Проблема нейросетевых коммуникаций

М.Ю. Леонтьев^{1,2}, В.Ю. Ислентьева³, А.В. Михеев³, К.В. Святов³, С.В. Сухов^{1,3}

¹Ульяновский филиал Института радиотехники и электроники им. В.А. Котельникова РАН, Спасская 14, Ульяновск, Россия, 432011

²Научно-исследовательский технологический институт им. С.П. Капицы Ульяновского государственного университета, Университетская Набережная 1, Ульяновск, Россия, 432017

³Ульяновский государственный технический университет, Северный Венец 32, Ульяновск, Россия, 432027

Аннотация. Несмотря на успешное использование искусственных нейронных сетей (ИНС) для решения множества задач (прогнозирование, языковой перевод, распознавание изображений и голоса и т.д.), ИНС являются обособленными единицами неспособными к коммуникации и обмену какой-либо информацией. В то же время способность к коммуникации является критичной для дальнейшего развития методов искусственного интеллекта. В данной работе предложены и протестированы несколько методов коммуникации и переноса информации между ИНС. Методы не требуют наличия изначальных тренировочных данных и используют для обмена информацией только внутренние параметры сетей. Предложены как итеративные, так и неитеративные методы передачи информации. Разработанные методы показывают точность классификации на тестовых наборах данных, схожую с точностью, получаемой при использовании ансамблей нейронных сетей.

1. Введение

Способность к коммуникации между искусственными нейронными сетями (ИНС) и к объединению знаний, содержащихся в них, является критичной для дальнейшего развития методов искусственного интеллекта, развития самообучающихся систем и для организации взаимодействия интеллектуального оборудования. Однако ИНС в настоящее время являются автономными объектами, неспособными к какому-либо обмену информацией. Во многом это определяется тем, что ИНС хранят приобретенное знание распределенным образом среди миллионов внутренних параметров (весов). Такое неявное представление информации не только затрудняет ее интерпретацию, но и препятствует ее обновлению, и тем более ее обмену с другими нейронными сетями. При необходимости совместного использования знаний, содержащихся в нескольких нейронных сетях, в настоящее время существует два подхода: 1) обучение заново новой сети на объединенном наборе данных; 2) использование ансамбля сетей для генерации совместных предсказаний [1]. В определенных ситуациях оба эти подхода могут оказаться неприемлемыми: использованные при обучении данные могут стать недоступными, а поддержка ансамбля сетей может оказаться слишком ресурсоемкой. Идеальной была бы ситуация, когда сети сами могли бы делиться своими знаниями. Результатом была бы единственная сеть, которая включала бы в себя объединенное знание.

Задачу объединения знаний нескольких нейросетей можно разделить на две отдельные подзадачи: выделение информации из одной сети и внедрение этой информации в другую сеть. При этом задача выделения знаний из ИНС является актуальной для понимания их работы. Без этого понимания непредсказуемость ИНС препятствует их использованию на транспорте и в медицине. Задача внедрения информации в нейронную сеть тесно связана с проблемой катастрофической интерференции: при обучении на новой информации ИНС очень быстро теряет все знание, приобретенное прежде [2]. Таким образом, решение задачи коммуникации нейросетей может одновременно решить и другие важные проблемы машинного обучения. В то же время можно постараться найти и методы, не требующие явного выделения и внедрения знаний, а оперирующие непосредственно с параметрами сети.

Данная работа направлена на развитие методов коммуникации между нейронными сетями, а именно, на решение задачи переноса знаний из одной сети в другую без разрушения уже содержащихся в сети знаний и без необходимости доступа к использованным для обучения сетей тренировочным данным. Нами разработаны как итеративные, так и неитеративные способы решения этой задачи. Неитеративные методы позволяют организовать обмен информацией без особых затрат в вычислительном плане; итеративные методы позволяют достичь большей точности переноса.

2. Постановка задачи

Две ИНС со схожей архитектурой обучены стандартными методами (например, методом обратного распространения ошибки) задачам классификации на различных наборах данных (например, распознаванию рукописных цифр на изображениях). После обучения каждая из нейронных сетей содержит свою часть знания (например, первая ИНС успешно распознает цифры от 0 до 4, а вторая от 5 до 9). Предлагается модифицировать параметры одной из сетей (например, путем изменения значений весов) таким образом, чтобы сеть могла воспроизводить отклик обеих сетей совместно со своим прежним откликом, как если бы она изначально была натренирована на объединенном наборе данных (рисунок 1). При объединении сетей мы дополнительно предполагаем, что ранее использованные тренировочные данные более недоступны.

Для рассматриваемых в данной работе примеров мы используем унитарное (one-hot) кодирование, при котором на выходе сети активируется только один нейрон соответствующего класса. Таким образом, выходной слой объединенной сети должен быть расширен, чтобы иметь возможность кодировать полный набор классов (рисунок 1).

Нами разработаны несколько методов решения поставленной задачи, которые описаны в следующем разделе.

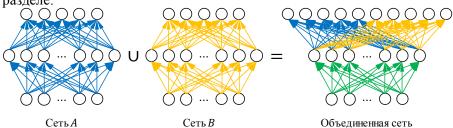


Рисунок 1. Постановка задачи по переносу знаний между нейронными сетями. Веса изначальных сетей A и B изменяются таким образом, что объединенная сеть $A \cup B$ будет способна классифицировать объединенный набор классов. Выходной слой объединенной сети соответственно расширен, чтобы иметь возможность кодировать полный набор классов.

3. Методы переноса знаний между искусственными нейронными сетями

3.1. Метод суммирования весов

Метод суммирования весов (МСВ) основан на вероятностном процессе сложения большого количества случайных величин, которыми в случае ИНС являются ее веса [3]. Веса

объединенной сети θ_F получаются путем непосредственного сложения весов объединяемых сетей A и B:

$$\boldsymbol{\theta}_F = \boldsymbol{\theta}_A + \boldsymbol{\theta}_B.$$

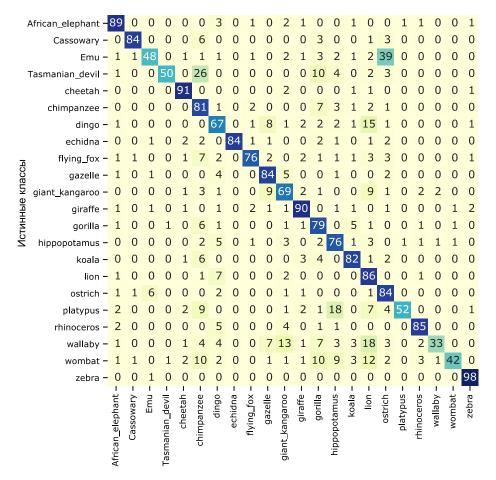
Несмотря на свою простоту, данный алгоритм приводит к довольно высокой точности классификации объединенной сети. МСВ был опробован на многослойных полносвязных сетях прямого прохождения и на глубоких сверточных сетях.

Лля объединения глубоких сетей дополнительно был использован метол «переноса обучения» (transfer learning). Согласно методу переноса обучения веса глубокой сети, обученной на одном наборе данных, можно использовать для ускорения обучения на другом наборе из сходной области [4]. Типичная архитектура глубоких сетей представляет собой сверточную часть, роль которой состоит в выделении признаков из необработанных входных данных, и полносвязный классификатор, который выполняет разделение признаков на классы. В нашем исследовании метод переноса обучения был использован для объединения знаний глубоких нейронных сетейклассификаторов, тренированных на различных наборах изображений. Процесс тренировки сверточных сетей состоял из нескольких этапов. На первом этапе для инициализации весов сверточной части использовалась сеть, обученная на большом наборе изображений, например, базе ImageNet [5]. Большой набор классов данной базы делает обученную таким образом сеть подходящим кандидатом для «переноса обучения». На втором этапе обученные сверточные части дополнялись необученными классификаторами, которые обучались различным задачам классификации (например, задачам классификации животных или городских объектов). На третьем этапе сверточная часть каждой сети подвергалась тонкой настройке (fine tuning). ведущей к изменению ее весов. В результате получался набор глубоких сетей с различным набором весов и содержащих различное знание, к которым можно было применить метод суммирования весов.

Эксперименты с полносвязными сетями проводились на наборе рукописных цифр MNIST [6]. Эксперименты показали, что ошибка классификации объединенной сети зависит от количества нейронов-узлов в скрытых слоях, количества скрытых слоев и количества нейронных сетей, знания которых объединяются. В случае двух двухслойных сетей, при увеличении количества нейронов в скрытом слое предсказательная эффективность объединенной сети приближалась к эффективности ансамбля сетей.

Эксперименты с глубокими сетями проводились на наборах изображений СІFAR-10 [7] и на отдельных классах изображений базы ImageNet. Эксперименты показали, что точность классификации объединенной сети зависит от схожести набора признаков объектов, распознаваемых изначальными сетями *А* и *В*. Так, если обе сети *А* и *В* были тренированы распознавать объекты одной категории, то объединенная сеть будет путать объекты со схожим набором признаков. На рисунке 2 показан результат объединения двух сетей в случае, когда одна сеть была натренирована распознавать африканских, а другая – австралийских животных. Объединенная сеть уверенно (с точностью порядка 90%) распознает животных с уникальными признаками, например, зебр, но путает схожих животных, живущих на разных континентах, например, эму и страусов. Средняя точность классификации объединенной сети составила 76%. Для сравнения, точность классификации того же набора классов ансамблем сетей составляет 81%.

В случае сильно отличающегося набора признаков объектов сетей А и В (например, в случае живых и неживых объектов) точность классификации объединенной сети становится выше. На рисунке 3 представлен результат объединения двух сетей в случае, когда одна сеть была натренирована распознавать африканских животных, а вторая – городские объекты. Средняя точность классификации объединенной сети в этом случае составляет 81%, что лучше, чем в предыдущем случае. Точность классификации ансамблем сетей составила 88%.



Предсказанные классы

Рисунок 2. Матрица неточностей классификации африканских и австралийских животных при объединении двух глубоких сетей методом сложения весов. Числа показывают процент классифицированных объектов соответствующей категории.

3.2 Метод эластичной консолидации весов

Второй метод, который может быть использован для объединения знаний ИНС основан на следующей идее. Если изменить веса двух ИНС А и В так, чтобы эти веса совпали при дополнительном условии, что функции потерь $L_A(\theta)$ and $L_B(\theta)$ увеличатся незначительно, то результирующая сеть будет иметь свойства обеих сетей A и B. Увеличение функции потерь будет минимальным, если мы изменим только наименее важные веса. Следуя работе [8], мы назвали этот метод методом эластичной консолидации весов (МЭКВ).

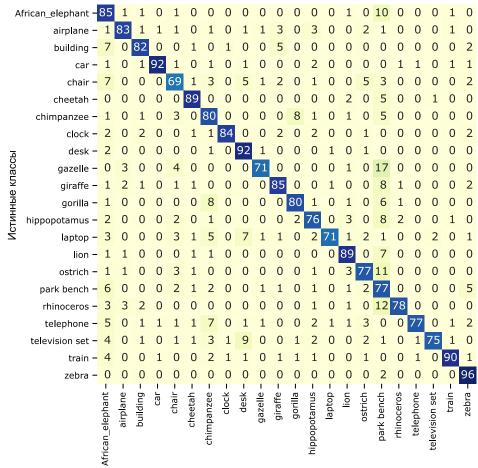
Для оценки изменения функции потерь, мы разложили ее в ряд Тейлора относительно весов

нейросети. Для сети
$$A$$
, например, это разложение выглядит следующим образом:
$$L_{A}(\boldsymbol{\theta}) \approx L(\boldsymbol{\theta}_{A}) + \sum_{i} \frac{\partial L}{\partial \theta_{i}} \bigg|_{\theta_{i} = \theta_{A,i}} \left(\theta_{i} - \theta_{A,i}\right) + \frac{1}{2} \sum_{i,j} \frac{\partial^{2} L}{\partial \theta_{i} \partial \theta_{j}} \bigg|_{\substack{\theta_{i} = \theta_{A,i} \\ \theta_{j} = \theta_{A,j}}} \left(\theta_{i} - \theta_{A,i}\right) \left(\theta_{j} - \theta_{A,j}\right). \tag{1}$$

 θ_{A} – оптимальные веса тренированной сети A, суммирование в уравнении (1) происходит по всем весам. Так как количество параметров θ_A в современных нейронных сетях достигает миллионов, вычисление и хранение полной матрицы $\partial^2 L/(\partial \theta_i \partial \theta_i)$ современными техническими средствами невозможно. В соответствие с этим, мы аппроксимировали полную матрицу ее диагональной частью [8]:

$$L_A(\boldsymbol{\theta}) \approx \frac{1}{2} \sum_i F_{A,i} \left(\theta_i - \theta_{A,i} \right)^2,$$
 (2)

где $F_{A,i} \equiv \partial^2 L_A/\partial \theta_i^2$. Выражения аналогичные (1) и (2) записываются и для сети B. Коэффициенты $F_{A,i}$, $F_{B,i}$ в уравнении (2) выражают важность весов $\theta_{A,i}$, $\theta_{B,i}$ и обычно должны быть вычислены заранее на этапе обучения сети.



Предсказанные классы

Рисунок 3. Матрица неточностей классификации африканских животных и городских объектов при объединении двух глубоких сетей методом сложения весов. Числа показывают процент классифицированных объектов соответствующей категории.

Набор весов объединенной сети, который минимизирует суммарную функцию потерь $L_F =$ L_A+L_B можно рассчитать по следующей формуле: $\theta_{F,i}=\frac{F_{A,i}\theta_{A,i}+F_{B,i}\theta_{B,i}}{F_{A,i}+F_{B,i}}.$

$$\theta_{F,i} = \frac{F_{A,i}\theta_{A,i} + F_{B,i}\theta_{B,i}}{F_{A,i} + F_{B,i}}.$$
 (3)

В принципе, уравнение (3) решает поставленную задачу объединения двух ИНС. Однако, для ИНС тренированных независимо, их веса θ_A , θ_B не обязательно расположены вблизи друг друга, и разложение (1) может оказаться недостаточным. Для того, чтобы приблизить значения весов θ_A и θ_B , мы производили «выравнивание» сетей, решая задачу о назначениях [9] и определяя расположение нейронов в скрытых слоях, минимизирующее L_F .

Несмотря на большую вычислительную сложность, в экспериментах МЭКВ показал эффективность схожую с МСВ. Это говорит о том, что неитеративные методы фундаментально ограничены в достижении высокой точности классификации, и для достижения большей эффективности нужны методы, которые активно выделяют признаки, отличающие объекты разных классов сетей A и B. Такие методы могут быть развиты на основе генеративных подходов.

3.3 Генеративные методы

В последние годы были разработаны нейронные сети, которые сами могут воспроизводить данные, сходные по типу и по вероятностному распределению с тренировочными. Одним из видов подобных сетей являются генеративно-состязательные сети (ГСС) [10]. ГСС успешно используются при генерации изображений, предсказания видео и в других приложениях. Другим типом генеративных нейронных сетей может служить вариационный авто-кодировщик (ВАК) [11]. ВАК старается воспроизвести на выходе тот же самый сигнал, что подается на вход. Отличие от обычных авто-кодировщиков состоит в том, что входной сигнал сначала переводится в случайную переменную, которая выбирается из определенного (обычно нормального) распределения.

Генерация входных данных может быть достигнута и в обычных сетях прямого прохождения при использовании байесовских методов. Байесовское обучение нейронной сети с определенным количеством шума позволяет получить образцы из апостериорной функции вероятности [12], которые и представляют собой искусственные тренировочные данные. Эти сгенерированные данные можно затем использовать для передачи информации между нейронными сетями. Существует мнение, что схожие вероятностные вычисления выполняются и в системах мозга. В частности, было показано, что популяции нейронов вычисляют не только наиболее оптимальные стимулы, но вероятность их распределения [13].

В нашем исследовании мы разработали и опробовали вероятностные методы восстановления апостериорной функции вероятности распределения исходных данных при известных параметрах нейронной сети. Для восстановления функции вероятности были использованы стохастические методы, основанные на методе Монте Карло с использованием динамики Ланжевена [12] или гамильтоновой динамики [14]. При этом, эффективность объединенной сети определяется точностью аппроксимации вероятности распределения исходных данных.

4. Заключение

В данной работе мы показали принципиальную возможность переноса информации между нейронными сетями без доступа к первоначальным тренировочным данным. Разработанные методы пригодны как для полносвязных, так и для глубоких сверточных сетей прямого прохождения. Методы были протестированы на задачах классификации изображений с использованием общедоступных баз данных.

Неитеративные методы объединения знаний нейросетей (метод суммирования весов и метод эластичной консолидации весов) демонстрируют возможность быстрого объединения знаний сетей. При этом точность классификации объединенной сети сильно зависит от схожести признаков классов объединяемых сетей: точность классификации возрастает при объединении сетей со знанием из разных областей. Точность объединенной сети, полученной с помощью МСВ и МЭКВ, сходна с точностью классификации ансамблем сетей.

Генеративные итеративные методы являются более медленными для передачи знаний между нейросетями, но потенциально они могут увеличить аккуратность классификации и достигнуть точности, сопоставимой с точностью нейронной сети, изначально тренированной на всем объеме данных.

В данной работе мы рассмотрели примеры объединения знаний двух нейронных сетей, однако предложенные методы допускают простое обобщение на случай нескольких сетей и на случай сетей с различной архитектурой.

Помимо преодоления ограничений в сфере машинного обучения, развитие методов коммуникации нейронных сетей в перспективе будет полезно в том числе и в совершенно других областях таких, как, например, медицина - для развития методов нейро-протезирования и понимания работы биологических нейронных сетей (сетей мозга).

5. Литература

[1] Li, H. Research and development of neural network ensembles: a survey / H. Li, X. Wang, S. Ding // Artificial Intelligence Review. – 2018. – Vol. 49(4). – P. 455-479.

- [2] McCloskey, M. Catastrophic interference in connectionist networks: The sequential learning problem / M. McCloskey, N.J. Cohen // Psychology of learning and motivation. Academic Press. 1989. Vol. 24. P. 109-165.
- [3] Akhlaghi, M.I. Knowledge Fusion in Feedforward Artificial Neural Networks / M.I. Akhlaghi, S.V. Sukhov // Neural Processing Letters. 2018. Vol. 48(1). P. 257-272.
- [4] Pan, S.J. A survey on transfer learning / S.J. Pan, Q. Yang // IEEE Transactions on knowledge and data engineering. 2010. Vol. 22(10). P. 1345-1359.
- [5] Russakovsky, O. Imagenet large scale visual recognition challenge / O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, A.C. Berg // International Journal of Computer Vision. 2015. Vol. 115(3). P. 211-252.
- [6] LeCun, Y. Gradient-based learning applied to document recognition / Y. Lecun, L. Bottou, Y. Bengio, P. Haffner // Proceedings of the IEEE. 1998. Vol. 86(11). P. 2278-2324.
- [7] Krizhevsky, A. Learning multiple layers of features from tiny images / A. Krizhevsky, G. Hinton. Technical report, University of Toronto, 2009. Vol. 1(4). P. 7.
- [8] Pascanu, R. Overcoming catastrophic forgetting in neural networks / R. Pascanu, N. Rabinowitz, J. Veness, G. Desjardins, A.A. Rusu // Proceedings of the National Academy of Sciences. 2017. Vol. 114(13). P. 3521-3526.
- [9] Taha, H.A. Operations Research: An Introduction (10th Edition). Pearson, 2016. 848 p.
- [10] Goodfellow, I. Generative adversarial nets / I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, Y. Bengio // Advances in neural information processing systems. 2014. P. 2672-2680.
- [11] Kingma, D.P. Stochastic gradient VB and the variational auto-encoder / D.P. Kingma, M. Welling // Second International Conference on Learning Representations, 2014.
- [12] Welling, M. Bayesian learning via stochastic gradient Langevin dynamics / M. Welling, Y.W. Teh // Proceedings of the 28th International Conference on Machine Learning (ICML-11), 2011. P. 681-688.
- [13] Ma, W.J. Bayesian inference with probabilistic population codes / W.J. Ma, J.M. Beck, P.E. Latham, A. Pouget // Nature Neuroscience. 2006. Vol. 9(11). P. 1432.
- [14] Neal, R. MCMC using Hamiltonian dynamics // Handbook of Markov Chain Monte Carlo. 2011. Vol. 2(11). P. 2.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ и Правительства Ульяновской области в рамках научного проекта № 18-47-732006.

The problem of neural networks communication

M.Iu. Leontev^{1,2}, V.Iu. Islenteva³, A.V. Mikheev³, K.V. Sviatov³, S.V. Sukhov^{1,3}

¹Kotel'nikov Institute of Radio Engineering and Electronics of Russian Academy of Sciences (Ulyanovsk branch), Spasskaya Str.14, Ulyanovsk, Russia, 432011 ²S.P. Kapitsa Research Institute of Technology (Technological Research Institute) of Ulyanovsk State University, Universitetskaya Naberejnaya, Ulyanovsk, Russia, 432000 ³Ulyanovsk State Technical University, Severny Venets 32, Ulyanovsk, Russia, 432027

Abstract. In spite of successful application of artificial neural networks (ANNs) for the solution of multiple problems (forecasting, language translation, classification of images, voice recognition etc.), ANNs are still autonomous units incapable of communication or exchange of information. In the meantime, the ability to communicate for artificial neural networks is critical for further development of methods of artificial intelligence. In this work we propose and test several methods of communication and information exchange between ANNs. These methods do not require the presence of initial training data and use only internal parameters of ANNs to perform information exchange. We propose both iterative and non-iterative methods of communication. The developed methods show the classification accuracy similar to that provided by an ensemble of ANNs.