Robust Adversarial Learning via Sparsifying Front Ends

Soorya Gopalakrishnan, Student Member, IEEE, Zhinus Marzi, Upamanyu Madhow, Fellow, IEEE, and Ramtin Pedarsani, Member, IEEE

Abstract—It is by now well-known that small adversarial perturbations can induce classification errors in deep neural networks. In this paper, we take a bottom-up signal processing perspective to this problem and show that a systematic exploitation of sparsity in natural data is a promising tool for defense. For linear classifiers, we show that a sparsifying front end is provably effective against $\ell_\infty$-bounded attacks, reducing output distortion due to the attack by a factor of roughly $K/N$ where $N$ is the data dimension and $K$ is the sparsity level. We then extend this concept to deep networks, showing that a “locally linear” model can be used to develop a theoretical foundation for crafting attacks and defenses. We also devise attacks based on the locally linear model that outperform the well-known FGSM attack. We supplement our theoretical results with experiments on the MNIST handwritten digit database, showing the efficacy of the proposed sparsity-based defense schemes.

I. INTRODUCTION

Since Szegedy et al. [1] and Goodfellow et al. [2] pointed out the vulnerability of deep networks to small adversarial perturbations, there has been an explosion of research effort in adversarial attacks and defenses [3]. In this paper, we attempt to provide fundamental insight into both the vulnerability of deep networks to carefully designed perturbations, and a systematic, theoretically justified framework for designing defenses against adversarial perturbations.

Our starting point is the original intuition in Goodfellow et al. [2] that deep networks are vulnerable to small perturbations not because of their complex, nonlinear structure, but because of their being “too linear”. Consider the simple example of a binary linear classifier $w$ operating on $N$-dimensional input $x$, producing the decision statistic $g(x) = w^T x$. The effect of a perturbation $e$ to the input is given by $g(x+e) - g(x) = w^T e$. If $e$ is bounded by $\ell_\infty$ norm (i.e., $\|e\|_\infty = \max_i |e_i| \leq \epsilon$), then the largest perturbation that can be produced at the output is caused by $e = \epsilon \text{sgn}(w)$, and the resulting output perturbation is $\Delta = \epsilon \sum_{i=1}^N |w_i| = \epsilon \|w\|_1$. The latter can be made large unless the $\ell_1$ norm of $w$ is constrained in some fashion. To see what happens without such a constraint, suppose that $w$ has independent and identically distributed components, with bounded expected value and variance. It is easy to see that $\|w\|_1 = \Theta(N^{1/2})$ with high probability, which means that the effect of $\ell_\infty$-bounded input perturbations can be blown up at the output as the input dimension increases.

The preceding linear model provides a remarkably good approximation for today’s deep CNNs. Convolutions, subsampling, and average pooling are inherently linear. A ReLU unit is piecewise linear, switching between slopes at the bias point. A max-pooling unit is a switch between multiple linear transformations. Thus, the overall transfer function between the input and an output neuron can be written as $w_{eq}(x)^T x$, where $w_{eq}(x)$ is an equivalent “locally linear” transformation that exhibits input dependence through the switches corresponding to the ReLU and max pooling units. For small perturbations, relatively few switches flip, so that $w_{eq}(x+e) \approx w_{eq}(x)$. Note that the preceding argument also applies to more general classes of nonlinearities: the locally linear approximation is even better for sigmoids, since slope changes are gradual rather than drastic. These observations motivate us to begin with a study of linear classifiers, before extending our results to neural networks via a locally linear model.

As we discuss in Section II there are a number of defenses based on modifying the optimization procedures used for training neural networks. In contrast, we take a bottom-up signal processing perspective and exploit the rather general observation that input data must be sparse in some basis in order to avoid the curse of dimensionality. Sparsity is an intuitively plausible concept: we understand that humans reject small perturbations by focusing on the key features that stand out. Our proposed approach is based on this intuition. In this paper, we show via both theoretical results and experiments that a sparsity-based defense is provably effective against $\ell_\infty$-bounded adversarial perturbations.

Specifically, we assume that the $N$-dimensional input data has a $K$-sparse representation (where $K \ll N$) in a known orthonormal basis. We then employ a sparsifying front end that projects the perturbed data onto the $K$-dimensional subspace. The intuition behind why this can help is quite clear: small perturbations can add up to a large output distortion when the input dimension is large, and by projecting to a smaller subspace, we can limit the damage. Theoretical studies show that this attenuates the impact of $\ell_\infty$-bounded attacks by a factor of roughly $K/N$ (the sparsity level), and experiments show that sparsity levels of the order of 1-5% give an excellent tradeoff between the accuracy of input representation and rejection of adversarial perturbations.

A. Contributions

We develop a theoretical framework to assess and demonstrate the effectiveness of a sparsity-based defense against...
adversarial attacks on linear classifiers and neural networks. Our main contributions are as follows:

- For linear classifiers, we quantify the achievable gain of the sparsity-based defense via an ensemble-averaged analysis based on a stochastic model for weights. We prove that with high probability, the adversarial impact is reduced by a factor of roughly $K/N$, where $K$ is the sparsity of the signal and $N$ is the signal’s dimension.
- For neural networks, we use a “locally linear” model to provide a framework for understanding the impact of small perturbations. Specifically, we characterize a high SNR regime in which the fraction of switches flipping for ReLU nonlinearities for an $\ell_\infty$-bounded perturbation is small.
- Using the preceding framework, we show that a sparsifying front end is effective for defense, and devise a new locally linear attack that outperforms the well-known Fast Gradient Sign Method (FGSM) attack [2].
- We supplement our theoretical results with experiments on the MNIST dataset [4] for a variety of recent attacks.

B. Notation

Here we define the notations $\Theta(\cdot)$, $O(\cdot)$, $\omega(\cdot)$, and $o(\cdot)$:

- $f = O(g)$ if and only if there exists a constant $C > 0$ such that $|f/g| < C$.
- $f = \Theta(g)$ if and only if there exist two constants $C_1, C_2 > 0$ such that $C_1 < |f/g| < C_2$.
- $f = \omega(g)$ if and only if $g$ does not exist a constant $C > 0$ such that $|f/g| < C$, and
- $f = o(g)$ if and only if $g = \omega(f)$.

II. RELATED WORK

A. Sparse Representations

It is well-known that most natural data can be compactly expressed as a sparse linear combination of atoms in some basis [5–7]. Such sparse representations have led to state-of-the-art results in many fundamental signal processing tasks such as image denoising [8], [9], neuromagnetic imaging [10], [11], image super-resolution [12], inpainting [13], blind audio source separation [14], source localization [15], etc. There are two broad classes of sparsifying dictionaries employed in literature: predetermined bases such as wavelets [5, 16], and learnt bases which are inferred from a set of training signals [9], [17], [18]. The latter approach has been found to outperform predetermined dictionaries. Sparsity has also been suggested purely as a means of improving classification performance [19], which indicates that the performance penalty for appropriately designed sparsity-based defenses could be minimal.

B. Local Linearity Hypothesis

The existence of “blind spots” in deep neural networks [11] has been the subject of extensive study in machine learning literature [3]. It was initially surmised that this vulnerability is due to the highly complex, nonlinear nature of neural networks. However, the success of linearization-based attacks such as the Fast Gradient Sign Method (FGSM) [2] and DeepFool [20] indicates that it is instead due to their “excessive linearity”. This is further hacked up by work on the curvature profile of deep neural networks [21], [22] showing that the decision boundaries in the vicinity of natural data can be approximated as flat along most directions. Our work on attack and defense is grounded in a locally linear model for neural networks, and the results discussed later demonstrate the efficacy of this approach.

C. Defense Techniques

Existing defense mechanisms against adversarial attacks can be broadly divided into two categories: (a) empirical defenses, based purely on intuitively plausible strategies, together with experimental evaluations, and (b) provable defenses with theoretical guarantees of robustness. We briefly discuss the empirical work related to our defense, and then give an overview of provable defense techniques.

Empirical Defenses: Several empirical defenses utilize preprocessing techniques that are implicitly sparsity-based, including JPEG compression [23, 24], PCA [25] and projection onto generative models [26, 27]. However many such techniques were found to confer robustness purely by obfuscating gradients necessary for the adversary, and they were successfully defeated by gradient approximation techniques developed in [28]. In contrast our sparsity-based defense is robust to the attack techniques in [28]. Overall, the evaluations in such prior work have been purely empirical in nature. Our proposed framework, grounded in a locally linear model for neural networks, provides a foundation for systematic pursuit of sparsity-based preprocessing.

Provable Defenses: There is a growing body of work focused on developing provable guarantees of robustness against adversarial perturbations [29–42]. We do not provide an exhaustive discussion due to space constraints, but we illustrate some typical characteristics of these approaches.

Many provable defenses focus on retraining the network with an optimization criterion that promotes robustness towards all possible small perturbations around the training data. For example, Raghunathan et al. [29] develop semidefinite programs (SDP) to upper bound the $\ell_1$ norm of the gradient of the classifier around the data point, which they then optimize during training to obtain a more robust network. The certificates provided are quite loose, and are outperformed by other defenses, including ours. A tighter SDP relaxation is developed in [30] to certify the robustness of any given network, but it is not used to train a new robust model. Both the SDP certificates are computationally restricted to fully-connected networks. Another provable defense by Wong and Kolter [31] employs a linear programming (LP) based approach to bound the robust error. This is more efficient than the SDP approach, and can be scaled to larger networks [32]. The LP technique works well for small perturbations, but for larger perturbation sizes there is a drop in the accuracy of natural images.

A different training technique based on distributionally robust optimization was proposed by Sinha et al. [33], providing a certificate of robustness for attacks whose probability distribution is bounded in Wasserstein distance from the original
data distribution. Although the theoretical guarantees do not directly translate to norm-bounded attacks, this approach yields good results in practice for small perturbation sizes. Another defense that works well is that of Mirman et al. [34], who use the framework of abstract interpretation to develop various upper bounds on the adversarial loss which can be optimized over during training. Some other provable defenses try to limit Lipschitz constants related to the network output function, for example via cross-Lipschitz regularization [35] and ℓ2 matrix-norm regularization of weights [36] in order to defend against ℓ2-bounded attacks. However the bounds in [35] are limited to 2-layer networks, and [36] is based on layerwise bounds that have been shown to be loose [29, 31].

All of the above techniques try to train the network so as to make its output less sensitive to input perturbations by modifying the optimization framework employed for network training. In contrast, our defense takes a bottom-up signal processing approach, exploiting the sparsity of natural data to combat perturbations at the front end, while using conventional network training. It is therefore potentially complementary to defenses based on modifying network training. Parts of this work appeared previously in our conference paper [37] which focused on linear classifiers. In this paper, we provide a comprehensive treatment that applies to neural networks, by employing the concept of local linearity. Another related work that uses sparsity-based preprocessing is [38], which studies ℓ0-bounded attacks. These are not visually imperceptible (unlike the ℓ∞-bounded attacks that we study), but they are easy to realize in practice, for example by placing a small sticker on an image. For this class of attacks, [38] shows that the sparse projection can be reformulated as a compressive sensing (CS) problem, and obtain a provably good estimate of the original image via CS recovery algorithms.

There is also a line of work on verifying the robustness of a given network by using exact solvers based on discrete optimization techniques such as satisfiability modulo theory [39, 40] and mixed-integer programming [41, 42]. However these techniques have combinatorial complexity (in the worst-case, exponential in network size), and so far have not been scaled beyond moderate network sizes.

III. SPARSITY-BASED DEFENSE

A. Problem Setup

For simplicity we start with binary classification. Given a binary inference model \( g: \mathbb{R}^N \to \mathbb{R} \), we assume that its input data \( x \in \mathbb{R}^N \) has a \( K \)-sparse representation \( (K \ll N) \) in a known orthonormal basis \( \Psi: \| \Psi^T x \|_0 \leq K \). Let us denote by \( \hat{x} \) a modified version of the data sample \( x \). We now define a performance measure \( \Delta \) that quantifies the robustness of \( g(\cdot) \):

\[
\Delta(x, \hat{x}) = |g(\hat{x}) - g(x)|.
\]

For example, for a linear classifier \( g(x) = w^T x \), the performance measure is \( \Delta(x, \hat{x}) = |w^T(\hat{x} - x)| \).

We now consider a system comprised of the classifier \( g(\cdot) \) and two external participants: the adversary and the defense, depicted in Fig. 1.

![Fig. 1: Block diagram of the system, depicting an adversarial example \( x = x + e \) (with \( \ell_\infty \) constraint on \( e \)), a preprocessing defense \( f(\cdot) \) and a classifier \( g(\cdot) \).]

1. The adversary corrupts the input \( x \) by adding a perturbation \( e \), with the goal of causing misclassification:

\[
\max_e \Delta(x, \hat{x}) \quad \text{s.t.} \quad \|e\|_\infty < \epsilon.
\]

We are interested in perturbations that are visually imperceptible, hence we impose an \( \ell_\infty \)-constraint on the adversary.

2. The defense preprocesses the perturbed data via a function \( f: \mathbb{R}^N \to \mathbb{R}^N \), with the goal of minimizing the adversarial impact \( \Delta \).

This setup can be easily extended to multiclass classification as we show in Section V.E.

B. Sparsifying Front End Description

We propose a defense based on a sparsifying front end that exploits sparsity in natural data to combat adversarial attacks. Specifically, we preprocess the input via a front end that computes a \( K \)-sparse projection in the basis \( \Psi \). Figure 2 shows a block diagram of our model for a neural network, depicting an additive perturbation followed by sparsity-based preprocessing.

Here is an intuitive explanation of how this defense limits adversarial perturbations. If the data is exactly \( K \)-sparse in domain \( \Psi \), the front end leaves the input unchanged \( (\hat{x} = x) \) when there is no attack \( (e = 0) \). The front end attenuates the perturbation by projecting it onto the space spanned by the basis functions corresponding to the \( K \) retained coefficients. If the perturbation is small enough, then the \( K \) retained coefficients corresponding to \( x \) and \( x + e \) remain the same, in which case the neural network sees the original input plus the projected, and hence attenuated, perturbation.
Let $\mathcal{H}_K : \mathbb{R}^N \to \mathbb{R}^N$ represent the block that enforces sparsity by retaining the $K$ coefficients largest in magnitude and zeroing out the rest. We can now define the following:

- The support $S_K$ of the $K$-sparse representation of $x$, and the projection $P_K$ of $e$ onto the subspace that $x$ lies in are defined as follows:

$$S_K(x) \triangleq \text{supp}(\mathcal{H}_K(\Psi^T x)),$$

$$P_K(e, x) \triangleq \sum_{k \in S_K(x)} \psi_k \psi_k^T e.$$

- The high SNR regime is the operating region where the perturbation does not change the subspace that $x$ lies in:

$$\text{High SNR: } S_K(x) = S_K(x + e).$$

We characterize the conditions guaranteeing this in Prop. 1.

If we operate at high SNR, the front end preserves the signal and hence its output $\hat{x}$ can be written as follows:

$$\hat{x} = x + \sum_{k \in S_K(x)} \psi_k \psi_k^T e = x + P_K(e, x).$$

Thus the effective perturbation is $P_K(e, x)$, which lives in a lower dimensional space. Its impact is therefore significantly reduced. In Sections IV and V we quantify the reduction in adversarial impact via an ensemble-averaged analysis based on a stochastic model for the classifier $g(x)$.

C. Characterizing the High SNR Regime

We can gain valuable design insight by characterizing the conditions that guarantee high SNR operation of the sparsifying front end, as stated in the following proposition:

**Proposition 1.** For sparsity level $K$ and perturbation $e$ with $\|e\|_\infty \leq \epsilon$, the sparsifying front end preserves the input coefficients if the following SNR condition holds:

$$\text{SNR} \triangleq \frac{\lambda}{\epsilon} > \gamma,$$

where $\lambda$ is the magnitude of the smallest non-zero entry of $\mathcal{H}_K(\Psi^T x)$ and $\gamma = 2 \max_k \|\psi_k\|_1$.

**Proof.** By Holder inequality, the SNR condition implies that

$$\lambda > \epsilon \gamma \geq 2 \max_k \|\psi_k^T e\| > \|\psi_i^T e\| + \|\psi_j^T e\| \quad \forall \ i, j.$$

In particular, we can choose $i$ and $j$ such that

$$\min_{i \in S_K(x)} (\|\psi_i^T x\| - \|\psi_i^T e\|) > \max_{j \notin S_K(x)} \|\psi_j^T e\|,$$

where we have used the fact that $\lambda = \min_{i \in S_K(x)} \|\psi_i^T x\|$. We can now use the triangle inequality to get

$$\min_{k \in S_K(x)} \|\psi_k^T (x + e)\| > \max_{j \notin S_K(x)} \|\psi_j^T e\|.$$

It is easy to see that this is equivalent to $S_K(x + e) = S_K(x)$, which completes the proof.

A direct consequence of the SNR condition is that we expect basis functions that are small in $\ell_1$ norm to be more effective. As we will see later in Section IV-B this is also a favorable criterion for performance in the white box attack scenario. Another important design parameter is the value of $K$, which must be chosen to optimize the following tradeoff: lower sparsity levels allow us to impose high SNR even for larger perturbations, but if the data is only approximately $K$-sparse, this results in unwanted signal perturbation. We find in our experiments that a choice of $K'/N$ of the order of 1–5% provides an excellent balance to this tradeoff.

IV. ANALYSIS FOR LINEAR CLASSIFIERS

Consider a linear classifier $g(x) = w^T x$. We calculate the adversarial impact for various attack models and quantify the efficacy of our defense by using a stochastic model for $w$.

A. Impact of Adversarial Perturbation

When the front end is not present, the impact of the attack is $\Delta = w^T e$. By Holder inequality, we have

$$\Delta = w^T e \leq \|e\|_\infty \|w\|_1 \leq \epsilon \|w\|_1 \triangleq \Delta_0,$$

where the second inequality follows from the $\ell_\infty$ attack budget constraint. We can observe that $e_0 = \epsilon \text{sgn}(w)$ achieves equality in (2), which means that $e_0$ is the optimal attack when the adversary has knowledge of $w$. We use $\Delta_0 = \epsilon \|w\|_1$ as a baseline to assess the efficacy of our defense.

When the defense is present, the adversarial impact $\Delta$ becomes

$$\Delta = \|w^T(\hat{x} - x)\| = \|w^T P_K(e, x)\| = \|e^T P_K(w, x)\|,$$

where the second equality follows from the definition of $P_K(e, x)$. We can now consider two scenarios depending on the adversary’s knowledge of the defense and the classifier:

1. **Semi-white box scenario:** Here perturbations are designed based on the knowledge of $w$ alone, and therefore the attack remains $e_{SW} = \epsilon \text{sgn}(w)$. The output distortion becomes

$$\Delta_{SW} = \epsilon \|\text{sgn}(w^T) P_K(w, x)\|.$$  

We note that the attack is aligned with $w$.

2. **White box scenario:** Here the adversary has the knowledge of both $w$ and the front end, and designs perturbations in order to maximize $\Delta = \|e^T P_K(w, x)\|$. We can use the same Holder inequality based argument as before to prove that the optimal perturbation is $e_W = \epsilon \text{sgn}(P_K(w, x))$. The resulting output distortion can be written as

$$\Delta_W = \epsilon \|P_K(w, x)\|_1.$$  

Thus, instead of being aligned with $w$, $e_W$ is aligned to the projection of $w$ onto the subspace that $x$ lies in.
B. Ensemble Averaged Performance

We now quantify the gain in robustness conferred by the sparsifying front end by taking an ensemble average over randomly chosen classifiers \( w \).

**Assumption.** We assume a random model for \( w \), where the entries \( \{w_i\}_{i=1}^N \) are i.i.d. with zero mean and median. Let \( \mathbb{E}[|w_i|] = \mu = \Theta(1) \) and \( \mathbb{E}[w_i^2] = \sigma^2 = \Theta(1) \).

We observe that the baseline adversarial impact \( \Delta_0 = \epsilon \|w\|_1 \) scales with \( N \). This is formalized in the following proposition:

**Proposition 2.** \( \Delta_0/N \) converges to \( \epsilon \mu \) almost surely, i.e.

\[
\Pr\left( \lim_{N \to \infty} \frac{\Delta_0}{N} = \epsilon \mu \right) = 1.
\]

Thus, with no defense, the adversarial impact scales as \( \Theta(N) \).

**Proof.** \( \Delta_0 \) is the sum of i.i.d. random variables \( \epsilon |w_i| \) with finite mean: \( \mathbb{E}[|w_i|] = \epsilon \mu < \infty \). Hence we can apply the strong law of large numbers, which completes the proof.

We now state the following theorems that characterize the performance of the sparsifying front end defense in the semi-white box and white box scenarios.

1. **Semi-White Box Scenario:**

**Theorem 1.** As \( K \) and \( N \) approach infinity, \( \Delta_{SW}/K \) converges to \( \epsilon \mu \) in probability, i.e.

\[
\lim_{K \to \infty} \Pr\left( \frac{\Delta_{SW}}{K} - \epsilon \mu \leq \delta \right) = 1 \quad \forall \delta > 0.
\]

Thus, the impact of adversarial perturbation in the case of semi-white box attack is attenuated by a factor of \( K/N \) compared to having no defense.

**Proof.** Let us assume without loss of generality that \( S_K(x) = \{1, \ldots, K\} \). We can rewrite the adversarial impact \( \|Z_K\|_1 \) as

\[
\Delta_{SW} = \epsilon |Z_K|, \text{ where } Z_K = \sum_{i=1}^K \text{sgn}(w)^T \psi_k \psi_k^T w.
\]

The following lemma provides an upper bound on the mean and variance of \( Z_K \).

**Lemma 1.** The mean and variance of \( Z_K \) are bounded by linear functions of \( K \).

\[
\mathbb{E}[Z_K] = K \mu, \quad \text{var}(Z_K) \leq K (\sigma^2 + \mu^2).
\]

**Proof.** We can write \( Z_K = \sum_{i=1}^K U_i V_i \), where

\[
U_i = \sum_{m=1}^N \psi_i[m] w_m, \quad V_i = \sum_{m=1}^N \psi_i[m] \text{sgn}(w_m).
\]

We observe that for \( i, j \in \{1, \ldots, K\} \), \( \mathbb{E}[U_i V_i] = \mu \), and

\[
\text{var}(U_i V_i) = \sigma^2 + \mu^2 - 2\mu^2 \sum_{m=1}^N \psi_i^2[m],
\]

\[
\text{cov}(U_i V_i, U_j V_j) = -2\mu^2 \sum_{m=1}^N \psi_i^2[m] \psi_j^2[m], \quad i \neq j.
\]

Hence we get \( \mathbb{E}[Z_K] = K \mu \), and

\[
\text{var}(Z_K) = K \sum_{i=1}^K \text{var}(U_i V_i) - \sum_{i,j=1}^K \text{cov}(U_i V_i, U_j V_j)
\]

\[
= K (\sigma^2 + \mu^2) - 2\mu^2 \sum_{m=1}^N \sum_{i,j=1}^K \psi_i^2[m] \psi_j^2[m]
\]

\[
\leq K (\sigma^2 + \mu^2).
\]

We can now apply Chebyshev’s inequality to \( Y_K = Z_K/K \), using the bounds in the lemma to obtain

\[
\Pr(|Y_K - \mu| \leq \delta) \geq 1 - \frac{1}{K} \left( \frac{\sigma^2 + \mu^2}{\delta^2} \right) \quad \forall \delta \geq 0.
\]

Note that \( |\Delta_{SW}/K - \epsilon \mu| = \epsilon |Y_K| - \mu \leq \epsilon |Y_K| - \mu \). The statement of the theorem follows by \([5]\) and letting \( K \to \infty \) in the above inequality.

2. **White Box Scenario:**

We begin with the following lemma that provides a useful upper bound on the impact of the white box attack.

**Lemma 2.** An upper bound on the white box distortion \( \Delta_W \) is given by

\[
\Delta_W \leq \epsilon \sum_{k=1}^K \|\psi_k^T w\| \|\psi_k\|_1.
\]

**Proof.**

\[
\Delta_W = \epsilon \|P_K(w, x)\|_1 = \epsilon \sum_{k=1}^K \sum_{i=1}^N \psi_k^T w \psi_k[i]
\]

\[
\leq \epsilon \sum_{k=1}^K \sum_{i=1}^N \|\psi_k^T w\| \|\psi_k[i]\| = \epsilon \sum_{k=1}^K \|\psi_k^T w\| \|\psi_k\|_1.
\]

Note that this bound is exact if the supports of the \( K \) selected basis functions do not overlap, and consequently the white box distortion cannot grow slower than \( K \) since the bound has \( K \) terms. However, if the \( \ell_1 \) norms of the basis functions do not scale too fast with \( N \), we can show that the distortion scales as \( \mathcal{O}(K \log(N)) \), as stated in the following theorem.

**Theorem 2.** Under the assumptions \( \|\psi_k\|_1 = \mathcal{O}(\log N) \), \( \|\psi_k\|_\infty = \mathcal{O}(1) \) \( \forall k \in \{1, 2, \ldots, K\} \), and \( \|w\|_\infty = \mathcal{O}(1) \), we have the following upper bound for \( \Delta_W \):

\[
\lim_{N \to \infty} \Pr(\Delta_W \leq \mathcal{O}(K \log(N))) = 1.
\]

Thus, the impact of adversarial perturbation in the case of white box attack is attenuated by a factor of \( \mathcal{O}(K \log(N)/N) \) compared to having no defense.

**Proof.** We first state the following convergence result:

**Lemma 3.** \( \psi_k^T w \to \mathcal{N}(0, \sigma^2) \) in distribution.

**Proof.** We show that we can apply Lindeberg’s version of the central limit theorem, noting that \( \psi_k^T w = \sum_{i=1}^N Y_i \), where
\[ Y_i = \psi_k[i] w_i \] are independent random variables with \( \mathbb{E}[Y_i] = 0 \) and \( \text{var}(Y_i) = \sigma_i^2 \), with \( \sum_{i=1}^{N} \sigma_i^2 = \sigma^2 \).

Now, given \( \delta > 0 \), we investigate the following quantity in order to check Lindeberg's condition:

\[ L(\delta, N) = \frac{1}{\sigma^2} \sum_{i=1}^{N} \mathbb{E}[Y_i^2 1_{\{Y_i > \delta \sigma \}}] . \]

From the \( \ell_\infty \) assumptions on \( \psi_k \) and \( w \), we observe that

\[ \mathbb{E}[\psi_k^2[i] w_i^2 1_{\{Y_i > \delta \sigma \}}] \leq \sigma^2(1) \mathcal{O}^2(1) \Pr\left(\{|Y_i| > \delta \sigma\}\right) \]

\[ = \sigma^2(1) \mathcal{O}^2(1) \Pr\left(\{|w_i| > \delta \sigma / \mathcal{O}(1)\}\right) . \]

Also note that \( \forall \delta > 0, \exists M \) s.t. \( \forall N > M, |w_i| < \delta \sigma / \mathcal{O}(1) \) \( \forall i \in \{1, \ldots, N\} \). Hence we get \( \lim_{N \to \infty} L(\delta, N) = 0 \), which is Lindeberg's condition.

We can use Lemmas 2 and 3 to obtain

\[ \Pr(\Delta_W > \delta) \leq \Pr\left(\epsilon \sum_{k=1}^{K} |\psi_k| \|w\|_1 > \delta\right) \]

\[ \leq \Pr\left(\sum_{k=1}^{K} |\psi_k|^T w > \frac{\delta}{\epsilon K \|\psi_k\|_1}\right) \]

\[ \leq \sum_{k=1}^{K} \Pr\left(|\psi_k|^T w > \frac{\delta}{\epsilon K \|\psi_k\|_1}\right) \]

\[ = \sum_{k=1}^{K} 2Q\left(\frac{\delta}{\epsilon \sigma K \|\psi_k\|_1}\right) = 2KQ\left(\frac{\delta}{\epsilon \sigma} \mathcal{O}\left(\frac{1}{K \log N}\right)\right) , \]

where the last step follows from the \( \ell_1 \) assumption on \( \psi_k \), and \( Q(x) \) is the Gaussian tail distribution function \( \int_{-\infty}^{\infty} e^{-t^2/2} dt / \sqrt{2\pi} \). We complete the proof by setting \( \delta = \mathcal{O}(K \text{polylog}(N)) \) which makes the right-hand side of the above equation vanish as \( N \) approaches infinity.

A practical take-away from the above theoretical results is that, in order for the defense to be effective against a white box attack, not only do we need input sparsity (\( K \ll N \)), but we also need that the individual basis functions be localized (small in \( \ell_1 \) norm). The latter implies, for example, that sparsification with respect to a wavelet basis, which has more localized basis functions, should be more effective than with a DCT basis.

V. ANALYSIS FOR NEURAL NETWORKS

In this section, we build on the preceding insights for neural networks by exploiting locally linear approximations. For simplicity we start with a 2-layer, fully connected network trained for binary classification, and then extend our results to a general network for multi-class classification.

A. Locally Linear Representation

Consider first binary classification using a neural network with one hidden layer with \( M \) neurons, as depicted in Fig. 3. Since ReLU units are piecewise linear, switching between slopes of 0 and 1, they can be represented using input-dependent switches. Given input \( x \), we denote by \( s_i(x) \in \{0, 1\} \) the switch corresponding to the \( i \)th ReLU unit. Now the activations of the hidden layer neurons can be written as follows:

\[ a_i = \text{ReLU}(w_i^T x - b_i) = s_i(x) w_i^T x - s_i(x) b_i . \]

The output of the neural network can be written as

\[ y(x) = w_0^T a = \sum_{i=1}^{M} s_i(x) w_0[i] w_i^T x - \sum_{i=1}^{M} s_i(x) w_0[i] b_i = w_{eq}(x)^T x - b_{eq}(x) . \]

where

\[ w_{eq}(x) = \sum_{i=1}^{M} s_i(x) w_0[i] w_i, \quad b_{eq}(x) = \sum_{i=1}^{M} s_i(x) w_0[i] b_i . \]

This locally linear model extends to any standard neural network, since convolutions and subsampling are inherently linear and max-pooling units can also be modeled as switches. For more than 2 classes, we will apply this modeling approach to the “transfer function” from the input to the inputs to the softmax layer, as discussed in Section V-E.

B. Impact of Adversarial Perturbation

Now we consider the effect of an \( \ell_\infty \)-bounded perturbation \( e \) on the performance of the network. For ease of notation, we write \( w_{eq} = w_{eq}(x) \), \( \bar{w}_{eq} = w_{eq}(x + e) \), and \( \bar{b}_{eq} = b_{eq}(x + e) \). The distortion due to the attack can be written as

\[ \Delta = y(x + e) - y(x) = \bar{w}_{eq}^T (x + e) - \bar{b}_{eq} - w_{eq}^T x + b_{eq} \]

\[ = \bar{w}_{eq}^T e + [(\bar{w}_{eq} - w_{eq})^T x - (\bar{b}_{eq} - b_{eq})] . \]

We observe that the distortion can be split into two terms: (i) \( \bar{w}_{eq}^T e \) that is identical to the distortion for a linear classifier, and can be analyzed within the theoretical framework of Section IV and (ii) \( (\bar{w}_{eq} - w_{eq})^T x - (\bar{b}_{eq} - b_{eq}) \), that is determined by the ReLU units that flip due to the perturbation.
In the next section, we provide an analytical characterization of a “high SNR” regime in which the number of flipped switches is small, motivated by iterative attacks which gradually build up attack strength over a large number of iterations (with a per-iteration $\ell_\infty$-budget of $\delta \ll \epsilon$). When very few switches flip, the distortion is dominated by the first term in (6), and we can apply our prior results on linear classifiers to infer the efficacy of the sparsifying front end in attenuating the distortion. As we discuss via our numerical results, this creates a situation in which it might sometimes be better (depending on dataset and attack budget) for the adversary to try to make the most of network’s nonlinearity, spending the attack budget in one go trying to flip a larger number of switches in order to try to maximize the impact of the second term in (6).

### C. Characterizing the High SNR Regime

We now investigate the conditions that guarantee high SNR at neuron $i$, i.e. $s_i = s$, where $s_i$ denotes the switch when the adversary is present.

We observe that

$$s_i = \begin{cases} 1 - s_i, & w_i^T x - b_i \in \left[ \min (-w_i^T e, 0), \max (-w_i^T e, 0) \right] \\ s_i, & w_i^T x - b_i \notin \left[ \min (-w_i^T e, 0), \max (-w_i^T e, 0) \right] \end{cases}$$

This implies the following sufficient condition for high SNR at neuron $i$: $|w_i^T x - b_i| > |w_i^T e|$.  

**Assumptions.** To establish our theoretical result, we make a few mild technical assumptions:

1. The data is normalized in $\ell_2$-norm and bounded: $\|x\|_2 = 1$ and $\|x\|_\infty = o(1)$.
2. The $\ell_\infty$ budget $\delta \leq \|b_i\|/\|w_i\|_1 - C \quad \forall i = 1, \ldots, M$ and for some $C = \Theta(1) > 0$. Note that this assumption is justified in an iterative/optimization-based attack, where the adversary gradually spends the budget over many iterations.
3. The number of neurons $M = o(1)$ as $N$ gets large.
4. For each neuron $i = 1, \ldots, M$, we model the $\{w_i[k], k = 1, \ldots, N\}$ as i.i.d. with zero mean $\mathbb{E}[w_i[k]] = 0$. We assume that $\mathbb{E}[w_i[k]^2] = \sigma_i^2 = \Theta(1)$.

**Theorem 3.** With high probability, the high SNR condition ($s = s$) holds for $1 - o(1)$ fraction of neurons, i.e.

$$\lim_{N \to \infty} \Pr\left( \left| \frac{S}{M} - 1 \right| = o(1) \right) = 1,$$

where $S = \{i : |w_i^T x - b_i| > |w_i^T e|\}$.

**Proof.** We first state the following lemma:

**Lemma 4.** $w_i^T x \sim \mathcal{N}(0, \sigma_i^2)$ in distribution.

**Proof.** We show that we can apply Lindeberg’s version of the CLT, noting that $w_i^T x = \sum_{j=1}^N U_j$ is the sum of independent random variables, where $U_j = x_j w_i[j]$ with $\mathbb{E}[U_j] = 0$, $\text{var}(U_j) = \sigma_i^2 x_j^2$ and $\sum_{j=1}^N \sigma_i^2 x_j^2 = \sigma_i^2$.

Now given a constant $c_1 = \Theta(1) > 0$, we investigate the following quantity in order to check the Lindeberg condition:

$$L(c_1, N) = \frac{1}{\sigma_i^2} \sum_{j=1}^N \mathbb{E}[U_j^2 I_{\{|U_j| > c_1 \sigma_i\}}].$$

From the assumptions on $w_i$ and $x$, we observe that

$$\mathbb{E}\left[ x_j^2 w_i^2[j] I_{\{|U_j| > \sigma_i\}} \right] \leq c_2^2(1) \Theta(1) \Pr(|U_j| > c_1 \sigma_i)$$

$$= c_2^2(1) \Theta(1) \Pr\left(|w_i[j]| > c_1 \sigma_i/\Theta(1)\right).$$

The $\ell_\infty$ assumption on $w_i$ also implies that $\forall c_1 > 0, \exists N_0$ s.t. $|w_i[j]| < c_1 \sigma_i/\Theta(1), \forall j \in \{1, \ldots, N\}$, $N > N_0$. Hence we obtain that $\lim_{N \to \infty} L(\delta, N) = 0$, which verifies the Lindeberg condition.

Noting that $w_i^T x - b_i \sim \mathcal{N}(-b_i, \sigma_i^2)$, we can now write

$$\Pr(|w_i^T x - b_i| > |w_i^T e|) \geq \Pr(|w_i^T x - b_i| > \delta \|w_i\|_1)$$

$$= \Pr(|w_i^T x - b_i| > \delta \|w_i\|_1) + \Pr(|w_i^T x - b_i| < -\delta \|w_i\|_1)$$

$$\geq Q\left( \frac{\delta \|w_i\|_1 + b_i}{\sigma_i} \right) + Q\left( \frac{\delta \|w_i\|_1 - b_i}{\sigma_i} \right)$$

$$= Q\left( \Theta(1) \left( \delta - \frac{|b_i|}{\|w_i\|_1} \right) \right) \to 1 \quad \text{as} \quad N \to \infty,$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt$ and $\delta < \frac{|b_i|}{\|w_i\|_1}$ by Assumption 2. The theorem follows by using a union bound over $i = 1, \ldots, M$.

**D. Attacks**

We assume that the adversary knows the true label, a reasonable (mildly pessimistic) assumption given the high accuracy of modern neural networks. We consider attacks that focus on maximizing the first term in (6), using a high SNR approximation to the distortion:

$$\Delta = y(\hat{x}) - y(x) = w_{eq}^T P_K(e, x) - e^T P_K(w_{eq}, x),$$

Here $w_{eq} \approx w_{eq}(x) = \sum_{i=1}^M s_i w_i[i] w_i$ if we are applying a small perturbation to the input data. However, for iterative attacks with multiple small perturbations, $w_{eq}$ would evolve across iterations.

We can now define attacks in analogy with those for linear classifiers. The adversary can use an “effective input” $x_1$ to compute the locally linear model $w_{eq} = w_{eq}(x_1)$. For example, the adversary may choose $x_1 = x$ if making a small perturbation, or may iterate computation of its perturbation using $x_1 = x + e$. The adversary can also use a possibly different “effective input” $x_2$ to estimate the set of basis coefficients retained by the sparse front ends. Armed with this notation, we can define two attacks:

- **Semi-white box:** $A_{SW}(x_1, \epsilon) = \epsilon \text{sgn}(w_{eq}(x_1))$.
- **White box:** $A_{W}(x_1, x_2, \epsilon) = \epsilon \text{sgn}(P_K(w_{eq}(x_1), x_2))$.

We make no claims on the optimality of these attacks. They are simply sensible strategies based on the locally linear model.
and as we show in the next section, they are more powerful than existing FGSM attacks for multiclass classification.

For simplicity, we set $x_1 = x_2$ for the white box attack, and simplify notation by denoting it by $A_W(x_1, \epsilon)$. A (suboptimal) default choice is to set $x_1 = x_2 = x$, relying on a high SNR approximation for both the network switches and for the sparsifying front end. However, we can also refine these choices iteratively, as follows.

**Iterative versions:** We choose a particularly simple approach, in which we use a small attack budget $\delta$ to change $w_{eq}$ by small amounts and update the “direction” of the attack, maintaining the overall $\ell_\infty$ constraint at each stage:

$$
eq_{k+1} = e_{k} + A(x + e_{k}, \delta)$$

$$e_{k+1} = \text{clip}_\epsilon(e_{k+1}),$$

where $\text{clip}_\epsilon(e) \triangleq \max(\min(e, \epsilon), -\epsilon)$. We believe there is room for improvement in how we iterate, but this particular choice suffices to illustrate the power of locally linear modeling.

**Remark.** The Fast Gradient Sign Method (FGSM) attack puts its attack budget along the gradient of the cost function $J(\cdot)$ used to train the network. For binary classification and the cross-entropy cost function, we can show that it is equivalent to the semi-white box attack with $x_1 = x$. Specifically, we can show that

$$e_{\text{FGSM}} = \epsilon \text{sgn}(\nabla_x J(x, l)) = A_{SW}(x, \epsilon),$$

where $l$ is the true label, by verifying that the gradient is proportional to $w_{eq}(x)$. For a larger number of classes, however, insights from our locally linear modeling can be used to devise more powerful attacks than FGSM.

**E. Multiclass Classification**

In this subsection, we consider a multilayer (deep) network with $L$ classes. Each of the outputs of the network can be modeled using the analysis in the previous section as follows:

$$y_i = w_{eq}^{(i)} T x - b_{eq}^{(i)}, \quad i = 1, \ldots, L,$$

where $y = [y_1, y_2, \ldots, y_L]^T$, $p_i = S_i(y)$, and the softmax function $S_i(y) = e^{y_i} / \left(\sum_{j=1}^{L} e^{y_j}\right)$. Assume that $x$ belongs to class $t$ (with label $t$ known to the adversary).

**Locally linear attack:** The adversary can sidestep the nonlinearity of the softmax layer, since its goal is simply to make $y_i > y_t$ for some $i \neq t$. Thus, the adversary can consider $L-1$ binary classification problems, and solve for perturbations aiming to maximize $y_i - y_t$ for each $i \neq t$. We now apply the semi-white and white box attacks, and their iterative versions, to each pair, with $w_{eq}^{(i)} = w_{eq}^{(i)} - w_{eq}^{(i)}$ being the equivalent locally linear model from the input to $y_i - y_t$. After computing the distortions for each pair, the adversary applies its attack budget to the worst-case pair for which the distortion is the largest:

$$\max_{i : \epsilon} \quad y_i(x + \epsilon) - y_t(x + \epsilon), \quad \text{s.t.} \quad \|\epsilon\|_\infty \leq \epsilon.$$

**FGSM:** Unfortunately, the FGSM attack does not have a clean interpretation in the multiclass setting. Taking the gradient of the cross-entropy between one-hot encoded vector of the true label $l$ ($l[k] = \delta_{tk}$) and the final output of the model $p = [p_1, p_2, \ldots, p_L]$, with $J(l, p) = -\sum_{i=1}^{L} l_i \log(p_i)$, we obtain

$$e_{\text{FGSM}} = \epsilon \text{sgn}(\sum_{k=1}^{L} \sum_{k \neq i}^{L} w_{eq}^{(k)} p_k).$$

This does not take the most direct approach to corrupting the desired label, unlike our locally linear attack, and is expected to perform worse.

**VI. EXPERIMENTAL RESULTS**

In this section we demonstrate the effectiveness of sparsifying front ends on inference tasks on the MNIST database of handwritten digits [4]. Code is available at https://github.com/soorya19/sparsity-based-defenses.

**A. Linear Classifiers**

**Setup:** Here we train a linear SVM $g(x) = w^T x + b$ to classify digit pairs $d_1$ and $d_2$ from the MNIST dataset. The “direction” of the attack is opposite that of the correct class: if the SVM predicts class $d_1$ when $g(x) < 0$ and $d_2$ when $g(x) > 0$, the perturbation is of the form $\tilde{x} = x + \epsilon \text{sgn}(w)$ for images of class $d_1$, and $\tilde{x} = x - \epsilon \text{sgn}(w)$ for class $d_2$. We assume that the adversary has access to the true labels. For

|                | No defense | Sparsifying front end |
|----------------|------------|-----------------------|
| Semi-white box attack | 0.25       | 98.37                 |
| White box attack       | 0.25       | 95.37                 |
When no defense is present, an attack white box attacks that do better by refining the estimate of the various sparsity levels) before evaluating performance. Proposition 1 is no longer satisfied, hence the white box attack is attacking the “wrong subspace”. It is easy to devise iterative attacks in the white box setting: (a) the locally linear attack, (b) its iterative version, (c) FGSM [2], (d) iterative FGSM [44], (e) projected gradient descent (PGD) [45], and (f) momentum iterative FGSM [46] (winner of the NIPS 2017 competition on adversarial attacks and defenses [47]). For PGD, we use multiple random restarts and calculate accuracy over the most successful restart(s) for each image. We evaluate three versions of the attacks: one that uses the backward pass differential approximation (BPDA) technique of [28] to approximate the gradient of the front end as \( \mathbf{1} \), a second version where the defense uses \( \rho = 2\% \) and attack budget \( \epsilon \).

Results: We consider the case of 3 versus 7 classification. When no defense is present, an attack \( x' = x + \epsilon \mathbf{w} \) with \( \epsilon = 0.1 \) renders the classifier useless, with accuracy dropping from 98.64% to 0.25% as depicted in Fig. 5(a). Fig. 5(b) illustrates the sparsifying front end at work, showing an image, its perturbed version and the effect of sparsification. Insertion of the front end greatly improves resilience to adversarial attacks: as shown in Table I, accuracy is restored to near-baseline levels at low sparsity levels. As discussed in Section III-C, the choice of sparsity level \( \rho \) must optimize the tradeoff between attack attenuation and unwanted signal distortion. We find that a value of \( \rho \) between 1–5% works well for all digit pairs, with \( \rho = 2\% \) being the optimal choice for the 3 vs. 7 scenario.

Fig. 6 reports on accuracy as a function of sparsity level \( \rho \) and attack budget \( \epsilon \). At the small values of \( \rho \) and \( \epsilon \) that we are interested in, the white box attack causes more damage than the semi-white box attack. At larger \( \rho \) and \( \epsilon \), it performs poorer than the semi-white box attack: the high SNR condition in Proposition 1 is no longer satisfied, hence the white box attack is attacking the “wrong subspace”. It is easy to devise iterative white box attacks that do better by refining the estimate of the \( K \)-dimensional subspace in the following manner:

\[
e^{[i+1]} = \epsilon \text{sgn}(P_K(\mathbf{w}, x + e^{[i]})),
\]

\(2\)The reported values of \( \epsilon \) correspond to images normalized to \( [0, 1] \).

Fig. 5: Sample images depicting the interplay between attack and defense: tiny adversarial attacks can fool a classifier, but sparsity-based preprocessing can restore accuracy by projecting the attack down to a lower dimensional subspace.

Fig. 6: Binary classification accuracies for the linear SVM as a function of the sparsity level \( \rho \) and attack budget \( \epsilon \). with a possible initialization of \( e^{[0]} = e_{SW} \). Essentially, we refine our estimate of \( S_K(x + e) \) at each iteration by calculating the projection of \( \mathbf{w} \) onto the top \( K \) basis vectors of \( x + e \) (rather than just \( x \)). We can observe from the figures that the attack with iterated projections performs better in the low SNR region. However, this scenario is not of practical interest, since front ends with large \( \rho \) do not provide enough attenuation of the adversarial perturbation, and perturbations with large \( \epsilon \) are no longer visually imperceptible.

B. Neural Networks

For neural networks, we perturb images with the following attacks in the white box setting: (a) the locally linear attack, (b) its iterative version, (c) FGSM [2], (d) iterative FGSM [44], (e) projected gradient descent (PGD) [45], and (f) momentum iterative FGSM [46] (winner of the NIPS 2017 competition on adversarial attacks and defenses [47]).
TABLE II: Multiclass classification accuracies for 4-layer CNN, with $\epsilon = 0.2$ for attacks and $\rho = 3.5\%$ for defense.

|                      | No defense | Sparsifying front end |
|----------------------|------------|-----------------------|
| Locally linear attack| 28.43      | 78.27                 |
| FGSM                 | 42.01      | 85.35                 |
| Iterative locally linear attack | 7.36      | 74.38                 |
| Iterative FGSM       | 6.34       | 74.97                 |
| Momentum iterative FGSM | 6.99      | 73.55                 |
| PGD (100 random restarts) | 5.12      | 61.04                 |

gradient is calculated as the projection onto the top $K$ basis vectors of the input, and a third version where we iteratively refine the projection as described in the previous section. We report accuracies for the version that causes the most damage.

Setup: For multiclass MNIST classification, we use a 4-layer CNN consisting of two convolutional layers (containing 20 and 40 feature maps, each with 5x5 filters) and two fully connected layers (containing 1000 neurons each, with dropout) [48]. We use a fully connected network with 1 hidden layer (containing 10 neurons) for binary classification of digits 3 and 7. For the sparsifying front end, we use the Coiflet-1 wavelet for multiclass and Daubechies-5 for binary classification, and retrain the networks with sparsified images.

Results: Table II reports on multiclass classification accuracies for the 4-layer CNN where the attacks use an $\ell_\infty$ budget of $\epsilon = 0.2$. Iterative attacks are run for 1000 steps with a per-iteration budget of $\delta = 0.01$, except for PGD and the iterative locally linear attack which use 100 steps of $\delta = 0.05$. Without any defense, a strong adversary can significantly degrade performance, reducing accuracy from 99.31% to 5.12%. In contrast, when a sparsifying front end is present (with sparsity level $\rho = 3.5\%$), the network robustness measurably improves, increasing accuracy to 61.04% in the worst-case scenario. We note that the locally linear attack is stronger than FGSM, and the iterative locally linear attack is competitive with single runs of the other iterative attacks.

Figure 7 reports on binary classification accuracies for the 2-layer NN as a function of attack budget, with the front end improving robustness across a range of $\epsilon$. As shown in Section V-D, FGSM is identical to the locally linear attack for binary classification, so we do not label it in the figure. We note that images are normalized to the range $[0, 1]$, so by the end of the chosen range of $\epsilon$, perturbations are no longer visually imperceptible.

VII. CONCLUSIONS

Our results make the case that sparsity is a crucial tool for limiting the impact of adversarial attacks on neural networks. We have also shown that a “locally linear” model for the network provides key design insights, both for devising and combating adversarial perturbations. Our proposed sparsifying front end makes an implicit assumption on the generative model for the data that we believe must hold quite generally for high-dimensional data, in order to evade the curse of dimensionality. We believe that these results are the first steps towards establishing a comprehensive design framework, firmly grounded in theoretical fundamentals, for robust neural networks, that is complementary to alternative defenses based on modifying the manner in which networks are trained.

There are many directions for future research. Developing sparse generative models for various datasets is required for design of sparsifying front ends. For the simple datasets considered here, the orthogonal wavelet basis considered here was a good first guess, but it could be improved upon by learning from data, and by use of overcomplete bases. Our placeholder scheme of picking the largest $K$ coefficients could be improved by devising computationally efficient and data-adaptive techniques for enforcing sparsity. Finally, while we have restricted attention to simple datasets and small networks in this paper in order to develop insight, the design of larger (deeper) networks for more complex datasets is our ultimate objective.

ACKNOWLEDGMENT

This work was supported in part by the National Science Foundation under grants CNS-1518812 and CCF-1755808, by
Systems on Nanoscale Information fabriCs (SONIC), one of the six SRC STARnet Centers, sponsored by MARCO and DARPA, and by the UC Office of the President under grant No. LFR-18-548175.

REFERENCES

[1] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, “Intriguing properties of neural networks,” in International Conference on Learning Representations, 2014.

[2] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” in International Conference on Learning Representations, 2015.

[3] A. Fawzi, S.-M. Moosavi-Dezfooli, and P. Frossard, “The robustness of deep networks: A geometrical perspective,” IEEE Signal Processing Magazine, vol. 34, no. 6, pp. 50–62, 2017.

[4] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

[5] S. Mallat and Z. Zhang, “Matching pursuits with time-frequency dictionaries,” IEEE Transactions on Signal Processing, vol. 41, no. 12, pp. 3397–3415, 1993.

[6] T. Blumensath and M. E. Davies, “Gradient pursuits,” IEEE Transactions on Signal Processing, vol. 56, no. 6, pp. 2370–2382, 2008.

[7] A. M. Bruckstein, D. L. Donoho, and M. Elad, “From sparse solutions of systems of equations to sparse modeling of signals and images,” SIAM Review, vol. 51, no. 1, pp. 34–81, 2009.

[8] D. L. Donoho, I. M. Johnstone et al., “Ideal denoising in an orthonormal basis chosen from a library of bases,” Comptes rendus de l’Académie des sciences. Série I, Mathématique, vol. 319, no. 12, pp. 1317–1322, 1994.

[9] M. Aharon, M. Elad, and A. Bruckstein, “k-SVD: An algorithm for designing overcomplete dictionaries for sparse representation,” IEEE Transactions on Signal Processing, vol. 54, no. 11, pp. 4311–4322, 2006.

[10] I. F. Gorodnitsky and B. D. Rao, “Sparse signal reconstruction from limited data using FOCUSS: A re-weighted minimum norm algorithm,” IEEE Transactions on Signal Processing, vol. 45, no. 3, pp. 600–616, 1997.

[11] S. J. Wright, R. D. Nowak, and M. A. Figueiredo, “Sparse reconstruction by separable approximation,” IEEE Transactions on Signal Processing, vol. 57, no. 7, pp. 2479–2493, 2009.

[12] J. Yang, J. Wright, T. S. Huang, and Y. Ma, “Image super-resolution via sparse representation,” IEEE Transactions on Image Processing, vol. 19, no. 11, pp. 2861–2873, 2010.

[13] M. Elad, J.-L. Starck, P. Querre, and D. L. Donoho, “Simultaneous cartoon and texture image inpainting using morphological component analysis (MCA),” Applied and Computational Harmonic Analysis, vol. 19, no. 3, pp. 340–358, 2005.

[14] M. Zibulevsky and B. A. Pearlmutter, “Blind source separation by sparse decomposition in a signal dictionary,” Neural Computation, vol. 13, no. 4, pp. 863–882, 2001.

[15] D. Malioutov, M. Cetin, and A. S. Willsky, “A sparse signal reconstruction perspective for source localization with sensor arrays,” IEEE Transactions on Signal Processing, vol. 53, no. 8, pp. 3010–3022, 2005.

[16] S. Mallat, A Wavelet Tour of Signal Processing. Elsevier, 1999.

[17] K. Skretting and K. Engan, “Recursive least squares dictionary learning algorithm,” IEEE Transactions on Signal Processing, vol. 58, no. 4, pp. 2121–2130, 2010.

[18] R. Rubinstein, T. Peleg, and M. Elad, “Analysis K-SVD: A dictionary-learning algorithm for the analysis sparse model,” IEEE Transactions on Signal Processing, vol. 61, no. 3, pp. 661–677, 2013.

[19] A. Makhzani and B. Frey, “k-Sparse autoencoders,” in International Conference on Learning Representations, 2014.

[20] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, “DeepFool: A simple and accurate method to fool deep neural networks,” in IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 2574–2582.

[21] A. Fawzi, S.-M. Moosavi-Dezfooli, P. Frossard, and S. Soatto, “Classification regions of deep neural networks,” arXiv preprint arXiv:1705.09552, 2017.

[22] B. Poole, S. Lahiri, M. Raghu, J. Sohl-Dickstein, and S. Ganguli, “Exponential expressivity in deep neural networks through transient chaos,” in Advances in Neural Information Processing Systems, 2016, pp. 3360–3368.

[23] C. Guo, M. Rana, M. Cisse, and L. van der Maaten, “Countering adversarial images using input transformations,” in International Conference on Learning Representations, 2018.

[24] N. Das, M. Shanbhogue, S.-T. Chen, F. Hohman, L. Chen, M. E. Kounavis, and D. H. Chau, “Keeping the bad guys out: Protecting and vaccinating deep learning with JPEG compression,” arXiv preprint arXiv:1705.02900, 2017.

[25] A. N. Bhagoji, D. Cullina, C. Sitawarin, and P. Mittal, “Enhancing robustness of machine learning systems via data transformations,” in 52nd Annual Conference on Information Sciences and Systems (CISS), 2018, pp. 1–5.

[26] A. Ilyas, A. Jalal, E. Asteri, C. Daskalakis, and A. G. Dimakis, “The robust manifold defense: Adversarial training using generative models,” arXiv preprint arXiv:1712.09196, 2017.

[27] P. Samangouei, M. Kabkab, and R. Chellappa, “Defense-GAN: Protecting classifiers against adversarial attacks using generative models,” in International Conference on Learning Representations, 2018.

[28] A. Athalye, N. Carlini, and D. Wagner, “Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples,” in International Conference on Machine Learning, 2018, pp. 274–283.

[29] A. Raghunathan, J. Steinhardt, and P. Liang, “Certified defenses against adversarial examples,” in International Conference on Learning Representations, 2018.

[30] ——, “Semidefinite relaxations for certifying robustness to adversarial examples,” in Advances in Neural Information Processing Systems, 2018, pp. 10 900–10 910.

[31] E. Wong and Z. Kolter, “Provable defenses against adversarial attacks through natural perturbations,” in International Conference on Machine Learning, 2017.
sarial examples via the convex outer adversarial polytope,” in *International Conference on Machine Learning*, 2018, pp. 5283–5292.

[32] E. Wong, F. Schmidt, J. H. Metzen, and J. Z. Kolter, “Scaling provable adversarial defenses,” in *Advances in Neural Information Processing Systems*, 2018, pp. 8410–8419.

[33] A. Sinha, H. Namkoong, and J. Duchi, “Certifying some distributional robustness with principled adversarial training,” in *International Conference on Learning Representations*, 2018.

[34] M. Mirman, T. Gehr, and M. Vechev, “Differentiable abstract interpretation for provably robust neural networks,” in *International Conference on Machine Learning*, 2018, pp. 3575–3583.

[35] M. Hein and M. Andriushchenko, “Formal guarantees on the robustness of a classifier against adversarial manipulation,” in *Advances in Neural Information Processing Systems*, 2017, pp. 2266–2276.

[36] M. Cisse, P. Bojanowski, E. Grave, Y. Dauphin, and N. Usunier, “Parseval networks: Improving robustness to adversarial examples,” in *International Conference on Machine Learning*, 2017, pp. 854–863.

[37] Z. Marzi, S. Gopalakrishnan, U. Madhow, and R. Pedarsani, “Sparsity-based defense against adversarial attacks on linear classifiers,” in *IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 31–35.

[38] M. Bafna, J. Murtagh, and N. Vyas, “Thwarting adversarial examples: An $L_0$-robust sparse fourier transform,” in *Advances in Neural Information Processing Systems*, 2018, pp. 10 096–10 106.

[39] G. Katz, C. Barrett, D. L. Dill, K. Julian, and M. J. Kochenderfer, “Reluplex: An efficient SMT solver for verifying deep neural networks,” in *International Conference on Computer Aided Verification*. Springer, 2017, pp. 97–117.

[40] R. Ehlers, “Formal verification of piece-wise linear feedforward neural networks,” in *International Symposium on Automated Technology for Verification and Analysis*. Springer, 2017, pp. 269–286.

[41] C.-H. Cheng, G. Nührenberg, and H. Ruess, “Maximum resilience of artificial neural networks,” in *International Symposium on Automated Technology for Verification and Analysis*. Springer, 2017, pp. 251–268.

[42] S. Dutta, S. Jha, S. Sankaranarayanan, and A. Tiwari, “Output range analysis for deep feedforward neural networks,” in *NASA Formal Methods Symposium*. Springer, 2018, pp. 121–138.

[43] I. Daubechies, *Ten Lectures on Wavelets*. Siam, 1992, vol. 61.

[44] A. Kurakin, I. Goodfellow, and S. Bengio, “Adversarial machine learning at scale,” in *International Conference on Learning Representations*, 2017.

[45] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vlud, “Towards deep learning models resistant to adversarial attacks,” in *International Conference on Learning Representations*, 2018.

[46] Y. Dong, F. Liao, T. Pang, H. Su, J. Zhu, X. Hu, and J. Li, “Boosting adversarial attacks with momentum,” in *IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 9185–9193.

[47] A. Kurakin, I. Goodfellow, S. Bengio, Y. Dong, F. Liao, M. Liang, T. Pang, J. Zhu, X. Hu, C. Xie et al., “Adversarial attacks and defences competition,” in *The NIPS’17 Competition: Building Intelligent Systems*. Springer, 2018, pp. 195–231.

[48] M. A. Nielsen, *Neural Networks and Deep Learning*. Determination Press, 2015.

[49] N. Carlini and D. Wagner, “Towards evaluating the robustness of neural networks,” in *IEEE Symposium on Security and Privacy*, 2017, pp. 39–57.
APPENDIX

ADDITIONAL EMPIRICAL RESULTS

A. SNR of sparsifying front end

Figure 8 reports on the overlap in the $K$-dimensional supports of $x$ and $x + e$ for attacks on linear SVM and CNN. We can observe that the SNR condition in Section VI-C is approximately satisfied for most of the images.

Figure 11 depicts perturbed images with various support overlaps for the SVM, showing an example in each scenario where the defense succeeds and another where the defense fails. For the fraction of images with low SNR, the adversary can cause significant image distortion by shifting the support of the $K$ selected basis functions, but however such distortions do not necessarily lead to misclassification. As we can observe from the histograms, the distribution of SNRs for images where the defense fails is almost identical to those for which it succeeds.

B. SNR of ReLU units

Figure 9 reports on the percentage of ReLU units that flip in one iteration of the iterative locally linear attack with $\delta = 0.01$. When the defense is present, the high SNR condition in Section V-B is approximately satisfied. Figure 10 shows the evolution of the SNR condition with attack step for a 1000-step iterative FGSM attack. We can observe that on average, the percentage of ReLUs that flip in each iteration stays relatively small over attack iterations.

However, as the next section shows, it could be better for the adversary to try to affect the most of the network’s nonlinearity, for example by using iterative attacks with random initializations (PGD), so as to cause a large number of switches to flip to maximize the impact of the second term in Eq. (6).

C. More details on attack performance

Table III reports on attack performance for the 3 versions described in Section VI-B, one that uses the backward pass differential approximation (BPDA) technique of [28] to approximate the gradient of the front end as 1, a second version where the gradient is calculated as the projection onto the top $K$ basis vectors of the input, and a third version where we iteratively refine the projection. For iterative attacks, we refine the projection for 20 steps within each attack step. For PGD, we use 100 random restarts and report accuracy over the most successful restart(s) for each image. We report on the effect of changing the per-iteration budget and number of steps for iterative FGSM in Table IV.

D. Effect of sparsification on performance without attacks

Sparsification causes a slight performance hit in the accuracy without attacks: for the 4-layer CNN, accuracy reduces from 99.31% to 98.97%. For the 2-layer NN, we report implicitly on this effect in Figure 7 (the $\epsilon = 0$ points): the accuracy goes from 99.33% to 99.28%. We note that sparsity has also been suggested purely as a means of improving classification performance (e.g., see Makhzani and Frey [19]) and hence believe that with additional design effort, the performance penalty will be minimal.

| TABLE III: Multiclass classification accuracies for 4-layer CNN on MNIST, with $\epsilon = 0.2$ for attacks and $\rho = 3.5\%$ for defense. Iterative attacks were run for 1000 steps of $\delta = 0.01$, except for the attacks marked * which use 100 steps of $\delta = 0.05$. Projections were iterated for 20 steps within each attack step. |
|---------------------------------|----------------------|-----------------|-----------------|
| Method                          | BPDA of 1            | Projections     | Iterated projections |
| Locally linear attack           | 82.02                | 86.08           | 78.27            |
| FGSM                            | 85.35                | 88.18           | 85.84            |
| Iter. locally linear attack     | 76.00                | 77.27           | 74.38*           |
| Iter. FGSM                      | 74.97                | 79.88           | 75.33            |
| Momentum iter. FGSM             | 74.79                | 73.55           | —                |
| PGD (100 restarts)             | 64.62*               | 65.48*          | 61.04*           |

| TABLE IV: Iterative FGSM accuracies ($\epsilon = 0.2$) as a function of the per-iteration budget $\delta$ and number of steps used, for the 4-layer CNN with front end ($\rho = 3.5\%$), using BPDA of 1. |
|-------------------|-------------------|-------------------|
| $\delta = 0.01$   | $\delta = 0.05$   | $\delta = 0.1$   |
| 20 steps          | 80.84             | 75.52             | 75.32             |
| 100 steps         | 75.13             | 75.17             | 75.02             |
| 1000 steps        | 74.97             | 75.10             | 75.02             |

E. Experiments on the Carlini-Wagner $\ell_2$ attack

Since the Carlini-Wagner $\ell_2$ attack does not have a fixed bound on the distance between adversarial and true images [49], we report on histograms of distances in Figure 12 (for the 4-layer CNN). We set the confidence level of the attack to 0, which corresponds to the smallest possible $\ell_2$ distance in the C&W attack formulation. The final classification accuracy is 0.92%, but 94.18% of the perturbed images lie outside the $\ell_\infty$ budget of interest ($\epsilon = 0.2$). The attack is successful in terms of causing misclassification, but since it is an $\ell_2$ attack, it fails to produce perturbations conforming to the $\ell_\infty$ budget. We generate the attack using the CleverHans library (v2.1.0), with default values of attack hyperparameters (listed below) and a backward pass differential approximation (BPDA) [28] of 1 for the gradient of the front end.

| hyperparameters |
|------------------|
| learning_rate = 5e-3, binary_search_steps = 5, max_iterations = 1000, initial_const = 1e-2. |
(a) Support overlap for white box attack on linear SVM with $\epsilon = 0.1$ and $K = 15$.

(b) Support overlap for PGD attack (with 100 random restarts) on CNN with $\epsilon = 0.2$ and $K = 27$.

Fig. 8: Histograms of support overlap, i.e. $|S_K(x) \cap S_K(x + e)|$ for attacks on linear SVM and CNN. Plots are normalized to be probability densities, i.e. the area under each histogram sums to 1.
Fig. 9: Histograms of the percentage of ReLU units that flip in a single step of the iterative locally linear attack with \( \delta = 0.01 \), for the 4-layer CNN on MNIST. Plots are normalized to be probability densities.

(a) No defense.

(b) With sparsifying front end (\( \rho = 3.5\% \)).

Fig. 10: Plots showing the mean percentage of ReLU units that flip in each attack step, for a 1000-step iterative FGSM attack with \( \delta = 0.01 \) and \( \epsilon = 0.2 \) on the 4-layer CNN with defense (\( \rho = 3.5\% \)). Error bars represent 1 standard deviation from the mean.
Defense success. Support overlap $|S_K(x) \cap S_K(x + e)| = 15$, $K = 15$.

(a) Defense success, high support overlap.

Defense success. Support overlap $|S_K(x) \cap S_K(x + e)| = 9$, $K = 15$.

(b) Defense success, low support overlap.

Defense failure. Support overlap $|S_K(x) \cap S_K(x + e)| = 15$, $K = 15$.

(c) Defense failure, high support overlap.

Defense failure. Support overlap $|S_K(x) \cap S_K(x + e)| = 9$, $K = 15$.

(d) Defense failure, low support overlap.

Fig. 11: Sample images with low and high support overlap, for white box attack on the linear SVM with $\epsilon = 0.1$ and $\rho = 2\%$. The first row of each subfigure shows the original image, the perturbation and the attacked image, while the second row shows the effect of sparsification. Here $P_K(x + e)$ denotes the projection of $x + e$ onto its own $K$-dim. support i.e. $S_K(x + e)$.

Fig. 12: Histograms of adversarial examples generated by the C&W $\ell_2$ attack on the 4-layer CNN.