Reducing DNN Properties to Enable Falsification with Adversarial Attacks

David Shriver  
Department of Computer Science  
University of Virginia  
Charlottesville, Virginia, USA  
dlss2fc@virginia.edu

Sebastian Elbaum  
Department of Computer Science  
University of Virginia  
Charlottesville, Virginia, USA  
selbaum@virginia.edu

Matthew B. Dwyer  
Department of Computer Science  
University of Virginia  
Charlottesville, Virginia, USA  
matthewbdwyer@virginia.edu

Abstract—Deep Neural Networks (DNN) are increasingly being deployed in safety-critical domains, from autonomous vehicles to medical devices, where the consequences of errors demand techniques that can provide stronger guarantees about behavior than just high test accuracy. This paper explores broadening the application of existing adversarial attack techniques for the falsification of DNN safety properties. We contend and later show that such attacks provide a powerful repertoire of scalable algorithms for property falsification. To enable the broad application of falsification, we introduce a semantics-preserving reduction of multiple safety property types, which subsume prior work, into a set of equivalent correctness problems amenable to adversarial attacks. We evaluate our reduction approach as an enabler of falsification on a range of DNN correctness problems and show its cost-effectiveness and scalability.

Index Terms—falsification, formal methods, neural nets

I. INTRODUCTION

As the performance and applicability of Deep Neural Networks (DNN) continues to increase, their deployment has been explored for use in safety-critical domains, such as autonomous vehicles [9], [15], [35] and medicine [17], [23], [56]. As a result, checking the correctness of DNNs has emerged as a key challenge to ensuring the safety of these systems. For example, for the DroNet DNN that predicts a steering angle and a probability of collision for an autonomous quadrotor system [35], one such correctness property may specify that if the probability of collision is low, then the steering angle should not be extremely large.

One approach to checking correctness of DNN models is verification. In the past 3 years alone, dozens of DNN verification techniques have been introduced for proving properties of DNN models [7], [11], [13], [19]–[21], [24], [28]–[30], [43], [44], [46], [47], [51], [54], [55], [57]–[59]. Unfortunately, these approaches are often limited in their applicability, due to their simplifying assumptions about DNN structure or to high computational cost, making it difficult to apply them to real models [45], [61]. For example, due to the large size and complex computation graph of DroNet, existing verifiers fail to run or cannot finish in a reasonable time.

A complementary approach to verification is that of falsification, which attempts to find violations of a property. While verifiers can show that a property is true, falsifiers can often find violations more quickly than verifiers when the property is false. Falsification is an active area of research spanning property types and application domains [1], [4], [16], [18]. In the context of DNNs, one can view adversarial attacks [26], [32], [36], [37], [49], [50] as falsifiers for DNN local robustness properties. While these techniques often scale to real-world DNNs, they are currently limited in the range of properties they can falsify. For the DroNet example, adversarial attacks support the scale and complex structure of the DNN, but are designed only to find violations of robustness properties and not safety properties like those relating speed and probability of collision. As we discuss in §II-A, there is a broad range of properties that could benefit from the speed and applicability of these falsifiers.

Driven in part by the cost of DNN verification, and in part by the limited property support for DNN falsification, we identify the key insight that many valuable property types could be reduced into the more commonly supported form of local robustness properties. We build on this insight to develop an approach for reducing properties in an expressive, general form to an equivalent set of local robustness properties, which have wide support among both falsifiers and verifiers. Such translation has the potential to bring existing techniques to bear on falsifying DNN properties, leaving verifiers to focus on proving that a property holds.

Our community has exploited property reduction for verification and program analysis for decades. Perhaps best known is the reduction from stateful safety properties to reachability properties. For example, partial order reductions were broadened in applicability by reducing stateful properties to a form of deadlock [25], and both data flow analyses [40], [48] and SAT solving [8] were applied to verify stateful properties by formulating the reachability of error states. A second use of reductions is to enable more efficient algorithmic methods to be employed. For instance, the -safety option of the SPIN model checker permits it to use a significantly faster reachability algorithm [27]. Such reductions are now considered standard in verification and program analysis. In the new domain of DNN verification and falsification, however, the lessons of such reductions have not yet taken root.

In this paper, we introduce an approach for reducing a DNN and an associated safety property – which we refer to as a correctness problem – into an equivalent set of correctness
A. Properties of DNNs

Given a DNN, \( \mathcal{N} : \mathbb{R}^n \rightarrow \mathbb{R}^m \), a property, \( \phi(\mathcal{N}) \), defines a set of constraints over the inputs, \( \phi_X \) – the pre-condition, and a set of constraints over the outputs, \( \phi_Y \) – the post-condition. Checking property \( \phi(\mathcal{N}) \) attempts to prove or falsify: \( \forall x \in \mathbb{R}^n : \phi_X(x) \rightarrow \phi_Y(\mathcal{N}(x)) \).

A survey on verification of neural networks [33] identifies different representations for the input and output constraints used by verification techniques; two of these representations are particularly useful in this work. A hyperrectangle is an \( n \)-dimensional rectangle where constraints are formulated as \( (x_i \geq b_i) \wedge (x_i \leq u_i) \), where \( b_i, u_i \in \mathbb{R} \) and \( 0 \leq i < n \) define the lower and upper bounds on the value of each dimension of \( x \), respectively. A special case of hyperrectangles used in our approach is the unit hypercube which is a hyperrectangle where \( \forall i. (b_i = 0) \wedge (u_i = 1) \); an \( n \)-dimensional hypercube is denoted \([0, 1]^n\). A halfspace-polytope is a polytope which can be represented as a set of linear inequality constraints, \( Ax \leq b \), where \( A \in \mathbb{R}^{n \times k} \), \( b \in \mathbb{R}^k \), \( k \) is the number of constraints and \( n \) is the dimension of \( x \).

Using such encodings, researchers have specified a range of desirable properties of DNNs. Here we distinguish three broad categories: robustness, reachability, and differential properties.

Robustness properties originated with the study of adversarial examples [50], [62]. Robustness properties apply to classification models and specify that inputs from a specific region of the input space must all produce the same output class. Robustness properties can be further classified as either local or global robustness; the former asserts robustness in a local region of the input domain and the latter over the entire input domain. Detecting violations of robustness properties has been widely studied, and they are a common type of property for evaluating verifiers [21], [46], [47], [51], [54].

Reachability properties define the post-condition using constraints over output values rather than output classes, and are thus not limited to classification models. Such properties have been used to evaluate DNN verifiers [29], [54]. Reachability properties specify that inputs from a given region of the input space must produce outputs that lie in a given region of the output space. For example, a DNN model controlling the velocity of an autonomous vehicle may have a safety property specifying that the model never produces a desired velocity value greater than the vehicle’s maximum physical speed for any input in the input domain. Similarly to robustness, reachability properties can be further classified as local or global. For example, a global halfspace-polytope reachability (GHPR) property would specify a halfspace-polytope constraint on network output values that must hold for all inputs.

Differential properties are the most recently introduced DNN property type [42]. These properties specify a difference (or lack thereof) between outputs of multiple DNNs. One type of differential property is equivalence, which states that for every input, two DNN models produce the same output. Such a property can be used to check that DNN semantics are preserved after some modification, such as quantization or pruning. Differential properties can be supported by combining multiple DNNs into a single network and expressing properties over their combined input and output domains.

In addition to these three categories and as alluded earlier, properties can also be classified by the form of their input pre-condition. Global properties have the most permissive pre-condition, enforcing the post-condition for any input in the input domain of the DNN. For example, a DNN that operates on images may accept values in \([0, 1]^n\). The pre-condition of a global property would not restrict this domain any further. Local properties only enforce the post-condition for inputs within a designated region of the input domain. For example, a local property for an image processing network may have the precondition that inputs are within distance \( \epsilon \) of some given input \( x \). This is especially common in robustness properties.

B. Adversarial Attacks and Fuzzing

One approach to checking properties of DNNs is through the use of algorithms that seek to find examples that violate a given specification for a given model. Two categories of techniques have been developed for DNNs that can be used to falsify DNN property specifications.

Adversarial attacks are methods that are optimized to detect violations of robustness properties [2], [62]. In general, adversarial attacks take in a DNN model and an initial input, and attempt to produce a perturbation that, when applied to the input, will change the class predicted by the given model.
These perturbations are often also subject to some constraints, such as remaining within a given distance of some original input. A perturbed input, commonly known as an adversarial example, is an example that is not an input domain defined as a unit hypercube. This modification ensures that the properties and networks have input domains defined as unit hypercubes, and output domains consist of two values — indicating property satisfaction and falsification:

\[ \forall (\mathcal{N}_i, \phi_i) \in \text{reduce}(\psi), \mathcal{N}_i : [0,1]^n \rightarrow \mathbb{R}^2 \]

As we demonstrate in §IV, reduction enables the application of a broad array of efficient DNN analysis techniques to compute problem validity and/or invalidity.

As defined, reduction has two key properties. The first property is that the set of resulting problems is equivalent with the original correctness problem (a proof of this theorem is included in Appendix A).

### III. Approach

A. Defining Property Reduction

A correctness problem is a pair, \( \psi = (\mathcal{N}, \phi) \), of a DNN, \( \mathcal{N} \), and a property specification \( \phi \), formed to determine whether \( \mathcal{N} \models \phi \) is valid or invalid.

Reduction, \( \text{reduce} : \Psi \rightarrow P(\Psi) \), aims to transform a correctness problem, \( (\mathcal{N}, \phi) = \psi \in \Psi \), to an equivalent form, \( \text{reduce}(\psi) = \{ (\mathcal{N}_1, \phi_1), \ldots, (\mathcal{N}_r, \phi_r) \} \), in which property specifications define robustness properties:

\[ \phi_i = \forall x. x \in [0,1]^n \rightarrow \mathcal{N}_i(x) > \mathcal{N}_i(x) \]

and networks have input domains defined as unit hypercubes, and output domains consist of two values — indicating property satisfaction and falsification:

\[ \forall (\mathcal{N}_i, \phi_i) \in \text{reduce}(\psi), \mathcal{N}_i : [0,1]^n \rightarrow \mathbb{R}^2 \]

As we demonstrate in §IV, reduction enables the application of a broad array of efficient DNN analysis techniques to compute problem validity and/or invalidity.

As defined, reduction has two key properties. The first property is that the set of resulting problems is equivalent with the original correctness problem (a proof of this theorem is included in Appendix A).

### B. Overview

To illustrate, consider a property for DroNet [35]: a DNN for controlling an autonomous quadrotor. Inputs to this network are 200 by 200 pixel grayscale images with pixel values between 0 and 1. For each image, DroNet predicts a steering angle and a probability that the drone is about to collide with an object. The property states that for all inputs, if the probability of collision is no greater than 0.1, then the steering angle is capped at \pm 5 degrees and is specified as:

\[ \forall x. (x \in [0,1]^{40000}) \land (\mathcal{N}(x)_{\text{col}} \leq 0.1) \rightarrow (-5° \leq \mathcal{N}(x)_{\text{steer}} \leq 5°) \]

Adversarial attacks cannot be used off the shelf to falsify this property, since it is not a robustness property.

To enable the application of adversarial attacks, we reduce the property to a set of correctness problems with robustness properties, such as the one shown in Figure 2. This particular example is reduced to two correctness problems with robustness properties. Each of the problems pair a robustness property (shown in the bottom of Figure 2) with a modified version of the original DNN. The new DNN is created through two key transformations. First, incorporating a prefix network (shown in green in Figure 2) to reduce the input domain to a unit-hypercube. This modification ensures that the properties for reduced problems can all use the same pre-condition. Second, incorporating a suffix network (shown in blue in Figure 2) that takes in the inputs and outputs of the original DNN and classifies whether they constitute a violation of the original property. This suffix transforms the network into a classifier for which violations of a robustness property correspond to violations of the original property.

### C. Reduction Transformation

We rely on three assumptions to transform a correctness problem into a reduced form. First, the constraints on the network inputs must be represented as a union of convex polytopes. Second, the constraints on the outputs of the
network must be represented as a union of convex polytopes. Third, we assume that each convex polytope is represented as a conjunction of linear inequalities. Complying with these assumptions still enables properties to retain a high degree of expressiveness as unions of polytopes are extremely general and subsume other geometric representations, such as intervals and zonotopes. §IV-A shows that these assumptions are sufficient to support existing DNN correctness problems.

Algorithm 1 defines the reduction transformation at a high level. We present each step of the algorithm and describe their application to the DroNet example described above.

1) Reformulate the Property: Reduction first negates the original property specification and converts it to disjunctive normal form (DNF) – line 2. Negating the specification means that a satisfying model falsifies the original property. The DNF representation allows us to construct a property for each disjunct, such that if any are violated, the negated specification is satisfied and thus the original specification is falsified. For each of these disjunctions the approach defines a new robustness problem, as described below.

2) Transform into halfspace-polytopes: Constraints in each disjunct are converted to halfspace-polytope constraints, defined over the concatenation of the input and output domains – disjunct_to_hpolytope() on line 5. This conversion is described in Algorithm 2. A halfspace-polytope can be represented in the form $A^*x \leq b$, where $A$ is a matrix of $k$ rows, where each row represents 1 constraint, and $d$ columns, one for each variable. In this case, $d$ is equal to $m + n$, the size of the output space, plus the size of the input space. This representation facilitates the transformation of constraints into network operations. To build the matrix $A$ and vector $b$, we first transform all inequalities in the conjunction to $\leq$ inequalities with variables on the left-hand-side and constants on the right-hand-side. The transformation first converts $\geq$ to $\leq$ and $> >$ to $\leq$ lines 4-7 of Algorithm 2. Then, all variables are moved to the left-hand-side and all constants to the right-hand-side – line 8. Next, $\leq$ constraints are converted to $\leq$ constraints by decrementing the constant value on the right-hand-side – lines 9-10. This transformation assumes that there exists a representable number with greatest possible value that is less than the right-hand-side. Finally, each inequality is converted to a row of $A$ and value in $b$ – lines 11-12.

3) Prefix Construction: Using the constructed halfspace-polytope, Algorithm 1 next constructs a prefix to the original network to ensure the input domain of the resulting network is $[0,1]^n$, where $n$ is the input dimensionality of the original network – construct_prefix() on line 6. The algorithm to construct the prefix is shown in Algorithm 3. The prefix is constructed by first extracting lower and upper bounds for every input variable – lines 2-8. This extracts the minimal axis-aligned bounding hyperrectangle. The lower and upper bounds can then be used to construct the prefix network, which is a single n-dimensional fully-connected layer, with no activation function, which has a diagonal weight matrix with values equal to the ranges of the input variables, and biases.
equal to the lower bounds of each input. The prefix operates on unit hypercubes, reducing the input space to the correctness problems. The prefix also encodes any interval constraints over the original input space, allowing them to be removed before suffix construction, which simplifies the suffix networks. For the DroNet example, the diagonal of this matrix is a vector of ones, while the biases are all 0.

Next, the original input values are forwarded to the end of the original network and concatenated with the original output layer – line 7. Because constraints will be encoded as a network suffix that classifies whether inputs are property violations, this step is necessary to enable the encoding of constraints over the inputs.

4) Suffix Construction: The suffix subnetwork classifies whether inputs satisfy the specification – construct_suffix() on line 8. The algorithm for constructing the suffix from the halfspace-polytope constraints is shown in Algorithm 4. The constructed suffix has two layers, a hidden fully-connected layer with ReLU activations, and dimension equal to the number of constraints in the halfspace-polytope defined by the current disjunct, and a final output layer of size 2.

The hidden layer of the suffix has a weight matrix equal to the constraint matrix, A, of the halfspace-polytope representation, and a bias equal to \(-b\) – line 2. With this construction, each neuron will only have a value greater than 0 if the corresponding constraint is not satisfied, otherwise it will have a value less than or equal to 0, which becomes equal to 0 after the ReLU activation is applied. In the DroNet problem for example, one of the constraints for a disjunct is \(N(x) \leq -5\). For this conjunct we define the weights for one of the neurons to have a weight of 1 from \(N(x)\), a weight of 0 from \(N(x)\), and a bias of 5.

The output layer of the suffix has 2 neurons, each with no activation function. The first of these neurons is the sum of all neurons in the previous layer, and has a bias value of 0. Because the neurons in the previous layer each represent a constraint, and each of these neurons is 0 only when the constraint is satisfied, if the sum of all these neurons is 0, then the conjunction of the constraints is satisfied, indicating that a violation has been found. The second of these neurons has a constant value of 0 – all incoming weights and bias are 0. The resulting network will predict class 1 if the input satisfies the corresponding disjunct and class 0 otherwise.

5) Correctness Problem Construction: Lines 9-11 of Algorithm 1 define the reduced subproblem comprised of the network that we have constructed and a robustness property. The robustness property specification is always the same and states that the network should classify all inputs in the d-dimensional hypercube as class 0 – no violations. If a violation is found to this property, then, according to Theorem 2, the original property is violated by the unreduced input that violated the robustness property. In the end, we have generated a set of correctness problems such that, if any of the problems is violated, then the original problem is also violated. This comes from our construction of a property for each disjunct in the DNNF of the negation of the original property.

D. Properties Over Multiple Networks

While Algorithm 1 is defined over properties with a single network, it can easily be applied to properties over multiple networks, by combining those networks into a single large network. This is specially relevant to check for equivalence properties. This can be done by concatenating their input and output vectors. This results in a single large network with a computation path for each network. The transformation algorithm can then be applied as before.

E. Implementation.

We implemented our approach in a system named DNNF1, which accepts a DNN property specification and corresponding DNN as input, and returns whether a violation is found. Whereas the reduction algorithm in §IV applies to properties with unions of polytopes as input constraints, the current implementation works on unions of hyperrectangles in the input space. This was a convenience choice to simplify the implementation while still accommodating most properties in the verification literature, as demonstrated in §IV-A.

IV. Empirical Evaluation

We now assess the cost-effectiveness of reducing DNN properties for falsification by applying it to a range of DNN property benchmarks that provide diversity in terms of property types and DNN complexity. Our evaluation will attempt to answer the following research questions:

- RQ1: How expressive are the properties supported by property reduction?
- RQ2: How cost-effective is falsification at finding property violations?
- RQ3: How scalable is falsification?

A. RQ1: On the Expressiveness of Reduction

We first evaluate whether the assumptions about the property specification required by reduction, namely that the original property is specified as a logical formula of linear inequalities, is expressive enough to support DNN correctness properties that have been proposed in existing work.

1) Setup: To evaluate the expressiveness of properties supported by our reduction, we analyze and catalog the benchmarks used by the five verifiers used in our later study, as well as the benchmarks of a recent DNN verifier competition, VNN-Comp [34]. Additionally, we surveyed published papers on DNN verification in the past two years identifying 4 additional works [6], [22], [52], [53]. Finally, we include the 2 new benchmarks introduced in this work.

2) Results: We summarize the results in Table I, which lists the benchmarks used in each work, the type and number of properties in the benchmark and whether the properties are supported by Algorithm 1 and our current implementation. The property types use abbreviated names with the following encoding: the first symbol indicates whether the property is global (G) or local (L); the second symbol indicates whether

1 https://github.com/dlshriver/DNNF
the input constraint can be represented as a hyper-rectangle (□) or not (□); the third symbol indicates whether the property is a robustness (□) property, a reachability (□) property, or a differential (□) property. Each cell under a property type indicates the number of properties in the corresponding benchmark of that type. The benchmark properties are used later in the study for the evaluation of RQ2 and RQ3. We describe the details of these benchmarks in more detail below.

The first benchmark is ACAS Xu, introduced for the study of the Reluplex verifier [29], and used extensively since [6], [12], [13], [30], [34], [54], [55]. The benchmark consists of 10 properties. Properties \( \phi_1, \phi_2, \phi_3, \phi_4, \phi_5 \) are reachability properties, while \( \phi_6, \phi_7, \phi_8, \) and \( \phi_9 \) are traditional class robustness properties. All 10 properties have hyper-rectangles constraints over the inputs and are fully supported by our property reduction.

The next benchmark is from the evaluation of the Planet verifier. First is the Collision Avoidance benchmark, which consists of 500 safety properties that check the robustness of a network that classifies whether 2 simulated vehicles will collide, given their current state. All 500 properties are L^r properties, and are all fully supported. Second is a set of 7 properties on an MNIST network. The first 4 of these are CER properties, while the next 2 are L^C properties, and the final property is an L^D property. In addition to restricting the amount of noise that can be added to each pixel in the input image, the final property constrains the difference in the noise between neighboring pixels. DNNF currently supports 6 of these properties, while the final is supported by Algorithm 1.

The Neurify verifier was evaluated on the ACAS Xu benchmark and on properties of 4 MNIST networks, 3 android app malware classification networks, and 1 self-driving car network. The evaluation on MNIST used 500 L^C properties across 4 networks, all of which we support. Neurify was also evaluated on 3 networks trained on the Drebin dataset [5] to classify apps as benign or malicious. This benchmark also includes 500 L^C properties, which are fully supported. Finally, Neurify was evaluated on local reachability properties for a modified version of the DAVE self-driving car network [10]. This benchmark consists of 200 local reachability properties, with 4 different types of input constraints (50 properties of each type). The first type of input constraint is an \( L_\infty \) constraint, which is equivalent to a hyper-rectangle constraint. The second type of input constraint is an \( L_1 \) constraint, which can be written as a halfspace polytope constraint. The third and fourth type of input constraint is an image brightness and contrast, which can also be written as a halfspace polytope constraints. DNNF currently supports the first 50 of these properties and the remainder are supported by Algorithm 1.

The DeepZono abstract domain of the ERAN verifier used in our study [46], was evaluated on 3300 L^C properties applied to a set of 24 MNIST networks and 13 CIFAR10 networks. All of the properties in this benchmark are fully supported by our approach.

The ReluDiff verifier was designed to support differential properties in order to show equivalence between two networks [42]. The verifier was evaluated on L^D properties. Each property was defined over a network \( N \) and a modified version of the same network with quantized weights, \( N' \). The property checked whether \( |N'(x) - N'(x)| < \epsilon \) held in a local region of the input space. 14 of these properties were verified over networks from the ACAS Xu benchmark [29], 200 properties on networks trained with the MNIST dataset, and 100 properties on a network trained for Human Activity Recognition [3]. All 314 differing properties are fully supported by our approach.

The recent VNN-Comp competition used 3 benchmarks. The first is a benchmark with properties applied to networks with piecewise linear activation functions. This benchmark consists of the ACAS Xu benchmark [29] with 4 L^C properties and 6 L^C properties, as well as a set of 50 local robustness properties with hyper-rectangle input constraints applied to 3 MNIST networks. All of these properties are supported by our approach. The second is a set of 300 local robustness properties with hyper-rectangle input constraints applied to convolutional neural networks trained on MNIST and CIFAR10. All of these properties are supported by our approach. The final benchmark is a set of 32 local robustness properties with hyper-rectangle input constraints applied to neural networks with non-linear activation functions (sigmoid and tanh) trained on MNIST. All of these properties are supported by our approach.

Several DNN verifiers have been introduced recently. The nnenum verifier [6] and an abstraction-refinement approach for DNN verification [22] were evaluated on the ACAS Xu benchmark. The reachability set representation of ImageS ters [52] was evaluated on two benchmarks of local robustness properties applied to MNIST and ImageNet networks. The benchmark on the MNIST networks used a version of 900 local robustness where pixels could be independently darkened, enabling input constraints to be represented as hyper-rectangles. The benchmark on the ImageNet networks uses 6 properties created from an original image and a corresponding adversarial example. The properties specify that for a given region along the line between the original image and adversarial example, all inputs along the segment are classified as the correct class. While the MNIST benchmark is supported by our current reduction implementation, the ImageNet benchmark requires polytope constraints in the input space and is therefore supported just by Algorithm 1. The NN verifier [53] also introduced a benchmark with an adaptive cruise control (ACC) system. It checks a temporal property not currently supported by Algorithm 1, but we see the potential to support such properties through unrolling in future work.

Overall, we find that the property specifications accepted by Algorithm 1 are rich enough to express 7 of the 8 property types found in the explored benchmarks.

When considering the listed benchmarks, Algorithm 1 fully supports 16 of the 17 benchmarks. Our current implementation completely supports the properties from 13 of the 17 bench-
B. RQ2: On the Cost-Effectiveness of Reduction-Enabled Falsification

To evaluate the cost-effectiveness of falsification enabled by the proposed reduction, we identify a set of falsifiers and verifiers to compare their complementary performance, problem benchmarks, and metrics that constitute the basis for the studies around RQ2 and RQ3.

1) Setup: Falsifiers. As falsification methods, we will use several common adversarial techniques, as well as a DNN fuzzing tool. For adversarial attacks, we choose a subset of the methods from two surveys [2], [62]. We select the methods common to both surveys with $L^\infty$ input constraints (which matches our implementation) and with implementations available in the cleverhans tool [41]. The chosen adversarial attacks are LBFGS [50], FGSM [26], Basic Iterative Method (BIM) [32], and DeepFool [37]. Of these attacks, none use random initialization, and thus will produce the same result over multiple runs. In order to observe the potential benefits of random initialization, we also include Projected Gradient Descent (PGD) [36], which was only included in one of the surveys. Therefore, we run each attack, except PGD, once, and if no adversarial example is found, we return an unknown result. For PGD, if no adversarial example is found, we try again, until one is found, or the given time limit is reached. We use the default parameters for each attack, as specified by cleverhans. For DNN fuzzing, we use TensorFuzz [39] for its easily accessible implementation [38]. TensorFuzz requires the definition of an oracle for recognizing property violations. We provide a version of TensorFuzz with an oracle that identifies violations by checking whether $N(x)_0 \leq N(x)_1^2$.

Verifiers. For comparison to verification, we select four verifiers: Reluplex [29], Planet [21], ERAN using the DeepZono abstract domain [46], and Neurify [54]. Neurify and ERAN have been shown to be fastest and most accurate in recent studies [61], and all four verifiers are supported by DNNV, which makes them easy to run and allows us to use a common property specification for all verifiers and falsifiers. For differential properties we also consider ReluDiff [42] since it is currently the only verifier built to handle such properties.

Portfolios. In addition to the individual falsifiers and verifiers, we simulate portfolios of these methods, which run analyses in parallel and return the first result. We use 3 portfolios: All Falsifiers, which includes the 6 falsifiers described above; All Verifiers which includes all verifiers run on each benchmark; Total which includes all methods used in this study. To simulate running each portfolio, we take the union of the violations found by each method in the portfolio, and consider the time to find each violation to be the fastest time among the methods in the portfolio which found that violation.

Problem Benchmarks. We evaluate our approach on two common and representative benchmarks from the verification literature, and two created for this work to provide a range of networks and property types. Our selection criteria was meant to achieve two objectives. First, we wanted to select enough benchmarks to explore all property types with hyper-rectangle input constraints. Second, we wanted to select benchmarks

---

**TABLE I: Property types of existing benchmarks and their support by reduction.** The property type names use the following encoding: the first symbol indicates a global (G) or local (L) property; the second symbol indicates whether the input constraint can be represented as a hyper-rectangle (R) or not (E); the third symbol indicates the property class as robustness (R), reachability (R), or differential (D). Bolded benchmarks are used later in the study to evaluate RQ2 and RQ3.

| Benchmark            | L/E | L/R | # of Property of Each Type | Support               |
|----------------------|-----|-----|---------------------------|-----------------------|
| ACAS Xu [29]         | 4   | 6   | 4 1 0 1 0 1 0             | 10 10                 |
| Collision Avoidance [21] | 500 | 500 7 6 500 500          |                        |
| Planet-MNIST [21]    | 2   | 1   | 2 4 4 50                   | 500 500               |
| Neurify-MNIST [54]   | 500 | 500 | 500 500 500 500            | 500 500               |
| Neurify-Dave [54]    | 500 | 500 | 500 500 500 500            | 500 500               |
| ERAN-MNIST [46]      | 1700| 1700| 1700                      | 1700 1700             |
| ERAN-CIFAR [46]      | 1600| 1600| 1600                      | 1600 1600             |
| ReluDiff ACAS [42]   | 14  | 14  | 14                        | 14 14                 |
| ReluDiff-MNIST [42]  | 100 | 100 | 100                       | 100 100               |
| ReluDiff-HAR [42]    | 100 | 100 | 100                       | 100 100               |
| VNN-COMP-CNN [34]    | 300 | 300 | 300                       | 300 300               |
| VNN-COMP-PW1 [34]    | 54  | 6   | 6                         | 60 60                 |
| VNN-COMP-SNLX [34]   | 10  | 100 | 100                       | 100 100               |
| ImageStars-MNIST [52] | 900 | 900 | 900                       | 900 900               |
| ImageStars-ImageNet [52] | 6   | 6   | 6                         | 6 0                   |
| VNN-ACC [53]         | 22  | 22  | 22                        | 22 22                 |
| GHPR                 | 20  | 20  | 20                        | 20 20                 |
| CIFAR-EQ             | 91  | 200 | 291                       | 291 291               |
with networks that varied in both size and structure since these factors have been shown to affect verifier performance [61].

From the verification literature, we select ACAS Xu, the most commonly used benchmark, and a slightly modified version of the Neurify-DAVE benchmark. For Neurify-DAVE, we select the 50 LCR properties supported by our current implementation, and we augment the benchmark with an additional network. The new network is the original DAVE DNN on which the smaller network in the benchmark was based. While the small DNN has 10277 neurons, the original DAVE network that we add has 82669 neurons, which will allow us to explore the scalability of reduction and falsification. The two networks in this benchmark are convolutional networks and are much larger than the networks in the ACAS Xu benchmark.

We developed 2 new benchmarks to cover property types that are not yet covered by existing benchmarks. The GHPR benchmark is a new DNN property benchmark that contains GCR properties applied to several network architectures of varying size and structure. It consists of 30 correctness problems, 20 of which are 10 GHPR properties applied to 2 MNIST networks, and 10 of which are GHPR properties applied to the DroNet DNN described previously. The DroNet DNN is one of the largest in our study, with more than 475,000 neurons. The MNIST properties are of the form: for all inputs, the output values for classes $a$ and $b$ are closer to one another than either is to the output value of class $c$. The DroNet properties are of the form: for all inputs, if the probability of collision is between $p_{\text{min}}$ and $p_{\text{max}}$, then the steering angle is within $d$ degrees of 0. These properties are described in more detail in the supplementary material.

The CIFAR-EQ benchmark is a new DNN property benchmark with differential properties applied to large networks with complex structures. It contains a mix of both global and local equivalence properties. It is the only benchmark to contain GCCD properties, which were absent in the property benchmarks that we found. It consists of 291 properties: 91 global equivalence properties and 200 local equivalence properties. Of the global properties, 1 is untargeted, while the other 90 are targeted equivalence properties. Of the 200 local properties, 20 are untargeted, while the other 180 are targeted equivalence properties. The properties are applied to a pair of neural networks trained on the CIFAR dataset [31]. The first network is a large convolutional network with 62,464 neurons and the second is a ResNet-18 network with over 588,000 neurons. These properties are described in more detail in the supplementary material. Because the verifiers do not support the multiple computation path structure formed during network composition, we do not run them on this benchmark.

Metrics. For each verification and falsification approach, we will measure the number of property violations found and the total time to find each violation. The total time to find a violation includes both the time to transform the property, as well as to run the falsifier on the resulting properties.

Computing resources. Experiments were run on compute nodes with Intel Xeon Silver 4214 processors at 2.20 GHz and 512GB of memory. Jobs were allowed to use up to 8 processor cores, 64GB of memory, with a time limit of 1 hour.

2) Results: Figure 3 shows the number of violations found by each falsifier and verifier, reduced by the total number of potentially falsifiable properties. The number above each bar gives the total number of violations found. An exclamation point indicates that a verifier could not be run on a property due to the structure of the network.
the falsifiers find 82 violations, subsuming the 33 violations from the verifiers. The best performing falsification method on this benchmark was BIM, with 74 violations found. PGD and FGSM follow closely with 73 and 69 violations found, respectively. TensorFuzz, the top performing falsification method on the ACAS benchmark, does not find any violations. We conjecture that this is due to the much larger input space. While the ACAS Xu networks have an input dimension of 5, the DAVE networks have an input dimension of 30000, which is more difficult to cover by random fuzzing.

On the GHPR MNIST benchmark, the verifiers can find 17 violations for the 20 properties, while 3 falsifiers, BIM, PGD, and TensorFuzz, can find violations for every property.

On the GHPR DroNet benchmark, the verifiers cannot find any violations, due to not supporting the residual block structures present in the DroNet network. Many of the falsifiers also struggle on these properties, except for PGD and BIM, which can find violations to all 10 properties.

Finally, on the CIFAR-EQ benchmark, the verifiers did not find any violations because they could not be run. Reluplex, Planet, ERAN, and Neurify do not support properties over multiple networks or networks with multiple computation paths, while ReluDiff is limited to networks with only fully-connected layers. Additionally, while PGD finds the most violations, it is complemented by the other falsification approaches, with BIM, DeepFool, and TensorFuzz each finding violations for at least 1 unique property. We conjecture that much of PGD’s success is due to its random initialization, which allows it to run multiple times with different results, increasing the chance of finding a violation.

Note that the Planet and ERAN verifiers find no violations for any benchmark. For these benchmarks ERAN cannot find violations since its algorithmic approach focuses on proving that a property holds, which suggests its complementarity with falsification methods. Planet fails to find violations due to the complexity of the problem, and internal tool errors that cause Planet to crash on almost 20% of the correctness problems. We also see that the Reluplex verifier only finds violations for the ACAS Xu benchmark. It cannot find violations on the other benchmarks, since it does not support the architectures of the networks in those benchmarks.

Overall, we find that falsifiers can detect many property violations usually complementing those found by verification, that applying them in a parallel portfolio can leverage their unique strengths, and that they successfully scale to more complex benchmarks.

Box plots of the distributions of time to find violations for each method are shown in Figure 4. Figure 4a shows that the verifiers can be effective on the ACAS Xu benchmark, with Neurify often outperforming the falsifiers. This is likely due to the extremely small size of the ACAS Xu networks enabling verification to run efficiently. These plots also show the efficiency struggle of the verifiers as the network get larger. For example, on the Neurify-DAVE benchmark, even when the verifiers can find a property violation, the falsifiers can find violations an order of magnitude faster. For more complex benchmarks, the verifiers cannot find violations within the timeout, so we only report the time for the falsifiers.

We find that falsification can efficiently find property violations even for the most complex benchmarks, with a median time to find a violation across all benchmarks and falsifiers of 16 seconds.

Figures 3 and 4 also reveal that no single falsifier always outperforms the others. While PGD performs well for the benchmarks studied here, we can still increase the number of violations by running multiple falsifiers. Additionally, the falsifiers that find the most violations, do not necessarily always find them the fastest. Based on these two observations, we recommend using a portfolio approach, running many falsifiers in parallel and stopping as soon as a violation is found by any technique, such as the All Falsifiers method shown in the previous figures. This approach finds all the violations found by the verifiers as quickly as the fastest falsifier. We also recommend using falsifiers in conjunction with verifiers, since while falsifiers can often quickly find violations, they cannot prove when a property holds.
C. RQ3: On the Scalability of Reduction-Enabled Falsification

1) Setup: To explore the scalability of falsification with reduction, we want to evaluate a set of properties across networks that vary in size. To do this we applied the Neurify-DAVE properties to both the small DAVE network [54] and the original larger DAVE network [10]. This will allow us to see how performance of the verifiers and falsifiers change with respect to the size of the network being verified.

2) Results: We present the results of checking the properties in Figures 5a and 5b, as well as the box plots of the times to find violations for each method in Figures 5c and 5d.

On the smaller DAVE network, the verifiers struggle to verify the properties. Reluplex does not run at all, due to its lack of support for convolutional layers, while Planet does run, but reaches the timeout for all properties. The ERAN verifier does not timeout on the small network, but cannot verify any of the properties. Neurify was the only verifier that returned accurate results on the small network, successfully falsifying 33 of the 50 properties, and reaching the time limit on the other 17. While only a single verifier was able to falsify any properties, 4 of the 6 falsification approaches were able to falsify properties, all of them finding more violations than Neurify. The falsifiers were also faster than Neurify, finding violations almost an order of magnitude faster than Neurify on the small DAVE network.

While one verifier was able to find violations on the smaller network, none of the verifiers were able to find violations on the larger DAVE network, which has more than 8 times more neurons. Similar to the small network, Reluplex does not support the network structure, while Planet reaches the time limit for all properties. However, ERAN and Neurify both perform slightly differently. While ERAN was previously able to finish its analysis on the small network, it reaches the time limit for 34 properties on the large network, indicating that it could not scale to the larger network size. Similarly, while Neurify previously found property violations for the small network, it reaches the memory limit on the large network before any violations are found. The falsifiers on the other hand still perform well, with 3 of the 6 verifiers finding property violations. Surprisingly, the DeepFool falsifier goes from 44 violations found on the small network, to 0 violations on the large DAVE network. We conjecture that this may be due to the use of the default parameters for DeepFool, and that adjusting these parameters may yield better results. Additionally, the falsifiers show only a minor increase in the time needed to find a violation, from a median time of 20.2 seconds to 20.7 seconds.

Overall we find that, on the benchmarks explored here, DNN property reduction scales well to larger networks, and enables the application of scalable falsification approaches such as adversarial example generation.

V. CONCLUSION

In this work we present an approach for reducing DNN correctness problems to facilitate the application of falsifiers, in particular adversarial attacks, for finding DNN property violations. We implement our approach and apply it to a range of correctness problem benchmarks and find that 1) the reduction approach covers a rich set of properties, 2) reducing problems enables falsifiers to find property violations, and 3) since falsifiers tend to have different strengths, a portfolio approach can increase the violation finding ability. In future work we plan to extend DNNF to support the full range of properties supported by our algorithmic approach, perform a systematic evaluation of what factors may influence falsifier performance, and explore how reduction can also broaden the applicability of verifiers.

DATA AVAILABILITY

We make DNNF available at https://github.com/dlshriver/DNNF, and we provide an artifact containing the tool, as well as the data and scripts required to replicate our study at https://doi.org/10.5281/zenodo.4439219.

ACKNOWLEDGMENTS

This material is based in part upon work supported by National Science Foundation awards 1900676 and 2019239.
Appendix

A. Proofs

Lemma 1. Let \( \phi \) be a conjunction of linear inequalities over the variables \( x_i \) for \( i \) from 0 to \( n - 1 \). We can construct an H-polytope \( H = (A, b) \) with Alg. 2 s.t. \( (Ax \leq b) \iff (x \models \phi) \).

Proof. Let \( f(x) = \sum_{i=0}^{n-1} a_i x_i \). We first show that every linear inequality in the conjunction can be reformulated to the form \( f(x) \leq b \). It is trivial to show the ineq. can be manipulated to have variables on lhs and a constant on rhs, that can be manipulated to become \( < \) comparison by decrementing the rhs constant from \( b \) to \( b' \) where \( b' \) is the largest representable number less than \( b \). We prove ineq. with \( \leq \) can be reformulated to use \( \leq \) by contradiction. Assume either \( f(x) < b \) and \( f(x) > b \) or \( f(x) \geq b \) and \( f(x) \leq b' \). Either \( b' < f(x) < b \), a contradiction, since \( f(x) \) cannot be both larger than the largest representable number less than \( b \) and also less than \( b' \). Or \( b \leq f(x) \leq b' \), a contradiction, since \( b' < b \) by definition.

Given a conjunction of lin. ineq. in the form \( f(x) \leq b \), Alg. 2 constructs \( A \) and \( b \) with a row in \( A \) and value in \( b \) corresponding to each conjunct. There are two cases: \( (Ax \leq b) \iff (x \models \phi) \) and \( (Ax \not\leq b) \iff (x \not\models \phi) \).

We prove case 1 by contradiction. Assume \( (Ax \leq b) \) and \( (x \not\models \phi) \). By construction of \( H \) in Alg. 2, each conjunct of \( \phi \) is exactly 1 constraint in \( H \). If \( Ax \not\leq b \), then all constraints in \( H \) must be satisfied, and thus all conjuncts in \( \phi \) must be satisfied and \( x \not\models \phi \), a contradiction.

We prove case 2 by contradiction. Assume \( (x \models \phi) \) and \( (Ax \not\leq b) \). By construction of \( H \) in Alg. 2, each conjunct of \( \phi \) is exactly 1 constraint in \( H \). If \( x \models \phi \), then all conjuncts in \( \phi \) must be satisfied, and thus all constraints in \( H \) must be satisfied and \( Ax \not\leq b \), a contradiction.

Lemma 2. Let \( H = (A, b) \) be an H-polytope s.t. \( Ax \not\leq b \). Alg. 4 constructs a DNN, \( N' \), that classifies whether inputs satisfy \( Ax \leq b \). Formally, \( x \in H \iff N'_0(x) \leq N'_1(x) \).

Proof. There are 2 cases:
1) \( x \in H \rightarrow N'_0(x) \leq N'_1(x) \)
2) \( N'_0(x) > N'_1(x) \rightarrow x \notin H \)

We prove case 1 by contradiction. Assume \( x \in H \) and \( N'_0(x) > N'_1(x) \). From Alg. 4, each neuron in the hidden layer of \( N' \) corresponds to one constraint in \( H \). The weights of each neuron are the values in the corresponding row of \( A \), and the bias is the negation of the corresponding value of \( b \). If input \( x \) satisfies the constraint, then the neuron value will be at most 0, otherwise it will be greater than 0. After the ReLU, each neuron will be equal to 0 if the corresponding constraint is satisfied by \( x \) and greater than 0 otherwise. The first output neuron sums all neurons in the hidden layer, while the second has a constant value of 0. If \( x \in H \), then all neurons in the hidden layer after activation must have a value of 0 since all constraints are satisfied. However, if all neurons have value 0, then their sum must also be 0, and therefore \( N'_0(x) = N'_1(x) \), a contradiction.

We prove case 2 by contradiction. Assume \( N'_0(x) \leq N'_1(x) \) and \( x \not\in H \). If \( x \not\in H \), at least one neuron in the hidden layer must have a value greater than 0 after the ReLU since at least one constraint is not satisfied. Because some neuron has a value greater than 0, their sum must also be greater than 0, and therefore \( N'_0(x) > N'_1(x) \), a contradiction.

Lemma 3. Let \( H = (A, b) \) be an H-polytope s.t. \( Ax \leq b \). Alg. 3 constructs a DNN, \( N'' \), that maps values from the \( n \)-dimensional unit hypercube to the axis aligned hyperrectangle that minimally bounds \( H \). The range of this mapping does not exclude any \( x \) s.t. \( Ax \leq b \). Formally, \( \forall x \in H \exists x' \in [0, 1]^n. x' = N''(x) \).

Proof. The proof is by contradiction. Let the axis aligned hyperrectangle that minimally bounds \( H \) be specified by lower bounds \( b \) and upper bounds \( ub \) s.t. \( \forall x \in H. x \leq b \land x \geq ub \). Alg. 3 constructs a DNN, \( N'' \), that computes \( N''_0(x) = W^T z + b \), where \( W = \text{diag}(ub - lb) \) and \( b = lb \). This function is invertible: \( N''^{-1}(x) = W^{-1}(x - lb) \). Formally, \( \exists x \in H. \exists H. (x = N''^{-1}(z) \land (z_1 < 0 \lor z_1 > 1)). \) From the def. of \( N''^{-1} \), we get \( N''^{-1}(lb) \leq z_1 \leq N''^{-1}(ub) \) and \( z_1 \leq N''^{-1}(lb) - N''^{-1}(ub) = \left( ub_i - lb_i \right) \). Therefore \( \left( lb_i \leq z_1 \leq ub_i \right) \rightarrow (0 \leq z_1 \leq 1) \), a contradiction.

Theorem 2. Let \( \psi = \langle N', \phi \rangle \) be a correctness problem with its property defined as a formula of disjunctions and conjunctions of linear inequalities over the inputs and outputs of \( N \). Property Reduction (Alg. 1) maps \( \psi \) to an equivalent set of correctness problems \( \langle N'_1, \phi_1 \rangle, \ldots, \langle N'_{n}, \phi_{n} \rangle \).

Proof. A model that satisfies any disjunction of \( DNF(\neg \phi) \) falsifies \( \phi \). If \( \phi \) is falsifiable, then at least one disjunct of \( DNF(\neg \phi) \) is falsifiable.

Alg. 1 constructs a correctness problem for each disjunct. For each disjunct, Alg. 1 constructs an H-polytope, \( H \), which is used to construct a prefix network, \( N'_p \), and suffix network, \( N_s \). The algorithm then constructs networks \( N''(x) = \text{concat}(N'_p(x), x) \) and \( N''(x) = N_s(N'_p(N''(x))) \). Alg. 1 pairs each constructed network with the property \( \phi = \forall x. x \in [0, 1]^n \rightarrow N''(x) \). A violation occurs only when \( N''(x) \not< N''(x) \). By Lemmas 1, 2, and 3, we get that \( N''(x) \leq N''(x) \) if and only if \( N''(x) \in H \). If \( N''(x) \not\in H \) then \( N''(x) \) satisfies the disjunct and is therefore a violation of the original property.

B. On Existence of a Bounded Largest Representable Number

Our proof that property reduction generates a set of robustness problems equivalent to an arbitrary problem relies on the assumption that strict inequalities can be converted to non-strict inequalities. To do so we rely on the existence of a largest representable number that is less than some given value. While this is not necessarily true for all sets of numbers (e.g., \( \mathbb{R} \)), it is true for for most numeric representations used in computation (e.g., IEEE 754 floating point arithmetic).
REFERENCES

[1] Arvind Adinomool, Thao Dang, Alexandre Donzé, James Kapinski, and Xiaojing Jin. Classification and coverage-based falsification for embedded control systems. In International Conference on Computer Aided Verification, pages 483–503, Springer, 2017.

[2] N. Alkbar and A. Mian. Threat of adversarial attacks on deep learning in computer vision: A survey. IEEE Access, 6:14410–14430, 2018.

[3] Davide Anguita, Alessandro Aghio, Luca Oneto, Xavier Parra, and Jorge Luis Reyes-Ortiz. A public domain dataset for human activity recognition using smartphones. In 21st European Symposium on Artificial Neural Networks, ESANN 2013, Bruges, Belgium, April 24-26, 2013.

[4] Yashwanth Annapureddy, Che Liu, Georgios Fainekos, and Sriram Vatsyayan. S-talo: A tool for temporal logic falsification for hybrid systems. In International Conference on Tools and Algorithms for the Construction and Analysis of Systems, pages 254–257. Springer, 2011.

[5] Daniel Arp, Michel Spreitzer, Helio H. Lopes, and Konrad Rieck. DREBIN: effective and explainable detection of android malware. CoRR, abs/1412.0368, 2014.

[6] Stanley Balk, Hoang-Dung Tran, Kerianne Hobbs, and Taylor T. Johnson. Improved geometric path enumeration for verifying relu neural networks. In Shavendra K. Lahiri and Chao Wang, editors, Computer Aided Verification, pages 66–96, Cham, 2020. Springer International Publishing.

[7] Osbert Bastani, Yani Ioannou, Leonidas Lampropoulos, Dimitrios Vytiniotis, Aditya V. Nori, and Antonio Criminisi. Measuring neural network robustness with constraints. In Proceedings of the 15th International Conference on Neural Information Processing Systems, NIPS’16, pages 2621–2629, USA, 2016. Curran Associates Inc.

[8] Armin Bierz, Alessandro Cimatti, Edmund M Clarke, Masahiro Fujita, and Yumah Zhu. Symbolic model checking using sat procedures instead of bdd's. In Proceedings of the 38th annual ACM/IEEE Design Automation Conference, pages 317–320, 1999.

[9] Mariusz Bojarski, Davide Del Testa, Daniel Dworakowski, Bernhard F. Codevilla, M. Miiller, A. Lopez, V. Koltun, and A. Dosovitskiy. End-to-end driving via conditional imitation learning. In International Conference on Robotics and Automation (ICRA), pages 4795–4804, 2018.

[10] Raj Kumar Boopathy, Tsui-Wei Weng, Pin-Yu Chen, Sijia Liu, and Luca Daniel. Can-cert: An efficient framework for certifying robustness of convolutional neural networks. In AAAI, Jan 2019.

[11] Elena Boteva, Panajiotis Kouvaros, Jan Kronqvist, Alessio Lomuscio, and Ruth Misener. Efficient verification of relu-based neural networks via dependency analysis. In The Thirty-Fourth AAAI Conference on Artificial Intelligence, AAAI 2020, The Thirty-Second Innovative Applications of Artificial Intelligence Conference, IAAI 2020, The Tenth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2020, New York, NY, USA, February 7-12, 2020, pages 3291–3299. AAAI Press, 2020.

[12] Rudy B. Band, Ilker Turkaslan, Philip H. S. Torr, Pushmeet Kohli, and Pawan Kumar Mudigonda. A unified view of piecewise linear neural network verification. In NeurIPS, pages 4795–4804, 2018.

[13] Nicholas Carlini and David A. Wagner. Towards evaluating the robustness of neural networks. CoRR, abs/1604.06902, 2016.

[14] Jeffrey De Fauw, Joseph R. Lelisnam, Bernardino Romero-Parades, Stanislav Nikolov, Nadia Tomasev, Sam Blackwell, Harry Askham, Xavier Golot, Brendan O’Donoghue, Daniel Visentin, George van den Driessche, Balaji Lakshminarayanan, Clemens Meyer, Faith Mackinder, Shi, and Alexander T. Johnson. Cas: Deep learning on the edge. In Conference on Computer Vision and Pattern Recognition (CVPR), pages 3323–3332, 2019.

[15] Jeffery De Fauw, Joseph R. Lelisnam, Bernardino Romero-Parades, Stanislav Nikolov, Nadia Tomasev, Sam Blackwell, Harry Askham, Xavier Golot, Brendan O’Donoghue, Daniel Visentin, George van den Driessche, Balaji Lakshminarayanan, Clemens Meyer, Faith Mackinder, Shi, and Alexander T. Johnson. Cas: Deep learning on the edge. In Conference on Computer Vision and Pattern Recognition (CVPR), pages 3323–3332, 2019.

[16] Alex Krizhevsky and Geoffrey Hinton. Learning multiple layers of features from tiny images. 2009.

[17] Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio. Adversarial examples. In 34th International Conference on Machine Learning, ICML 2017, Sydney, Australia, 6-11 August, 2017, pages 182–190. JMLR.org, 2017.

[18] T. Gehr, M. Mirman, D. Drachsler-Cohen, P. Tsankov, S. Chaudhuri, and M. Vochev. A2: Safety and robustness certification of neural networks with abstract interpretation. In Proceedings of the 3rd International Symposium on Security and Privacy (SP), pages 3–18, May 2018.

[19] Patrick Godefroid and Pierre Wolper. Using partial orders for the efficient verification of deadlock freedom and safety properties. In International Conference on Computer Aided Verification, pages 332–347. Springer, 1991.

[20] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. In Yoshua Bengio and Yann LeCun, editors, 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings, 2015.

[21] S. Goyal and Y. Zeki. Towards generating adversarial examples for neural networks. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, London, UK, November 6-10, 2017, pages 741–754. ACM, 2017.

[22] Guy Katz, Clark W. Barrett, David L. Dill, Kyle Julian, and Mykel J. Kochenderfer. Reluplex: An efficient SMT solver for verifying deep neural networks. In Computer Aided Verification - 29th International Conference, CAV 2017, Heidelberg, Germany, July 24–28, 2017, Proceedings, Part I, pages 254–257. Springer, 2018.

[23] Guy Katz, Derek A. Huang, Sujan Dravida, Prathap Thulasidasan, and Yunshan Zhu. Symbolic model checking using sat procedures instead of bdd's. In Proceedings of the 38th annual ACM/IEEE Design Automation Conference, pages 317–320, 1999.

[24] T. Gehr, M. Mirman, D. Drachsler-Cohen, P. Tsankov, S. Chaudhuri, and M. Vochev. A2: Safety and robustness certification of neural networks with abstract interpretation. In Proceedings of the 3rd International Symposium on Security and Privacy (SP), pages 3–18, May 2018.

[25] P. Tsankov, S. Chaudhuri, and M. Vochev. A2: Safety and robustness certification of neural networks with abstract interpretation. In Proceedings of the 3rd International Symposium on Security and Privacy (SP), pages 3–18, May 2018.

[26] Patent Godefroid and Pierre Wolper. Using partial orders for the efficient verification of deadlock freedom and safety properties. In International Conference on Computer Aided Verification, pages 332–347. Springer, 1991.

[27] Alekh Krizhevsky and Geoffrey Hinton. Learning multiple layers of features from tiny images. 2009.

[28] Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio. Adversarial examples. In 34th International Conference on Machine Learning, ICML 2017, Sydney, Australia, 6-11 August, 2017, pages 182–190. JMLR.org, 2017.

[29] Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio. Adversarial examples. In 34th International Conference on Machine Learning, ICML 2017, Sydney, Australia, 6-11 August, 2017, pages 182–190. JMLR.org, 2017.

[30] Guy Katz, Clark W. Barrett, David L. Dill, Kyle Julian, and Mykel J. Kochenderfer. Reluplex: An efficient SMT solver for verifying deep neural networks. In Computer Aided Verification - 29th International Conference, CAV 2017, Heidelberg, Germany, July 24–28, 2017, Proceedings, Part I, pages 254–257. Springer, 2018.

[31] Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio. Adversarial examples. In 34th International Conference on Machine Learning, ICML 2017, Sydney, Australia, 6-11 August, 2017, pages 182–190. JMLR.org, 2017.

[32] Guy Katz, Derek A. Huang, Sujan Dravida, Prathap Thulasidasan, and Yunshan Zhu. Symbolic model checking using sat procedures instead of bdd's. In Proceedings of the 38th annual ACM/IEEE Design Automation Conference, pages 317–320, 1999.

[33] P. Tsankov, S. Chaudhuri, and M. Vochev. A2: Safety and robustness certification of neural networks with abstract interpretation. In Proceedings of the 3rd International Symposium on Security and Privacy (SP), pages 3–18, May 2018.

[34] Patent Godefroid and Pierre Wolper. Using partial orders for the efficient verification of deadlock freedom and safety properties. In International Conference on Computer Aided Verification, pages 332–347. Springer, 1991.

[35] Alekh Krizhevsky and Geoffrey Hinton. Learning multiple layers of features from tiny images. 2009.
