relaxation and denote by \(\hat{L}^q_{F,\mathcal{S}}\) the upper bound of \(\hat{L}^q_{F,\mathcal{S}}\) by Shor’s relaxation, i.e., \(\hat{L}^q_{F,\mathcal{S}} \leq \hat{L}^q_{F,\mathcal{S}}\). Define \(\delta := \varepsilon \hat{L}^q_{F,\mathcal{S}}\). By equations (4), if
$E \subset S$, using Lemma 3.2 and the fact that $\| \cdot \|_\infty \leq \| \cdot \|_q$, we have $\| F(x) - F(x_0) \|_\infty \leq \delta$, yielding the following criterion:

**Certification criterion:** Let $y_0$ be the label of $x_0$. Define $\tau := F(x_0)y_0 - \max_{k \neq y_0} F(x_k)_k$. If $2\delta < \tau$, then the network $F$ is $\varepsilon$-robust at $x_0$.

**Remark:** In order to avoid some possible numerical issues, we add some bound constraints and redundant constraints to problem (LipMON), see Appendix A.2 for details. Shor’s relaxation of Lipschitz Model for DNNs has already been extensively investigated in [4–8]. If one want to certify robustness for several input test examples, then one may choose $S$ to be a ball containing all such examples with an additional margin of $\epsilon$. Choosing a big ball for all input points requires to solve only one optimization problem, while choosing one ball for each input point (say among $N$) requires to solve $N$ optimization problems, which is much more costly. In this case it is more favorable to use the Certification Model directly.

### 3.3 Ellipsoid Model

As above, the input region $E$ is a neighborhood of input $x_0 \in \mathbb{R}^p_0$ with radius $\varepsilon$ for the $L_q$ norm, i.e., $E = \{x \in \mathbb{R}^p : \|x - x_0\|_q \leq \varepsilon\}$. More generally, $E$ could be other general semialgebraic sets, such as polytopes or zonotopes. Denote by $F(E)$ the image of $E$ by $F$. In this section, we aim at finding a semialgebraic set $C$ such that $F(E) \subseteq C$. We choose $C$ to be an ellipsoid which can in turn be used for robustness certification. Our goal is to find such outer-approximation ellipsoid with minimum volume. Let $C := \{x \in \mathbb{R}^d : \|Qx + b\|_2 \leq 1\}$ be an ellipsoid in the output space $\mathbb{R}^d$ parametrized by $Q \in S^d$ and $b \in \mathbb{R}^d$, where $S^d$ is the set of PSD matrices of size $d \times d$. The problem of finding the minimum-volume ellipsoid containing the image $F(E)$ can be formulated as

$$\max_{Q \in S^d, b \in \mathbb{R}^d} \{\det(Q) : x \in E, \|Q(Cz + c) + b\|_2 \leq 1, z = \text{ReLU}(Wz + Ux + u)\}.$$  
(EllipMON-POP)

By semialgebraicity of both ReLU in (1) and $C$, problem (EllipMON-POP) can be cast as a POP (the determinant being a polynomial). We no longer apply Shor’s relaxation, we rather replace the non-negativity output constraint $1 - \|Q(Cz + c) + b\|_2 \geq 0$ by a stronger Putinar’s certificate related to both ReLU and input constraints. We can then relax the non-convex problem (EllipMON-POP) to a problem with SOS constraints, which can be reformulated by (convex) SDP constraints. This is due to the fact that a polynomial $f$ of degree at most $2d$ is SOS if and only if there exists a PSD matrix $M$ (called a *Gram matrix*) such that $f(x) = v(x)^T M v(x)$, for all $x \in \mathbb{R}^p$, with $v(x)$ being the vector containing all monomials of degree at most $d$. In summary, we relax problem (EllipMON-POP) to an SOS constrained problem keeping the determinant unchanged:

$$\max_{Q \in S^d, b \in \mathbb{R}^d} \{\det(Q) : 1 - \|Q(Cz + c) + b\|_2^2 = \sigma_0(x, z) + \sigma_1(x, z)^T g_q(x - x_0) + \tau(x, z)^T (z - Wz - Ux - u) + \sigma_2(x, z)^T (z - Wz - Ux - u) + \sigma_3(x, z)^T z\}.$$  
(EllipMON-SOS-d)

where $g_q(x) = \varepsilon^q - \|x\|_q^q$ for $q < +\infty$ and $g_\infty(x) = \varepsilon^2 - \|x\|^2$ for $q = +\infty$, $\sigma_0$ is a vector of SOS polynomials of degree at most $2d$, $\sigma_1$ is a vector of SOS polynomials of degree at most $2(d - \lfloor q/2 \rfloor)$ for $q < +\infty$ and $2d - 2$ for $q = +\infty$, $\sigma_2$, $\sigma_3$ are vectors of SOS polynomials of degrees at most $2d - 2$, $\tau$ is a vector of polynomials of degree at most $2d - 2$. Problem (EllipMON-SOS-d) provides an ellipsoid feasible for (EllipMON-POP), that is an ellipsoid which contains $F(E)$. In practice, the determinant is replaced by a log-det objective because there exist efficient solver dedicated to optimize such objectives on SDP constraints. By increasing the relaxation order $d$ in problem (EllipMON-SOS-d), one is able to obtain a hierarchy of log-det objectied SDP problems for which the outer-approximation ellipsoids have decreasing volumes.

In this paper, we only consider the case $p = 2, \infty$, and order-1 relaxation ($d = 1$). Therefore, $\sigma_i$ and $\tau$ are all (vectors of) real (non-negative) numbers for $i = 1, 2, 3$, except that $\sigma_0$ is an SOS polynomial of degree at most $2$. In this case, problem (EllipMON-SOS-d) is equivalent to a problem with log-det objective and SDP constraints, as the following lemma states (proof postponed to Appendix A.3):

**Lemma 2** For $p = 2$ or $p = \infty$, problem (EllipMON-SOS-d) with $d = 1$ is equivalent to

$$\max_{Q \in S^d, b \in \mathbb{R}^d, \sigma_1, \sigma_2, \sigma_3 \geq 0, \tau \in \mathbb{R}} \{\log \det(Q) : -M \preceq 0\}.$$  
(EllipMON-SDP)
where $M \in \mathbb{S}^{(p_0+p+1) \times (p_0+p+1)}$ is a symmetric matrix parametrized by the decision variables $(Q, b)$, the coefficients $(\sigma_1, \sigma_2, \sigma_3, \tau)$, and the parameters of the network $(W, U, u, C, c)$.

Since the outer-approximation ellipsoid $C = \{\xi \in \mathbb{R}^K : ||Q\xi + b||_2 \leq 1\}$ contains the image $F(\mathcal{E})$, i.e., all possible outputs of the input region $\mathcal{E}$, one is able to certify robustness by solving the following optimization problems.

**Certification criterion:** Let $y_0$ be the label of $x_0$. For $i \neq y_0$, define $\delta_i := \max_{\xi \in \mathbb{R}^K} \{\xi_i - \xi_{y_0} : ||Q\xi + b||_2 \leq 1\}$. If $\delta_i < 0$ for all $i \neq y_0$, then the network $F$ is $\varepsilon$-robust at $x_0$.

The certification criterion for Ellipsoid Model has a geometric explanation: for $i \neq y_0$, denote by $P_i$ the projection map from output space $\mathbb{R}^K$ to its 2-dimensional subspace $\mathbb{R}_{y_0} \times \mathbb{R}_i$, i.e., $P_i(\xi) = [\xi_{y_0}, \xi_i]^T$ for all $\xi \in \mathbb{R}^K$. Let $L_i$ be the line in subspace $\mathbb{R}_{y_0} \times \mathbb{R}_i$ defined by $\{[\xi_{y_0}, \xi_i]^T \in \mathbb{R}_{y_0} \times \mathbb{R}_i : \xi_{y_0} = \xi_i\}$. Then the network $F$ is $\varepsilon$-robust if the projection $P_i(C)$ lies strictly below the line $L_i$ for all $i \neq y_0$. We give an explicit example in Section 4.3 to visually illustrate this.

### 3.4 Summary of the Models

We have already presented three models which can all be dedicated to certify robustness of neural networks. However, the size and complexity of each model are different. We summarize the number of variables in each model and the maximum size of PSD matrices in the resulting Shor’s relaxation, see Table 1. The complexity of our models only depends on the number of neurons in the input layer and implicit layer. The size of PSD matrices is a limiting factor for SDP solvers, our models are practically restricted to network for which such size can be handled by SDP solvers. For the popular dataset MNIST [46], whose input dimension is $28 \times 28 = 768$, we are able to apply our model on monDEQs with moderate size implicit layers (87) and report the corresponding computation time.

<table>
<thead>
<tr>
<th>Model</th>
<th>Num. of variables</th>
<th>Max. size of PSD matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robustness Model</td>
<td>$p_0 + p$</td>
<td>$1 + p_0 + p$</td>
</tr>
<tr>
<td>Lipschitz Model</td>
<td>$2p_0 + 4p + 2K$</td>
<td>$1 + 2p_0 + 4p + 2K$</td>
</tr>
<tr>
<td>Ellipsoid Model</td>
<td>$p_0 + 3p + K + K^2$</td>
<td>$1 + p_0 + p$</td>
</tr>
</tbody>
</table>

### 4 Experiments

In this section, we present the experimental results of Robustness Model, Lipschitz Model and Ellipsoid Model described in Section 3 for a pretrained monDEQ on MNIST dataset. The network we use consists of a fully-connected implicit layer with 87 neurons and we set its monotonicity parameter $m$ to be 20. The training hyperparameters are set to be the same as in Table D1 of [45], where the training code (in Python) is available at [https://github.com/locuslab/monotone_op_net](https://github.com/locuslab/monotone_op_net). Training is based on the normalized MNIST database in [45], we use the same normalization setting on each test example with mean $\mu = 0.1307$ and standard deviation $\sigma = 0.3081$, which means that each input is an image of size $28 \times 28$ with entries varying from $-0.42$ to $2.82$. And for every perturbation $\varepsilon$, we also take the normalization into account, i.e., we use the normalized perturbation $\varepsilon/\sigma$ for each input.

Since all our three models can be applied to certify robustness of neural networks, we first compare the performance of each model in certification of the first 100 test MNIST examples. Then we compare the upper bounds of Lipschitz Model with the upper bounds proposed in [33]. Finally we show that Ellipsoid Model can also be applied for reachability analysis. For Certification model and Lipschitz model, we implement them in Julia [5] with JuMP [11] package; for Ellipsoid model, we implement it in Matlab [39] with CVX [12] package. For all the three models, we use Mosek [29] as a backend to solve the targeted POPs. All experiments are performed on a personal laptop with an Intel 5-Core i7-8665U CPU @ 1.90GHz Ubuntu 18.04.5 LTS, 32GB RAM. The code of all our models is available at [https://github.com/NeurIPS2021Paper4075/SemiMonDEQ](https://github.com/NeurIPS2021Paper4075/SemiMonDEQ)
4.1 Robustness certification

We consider $\varepsilon = 0.1$ for the $L_2$ norm and $\varepsilon = 0.1, 0.05, 0.01$ for the $L_\infty$ norm. For each model, we compute the ratio of certified test examples among the first 100 test inputs. Following [33], we also compute the projected gradient descent (PGD) attack accuracy using Foolbox library [37], which indicates the ratio of non-successful attacks among our 100 inputs. Note that the ratio of certified examples should always be less or equal than the ratio of non-successful attacks. The gaps between them shows how many test examples there are for which we are neither able to certify robustness nor find adversarial attacks.

Remark: For Lipschitz Model, we use inequality (3) to test robustness, i.e., we compute directly the upper bound of the Lipschitz constant of $F$ rather than $z$ (seen as a function of $x$) where $S$ is a big ball containing all test examples.

Table 2: Ratio of certified test examples and running time per example by different methods. We consider $L_2$ norm with $\varepsilon = 0.1$ and $L_\infty$ norm with $\varepsilon = 0.1, 0.05, 0.01$. The ratio is based on the first 100 MNIST test examples, and we count the average computation time (with unit second) for one example of each method. The ratio in parentheses of the column “Lipschitz Model” are computed by the upper bound of Lipschitz constant given in [33] (see Section 4.2 for details). Exact binomial 95% confidence intervals are given in bracket.

<table>
<thead>
<tr>
<th>Norm</th>
<th>$\varepsilon$</th>
<th>Robustness Model (1500s / example)</th>
<th>Lipschitz Model (1500s in total)</th>
<th>Ellipsoid Model (500s / example)</th>
<th>PGD Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.1</td>
<td>99% [&gt;94]</td>
<td>91% (91%) [&gt;83]</td>
<td>99%[&gt;94]</td>
<td>99%[&gt;94]</td>
</tr>
<tr>
<td>$L_2$</td>
<td>0.1</td>
<td>0% [&lt;4]</td>
<td>0% (0%) [&lt;4]</td>
<td>0% [&lt;4]</td>
<td>15% [8, 24]</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>24% [16, 34]</td>
<td>0% (0%) [&lt;4]</td>
<td>0% [&lt;4]</td>
<td>82% [73, 89]</td>
</tr>
<tr>
<td></td>
<td>0.01</td>
<td>99% [&gt;94]</td>
<td>24% [16, 34] (0%) [&lt;4]</td>
<td>92% [&gt;84]</td>
<td>99% [&gt;94]</td>
</tr>
</tbody>
</table>

Figure 2 in Appendix A.4 shows the original image of the first test example (2a) and an adversarial attack (2b) for the $L_\infty$ norm with $\varepsilon = 0.1$ found by the PGD algorithm in [37].

4.2 Comparison with Lipschitz constants

In this section, we compare the upper bounds of Lipschitz constants computed by Lipschitz Model with the upper bounds proposed in [33]. Notice that the upper bounds in [33] only involve the function $z(x)$, hence we are only able to use inequality (4) to test robustness. In fact the quantity $\|C\|_q \cdot L^q_{z,S}$ can be regarded as an upper bound of $L^q_{F,S}$, the Lipschitz constant of $F$. We denote by $\text{UB}^2_z$ the upper bound of the Lipschitz constant of $z$ w.r.t. the $L_2$ norm, given by $B^2_z = \|U\|_2/m$ according to [33], where $U$ is the parameter of the network and $m$ is the monotonicity factor. We can then compute the upper bound w.r.t. the $L_\infty$ norm by $B^\infty_z = \sqrt{m_0} \cdot UB^2_z$ where $m_0$ is the input dimension. The upper bound of Lipschitz constant of $F$ is computed via the upper bound of $z$: $UB^\infty_z = \|C\|_q \cdot UB^2_z$. Denote similarly by $\text{SemiUB}^2_F$, the upper bounds of Lipschitz constants of $F$ provided by Lipschitz Model, w.r.t. the $L_2$ norm.
Table 3: Comparison of upper bounds of Lipschitz constant for $L_2$ and $L_{\infty}$ norm, and the corresponding computation time (with unit second).

<table>
<thead>
<tr>
<th>$q = 2$</th>
<th>$q = \infty$</th>
</tr>
</thead>
<tbody>
<tr>
<td>bound</td>
<td>time (s)</td>
</tr>
<tr>
<td>$UB_{q}^{F}$</td>
<td>4.80</td>
</tr>
<tr>
<td>$SemiUB_{q}^{F}$</td>
<td>4.67</td>
</tr>
</tbody>
</table>

From Table 3, we see that Lipschitz Model provides consistently tighter upper bounds than the ones in [33]. Especially for $L_{\infty}$ norm, the upper bound computed by $\|C\|_{\infty} \cdot UB_{z}^{\infty}$ is rather crude compared to the bound obtained directly by Lipschitz Model. Therefore, we are able to certify more examples using $SemiUB_{q}^{F}$ than $UB_{q}^{F}$, see Table 2.

4.3 Outer ellipsoid approximation

In this section, we provide a visible illustration of how Ellipsoid Model can be applied to certify robustness of neural networks.

Take the first MNIST test example (which is classified as 7) for illustration. For $\varepsilon = 0.1$, this example is certified to be robust for the $L_2$ norm but not for the $L_{\infty}$ norm. We show the landscape of the projections onto $\mathbb{R}_7 \times \mathbb{R}_3$, i.e., the $x$-axis indicates label 7 and the $y$-axis indicates label 3. In Figure 1, the red points are projections of points in the image $F(E)$, for $E$ an $L_2$ or $L_{\infty}$ norm perturbation zone, the black circles are projections of some (successful and unsuccessful) adversarial examples found by the PGD algorithm. Notice that the adversarial examples also lie in the image $F(E)$. The blue curve is the boundary of the projection of the outer-approximation ellipsoid (which is an ellipse), and the blue dashed line plays the role of a certification threshold. Figure 1a shows the landscape for the $L_2$ norm, we see that the ellipse lies strictly below the threshold line, which means that for all points $\xi \in C$, we have $\xi_3 < \xi_7$. Hence for all $\xi \in F(E)$, we also have $\xi_3 < \xi_7$. On the other hand, for the $L_{\infty}$ norm, we see from Figure 1b that the threshold line crosses the ellipse, which means that we are not able to certify robustness of this example by Ellipsoid Model. Indeed, we can find adversarial examples with the PGD algorithm, as shown in Figure 1b by the black circles that lie above the threshold line. The visualization of one of the attack examples is shown in Figure 2 in Appendix A.4.

Figure 1: Visualization of the outer-approximation ellipsoids and outputs with $\varepsilon = 0.1$ for $L_2$ norm (left) and $L_{\infty}$ norm (right). The red points are image of the input region, the blue curve is the ellipsoid we compute, the blue dashed line is the threshold line used for certifying robustness of inputs, and the black circles are attack examples found by PGD algorithm.
5 Conclusion and Future Works

In this paper, we introduce semialgebraic representations of monDEQ and propose several POP models that are useful for certifying robustness, estimating Lipschitz constants and computing outer-approximation ellipsoids. For each model, there are several hierarchies of relaxations that allow us to improve the results by increasing the relaxation order. Even though we simply consider the order-1 relaxation, we obtain tighter upper bounds of Lipschitz constants compared to the results in [33]. Consequently, we are able to certify robustness of more examples.

Our models are based on SDP relaxation, hence requires an efficient SDP solver. However, the state-of-the-art SDP solver Mosek (by interior-point method) can only handle PSD matrices of moderate size (smaller than 5000). This is the main limitation of our method if the dimension of the input gets larger. Moreover, we only consider the fully-connected monDEQ based on MNIST datasets for illustration. One important and interesting future work is to generalize our model to single and multi convolutional monDEQ, and to other datasets such as CIFAR [26] and SVHN [32]. Directly using off-the-shelves interior point SDP solvers to solve the problems for convolutional networks is not possible because of their current size limitation. Fortunately, a convolutional layer can be regarded as a fully-connected layer with a larger (but sparse) weight matrix. Hence one is able to build similar models via sparse polynomial optimization tools.

The authors in [10] provide an interesting and promising first-order method as an alternative to the costly interior point methods for solving semidefinite relaxations associated with robustness certification of DNNs. What is crucial in [10] is to exploit the network layer structure for efficient back-propagation in gradient computation. In particular, the algorithm requires memory only linear in the total number of network activations and only requires a fixed number of forward/backward passes through the network per iteration. This enables the algorithm to certify robustness of large-scaled networks more efficiently and accurately. However, the auto-differentiation technique for computing subgradients in DNNs does not apply directly to monDEQs, since computing subgradients in monDEQs involves solving fixed-point equations. Therefore, adapting the approach of [10] for solving more efficiently our semidefinite relaxations associated with monDEQs is certainly worth considering but not straightforward. It is a topic of further investigation.

The authors in [33] showed that we can train DEQs with small Lipschitz constants for the $L_2$ norm, by controlling the monotonicity of the weight matrix. This guarantees the robustness of monDEQ w.r.t. the $L_2$ norm but not for the $L_\infty$ norm. A natural investigation track is to adapt this training technique to the $L_\infty$ norm with a better control of the associated Lipschitz constant.

Acknowledgments and Disclosure of Funding

The authors acknowledge the support of AI Interdisciplinary Institute ANITI funding, through the French “Investing for the Future – PIA3” program under the Grant agreement ANR-19-PI3A-0004. Edouard Pauwels acknowledges the support of Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant numbers FA9550-19-1-702 6and ANR MaSDOL 19-CE23-0017-01. This work was supported by the National Research Foundation, Prime Minister’s Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme. Victor Magron was supported by the FMJH Program PGMO (EPICS project) and EDF, Thales, Orange et Criteo, as well as from the Tremplin ERC Stg Grant ANR-18-ERC2-0004-01 (T-COPS project). This work has benefited from the European Union’s Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Actions.

References


[46] LeCun Yann, Cortes Corinna, and Burges Christopher J. C. Mnist handwritten digit database. 2010. [ATT Labs Online].


Checklist

1. For all authors...
   (a) Do the main claims made in the abstract and introduction accurately reflect the paper’s contributions and scope? [Yes] All the claims made in the abstract are justified in methodological sections 2 and 3 or experimental section 4.
   (b) Did you describe the limitations of your work? [Yes] We restrict ourselves to fully-connected ReLU monDEQs as presented in Sections 2 and 3. We also discuss the limitation due to the size of PSD matrices which can be handled by SDP solvers in Section 3.4.
   (c) Did you discuss any potential negative societal impacts of your work? [No] Our work is methodological and we do not foresee any direct negative societal impact of this work.
   (d) Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes] The paper conforms to the guidelines.

2. If you are including theoretical results...
   (a) Did you state the full set of assumptions of all theoretical results? [Yes] As presented in Section 2, we consider monDEQ models, which is our main assumption, no further assumption is required for all our models.
   (b) Did you include complete proofs of all theoretical results? [Yes] The methodological sections 2 and 3 describe all proof arguments for the soundness of our models. Proofs of some technical lemmas are postponed to the appendix.

3. If you ran experiments...
   (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? [Yes] The code is available at https://github.com/NeurIPS2021Paper4075/SemiMonDEQ which is included in the main text.
   (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? [Yes] We discuss training details in Section 4, we report the code used for training at https://github.com/locuslab/monotone_op_net.
   (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? [Yes] We report exact 95% binomial confidence intervals for proportions reported in Table 2.
   (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? [Yes] We report in Section 4 the number of experiments, the average computation time and the type of personal computer used to perform all these experiments.

4. If you are using existing assets (e.g., code, data, models) or curating/releasing new assets...
   (a) If your work uses existing assets, did you cite the creators? [Yes] We cited references for all the software used in our experiments.
   (b) Did you mention the license of the assets? [Yes] We report licenses for all assets used in the paper in Appendix A.5.
   (c) Did you include any new assets either in the supplemental material or as a URL? [Yes] We include code to reproduce our experiments as a separate URL.
   (d) Did you discuss whether and how consent was obtained from people whose data you’re using/curating? [No] We did not obtain any kind of new data.
   (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? [No] We did not obtain any kind of new data.

5. If you used crowdsourcing or conducted research with human subjects...
   (a) Did you include the full text of instructions given to participants and screenshots, if applicable? [N/A] We did not use crowdsourcing.
   (b) Did you describe any potential participant risks, with links to Institutional Review Board (IRB) approvals, if applicable? [N/A] We did not use crowdsourcing.
   (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? [N/A] We did not use crowdsourcing.