

ИССЛЕДОВАНИЕ МЕТОДОВ ОБУЧЕНИЯ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ПРИ НАЛИЧИИ НЕВЕРНО РАЗМЕЧЕННЫХ ДАННЫХ

Мещеряков Алексей Олегович

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: s02190151@gse.cs.msu.ru

Научный руководитель — Буряк Дмитрий Юрьевич

Для тренировки сверточных нейронных сетей для распознавания изображений требуются большие выборки размеченных обучающих данных. Такие выборки обычно размечаются людьми, но это не может гарантировать полностью правильную разметку объектов на изображениях — согласно исследованиям [1], средняя человеческая ошибка на наборе данных ImageNet составляет 5%, что больше ошибки современных сетей. Сверточные сети не устойчивы к ответам-шумам, поэтому точность разметки сильно влияет на качество модели. В таких условиях для улучшения качества сетей необходимы алгоритмы, которые могут справляться с шумом в обучающих выборках.

Целью данной работы является проведение исследования эффективности современных подходов к решению задачи обучения сверточных нейросетей на данных, содержащих ошибки в метках классов. Алгоритмы для решения этой задачи можно поделить на три группы [5]:

1) Методы, отбирающие достоверные образцы, и обучающие сеть только на этих данных. Примером таких методов является DivideMix [3].

2) Методы, исправляющие метки. Они пытаются найти в выборке неверные метки и исправить их на правильные. Примером является алгоритм PENCIL [3].

3) Методы, использующие устойчивые к неправильным меткам классы функции потерь при обучении [4].

Для исследования был выбран алгоритм обучения из 2 группы REED [5]. Это один из последних опубликованных алгоритмов, выбор обоснован тем что в статье приводились лучшие относительно других алгоритмов результаты.

REED состоит из 3 этапов:

1) На первом этапе обучение нейросети проводится методом обучения без учителя, когда сети предоставляют данные без ответов.

2) Полученная сеть переобучается на размеченных данных и используется чтобы определить, какие данные из набора являются ошибочно размеченными. Для этой цели данные кластеризуются на основе распределения значений функции потерь с помощью двухкомпонентных Гауссовых смесей распределений (GMM)."

3) На третьем этапе сеть повторно обучается на заново размеченных метках путем полуконтролируемого обучения — метода, при котором только часть данных имеет обучающую разметку. В данном случае, те данные, которые были признаны верными на втором этапе, будут размечены, а метки зашумленных данных будут убраны.

В рамках данной работы особое внимание было уделено исследованию эффективности этапа детектирования ошибочных меток и их коррекции.

Для испытаний были выбраны следующие наборы данных: FASHION-MNIST (набор изображений одежды); CIFAR 10, 100 (наборы изображений различных предметов из 10 и 100 классов соответственно); EMNIST — набор изображений букв

В ходе тестов было обнаружено возможное улучшение алгоритма — в случаях, когда процент шума в выборке составляет менее 50% предварительный процесс “warm up” сверточной сети на втором этапе, следуя [2], позволяет увеличить точность разбиения данных на 2-5%.

Результаты проверки эффективности этапа выделения и коррекции неправильных меток показаны на рисунке 1. На графиках сравниваются результаты алгоритма REED на базе сети resnet18 с 5 эпохами самообучения на первом этапе и 5 эпохами переобучения на втором и результаты сети без применения и с частичным применением метода. По оси X - процент зашумления выборки, шум симметричный (для любой неправильной метки из выборки вероятность принадлежности любому классу, кроме верного, одинакова). Используемые метрики:

Assiguasy — отношение количества верно предсказанных меток ко всем меткам в наборе данных.

Точность (precision) — отношение правильно предсказанных положительных наблюдений к общему количеству предсказанных положительных наблюдений

Чувствительность (recall) — отношение правильно предсказанных положительных наблюдений ко всем наблюдениям в реальном классе

F1 — средневзвешенное значение точности и чувствительности.

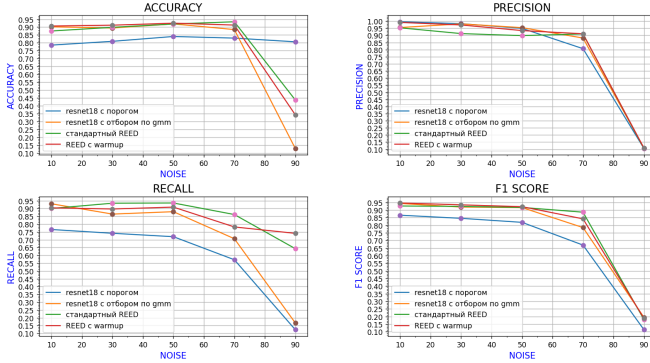


Рис. 1. Сравнительные графики методов: 1) стандартный алгоритм обучения — данные считались верными, если класс с максимальной предсказанной вероятностью совпадал с ответом. 2) стандартный алгоритм обучения, для отбора использован метод GMM, как во втором этапе REED 3) алгоритм REED 4) Улучшение REED с помощью WarmUp

Исходя из полученных данных можно утверждать о преимуществе REED перед стандартными методами обучения сверточных нейросетей при наличии в данных ошибок. Если количество ошибок оценивается менее чем в половину выборки, применение WarmUp к полученной сети позволяет получить лучшую точность.

Работа выполнялась при поддержке гранта РФФИ № 20-07-01053 А.

Литература

1. Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification <https://arxiv.org/abs/1502.01852>
2. Junnan Li, Richard Socher, Steven C.H. Hoi DivideMix: Learning with Noisy Labels as Semi-supervised Learning <https://arxiv.org/abs/2002.07394>
3. Kun Yi, Jianxin Wu Probabilistic End-to-end Noise Correction for Learning with Noisy Labels <https://arxiv.org/abs/1903.07788>
4. Jonathan T. Barron A General and Adaptive Robust Loss Function <https://arxiv.org/abs/1701.03077>
5. Hui Zhang, Quanming Yao Decoupling Representation and Classifier for Noisy Label Learning <https://arxiv.org/abs/2011.08145>