Augmented Self-paced Learning with Generative Adversarial Networks

Xiao-Yu Zhang[1], Shupeng Wang[1*], Yanfei Lv[2*], Peng Li[3*], and Haiping Wang[1]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China
[3] China University of Petroleum (East China), Qingdao, China
[*] *Corresponding authors*
zhangxiaoyu@iie.ac.cn

Abstract. Learning with very limited training data is a challenging but typical scenario in machine learning applications. In order to achieve a robust learning model, on one hand, the instructive labeled instances should be fully leveraged; on the other hand, extra data source need to be further explored. This paper aims to develop an effective learning framework for robust modeling, by naturally combining two promising advanced techniques, i.e. generative adversarial networks and self-paced learning. To be specific, we present a novel augmented self-paced learning with generative adversarial networks (ASPL-GANs), which consists of three component modules, i.e. a generator G, a discriminator D, and a self-paced learner S. Via competition between G and D, realistic synthetic instances with specific class labels are generated. Receiving both real and synthetic instances as training data, classifier S simulates the learning process of humans in a self-paced fashion and gradually proceeds from easy to complex instances in training. The three components are maintained in a unified framework and optimized jointly via alternating iteration. Experimental results validate the effectiveness of the proposed algorithm in classification tasks.

Keywords: Self-paced Learning, Generative Adversarial Networks, Joint Optimization, Dynamic Curriculum.

1 Introduction

With the evolution of devices and techniques for information creation, acquisition and distribution, all sorts of digital data emerge remarkably and have been enriching people's everyday life. In order to manipulate the large scale data effectively and efficiently, machine learning models need to be developed for automatic content analysis and understanding [1][2]. The learning performance of a data-driven model is largely dependent on two key factors [3][4], i.e. the number and quality of the training data, and the modeling strategy designed to explore the training data. On one hand, the acquisition of labeled instances requires intensive human effort from manual labeling. As

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39

a result, the accessible training data are usually very limited, which inevitably jeopardize the learning performance. On the other hand, the inference of projection function from the training data is a process that mimics human perception of the world. To bridge the gap between low-level features and high-level concepts, the sophisticated mechanism behind the learning process of humans should be formulated into the model [5]-[7].

The idea of automatically generating extra instances as extension of the limited training data is rather attractive, because it is relatively a much more cost-effective way to collect a large number of instances. As a deep learning [8]-[10] method for estimating generative models based on game theory, generative adversarial networks (GANs) [11] have aroused widespread academic concern. The main idea behind GANs is a minimax two-player game, in which a generator and a discriminator are trained simultaneously via an adversarial process with conflicting objectives. After convergence, the GANs model is capable of generating realistic synthetic instances, which have great potential as augmentation to the existing training data. As for the imitation of learning process of humans, self-paced learning (SPL) [12][13] is a recently rising technique following the learning principle of humans, which starts by learning easier aspects of the learning task, and then gradually takes more complex instances into training. The easiness of an instances is highly related to the loss between ground truth and estimation, based on which the curriculum is dynamically constructed and the training data are progressively and effectively explored.

In this paper, we propose a novel augmented self-paced learning with generative adversarial networks (ASPL-GANs) algorithm to cope with the issues of training data and learning scheme, by absorbing the powers of two promising advanced techniques, i.e. GANs and SPL. In brief, our framework consists of three component modules: a generator G, a discriminator D, and a self-paced learner S. To extend the limited training data, realistic synthetic instances with predefined labels are generated via G vs. D rivalry. To fully explore the augmented training data, S dynamically maintains a curriculum and progressively refines the model in a self-paced fashion. The three modules are jointly optimized in a unified process, and a robust model is achieve with satisfactory experimental results.

2 Augmented Self-paced Learning with GANs

In the text that follows, we let $\boldsymbol{x}$ denote an instance, and a C-dimensional vector $\boldsymbol{y} = [y_1, \dots, y_C]^T \in \{0,1\}^C$ denote the corresponding class label, where C is the number of classes. The ith element y_i is a class label indicator, i.e. $y_i = 1$ if instance $\boldsymbol{x}$ falls into class i, and $y_i = 0$ otherwise. $D(\boldsymbol{x})$ is a scalar indicating the probability that $\boldsymbol{x}$ comes from real data. $S(\boldsymbol{x})$ is a C-dimensional vector whose elements indicate the probabilities that $\boldsymbol{x}$ falls into the corresponding classes.

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39

2.1 Overview

The framework and architecture of ASPL-GANs is illustrated in Fig. 1, which consists of three components, i.e. a generator G, a discriminator D and a self-paced learner S. The generator G produces synthetic instances that fall into different classes. The discriminator D and the self-paced learner S are both classifiers: the former is a binary classifier that distinguishes the synthetic instances from the real ones, and the latter is a multi-class classifier that categorizes the instances into various classes. By competing with each other, G generates more and more realist synthetic instances, and meanwhile D's discriminative capacity is constantly improved. As a self-paced learner, S embraces the idea behind the learning process of humans that gradually incorporates easy to more complex instances into training and achieves robust learning model. Moreover, the synthetic instances generated by G are leveraged to further augment the classification performance. The three components are jointly optimized in a unified framework.

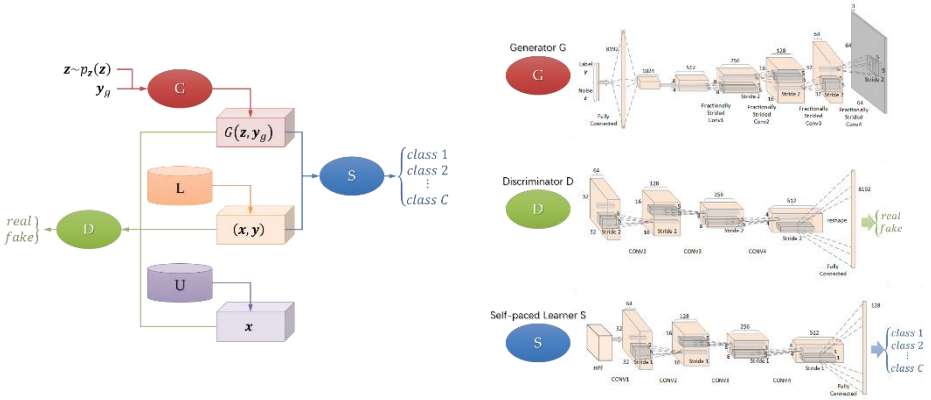


Fig. 1. The framework (left) and architecture (right) of ASPL-GANs.

2.2 Formulation

Firstly, based on the two classifiers in ASPL-GANs, i.e. D and S, we formulate two classification losses on an instance $\boldsymbol{x}$, i.e. ℓ_d and ℓ_s, as follows.

$$\begin{aligned}\ell_d(\boldsymbol{x}) &= -I(\boldsymbol{x}\in\mathcal{X})\log\big(P(\text{source}(\boldsymbol{x})=real|\boldsymbol{x})\big)\\ &\quad -I\big(\boldsymbol{x}\in\mathcal{X}_{syn}\big)\log\big(P(\text{source}(\boldsymbol{x})=synthetic|\boldsymbol{x})\big)\\ &= -I(\boldsymbol{x}\in\mathcal{X})\log\big(D(\boldsymbol{x})\big)-I\big(\boldsymbol{x}\in\mathcal{X}_{syn}\big)\log\big(1-D(\boldsymbol{x})\big)\end{aligned} \tag{1}$$

$$\begin{aligned}\ell_s(\boldsymbol{x}) &= -\textstyle\sum_{i=1}^{C} I(y_i=1)\log\big(P(y_i=1|\boldsymbol{x})\big)\\ &= -\boldsymbol{y}^T\log\big(S(\boldsymbol{x})\big)\end{aligned} \tag{2}$$

where $\mathcal{X}$ and $\mathcal{X}_{syn}$ denote the collection of real and synthetic instances, respectively. Note that $\mathcal{X}$ is divided into labeled and unlabeled subsets according to whether or not the instances' labels are revealed, i.e. $\mathcal{X}=\mathcal{X}_L\cup\mathcal{X}_U$, whereas $\mathcal{X}_{syn}$ can be regarded as

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39

"labeled" because in the framework the class label is already predefined before a synthetic instance is generated. The indicator function is defined as:

$$I(condition) = \begin{cases} 1, & condition = true \\ 0, & condition = false \end{cases} \tag{3}$$

ℓ_d depicts the consistency between the real source and the predicted source of an instance, whereas ℓ_s measures the consistency between the real class label and the predicted label of an instance. Based on (1) and (2), the three component modules of ASPL-GANs, i.e. G, D and S, can be formulated according to their corresponding objectives, respectively.

Generator G. In ASPL-GANs, by jointly taking a random noise vector $\boldsymbol{z}\sim p_{noise}$ and a class label vector $\boldsymbol{y}_g \in \{0,1\}^C$ as input, G aims to generate a synthetic instance $x_g = G(z, \boldsymbol{y}_g)$ that is hardly discernable from the real instances and meanwhile consistent with the given class label. The loss function for G is formulated as:

$$\begin{aligned} \mathcal{L}_G &= \sum_{x_g \in \mathcal{X}_{syn}} \left(-\ell_d(\boldsymbol{x}_g) + \alpha \ell_s(\boldsymbol{x}_g) \right) \\ &= \sum_{\boldsymbol{z}\sim p_{noise}} \left(\log\left(1 - D\left(G(z, \boldsymbol{y}_g)\right)\right) - \alpha \boldsymbol{y}_g^T \log\left(S\left(G(z, \boldsymbol{y}_g)\right)\right)\right) \end{aligned} \tag{4}$$

The first term in the summation encourages the synthetic instances that are inclined to be mistakenly identified with low discriminative probabilities from D. The second term, however, is in favor of the synthetic instances that fall into the correct categories with their given class labels on generation. α is the parameter to balance the two items.

Discriminator D. Similar to the classic GANs, D receives both real and synthetic instances as input and tries to correctly distinguish the synthetic instances from the real ones. The loss function for D is formulated as:

$$\begin{aligned} \mathcal{L}_D &= \sum_{\boldsymbol{x} \in \mathcal{X} \cup \mathcal{X}_{syn}} \ell_d(\boldsymbol{x}) \\ &= -\sum_{\boldsymbol{x} \in \mathcal{X}} \log\left(D(\boldsymbol{x})\right) - \sum_{\boldsymbol{z}\sim p_{noise}} \log\left(1 - D\left(G(z, \boldsymbol{y}_g)\right)\right) \end{aligned} \tag{5}$$

D aims to maximize the log-likelihood that it assigns input to the correct source. For the real instances, both labeled and unlabeled one are leveraged in modeling D, because their specific class labels are irrelevant to the fact that they are real.

Self-paced Learner S. Different from the traditional self-paced learning model, S receives both real and synthetic instances as training data. In other words, S is trained on dataset $\mathcal{X}_L \cup \mathcal{X}_{syn}$, and aims to correctly classify . The training data are organized adaptively w.r.t their easiness, and the model learns gradually from the easy instances to the complex ones in a self-paced way. The loss function for S is formulated as:

$$\mathcal{L}_S = \sum_{\boldsymbol{x} \in \mathcal{X}_L \cup \mathcal{X}_{syn}} \left(v(\boldsymbol{x}) u(\boldsymbol{x}) \ell_d(\boldsymbol{x}) + f(v(\boldsymbol{x}), \lambda) \right) \tag{6}$$

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39

where

$$u(\boldsymbol{x}) = \begin{cases} 1, & \boldsymbol{x} \in \mathcal{X}_L \\ \gamma D(\boldsymbol{x}), & \boldsymbol{x} \in \mathcal{X}_{syn} \end{cases} \tag{7}$$

is a weight to penalize the fake training data, and $v(\boldsymbol{x})$ is the weight reflecting the instance's importance in the objective. Based on (6) and (7), the loss function can be re-whitened as:

$$\begin{aligned} \mathcal{L}_S &= \sum_{\boldsymbol{x}\in\mathcal{X}_L}\big(v(\boldsymbol{x})\ell_d(\boldsymbol{x}) + f(v(\boldsymbol{x}),\lambda)\big) \\ &\quad + \sum_{\boldsymbol{x}_g\in\mathcal{X}_{syn}}\Big(\gamma v(\boldsymbol{x}_g)D(\boldsymbol{x}_g)\ell_d(\boldsymbol{x}_g) + f\big(v(\boldsymbol{x}_g),\lambda\big)\Big) \\ &= \sum_{\boldsymbol{x}\in\mathcal{X}_L}\Big(-v(\boldsymbol{x})\boldsymbol{y}^T\log\big(S(\boldsymbol{x})\big) + f(v(\boldsymbol{x}),\lambda)\Big) \\ &\quad + \sum_{\boldsymbol{z}\sim p_{noise}}\begin{pmatrix} -\gamma v\left(G(z,\boldsymbol{y}_g)\right)D\left(G(z,\boldsymbol{y}_g)\right)\boldsymbol{y}^T\log\left(S\left(G(z,\boldsymbol{y}_g)\right)\right) \\ +f\left(v\left(G(z,\boldsymbol{y}_g)\right),\lambda\right) \end{pmatrix} \end{aligned} \tag{8}$$

where $f(v,\lambda)$ is the self-paced regularizer, where λ is the pace age parameter controlling the learning pace. Given λ, the easy instances (with smaller losses) are preferred and leveraged for training. By jointly learning the model parameter $\boldsymbol{\theta}_S$ and the latent weight $\boldsymbol{v}$ with gradually increasing λ, more instances (with larger losses) can be automatically included. In this self-paced way, the model learns from easy to complex to become a "mature" learner. S effectively simulates the learning process of intelligent human learners, by adaptively implementing a learning scheme embodied as weight $v(\boldsymbol{x})$ according to the learning pace. Apart from the real ones, the synthetic instances are leveraged as extra training data to further augment the learning performance. Prior knowledge is encoded as weight $u(\boldsymbol{x})$ imposed on the training instances. Under this mechanism, both predetermined heuristics and dynamic learning preferences are incorporated into an automatically optimized curriculum for robust learning.

3 Experiments

To validate the effectiveness of ASPL-GANs, we apply it to classification of handwritten digits and real-world images respectively. Detailed description of the datasets can be found in [2].

The proposed ASPL-GANs is compared with the follow methods:

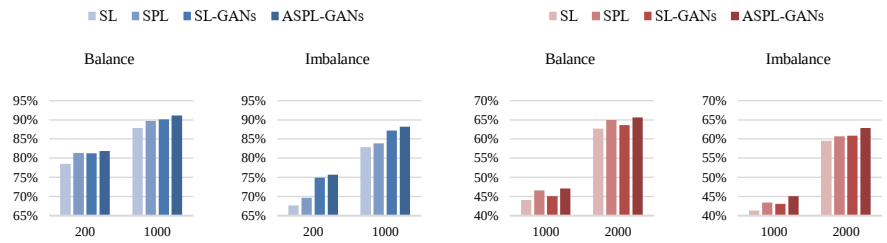
- SL: traditional supervised learning based on labeled dataset $\mathcal{X}_L$;
- SPL: self-paced learning based on labeled dataset $\mathcal{X}_L$;
- SL-GANs: supervised learning with GANs based on labeled dataset $\mathcal{X}_L$ and synthetic dataset $\mathcal{X}_{syn}$.

Softmax regression, also known as multi-class logistic regression, is adopted to classify the images. To be fair, all the methods have access to the same number of labeled real instances. We use two distributions to determine the numbers per class. One is uniform distribution according to which the labeled instances are equally divided be-

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39

tween classes. The other is Gaussian distribution in which the majority of labeled instances falls into only a few classes. The two settings simulate the balance and imbalance scenario of training data. For methods leveraging augmented training data, synthetic instances falling into the minority classes are inclined to be generated to alleviate the data imbalance problem.

Fig. 2 illustrates the classification results of SL, SPL, SL-GANs and ASPL-GANs on both handwritten digit and real-world image datasets. The horizontal axis shows the number of initial training data.



(1) (2)

Fig. 2. The classification accuracies on (1) handwritten digit dataset and (2) real-world image dataset.

Analysis of the experimental results are as follows.

- Traditional learning method SL is trained on the limited training data, and the training data are incorporated all at once indiscriminately. As a result, the learning performance is severely hampered.
- Both SPL and SL-GANs achieved improvement compared with SL. The former explores the limited training data in a more effective way, whereas the latter leverages extra training data via GANs. As we can see, SL-GANs is especially helpful for simpler dataset such as the handwritten digit dataset, because the generated instances can be more reliable. In contrast, the synthetic real-world images is less realistic, and thus less helpful in augmenting the learning performance. SPL successfully simulates the process of human cognition, and thus achieved consistent improvement for both datasets, especially for the balance scenario. The problem of data imbalance can be alleviated by generating minority instances.
- The proposed ASPL-GANs achieved the highest classification accuracy among all the methods. By naturally combination of GANs and SPL, the problem of insufficient training data and ineffective modeling are effectively addressed.

4 Conclusion

In this paper, we have proposed the augmented self-paced learning with generative adversarial networks (ASPL-GANs) to address the issues w.r.t. limited training data and unsophisticated learning scheme. The contributions of this work are three-fold. Firstly, we developed a robust learning framework, which consists of three component modules formulated with the corresponding objectives and optimized jointly in a unified process

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39

to achieve improved learning performance. Secondly, realistic synthetic instance with predetermined class labels are generated via competition between the generator and discriminator to provide extra training data. Last but not least, both real and synthetic are incorporated in a self-paced learning scheme, which integrates prior knowledge and dynamically created curriculum to fully explore the augmented training dataset. Encouraging results are received from experiments on multiple classification tasks.

5 Acknowledgement

This work was supported by National Natural Science Foundation of China (Grant 61501457, 61602517), Open Project Program of National Laboratory of Pattern Recognition (Grant 201800018), Open Project Program of the State Key Laboratory of Mathematical Engineering and Advanced Computing (Grant 2017A05), and National Key Research and Development Program of China (Grant 2016YFB0801305).

References

1. Bishop C. Pattern Recognition and Machine Learning (Information Science and Statistics), 1st edn. 2006. corr. 2nd printing edn. Springer, New York. 2007.
2. Zhang XY, Wang S, Yun X. Bidirectional active learning: a two-way exploration into unlabeled and labeled data set. IEEE Transactions on Neural Networks and Learning Systems. 2015 Dec; 26(12):3034-3044.
3. Zhang XY. Simultaneous optimization for robust correlation estimation in partially observed social network. Neurocomputing. 2016 Sep 12; 205:455-462.
4. Zhang XY, Wang S, Zhu X, Yun X, Wu G, Wang Y. Update vs. upgrade: Modeling with indeterminate multi-class active learning. Neurocomputing. 2015 Aug 25; 162:163-70.
5. Zhang X, Xu C, Cheng J, Lu H, Ma S. Effective annotation and search for video blogs with integration of context and content analysis. IEEE Transactions on Multimedia. 2009 Feb;11(2):272-85.
6. Liu Y, Zhang X, Zhu X, Guan Q, Zhao X. Listnet-based object proposals ranking. Neurocomputing. 2017 Dec 6;267:182-94.
7. Zhang X. Interactive patent classification based on multi-classifier fusion and active learning. Neurocomputing. 2014 Mar 15;127:200-5.
8. LeCun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015 May 28; 521(7553):436-444.
9. Bengio Y, Courville A, Vincent P. Representation learning: A review and new perspectives. IEEE Transactions on PAMI. 2013 Aug; 35(8):1798-1828.
10. Xu G, Wu HZ, Shi YQ. Structural design of convolutional neural networks for steganalysis. IEEE Signal Processing Letters. 2016 May; 23(5):708-712.
11. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y. Generative adversarial nets. In: Advances in Neural Information Processing Systems 2014 (pp. 2672-2680).
12. Meng D, Zhao Q, Jiang L. What objective does self-paced learning indeed optimize?. arXiv preprint arXiv:1511.06049. 2015 Nov 19.
13. Kumar MP, Packer B, Koller D. Self-paced learning for latent variable models. In: Advances in Neural Information Processing Systems 2010 (pp. 1189-1197).

ICCS Camera Ready Version 2018
To cite this paper please use the final published version:
DOI: 10.1007/978-3-319-93713-7_39