Adversarial Dropout for Supervised and Semi-Supervised Learning

Sungrae Park and Jun-Keon Park and Su-Jin Shin and Il-Chul Moon
Department of Industrial and System Engineering
KAIST
Deajeon, South Korea
{sungraepark and alex3012 and sujin.shin and icmoon}@kaist.ac.kr

Abstract
Recently, training with adversarial examples, which are generated by adding a small but worst-case perturbation on input examples, has improved the generalization performance of neural networks. In contrast to the biased individual inputs to enhance the generality, this paper introduces adversarial dropout, which is a minimal set of dropouts that maximize the divergence between 1) the training supervision and 2) the outputs from the network with the dropouts. The identified adversarial dropouts are used to automatically reconfigure the neural network in the training process, and we demonstrated that the simultaneous training on the original and the reconfigured network improves the generalization performance of supervised and semi-supervised learning tasks on MNIST, SVHN, and CIFAR-10. We analyzed the trained model to find the performance improvement reasons. We found that adversarial dropout increases the sparsity of neural networks more than the standard dropout. Finally, we also proved that adversarial dropout is a regularization term with a rank-valued hyper parameter that is different from a continuous-valued parameter to specify the strength of the regularization.

Introduction
Deep neural networks (DNNs) have demonstrated the significant improvement on benchmark performances in a wide range of applications. As neural networks become deeper, the model complexity also increases quickly, and this complexity leads DNNs to potentially overfit a training data set. Several techniques (Hinton et al. 2012; Poole, Sohl-Dickstein, and Ganguli 2014; Bishop 1995b; Lasserre, Bishop, and Minka 2006) have emerged over the past years to address this challenge, and dropout has become one of dominant methods due to its simplicity and effectiveness (Hinton et al. 2012; Srivastava et al. 2014).

Dropout randomly disconnects neural units during training as a method to prevent the feature co-adaptation (Baldi and Sadowski 2013; Wager, Wang, and Liang 2013; Wang and Manning 2013; Li, Gong, and Yang 2016). The earlier work by Hinton et al. (2012) and Srivastava et al. (2014) interpreted dropout as an extreme form of model combinations, a.k.a. a model ensemble, by sharing extensive parameters on neural networks. They proposed learning the model combination through minimizing an expected loss of models perturbed by dropout. They also pointed out that the output of dropout is the geometric mean of the outputs from the model ensemble with the shared parameters. Extending the weight sharing perspective, several studies (Baldi and Sadowski 2013; Chen et al. 2014; Jain et al. 2015) analyzed the ensemble effects from the dropout.

The recent work by Laine & Aila (2016) enhanced the ensemble effect of dropout by adding self-ensembling terms. The self-ensembling term is constructed by a divergence between two sampled neural networks from the dropout. By minimizing the divergence, the sampled networks learn from each other, and this practice is similar to the working mechanism of the ladder network (Rasmus et al. 2015), which builds a connection between an unsupervised and a supervised neural network. Our method also follows the principles of self-ensembling, but we apply the adversarial training concept to the sampling of neural network structures through dropout.

At the same time that the community has developed the dropout, adversarial training has become another focus of the community. Szegedy et al. (2013) showed that a certain neural network is vulnerable to a very small perturbation in the training data set if the noise direction is sensitive to the models' label assignment y given x, even when the perturbation is so small that human eyes cannot discern the difference. They empirically proved that robustly training models against adversarial perturbation is effective in reducing test errors. However, their method of identifying adversarial perturbations contains a computationally expensive inner loop. To compensate it, Goodfellow et al. (2014) suggested an approximation method, through the linearization of the loss function, that is free from the loop. Adversarial training can be conducted on supervised learning because the adversarial direction can be defined when true y labels are known. Miyato et al. (2015) proposed a virtual adversarial direction to apply the adversarial training in the semi-supervised learning that may not assume the true y value. Until now, the adversarial perturbation can be defined as a unit vector of additive noise imposed on the input or the embedding spaces (Szegedy et al. 2013; Goodfellow, Shlens, and Szegedy 2014; Miyato et al. 2015).

Our proposed method, adversarial dropout, can be viewed from the dropout and from the adversarial train-
Adversarial dropout can be interpreted as dropout masks whose direction is optimized adversarially to the model’s label assignment. However, it should be noted that adversarial dropout and traditional adversarial training with additive perturbation are different because adversarial dropout induces the sparse structure of neural network while the other does not make changes in the structure of the neural network, directly.

Figure 1 describes the proposed loss function construction of adversarial dropout compared to 1) the recent dropout model, which is Π model (Laine and Aila 2016) and 2) the adversarial training (Goodfellow, Shlens, and Szegedy 2014; Miyato et al. 2015). When we compare adversarial dropout to Π model, both divergence terms are similarly computed from two different dropped networks, but adversarial dropout uses an optimized dropped network to adapt the concept of adversarial training. When we compare adversarial dropout to the adversarial training, the divergence term of the adversarial training is computed from one network structure with two training examples: clean and adversarial examples. On the contrary, the divergence term of the adversarial dropout is defined with two network structures: a randomly dropped network and an adversarially dropped network.

Our experiments demonstrated that 1) adversarial dropout improves the performance on MNIST supervised learning compared to the dropout suggested by Π model, and 2) adversarial dropout showed the state-of-the-art performance on the semi-supervised learning task on SVHN and CIFAR-10 when we compare the most recent techniques of dropout and adversarial training. Following the performance comparison, we visualize the neural network structure from adversarial dropout to illustrate that the adversarial dropout enables a sparse structure compared to the neural network of standard dropout. Finally, we theoretically show the original characteristics of adversarial dropout that specifies the strength of the regularization effect by the rank-valued parameter while the adversarial training specifies the strength with the conventional continuous-valued scale.

Preliminaries

Before introducing adversarial dropout, we briefly introduce stochastic noise layers for deep neural networks. Afterwards, we review adversarial training and temporal ensembling, or Π model, because two methods are closely related to adversarial dropout.

Noise Layers

Corrupting training data with noises has been well-known to be a method to stabilize prediction (Bishop 1995a; Maaten et al. 2013; Wager, Wang, and Liang 2013). This section describes two types of noise injection techniques, such as additive Gaussian noise and dropout noise.

Let \( \mathbf{h}^{(l)} \) denote the \( l^{th} \) hidden variables in a neural network, and this layer can be replaced with a noisy version \( \tilde{\mathbf{h}}^{(l)} \). We can vary the noise types as the following.

- **Additive Gaussian noise:** \( \tilde{\mathbf{h}}^{(l)} = \mathbf{h}^{(l)} + \gamma \), where \( \gamma \sim \mathcal{N}(0, \sigma^2 \mathbf{I}_{d \times d}) \) with the parameter \( \sigma^2 \) to restrict the degree of noises.
- **Dropout noise:** \( \tilde{\mathbf{h}}^{(l)} = \mathbf{h}^{(l)} \odot \epsilon \), where \( \odot \) is the element-wise product of two vectors, and the elements of the noise vector are \( \epsilon_i \sim \text{Bernoulli}(1 - p) \) with the parameter \( p \).

To simply put, this function specifies that \( \epsilon_i = 0 \) with probability \( p \) and \( \epsilon_i = 1 \) with probability \( 1 - p \).

Both additive Gaussian noise and dropout noise are generalization techniques to increase the generality of the trained model, but they have different properties. The additive Gaussian noise increases the margin of decision boundaries while the dropout noise affects a model to be sparse (Srivastava et al. 2014). These noise layers can be easily included in a deep neural network. For example, there can be a dropout layer between two convolutional layers. Similarly, a layer of additive Gaussian noise can be placed on the input layer.

Self-Ensembling Model

The recently reported self-ensembling (SE) (Laine and Aila 2016), or Π model, construct a loss function that minimizes the divergence between two outputs from two sampled dropout neural networks with the same input stimulus. Their suggested regularization term can be interpreted as the following:

\[
\mathcal{L}_{SE}(x; \theta) := D[f_\theta(x, \epsilon^1), f_\theta(x, \epsilon^2)],
\]

where \( \epsilon^1 \) and \( \epsilon^2 \) are randomly sampled dropout noises in a neural network \( f_\theta \), whose parameters are \( \theta \). Also, \( D[y, y'] \) is a non-negative function that represents the distance between two output vectors: \( y \) and \( y' \). For example, \( D \) can be the cross entropy function, \( D[y, y'] = -\sum y_i \log y_i' \), where \( y \) and \( y' \) are the vectors whose \( i^{th} \) elements represent the probability of the \( i^{th} \) class. The divergence could be calculated between two outputs of two different structures, which turn this regularization to be semi-supervised. Π model is based on...
on the principle of \( \Gamma \) model, which is the ladder network by Rasmus et al. (2015). Our proposed method, adversarial dropout, can be seen as a special case of \( \Pi \) model when one dropout neural network is adversarially sampled.

Adversarial Training

Adversarial dropout follows the training mechanism of adversarial training, so we briefly introduce a generalized formulation of the adversarial training. The basic concept of adversarial training (AT) is an incorporation of adversarial examples on the training process. Additional loss function by including adversarial examples (Szegedy et al. 2013; Goodfellow, Shlens, and Szegedy 2014; Miyato et al. 2015) can be defined as a generalized form:

\[
L_{AT}(x, y; \theta, \delta) := D[g(x, y, \theta), f_\theta(x + \gamma^{adv})]
\]

where \( \gamma^\text{adv} := \arg\max_{\gamma : \|\gamma\|_\infty \leq \delta} D[g(x, y, \theta), f_\theta(x + \gamma)] \).

Here, \( \theta \) is a set of model parameters, \( \delta \) is a hyperparameter controlling the intensity of the adversarial perturbation \( \gamma^\text{adv} \). The function \( f_\theta(x) \) is an output distribution of a neural network to be learned. Adversarial training can be diversified by differentiating the definition of \( g(x, y, \theta) \), as the following.

- **Adversarial training (AT)** (Goodfellow, Shlens, and Szegedy 2014; Kurakin, Goodfellow, and Bengio 2016) defines \( g(x, y, \theta) \) as \( g(y) \) ignoring \( x \) and \( \theta \), so \( g(y) \) is an one-hot encoding vector of \( y \).

- **Virtual adversarial training (VAT)** (Miyato et al. 2015; Miyato, Dai, and Goodfellow 2016) defines \( g(x, y, \theta) \) as \( f_\hat{\theta}(x) \) where \( \hat{\theta} \) is the current estimated parameter. This training method does not use any information from \( y \) in the adversarial part of the loss function. This enables the adversarial part to be used as a regularization term for the semi-supervised learning.

Method

This section presents our adversarial dropout that combines the ideas of adversarial training and dropout. First, we formally define the adversarial dropout. Second, we propose a training algorithm to find the instantiations of adversarial dropout with a fast approximation method.

General Expression of Adversarial Dropout

Now, we propose the adversarial dropout (AdD), which could be an adversarial training method that determines the dropout condition to be sensitive on the model’s label assignment. We use \( f_\theta(x, \epsilon) \) as an output distribution of a neural network with a dropout mask. The below is the description of the additional loss function by incorporating adversarial dropout.

\[
L_{ADD}(x, y, \epsilon^s; \theta, \delta) := D[g(x, y, \theta), f_\theta(x, \epsilon^\text{adv})]
\]

where \( \epsilon^\text{adv} := \arg\max_{\epsilon : \|\epsilon\|_2 \leq \delta H} D[g(x, y, \theta), f_\theta(x, \epsilon)] \).

Here, \( D[\cdot, \cdot] \) indicates a divergence function; \( g(x, y, \theta) \) represents an adversarial target function that can be diversified by its definition; \( \epsilon^\text{adv} \) is an adversarial dropout mask under the function \( f_\theta \) when \( \theta \) is a set of model parameters; \( \epsilon^s \) is a sampled random dropout mask instance; \( \delta \) is a hyperparameter controlling the intensity of the noise; and \( H \) is the dropout layer dimension.

We introduce the boundary condition, \( \|\epsilon^s - \epsilon\|_2 \leq \delta H \), which indicates a restriction of the number of the difference between two dropout conditions. An adversarial dropout mask should be infinitesimally different from the random dropout mask. Without this constraint, the network with adversarial dropout may become a neural network layer without connections. By restricting the adversarial dropout with the random dropout, we prevent finding such irrational layer, which does not support the back propagation. We found that the Euclidean distance between two \( \epsilon \) vectors can be calculated by using the graph edit distance or the Jaccard distance. In the supplementary material, we proved that the graph edit distance and the Jaccard distance can be abstracted as Euclidean distances between two \( \epsilon \) vectors.

In the general form of adversarial training, the key point is the existence of the linear perturbation \( \gamma^\text{adv} \). We can interpret the input with the adversarial perturbation as this adversarial noise input \( x^{adv} = x + \gamma^\text{adv} \). From this perspective, the authors of adversarial training limited the adversarial direction only on the space of the additive Gaussian noise \( \gamma^0 \), where \( \gamma^0 \) is a sampled Gaussian noise on the input layer. In contrast, adversarial dropout can be considered as a noise space generated by masking hidden units, \( h^{adv} = h \odot \epsilon^{adv} \) where \( h \) is hidden units, and \( \epsilon^{adv} \) is an adversarially selected dropout condition. If we assume the adversarial training as the Gaussian additive perturbation on the input, the perturbation is linear in nature, but adversarial dropout could be non-linear perturbation if the adversarial dropout is imposed upon multiple layers.

Supervised Adversarial Dropout

**Supervised Adversarial dropout (SAdD)** defines \( g(x, y, \theta) \) as \( y \), so \( y \) is a one-hot vector of \( y \) as the typical neural network. The divergence term from Formula 3 can be converted as follows:

\[
L_{SAdD}(x, y, \epsilon^s; \theta) := D[g(y), f_\theta(x, \epsilon^\text{adv})]
\]

where \( \epsilon^\text{adv} := \arg\max_{\epsilon : \|\epsilon\|_2 \leq \delta H} D[g(y), f_\theta(x, \epsilon)] \).

In this case, the divergence term can be seen as the pure loss function for a supervised learning with a dropout regularization. However, \( \epsilon^{adv} \) is selected to maximize the divergence between the true information and the output from the dropout network, so \( \epsilon^{adv} \) eventually becomes the mask on the most contributing features. This adversarial mask provides the learning opportunity on neurons, so called dead filter, that was considered to be less informative.

**Virtual Adversarial Dropout**

**Virtual adversarial dropout (VAdD)** defines \( g(x, y, \theta) \) as \( g(x, y, \theta) \).

Virtual adversarial dropout (VAdD) defines \( g(x, y, \theta) \) as \( g(x, y, \theta) \).

This uses the loss function as a regularization term for semi-supervised learning. The divergence term in Formula 3 can be represented as bellow:

\[
L_{VAdD}(x, y, \epsilon^s; \theta, \delta) := D[f_\theta(x, \epsilon^s), f_\theta(x, \epsilon^\text{adv})]
\]

where \( \epsilon^\text{adv} := \arg\max_{\epsilon : \|\epsilon\|_2 \leq \delta H} D[f_\theta(x, \epsilon^s), f_\theta(x, \epsilon)] \).
VAIAD is a special case of a self-ensembling model with two dropouts. They are 1) a dropout, $e^s$, sampled from a random distribution with a hyperparameter and 2) a dropout, $e^{adv}$, composed to maximize the divergence function of the learner, which is the concept of the noise injection from the virtual adversarial training. The two dropouts create a regularization as the virtual adversarial training, and the inference procedure optimizes the parameters to reduce the divergence between the random dropout and the adversarial dropout. This optimization triggers the self-ensemble learning in (Laine and Aila 2016). However, the adversarial dropout is different from the previous self-ensembling because one dropout is induced by the adversarial setting, not by a random sampling.

Learning with Adversarial Dropout The full objective function for the learning with the adversarial dropout is given by

$$l(y, f_{\theta}(x, e^s)) + \lambda L_{Adv}(x, y, e^s; \theta, \delta)$$

where $l(y, f_{\theta}(x, e^s))$ is the negative log-likelihood for $y$ given $x$ under the sampled dropout instance $e^s$. There are two scalar-scale hyper-parameters: (1) a trade-off parameter, $\lambda$, for controlling the impact of the proposed regularization term and (2) the constraints, $\delta$, specifying the intensity of adversarial dropout.

Combining Adversarial Dropout and Adversarial Training Additionally, it should be noted that the adversarial training and the adversarial dropout are not exclusive training methods. A neural network can be trained by imposing the input perturbation with the Gaussian additive noise, and by enabling the adversarially chosen dropouts, simultaneously. Formula 7 specifies the loss function of simultaneously utilizing the adversarial dropout and the adversarial training.

$$l(y, f_{\theta}(x, e^s)) + \lambda_1 L_{Adv}(x, y, e^s) + \lambda_2 L_{AT}(x, y)$$

where $\lambda_1$ and $\lambda_2$ are trade-off parameters controlling the impact of the regularization terms.

Fast Approximation Method for Finding Adversarial Dropout Condition Once the adversarial dropout, $e^{adv}$, is identified, the evaluation of $L_{Adv}$ simply becomes the computation of the loss and the divergence functions. However, the inference on $e^{adv}$ is difficult because of three reasons. First, we cannot obtain a closed-form solution on the exact adversarial noise value, $e^{adv}$. Second, the feasible space for $e^{adv}$ is restricted under $\|e^s - e^{adv}\|_2 \leq \delta H$, which becomes a constraint in the optimization. Third, $e^{adv}$ is a binary-valued vector rather than a continuous-valued vector because $e^{adv}$ indicates the activation of neurons. This discrete nature requires an optimization technique like integer programming.

To mitigate this difficulty, we approximated the objective function, $L_{Adv}$, with the first order of the Taylor expansion by relaxing the domain space of $e^{adv}$. This Taylor expansion of the objective function was used in the earlier works of adversarial training (Goodfellow, Shlens, and Szegedy 2014; Miyato et al. 2015). After the approximation, we found an adversarial dropout condition by solving an integer programming problem.

To define a neural network with a dropout layer, we separate the output function into two neural sub-networks, $f_{\theta_1}(x, e) = f_{\theta_1}^{upper}(h(x) \circ e)$, where $f_{\theta_1}^{upper}$ is the upper part network of the dropout layer and $h(x) = f_{\theta_2}^{lower}(x)$ is the under part neural network. Our objective is optimizing an adversarial dropout noise $e^{adv}$ by maximizing the following divergence function under the constraint $\|e^s - e^{adv}\|_2 \leq \delta H$:

$$D(x, e; \theta, e^s) = D[f_{\theta_1}(x, e), f_{\theta_2}^{upper}(h(x) \circ e)]$$

where $e^s$ is a sampled dropout mask, and $\theta$ is a parameter of the neural network model. We approximate the above divergence function by deriving the first order of the Taylor expansion by relaxing the domain space of $e$ from the multiple binary spaces, $\{0, 1\}^H$, to the real value spaces, $[0, 1]^H$. This conversion is a common step in the integer programming research as (Hemmecke et al. 2010):

$$D(x, e; \theta, e^s) \approx D(x, e^0; \theta, e^0) + (e - e^0)^T J(x, e^0)$$

where $J(x, e^0)$ is the Jacobian vector given by $J(x, e^0) := \nabla_{e^s} D(x, e; \theta, e^s)|_{e^s = e^0}$ when $e^0 = 1$ indicates no noise injection. The above Taylor expansion provides a linearized optimization objective function by controlling $e$. Therefore, we reorganized the Taylor expansion with respect to $e$ as the below:

$$D(x, e; \theta, e^s) \propto \sum_i e_i J_i(x, e^0)$$

where $J_i(x, e^0)$ is the $i^{th}$ element of $J(x, e^0)$. Since we cannot proceed further with the given formula, we introduce an alternative Jacobian formula that further specifies the dropout mechanism by $\circ$ and $h(x)$ as the below.

$$J(x, e^0) \approx h(x) \circ \nabla_{h(x)} D(x, e^0; \theta, e^s)$$

where $h(x)$ is the output vector of the under part neural network of the adversarial dropout.

The control variable, $e^s$, is a binary vector whose elements are either one or zero. Under this approximate divergence, finding a maximal point of $e^s$ can be viewed as the 0/1 knapsack problem (Kellerer, Pferschy, and Pisinger 2004), which is one of the most popular integer programming problems.

To find $e^{adv}$ with the constraint, we propose Algorithm 1 based on the dynamic programming for the 0/1 knapsack problem. In the algorithm, $e^{adv}$ is initialized with $e^s$, and $e^{adv}$ changes its value by the order of the degree increasing the objective divergence until $\|e^s - e^{adv}\|_2 \leq \delta H$; or there is no increment in the divergence. After using the algorithm, we obtain $e^{adv}$ that maximizes the divergence with the constraint, and we evaluate the loss function $L_{Adv}$.

We should notice that the complex vector of the Taylor expansion is not $e^s$, but $e^s$. In the case of virtual adversarial dropout, whose divergence is formed as $D[f_{\theta_1}(x, e^s), f_{\theta_2}(x, e^s)]$, $e^s$ is the minimal point leading the gradient to be zero because of the identical distribution between the random and the optimized dropouts. This zero gradient affects the approximation of the divergence term as
In the first set of experiments, we benchmark our method on the MNIST dataset (LeCun et al. 1998), which consists of 70,000 handwritten digit images of size $28 \times 28$ where 60,000 images are used for training and the rest for testing.

Table 1: Test performance with 1,000 labeled (semi-supervised) and 60,000 labeled (supervised) examples on MNIST. Each setting is repeated for eight times.

| Method         | Error rate (%) with # labels |
|----------------|-------------------------------|
| Plain (only dropout) | $2.99 \pm 0.25$ , $0.53 \pm 0.03$ |
| AT             | $1.35 \pm 0.14$ , $0.50 \pm 0.01$ |
| VAT            | $1.00 \pm 0.08$ , $0.50 \pm 0.02$ |
| II model       | $0.46 \pm 0.01$ , $0.46 \pm 0.02$ |
| SAdD           | $0.99 \pm 0.07$ , $0.47 \pm 0.01$ |
| VAdD (KL)      | $0.99 \pm 0.09$ , $0.46 \pm 0.02$ |
| VAdD (QE)      | $0.99 \pm 0.07$ , $0.47 \pm 0.01$ |

zero. To avoid the zero gradients, we set the complex vector of the Taylor expansion as $\epsilon_0$.

This zero gradient situation does not occur when the model function, $f_\theta$, contains additional stochastic layers because $f_\theta(x, e', \rho') \neq f_\theta(x, e^*, \rho^*)$ when $\rho'$ and $\rho^*$ are independently sampled noises from another stochastic layers.

**Experiments**

This section evaluates the empirical performance of adversarial dropout for supervised and semi-supervised classification tasks on three benchmark datasets, MNIST, SVHN, and CIFAR-10. In every presented task, we compared adversarial dropout, II model, and adversarial training. We also performed additional experiments to analyze the sparsity of adversarial dropout.

**Supervised and Semi-supervised Learning on MNIST task**

In the first set of experiments, we benchmark our method on the MNIST dataset (LeCun et al. 1998), which consists
Table 2: Test performances of semi-supervised and supervised learning on SVHN and CIFAR-10. Each setting is repeated for five times. KL and QE indicate Kullback-Leibler divergence and quadratic error, respectively, to specify the divergence function, $D[y, \hat{y}]$

| Method                                      | SVHN with # labels | CIFAR-10 with # labels |
|---------------------------------------------|--------------------|------------------------|
|                                             | 1,000 | 73,257 (All) | 4,000 | 50,000 (All) |
| Π model (Laine and Aila 2016)              | 4.82 | 2.54       | 12.36 | 5.56       |
| Tem. ensembling (Laine and Aila 2016)     | 4.42 | 2.74       | 12.16 | 5.60       |
| Sajjadi et al. (Sajjadi, Javanmardi, and Tasdizen 2016) | -    | -         | 11.29 | -          |
| VAT (Miyato et al. 2017)                 | 3.86 | -          | 10.55 | 5.81       |
| Π model (our implementation)              | 4.35 ± 0.04 | 2.53 ± 0.05 | 12.62 ± 0.29 | 5.77 ± 0.11 |
| VAT (our implementation)                  | 3.74 ± 0.09 | 2.69 ± 0.04 | 11.96 ± 0.10 | 5.65 ± 0.17 |
| SAdD                                       | -    | 2.46 ± 0.05 | -    | 5.46 ± 0.16 |
| VAdD (KL)                                  | 4.16 ± 0.08 | 2.31 ± 0.01 | 11.68 ± 0.19 | 5.27 ± 0.10 |
| VAdD (QE)                                  | 4.26 ± 0.14 | 2.37 ± 0.03 | **11.32 ± 0.11** | **5.24 ± 0.12** |
| VAdD (KL) + VAT                            | **3.55 ± 0.05** | **2.23 ± 0.03** | 10.07 ± 0.11 | **4.40 ± 0.12** |
| VAdD (QE) + VAT                            | **3.55 ± 0.07** | 2.34 ± 0.05 | **9.22 ± 0.10** | 4.73 ± 0.04 |

3.55% of test error rates on SVHN, and 10.04% and 9.22% of test error rates on CIFAR-10. Additionally, VAdD alone achieved a better performance than the self-ensemble model (Π model). This indicates that considering an adversarial perturbation on dropout layers enhances the self-ensemble effect.

**Effect on Features and Sparsity from Adversarial Dropout**

Dropout prevents the co-adaptation between the units in a neural network, and the dropout decreases the dependency between hidden units (Srivastava et al. 2014). To compare the adversarial dropout and the standard dropout, we analyzed the co-adaptations by visualizing features of autoencoders on the MNIST dataset. The autoencoder consists with one hidden layer, whose dimension is 256, with the ReLU activation. When we trained the autoencoder, we set the dropout with $p = 0.5$, and we calculated the reconstruction error between the input data and the output layer as a loss function to update the weight values of the autoencoder with the standard dropout. On the other hand, the adversarial dropout error is also considered when we update the weight values of the autoencoder with the parameters, $\lambda = 0.2$, and $\delta = 0.3$. The trained autoencoders showed similar reconstruction errors on the test dataset.

Figure 2 shows the visualized features from the autoencoders. There are two differences identified from the visualization: 1) adversarial dropout prevents that the learned weight matrix contains black boxes, or dead filters, which may be all zero for many different inputs and 2) adversarial dropout tends to standardize other features, except for localized features viewed as black dots, while the standard dropout tends to ignore the neighborhoods of the localized features. These show that adversarial dropout standardizes the other features while preserving the characteristics of localized features from the standard dropout. These could be the main reason for the better generalization performance.

The important side-effect of the standard dropout is the sparse activations of the hidden units (Hinton et al. 2012). To analyze the sparse activations by adversarial dropout, we compared the activation values of the auto-encoder models with no-dropout, dropout, and adversarial dropout on the MNIST test dataset. A sparse model should only have a few highly activated units, and the average activation of any unit across data instances should be low (Hinton et al. 2012). Figure 3 plot the distribution of the activation values and their means across the test dataset. We found that the adversarial dropout has fewer highly activated units compared to others. Moreover, the mean activation values of the adversarial dropout were the lowest. These indicate that adversarial dropout improves the sparsity of the model than the standard dropout does.

**Discussion**

The previous studies proved that the adversarial noise injections were an effective regularizer (Goodfellow, Shlens, and Szegedy 2014). In order to investigate the different properties of adversarial dropout, we explore a very simple case of applying adversarial training and adversarial dropout to the linear regression.
Linear Regression with Adversarial Training

Let \( x_i \in \mathbb{R}^D \) be a data point and \( y_i \in \mathbb{R} \) be a target where \( i = \{1, ..., N\} \). The objective of the linear regression is finding \( w \in \mathbb{R}^D \) that minimizes \( l(w) = \sum_i \|y_i - x_i^Tw\|^2 \).

To express adversarial examples, we denote \( \tilde{x}_i = x_i + r_i^{adv} \) as the adversarial example of \( x_i \) where \( r_i^{adv} = \delta \text{sign}(\nabla_{x_i} l(w)) \) utilizing the fast gradient sign method (FGSM) (Goodfellow, Shlens, and Szegedy 2014), \( \delta \) is a control parameter representing the degree of adversarial noises. With the adversarial examples, the objective function of the adversarial training can be viewed as follows:

\[
l_{AT}(w) = \sum_i \|y_i - (x_i + r_i^{adv})^Tw\|^2 \tag{12}
\]

The above equation is translated into the below formula by isolating the terms with \( r_i^{adv} \) as the additive noise.

\[
l(w) + \sum_{ij} |\delta \nabla_{x_{ij}} l(w)| + \delta^2 w^T \Gamma_{AT} w \tag{13}
\]

where \( \Gamma_{AT} = \sum_i \text{sign}(\nabla_{x_i} l(w))^T \text{sign}(\nabla_{x_i} l(w)) \). The second term shows the \( L_1 \) regularization by multiplying the degree of the adversarial noise, \( \delta \), at each data point. Additionally, the third term indicates the \( L_2 \) regularization with \( \Gamma_{AT} \), which form the scales of \( w \) by the gradient direction differences over all data points. The penalty terms are closely related with the hyper-parameter \( \delta \). When \( \delta \) approaches to zero, the regularization term disappears because the inputs become adversarial examples, not anymore. For a large \( \delta \), the regularization constant grows larger than the original loss function, and the learning becomes infeasible. The previous studies proved that the adversarial objective function based on the FGSM is an effective regularizer. This paper investigated that training a linear regression with adversarial examples provides two regularization terms of the above equation.

Linear Regression with Adversarial Dropout

Now, we turn to the case of applying adversarial dropout to a linear regression. To represent the adversarial dropout, we denote \( \tilde{x}_i = \epsilon_i^{adv} \odot x_i \) as the adversarially dropped input of \( x_i \), where \( \epsilon_i^{adv} = \arg\max_{\epsilon \in \mathbb{R}^D} \|y_i - (\epsilon \odot x_i)^Tw\|^2 \) with the hyper-parameter, \( k \), controlling the degree of the adversarial dropout. For simplification, we used one vector as the sampled dropout, \( \epsilon_i \), of the adversarial dropout. If we apply Algorithm 1, the adversarial dropout can be defined as follows:

\[
\epsilon_i^{adv} = \begin{cases} 
0 & \text{if } x_{ij} \nabla_{x_{ij}} l(w) \leq \min\{s_{ik}, 0\} \\
1 & \text{otherwise}
\end{cases} \tag{14}
\]

where \( s_{ik} \) is the \( k \text{th} \) lowest element of \( x_i \odot \nabla_{x_i} l(w) \). This solution satisfies the constraint, \( \|\epsilon_i - \epsilon^s\|_2 \leq k \). With this adversarial dropout condition, the objective function of the adversarial dropout can be defined as the belows:

\[
l_{AdD}(w) = \sum_i \|y_i - (\epsilon_i^{adv} \odot x_i)^Tw\|^2 \tag{15}
\]

When we isolate the terms with \( \epsilon_i^{adv} \), the above equation is translated into the below formula.

\[
l(w) + \sum_i \sum_{j \in S_i} |x_{ij} \nabla_{x_{ij}} l(w)| + w^T \Gamma_{AdD} w \tag{16}
\]

where \( S_i = \{j | \epsilon_i^{adv} = 0\} \) and \( \Gamma_{AdD} = \sum_i ((1 - \epsilon_i^{adv}) \odot x_i)^T((1 - \epsilon_i^{adv}) \odot x_i) \). The second term is the \( L_1 \) regularization of the \( k \) largest loss changes from the features of each data point. The third term is the \( L_2 \) regularization with \( \Gamma_{AdD} \). These two penalty terms are related with the hyper-parameter \( k \) controlling the degree of the adversarial dropout, because the \( k \) indicates the number of elements of the set \( S_i \), \( \forall i \). When \( k \) becomes zero, the two penalty terms disappear because there will be no dropout by the constraint on \( \epsilon \).

There are two differences between the adversarial dropout and the adversarial training. First, the regularization terms of the adversarial dropout are dependent on the scale of the features of each data point. In \( L_1 \) regularization, the gradients of the loss function are re-scaled with the data points. In \( L_2 \) regularization, the data points affect the scales of the weight costs. In contrast, the penalty terms of adversarial training are dependent on the degree of adversarial noise, \( \delta \), which is a static term across the instances because \( \delta \) is a single-valued hyper parameter given in the training process. Second, the penalty terms of the adversarial dropout are selectively activated by the degree of the loss changes while the penalty terms of the adversarial training are always activated.

Conclusion

The key point of our paper is combining the ideas from the adversarial training and the dropout. The existing methods of the adversarial training control a linear perturbation with additive properties only on the input layer. In contrast, we combined the concept of the perturbation with the dropout properties on hidden layers. Adversarially dropped structure becomes a poor ensemble model for the label assignment.
even when very few nodes are changed. However, by learning the model with the poor structure, the model prevents over-fitting using a few effective features. The experiments showed that the generalization performances are improved by applying our adversarial dropout. Additionally, our approach achieved the state-of-the-art performances of 3.55% on SVHN and 9.22% on CIFAR-10 by applying VAdD and VAT together for the semi-supervised learning.

References

Baldi, P., and Sadowski, P. J. 2013. Understanding dropout. In Advances in Neural Information Processing Systems. 2814–2822.

Bishop, C. M. 1995a. Training with noise is equivalent to tikhonov regularization. Neural computation 7(1):108–116.

Bishop, C. M. 1995b. Regularization and complexity control in feed-forward networks.

Chen, N.; Zhu, J.; Chen, J.; and Zhang, B. 2014. Dropout training for support vector machines. arXiv preprint arXiv:1404.4171.

Goodfellow, I. J.; Shlens, J.; and Szegedy, C. 2014. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.

He, K.; Zhang, X.; Ren, S.; and Sun, J. 2016. Identity mappings in deep residual networks. In European Conference on Computer Vision, 630–645. Springer.

Hemmecke, R.; Köppe, M.; Lee, J.; and Weismantel, R. 2010. Nonlinear integer programming. In 50 Years of Integer Programming 1958-2008. Springer. 561–618.

Hinton, G. E.; Srivastava, N.; Krizhevsky, A.; Sutskever, I.; and Salakhutdinov, R. R. 2012. Improving neural networks by preventing co-adaptation of feature detectors. arXiv preprint arXiv:1207.0580.

Huang, G.; Liu, Z.; Weinberger, K. Q.; and van der Maaten, L. 2016. Densely connected convolutional networks. arXiv preprint arXiv:1608.06993.

Jain, P.; Kulkarni, V.; Thakurta, A.; and Williams, O. 2015. To drop or not to drop: Robustness, consistency and differential privacy properties of dropout. arXiv preprint arXiv:1503.02031.

Kellerer, H.; Pferschy, U.; and Pisinger, D. 2004. Introduction to np-completeness of knapsack problems. In Knapsack problems. Springer. 483–493.

Kingma, D., and Ba, J. 2014. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

Krizhevsky, A., and Hinton, G. 2009. Learning multiple layers of features from tiny images.

Kurakin, A.; Goodfellow, I.; and Bengio, S. 2016. Adversarial examples in the physical world. arXiv preprint arXiv:1607.02533.

Laine, S., and Aila, T. 2016. Temporal ensembling for semi-supervised learning. arXiv preprint arXiv:1610.02242.

Lasserre, J. A.; Bishop, C. M.; and Minka, T. P. 2006. Principled hybrids of generative and discriminative models. In Computer Vision and Pattern Recognition, 2006 IEEE Computer Society Conference on, volume 1, 87–94. IEEE.

LeCun, Y.; Bottou, L.; Bengio, Y.; and Haffner, P. 1998. Gradient-based learning applied to document recognition. Proceedings of the IEEE 86(11):2278–2324.

Lee, C.-Y.; Xie, S.; Gallagher, P.; Zhang, Z.; and Tu, Z. 2015. Deeply-supervised nets. In Artificial Intelligence and Statistics, 562–570.

Li, Z.; Gong, B.; and Yang, T. 2016. Improved dropout for shallow and deep learning. In Advances in Neural Information Processing Systems, 2523–2531.

Lin, M.; Chen, Q.; and Yan, S. 2013. Network in network. arXiv preprint arXiv:1312.4400.

Maaten, L.; Chen, M.; Tyree, S.; and Weinberger, K. Q. 2013. Learning with marginalized corrupted features. In Proceedings of the 30th International Conference on Machine Learning (ICML-13), 410–418.

Miyato, T.; Maeda, S.-i.; Koyama, M.; Nakae, K.; and Ishii, S. 2015. Distributional smoothing with virtual adversarial training. arXiv preprint arXiv:1507.00677.

Miyato, T.; Maeda, S.-i.; Koyama, M.; and Ishii, S. 2017. Virtual adversarial training: a regularization method for supervised and semi-supervised learning. arXiv preprint arXiv:1704.03976.

Miyato, T.; Dai, A. M.; and Goodfellow, I. 2016. Virtual adversarial training for semi-supervised text classification. stat 1050:25.

Netzer, Y.; Wang, T.; Coates, A.; Bissacco, A.; Wu, B.; and Ng, A. Y. 2011. Reading digits in natural images with unsupervised feature learning. In NIPS workshop on deep learning and unsupervised feature learning, volume 2011, 5.

Poole, B.; Sohl-Dickstein, J.; and Ganguli, S. 2014. Analyzing noise in autoencoders and deep networks. arXiv preprint arXiv:1406.1831.

Rasmus, A.; Berglund, M.; Honkala, M.; Valpola, H.; and Raiko, T. 2015. Semi-supervised learning with ladder networks. In Advances in Neural Information Processing Systems, 3546–3554.

Sajjadi, M.; Javanmardi, M.; and Tasdizen, T. 2016. Regularization with stochastic transformations and perturbations for deep semi-supervised learning. In Advances in Neural Information Processing Systems, 1163–1171.

Salimans, T., and Kingma, D. P. 2016. Weight normalization: A simple reparameterization to accelerate training of deep neural networks. In Advances in Neural Information Processing Systems, 901–901.

Salimans, T.; Goodfellow, I. J.; Zaremba, W.; Cheung, V.; Radford, A.; and Chen, X. 2016. Improved techniques for training gans. CoRR abs/1606.03498.

Sanfeliu, A., and Fu, K.-S. 1983. A distance measure between attributed relational graphs for pattern recognition. IEEE transactions on systems, man, and cybernetics (3):353–362.

Springenberg, J. T.; Dosovitskiy, A.; Brox, T.; and Ried-
nodes and \( \mathcal{N} \) \( \epsilon \) two dropout masks

**Proposition 1**

same as \( \mathcal{N} \) consider a hidden node (vertex) is revival, change of GED is

\[
\text{change} g_{\epsilon}, \epsilon
\]

When we consider a neural network as a graph, we can apply relative difference between two dropouted networks, \( g_{\epsilon} \) and \( g_{\epsilon} \), which can provide the number of different dropped nodes.

\[
\text{Adversarial dropout, } p = 0.5 \quad \delta = 0.005
\]

**A.2. Jaccard Distance**

When we consider a dropout condition \( \epsilon \) as a set of selected hidden nodes, we can apply Jaccard distance to measure difference two dropout masks, \( \epsilon_{1} \) and \( \epsilon_{2} \). The following equation is the definition of Jaccard distance:

\[
JD(\epsilon_{1}, \epsilon_{2}) = \frac{\|\epsilon_{1} \cup \epsilon_{2}\| - \|\epsilon_{1} \cap \epsilon_{2}\|}{\|\epsilon_{1} \cup \epsilon_{2}\|}
\]  

(20)

Since \( \epsilon_{1} \) and \( \epsilon_{2} \) are binary vectors, \( |\epsilon_{1} \cap \epsilon_{2}| \) can be converted as \( |\epsilon_{1} \cup \epsilon_{2}| \) and \( |\epsilon_{1} \cup \epsilon_{2}| \) can be viewed as \( \|\epsilon_{1} + \epsilon_{2} \| \). This leads the following proposition.

**Proposition 2**

Given two dropout masks \( \epsilon_{1} \) and \( \epsilon_{2} \), which are binary vectors, Jaccard distance between them can be defined as:

\[
JD(\epsilon_{1}, \epsilon_{2}) = \frac{\|\epsilon_{1} - \epsilon_{2}\|_{2}}{\|\epsilon_{1} + \epsilon_{2} - \epsilon_{1} \cap \epsilon_{2}\|_{2}}
\]  

(21)

**Appendix B. Detailed Experiment Set-up**

This section describes the network architectures and settings for the experimental results in this paper. The tensorflow implementations for reproducing these results can be obtained from https://github.com/sungraepark/Adversarial-Dropout.

**B.1. MNIST : Convolutional Neural Networks**

| Name   | Description                        |
|--------|------------------------------------|
| input  | 28 × 28 image                      |
| conv1  | 32 filters, 1 x 1, pad=’same’, ReLU |
| pool1  | Maxpool 2 x 2 pixels               |
| drop1  | Dropout, \( p = 0.5 \)             |
| conv2  | 64 filters, 1 x 1, pad=’same’, ReLU |
| pool2  | Maxpool 2 x 2 pixels               |
| drop2  | Dropout, \( p = 0.5 \)             |
| conv3  | 128 filters, 1 x 1, pad=’same’, ReLU |
| pool3  | Maxpool 2 x 2 pixels               |
| adt    | Adversarial dropout, \( p = 0.5 \), \( \delta = 0.005 \) |
| dense1 | Fully connected 2048 \( \rightarrow \) 625 |
| dense2 | Fully connected 625 \( \rightarrow \) 10 |

| output | Softmax                           |

The MNIST dataset (LeCun et al., 1998) consists of 70,000 handwritten digit images of size 28 × 28 where 60,000 images are used for training and the rest for testing. The CNN architecture is described in Table 1. All networks were trained using Adam (Kingma and Ba 2014) with a learning rate of 0.001 and momentum parameters...
of $\beta_1 = 0.9$ and $\beta_2 = 0.999$. In all implementations, we trained the model for 100 epochs with minibatch size of 128.

For the constraint of adversarial dropout, we set $\delta = 0.005$, which indicates 10 ($0.04 + 0.005$) adversarial changes from the randomly selected dropout mask. In all training, we ramped up the trade-off parameter, $\lambda$, for proposed regularization term, $L_{Add}$. During the first 30 epochs, we used a Gaussian ramp-up curve $\exp[-5(1 - T)^2]$, where $T$ advances linearly from zero to one during the ramp-up period. The maximum values of $\lambda_{max}$ are 1.0 for VADD (KL) and VAT, and 30.0 for VADD (QE) and II model.

### B.2. SVHN and CIFAR-10: Supervised and Semi-supervised learning

Table 4: The network architecture used on SVHN and CIFAR-10

| Name  | Description                  |
|-------|------------------------------|
| input | 32 X 32 RGB image            |
| noise | Additive Gaussian noise $\sigma = 0.15$ |
| conv1a| 128 filters, 3 x 3, pad='same', LReLU($\alpha = 0.1$) |
| conv1b| 128 filters, 3 x 3, pad='same', LReLU($\alpha = 0.1$) |
| conv1c| 128 filters, 3 x 3, pad='same', LReLU($\alpha = 0.1$) |
| pool1 | Maxpool 2 x 2 pixels |
| drop1 | Dropout, $p = 0.5$ |
| conv2a| 256 filters, 3 x 3, pad='same', LReLU($\alpha = 0.1$) |
| conv2b| 256 filters, 3 x 3, pad='same', LReLU($\alpha = 0.1$) |
| conv2c| 256 filters, 3 x 3, pad='same', LReLU($\alpha = 0.1$) |
| pool2 | Maxpool 2 x 2 pixels |
| conv3a| 512 filters, 3 x 3, pad='valid', LReLU($\alpha = 0.1$) |
| conv3b| 256 filters, 1 x 1, LReLU($\alpha = 0.1$) |
| conv3c| 128 filters, 1 x 1, LReLU($\alpha = 0.1$) |
| pool3 | Global average pool (6 x 6 -> 1 x 1) pixels |
| add  | Adversarial dropout, $p = 1.0$, $\delta = 0.05$ |
| dense | Fully connected 128 -> 10 |
| output | Softmax |

The both datasets, SVHN (Netzer et al. 2011) and CIFAR-10 (Krizhevsky and Hinton 2009), consist of $32 \times 32$ colour images in ten classes. For these experiments, we used a CNN, which used by (Laine and Aila 2016; Miyato et al. 2017) described in Table 2. In all layers, we applied batch normalization for SVHN and mean-only batch normalization (Salimans and Kingma 2016) for CIFAR-10 with momentum 0.999. All networks were trained using Adam (Kingma and Ba 2014) with the momentum parameters of $\beta_1 = 0.9$ and $\beta_2 = 0.999$, and the maximum learning rate 0.003. We ramped up the learning rate during the first 80 epochs using a Gaussian ramp-up curve $\exp[-5(1 - T)^2]$, where $T$ advances linearly from zero to one during the ramp-up period. Additionally, we annealed the learning rate to zero and the Adam parameter, $\beta_1$, to 0.5 during the last 50 epochs. The number of total epochs is set as 300. These learning setting are same with (Laine and Aila 2016).

For adversarial dropout, we set the maximum value of regularization component weight, $\lambda_{max}$, as 1.0 for VADD(KL) and 25.0 for VADD(QE). We also ramped up the weight using the Gaussian ramp-up curve during the first 80 epochs. Additionally, we set $\delta$ as 0.05 and dropout probability $p$ as 1.0, which means dropping 6 units among the full hidden units. We set minibatch size as 100 for supervised learning and 32 labeled and 128 unlabeled data for semi-supervised learning.

### Appendix C. Definition of Notation

In this section, we describe notations used over this paper.

Table 5: The notation used over this paper.

| Notation | Description |
|----------|-------------|
| $x$      | An input of a neural network |
| $y$      | A true label |
| $\theta$ | A set of parameters of a neural network |
| $\gamma$ | A noise vector of additive Gaussian noise layer |
| $\epsilon$ | A binary noise vector of dropout layer |
| $\delta$ | A hyperparameter controlling the intensity of the adversarial perturbation |
| $\lambda$ | A trade-off parameter controlling the impact of a regularization term |
| $D[y, y']$ | A nonnegative function that represents the distance between two output vectors: cross entropy(CE), KL divergence(KL), and quadratic error (QE) |
| $f_0(x)$ | An output vector of a neural network with parameters ($\theta$) and an input ($x$) |
| $f_0(x, \rho)$ | An output vector of a neural network with parameters ($\theta$), an input ($x$), and noise ($\rho$) |
| $f^{upper}_{\theta_1}$ | A upper part of a neural network, $f_0(x, \epsilon)$, of a adversarial dropout layer where $\theta = \{\theta_1, \theta_2\}$ |
| $f^{under}_{\theta_2}$ | A under part of a neural network, $f_0(x, \epsilon)$, of a adversarial dropout layer |

### Appendix D. Performance Comparison with Other Models

#### D.1. CIFAR-10: Supervised classification results with additional baselines

We compared the reported performances of the additional close family of CNN-based classifier for the supervised learning. As we mentioned in the paper, we did not consider the recent advanced architectures, such as ResNet (He et al. 2016) and DenseNet (Huang et al. 2016).

#### D.2. CIFAR-10: Semi-supervised classification results with additional baselines

We compared the reported performances of additional baseline models for the semi-supervised learning. Our implementation reproduced the closed performance from their reported results, and showed the performance improvement from adversarial dropout.
with the adversarial examples, the objective function controlling parameter representing the degree of adversarial δ

\[ \text{Linear Regression with Adversarial Training} \]

...tion terms from adversarial training and adversarial dropout.

Table 6: Supervised learning performance on CIFAR-10. Each setting is repeated for five times.

| Method                        | Error rate (%) |
|-------------------------------|----------------|
| Network in Network (2013)     | 8.81           |
| All-CNN (2014)                | 7.25           |
| Deep Supervised Net (2015)    | 7.97           |
| Highway Network (2015)        | 7.72           |
| II model (2016)               | 5.56           |
| Temporal ensembling (2016)    | 5.60           |
| VAT (2017)                    | 5.81           |
| II model (our implementation) | 5.77 ± 0.11    |
| VAT (our implementation)      | 5.65 ± 0.17    |
| AdD                           | 5.46 ± 0.16    |
| VAdD (KL)                     | 5.27 ± 0.10    |
| VAdD (QE)                     | 5.24 ± 0.12    |
| VAdD (KL) + VAT               | 4.40 ± 0.12    |
| VAdD (QE) + VAT               | 4.73 ± 0.04    |

Table 7: Semi-supervised learning task on CIFAR-10 with 4,000 labeled examples. Each setting is repeated for five times.

| Method                        | Error rate (%) |
|-------------------------------|----------------|
| Ladder network (2015)         | 20.40          |
| CatGAN (2015)                 | 19.58          |
| GAN with feature matching (2016) | 18.63      |
| II model (2016)               | 12.36          |
| Temporal ensembling (2016)    | 12.16          |
| Sajjadi et al. (2016)         | 11.29          |
| VAT (2017)                    | 10.55          |
| II model (our implementation) | 12.62 ± 0.29   |
| VAT (our implementation)      | 11.96 ± 0.10   |
| VAdD (KL)                     | 11.68 ± 0.19   |
| VAdD (QE)                     | **11.32 ± 0.11** |
| VAdD (KL) + VAT               | 10.07 ± 0.11   |
| VAdD (QE) + VAT               | **9.22 ± 0.10** |

**Appendix E. Proof of Linear Regression Regularization**

In this section, we showed the detailed proof of regularization terms from adversarial training and adversarial dropout.

**Linear Regression with Adversarial Training**

Let \( x_i \in \mathbb{R}^D \) be a data point and \( y_i \in \mathbb{R} \) be a target where \( i = \{1, ..., N\} \). The objective of linear regression is to find a \( w \in \mathbb{R}^D \) that minimizes \( l(w) = \sum_i \|y_i - x_i^T w\|^2 \).

To express adversarial examples, we denote \( x_i^\text{adv} = x_i + r_i^\text{adv} \) as the adversarial example of \( x_i \) where \( r_i^\text{adv} = \delta \text{sign}(\nabla_{x_i} l(w)) \) utilizing the fast gradient sign method (FGSM) (Goodfellow, Shlens, and Szegedy 2014). \( \delta \) is a controlling parameter representing the degree of adversarial noises. With the adversarial examples, the objective function of adversarial training can be viewed as follows:

\[
l_{\text{AT}}(w) = \sum_i \|y_i - (x_i + r_i^\text{adv})^T w\|^2 \tag{22}\]

This can be divided to

\[
l_{\text{AT}}(w) = l(w) - 2 \sum_i (y_i - x_i^T w) w^T r_i^\text{adv} + \sum_i w^T (r_i^\text{adv})^T (r_i^\text{adv}) w \tag{23}\]

where \( l(w) \) is the loss function without adversarial noise. Note that the gradient is \( \nabla_{x_i} l(w) = -2(y_i - x_i^T w) w_i \), and \( a^T \text{sign}(a) = \|a\|_1 \). The above equation can be transformed as the following:

\[
l_{\text{AT}}(w) = l(w) + \sum_{ij} \|\delta \nabla_{x_{ij}} l(w)\| + \delta^2 w^T \Gamma_{\text{AT}} w, \tag{24}\]

where \( \Gamma_{\text{AT}} = \sum_i \text{sign}(\nabla_{x_i} l(w))^T \text{sign}(\nabla_{x_i} l(w)) \).

**Linear Regression with Adversarial Dropout**

To represent adversarial dropout, we denote \( x_i^\text{adv} = \epsilon_i^\text{adv} \odot x_i \) as the adversarially dropped input of \( x_i \) where \( \epsilon_i^\text{adv} = \text{argmax}_{\|\epsilon_i\|_1 \leq k} (y_i - (\epsilon_i \odot x_i)^T w)^2 \) with the hyper-parameter, \( k \), controlling the degree of adversarial dropout. For simplification, we used one vector as the base condition of a adversarial dropout. If we applied our proposed algorithm, the adversarial dropout can be defined as follows:

\[
epsilon_{ij}^\text{adv} = \begin{cases} 0 & \text{if } x_{ij} \nabla_{x_{ij}} l(w) \leq \min\{s_{ik}, 0\} \\ 1 & \text{otherwise} \end{cases} \tag{25}\]

where \( s_{ik} \) is the \( k^{th} \) lowest element of \( x_i \odot \nabla_{x_i} l(w) \). This solution satisfies the constraint, \( \|\epsilon_i - 1\|_2 \leq k \). With this adversarial dropout condition, the objective function of adversarial dropout can be defined as the following:

\[
l_{\text{ADD}}(w) = \sum_i \|y_i - (\epsilon_i^\text{adv} \odot x_i)^T w\|^2 \tag{26}\]

This can be divided to

\[
l_{\text{ADD}}(w) = l(w) + 2 \sum_i (y_i - x_i^T w)((1 - \epsilon_i^\text{adv}) \odot x_i)^T w + \sum_i w^T ((1 - \epsilon_i^\text{adv}) \odot x_i)^T ((1 - \epsilon_i^\text{adv}) \odot x_i) w \tag{27}\]

The second term of the right handside can be viewed as

\[
2 \sum_i (y_i - x_i^T w) \sum_j (1 - \epsilon_{ij}^\text{adv}) x_{ij} w_j. \tag{28}\]

By defining a set \( S_i = \{j | \epsilon_{ij}^\text{adv} = 0\} \), the second term can be transformed as the following.

\[- \sum_i \sum_{j \in S_i} -2(y_i - x_i^T w) w_j x_{ij}. \tag{29}\]

Note that the gradient is \( \nabla_{x_{ij}} l(w) = -2(y_i - x_i^T w) w_j \) and \( x_{ij} \nabla_{x_{ij}} l(w) \) is always negative when \( j \in S_i \). The second term can be re-defined as the following.

\[
\sum_i \sum_{j \in S_i} |x_{ij} \nabla_{x_{ij}} l(w)| \tag{30}\]
Finally, the objective function of adversarial dropout is re-organized.

\[ l_{AdD}(w) = l(w) + \sum_{i} \sum_{j \in S_i} |x_{ij} \nabla_{x_{ij}} l(w)| + w^T \Gamma_{AdD} w, \]

(31)

where \( S_i = \{ j | \epsilon_{ij}^{adv} = 0 \} \) and \( \Gamma_{AdD} = \sum_i ((1 - \epsilon_i^{adv}) \odot x_i)T ((1 - \epsilon_i^{adv}) \odot x_i) \).