Basic literature review about machine learning

Machine learning is a process that train the program to process a set of raw data in order to learn the empirical pattern behind, and later be able to judge or make proper decision according to similar type of data. It is the core of artificial intelligence.

One of the classification standard is whether and how human supervise the training. There're supervised, unsupervised, semisupervised, and reinforcement learning.

Supervised learning is the most common category in machine learning. It uses data containing an input and its desired output, called label. There may be many features containing in the input, and what the machine should do is to adjust the "weight" for every feature and deduce the error of the calculated outputs by means of calculating gradient vector or others. For example, we give a set of meteorological data together with whether condition to let the machine learn to judge whether it will rain or not according to current data.

On the other hand, unsupervised learning will have no label. The machine learn itself. *It always uses clustering algorithm and visualization algorithms.* Some typical application scenarios are dimensionality reduction, anomaly detection and rule learning. For example, the machine may find that the one who buys chip will be very possible to buy soft drinks together, so the supermarket could place them close.

Semisupervised learning has most of data unlabeled and few of them labeled. Most semisupervised learning algorithms are a combination of supervised and unsupervised algorithms.

Reinforcement learning allows the machine to try everything it can in a certain environment, and gives reward or penalty accordingly. The machine would try to find out the best strategy that could maximize the reward. For example, a lot of robots use reinforcement learning to learn how to walk. AlphaGo also uses this learning method.

Normal machine learning algorithms includes linear regression, logistic regression, naive Bayesian classification, support vector machine, ensemble methods and so on. When it goes deeper to deep learning, the neural network is widely used. Convolutional neural network is one of the most advanced and popular algorithms at present. Other includes recurrent neural Network, long short-term memory and so on. Up to now, these algorithms are so developed and complicated that the adjustable weighs or the layers in neural networks could be hundreds or thousands.

There might be some problem that you should concern when applying machine learning. First is insufficient quantity of training data. Even the most simple task would expect thousands of trainings, while complicated ones would need millions. Second is overfitting. The learned model may fit well to the training data, but cannot generalize well. Another problem is non-representative data. To avoid this, the training data set should be carefully chosen that could represent the cases you want to generalize to. Other challenges include irrelevant data poor quality data and so on.

Currently, machine learning techniques are so widely used, and it seems that anything combining with machine learning will make a breakthrough. It has made great contribution to medical, biological, data analysis, recognition, image processing fields. Deep learning is the most popular category currently, and Enda Wu predict that transfer learning may be the future focus. Python is the most common framework and it has already developed a lot of mature libraries. As NVIDIA made large investment into machine learning, GPU based system is now able to greatly accelerate the training process.

There're still some potential challenges, or in other words, future development orientation. First, after retrained with a new set of data, the performance of the model may decrease on previous test data. Besides, machine needs thousands of millions of training to recognize apple, while human baby may need only few times of training. That means machine still works in a much different and less efficient way than human brain. In addition, the safety is also an issue. Attacker may let the machine completely misjudge or steal the customer data or model by importing some special input.

Goodfellow, Ian J., et al. "An empirical investigation of catastrophic forgetting in gradient-based neural networks." *arXiv preprint arXiv:1312.6211*. 2013.

Hazra, Abhishek, Prakash Choudhary, and M. Sheetal Singh. "Recent Advances in Deep Learning Techniques and Its Applications: An Overview." *Advances in Biomedical Engineering and Technology*: 103-122.

LeCun, Y., et al. "Deep learning." Nature 521(7553): 436-444. 2015.

Mitchell, Tom. "Introduction to machine learning." *Machine Learning* 7 : 2-5. 2016.

Tramèr, Florian, et al. "Stealing machine learning models via prediction apis." *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 2016.