

АНОТАЦІЯ

Баранов М.В. Використання технік навчання нейронних мереж на малому наборі даних для адаптації моделі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки». - Львівський національний університет імені Івана Франка, Львів, 2025.

Штучні нейронні мережі є універсальним та високоефективним інструментом для розв'язання широкого спектру завдань, особливо тих, для яких розробка безпосередніх алгоритмів виявляється складним та досить трудомістким процесом. Моделі, що базуються на принципах функціонування нейронних мереж, встановлюють складну статистичну залежність між вхідними даними, що подаються до моделі, та очікуваними результатами, які ця модель повинна генерувати. Завдяки використанню спеціальних алгоритмів навчання, отримані в результаті цього процесу моделі стають здатними розв'язувати такі задачі, які формально та чітко описати за допомогою математичних формул було б практично неможливо або вкрай складно.

Побудова прямих алгоритмів для вирішення конкретної задачі людиною зазвичай вимагає глибокого інтелектуального аналізу наявних даних, що базується на попередньому досвіді дослідника у відповідній предметній області. Моделі нейронних мереж, на відміну від людини, в загальному випадку не містять в собі попереднього досвіду або знань про предметну область, тому успішність розв'язку поставленої задачі цілком і повністю залежить від наявності достатнього за обсягом та якістю набору даних, що використовується для навчання моделі. Важливим фактором, що безпосередньо впливає на якість отриманої моделі, є розмір такого набору даних. Масштабний набір навчальних даних, як правило, призводить до

кращої генералізації отриманої вибірки та, як наслідок, до значно кращої якості результуючої моделі, яка здатна більш точно передбачати результати на нових, невідомих даних.

Побудова прямих алгоритмів для вирішення конкретної задачі людиною зазвичай вимагає глибокого інтелектуального аналізу наявних даних, що базується на попередньому досвіді дослідника у відповідній предметній області. Моделі нейронних мереж, на відміну від людини, в загальному випадку не містять в собі попереднього досвіду або знань про предметну область, тому успішність розв'язку поставленої задачі цілком і повністю залежить від наявності достатнього за обсягом та якістю набору даних, що використовується для навчання моделі. Важливим фактором, що безпосередньо впливає на якість отриманої моделі, є розмір такого набору даних. Масштабний набір навчальних даних, як правило, призводить до кращої генералізації отриманої вибірки та, як наслідок, до значно кращої якості результуючої моделі, яка здатна більш точно передбачати результати на нових, невідомих даних.

Вимога до наявності великої кількості попередньо розмічених даних є важливим фактором, який досить часто буває важко, а іноді й неможливо досягти в практичних задачах з цілої низки об'єктивних причин. По-перше, сам процес збору необхідних даних може бути надзвичайно трудомістким та часомістким (а в деяких унікальних випадках може виявитися зовсім неможливим, особливо якщо задача оперує рідкісними даними, такими як унікальні випадки рідкісних захворювань у людей або аномальні явища в природі, які трапляються вкрай нечасто). По-друге, процес анотації (розмітки) зібраних даних не є повністю автоматизованим процесом, оскільки часто вимагає залучення експертів для коректного визначення класів або значень. Ця потреба в експертному втручанні виникає через складність даних, необхідність глибоких знань у предметній області або суб'єктивність інтерпретації. І хоча на сьогоднішній день існує велика кількість різних технологій, які дають змогу значно спростити та оптимізувати цей процес, повністю виключити ручну роботу людини, особливо при роботі зі складними даними, часто є неможливим.

Наведені вище фактори в своїй сукупності мають негативний вплив як на загальний час, необхідний для збору великих обсягів навчальних даних, так і на загальну вартість такого збору, що може бути досить значною.

Протягом останніх років значної популярності набув один з перспективних напрямків глибокого навчання - навчання нейронних мереж на навчальних наборах даних обмеженого розміру. Основна ідея цього напрямку включає в себе розробку та побудову таких спеціальних алгоритмів навчання та/або таких особливих архітектур нейронних мереж, які б можна було б успішно навчати з використанням лише обмеженої кількості доступних навчальних даних, при цьому досягаючи прийнятної якості. Частина наукових підходів, що розвиваються в рамках цього напрямку, фокусується на розробці методів штучного збільшення наявної навчальної вибірки за рахунок застосування різних технік аугментації даних. Ще одним важливим підходом є переносне навчання, яке дає можливість повторно використовувати знання, отримані на великих наборах даних, для вирішення завдань з обмеженими тренувальними вибірками. Інші підходи зосереджені на пошуках оптимальних значень гіперпараметрів процесу навчання, які б призвели до кращої збіжності моделі при обмеженій кількості даних, та інші.

Навчання моделей з використанням обмеженої кількості даних ставить нові серйозні виклики перед процесом навчання таких моделей - нейронна мережа, з одного боку, повинна бути достатньо великою та складною, аби мати змогу ефективно розв'язувати комплексні задачі. Водночас, великі за розміром моделі, як правило, є більш схильними до виникнення ефекту перенавчання при недостатній кількості навчальних даних, що негативно впливає на їхню здатність до узагальнення. Це відбувається тому, що модель з великою кількістю параметрів може легко "запам'ятати" невеликий набір даних, включаючи шум та аномалії, замість того, щоб вивчати основні закономірності. Особливо складно досягти хорошої генералізації на основі малого навчального набору даних з огляду на можливі наявні похибки, неточності та навіть прямі помилки, які можуть бути присутні в анотаційних даних цього набору.

У даній науковій роботі детально досліджено застосування ймовірнісних моделей, які розроблені для ефективного навчання з використанням лише малої кількості наявних навчальних даних. Такі ймовірнісні моделі є розширенням класичної реалізації нейронних мереж, що використовують традиційний підхід до обробки та аналізу вхідних даних у модель, шляхом застосування ймовірнісного підходу для більш глибокого та інформативного аналізу вхідних даних у модель. А саме - основним результатом роботи такої моделі є не чіткий та однозначний прогноз, а деякий нечіткий прогноз, що характеризується певним розподілом ймовірностей. На противагу традиційним моделям, які видають лише один варіант відповіді, ймовірнісні моделі мають унікальну змогу прогнозувати не лише саму відповідь на поставлене питання, а й надійні ймовірності, що характеризують ступінь впевненості в цих прогнозах. Фактично, така модель прогнозує не окреме значення, а цілий розподіл ймовірностей можливих правильних відповідей. Це дає змогу системі не тільки давати відповідь, але й повідомляти, наскільки вона "впевнена" у цій відповіді, що є надзвичайно корисним для прийняття рішень в умовах ризику.

Окрім цього, такий підхід не лише дає змогу ефективно використовувати цю додаткову інформацію після завершення процесу навчання моделі, наприклад, для оцінки ризиків або прийняття більш обґрунтованих рішень, а й значно допомагає самій моделі краще узагальнювати наявний навчальний набір даних та ефективно уникати небажаного ефекту перенавчання. Це досягається шляхом зміни традиційної цільової функції втрат, яка зазвичай базується на обчисленні похибки між прогнозованими моделлю та реальними значеннями, на нову функцію втрат, що базується на обчисленні ймовірності того, що реальне значення належить до спрогнозованого моделлю розподілу ймовірностей. Це, своєю чергою, дає додаткову можливість краще контролювати сам процес навчання шляхом встановлення певних обмежень або регуляризаційних членів на прогнозований розподіл ймовірностей. Такий підхід використання ймовірнісного аналізу в моделях, які навчаються на малих наборах даних, вже продемонстрував значне покращення кінцевого

результату в порівнянні з традиційними підходами, які не використовують інформацію про ймовірності.

Класичні моделі машинного навчання, що застосовуються для навчання на основі малих наборів даних, архітектурно найчастіше побудовані для вирішення задачі бінарної класифікації за один прямий прохід (тобто, для надання відповіді на просте питання на кшталт "чи є подібними два вхідні об'єкти, чи ні?"). Розширення можливостей таких моделей до задач класифікації на велику кількість класів зазвичай вимагає послідовного використання цієї ж самої моделі декілька разів з різними комбінаціями вхідних даних, що значно ускладнює процес та збільшує час обчислень. У даній роботі окремо розглянуто підхід до побудови моделей на основі використання концепції множини експертів. Модель, що базується на парадигмі множини експертів, дає унікальну змогу ефективно акумулювати знання про складну предметну область у різних, відокремлених частинах моделі, які виступають у ролі окремих експертів, кожен з яких спеціалізується на певній підмножині даних або аспекті задачі.

Такі моделі з розподіленими знаннями є значно більш гнучкими з точки зору їхнього подальшого змінення та/або розширення існуючої архітектури (наприклад, у випадку необхідності додавання нового класу даних до вже існуючої системи класифікації). Запропоновані в даній роботі моделі з розподіленими знаннями представляють собою універсальний підхід, який може бути ефективно застосований для широкого кола задач у різних галузях, таких як сфера комп'ютерного зору, обробка та аналіз природної мови (тексту) та складні мультимодальні задачі, що оперують даними різної природи.

Окремо в роботі продемонстровано, що ефективна інтеграція моделей з розподіленими знаннями успішно розв'язує складну задачу багатокласової класифікації у моделях, які навчаються на навчальних наборах даних обмеженого розміру, з використанням лише єдиного прямого проходу таких моделей через обчислювальну графову структуру. На додаток до цього, інтеграція моделей, що базуються на розподілених знаннях, моделей, що розроблені для навчання на основі малих наборів даних, та ефективного ймовірнісного підходу до процесу навчання

дала змогу успішно розв'язати задачу багатокласової класифікації в складних умовах обмеженої кількості доступних даних для навчання, а також в умовах наявності певних похибок та неточностей у навчальних даних, а також у ситуаціях, що характеризуються значною невизначеністю та наявністю внутрішніх неузгодженостей в даних.

Ключові слова: штучні нейронні мережі, машинне навчання, глибинне навчання, ймовірнісне моделювання, техніки навчання на малому наборі даних, моделі з розподіленими знаннями, реляційні моделі, невизначеність в моделюванні, комп'ютерний зір, баєсівські нейронні мережі, мета-навчання, адаптація моделей, генералізація малих вибірок.

ABSTRACT

Baranov M.V. Few-shot learning approaches for model adaption — Manuscript.

Thesis for the degree of Doctor of Philosophy in the specialty 122 "Computer Science" — Ivan Franko National University of Lviv, Lviv, 2025.

Artificial neural networks are a versatile and highly effective tool for solving a wide range of tasks, especially those for which the development of direct algorithms proves to be a complex and rather laborious process. Models based on the principles of neural network functioning establish a complex statistical dependency between the input data fed into the model and the expected results that this model should generate. Through the use of specialized training algorithms, the models obtained as a result of this process become capable of solving tasks that would be practically impossible or extremely difficult to formally and clearly describe using mathematical formulas.

Building direct algorithms for solving a specific task by a human usually requires deep intellectual analysis of the available data, based on the researcher's prior experience in the relevant subject area. Neural network models, unlike humans, generally do not contain prior experience or knowledge about the subject area, so the success of solving the assigned task entirely depends on the availability of a sufficiently large and high-quality dataset used for training the model. An important factor that directly affects the quality of the obtained model is the size of such a dataset. A large-scale training dataset typically leads to better generalization of the obtained sample and, as a result, to significantly better quality of the resulting model, which is capable of more accurately predicting results on new, unseen data.

The requirement for a large amount of pre-labeled data is an important factor that is often difficult, and sometimes impossible, to achieve in practical tasks for a number of objective reasons. Firstly, the process of collecting the necessary data itself can be extremely laborious and time-consuming (and in some unique cases may turn out to be completely impossible, especially if the task operates on rare data, such as unique cases of

rare human diseases or anomalous phenomena in nature that occur very infrequently). Secondly, the process of annotation (labeling) the collected data is not a fully automated process, as it often requires the involvement of experts to correctly determine classes or values. The need for expert involvement arises due to the complexity of the data, the availability of in-depth knowledge in the subject area, or the subjectivity of interpretation. And although today there are a large number of different technologies that allow to significantly simplify and optimize this process, completely excluding manual human work, especially when working with complex data, is often impossible. The factors listed above collectively have a negative impact both on the total time required to collect large volumes of training data and on the total cost of such collection, which can be quite significant.

Over the past few years, one of the promising directions of deep learning – training neural networks on training datasets of limited size – has gained significant popularity. The main idea of this direction includes the development and construction of such specialized training algorithms and/or such special architectures of neural networks that could be successfully trained using only a limited amount of available training data, while achieving acceptable quality. Some scientific approaches developed within this direction focus on the development of methods for artificial expansion of the existing training sample through the application of various data augmentation techniques. Another important approach is transfer learning, which allows you to use knowledge gained on large data sets to solve problems with limited training samples. Other approaches focus on the search for optimal values of hyperparameters of the training process that would allow achieving better convergence of the model with a limited amount of data, and others.

Training models using a limited amount of data poses new serious challenges to the training process of such models – the neural network, on the one hand, must be large and complex enough to be able to effectively solve complex tasks. At the same time, large-sized models are generally more prone to overfitting with an insufficient amount of training data, which negatively affects their ability to generalize. It is especially difficult to achieve good generalization based on a small training dataset given the possible existing

inaccuracies, imprecisions, and even direct errors that may be present in the annotation data of this dataset.

This work investigates in detail the application of probabilistic models designed for effective training using only a small amount of training data. Such probabilistic models are an extension of the classical implementation of neural networks that use the traditional approach to processing and analyzing input data into the model, by applying a probabilistic approach for a deeper and more informative analysis of the input data into the model. Namely, the main result of such a model's operation is not a clear and unambiguous prediction, but a certain fuzzy prediction characterized by a certain probability distribution. In contrast to traditional models that output only one answer option, probabilistic models have a unique ability to predict not only the answer to the question posed, but also reliable probabilities that characterize the degree of confidence in these predictions. In fact, such a model predicts not a single value, but an entire probability distribution of possible correct answers. This allows the system to not only give an answer, but also to associate how “confident” it is in that answer, which is extremely useful for decision-making under risk.

This approach not only makes it possible to effectively use this additional information after the model training process is completed, for example, to assess risks or make more informed decisions, but also significantly helps the model itself to better generalize the available training dataset and effectively avoid the undesirable effect of overfitting. This is achieved by changing the traditional target loss function, which is usually based on calculating the error between the model's predicted and actual values, to a new loss function based on calculating the probability that the actual value belongs to the probability distribution predicted by the model. This, in turn, provides an additional opportunity to better control the training process itself by setting certain constraints or regularization terms on the predicted probability distribution. This approach of using probabilistic analysis in models trained on small datasets has already demonstrated a significant improvement in the final result compared to traditional approaches that do not use information about probabilities.

Classical machine learning models used for training based on small datasets are most often architecturally built to solve a binary classification problem in one forward pass (that is, to answer a simple question like "are two input objects similar or not?"). Expanding the capabilities of such models to classification tasks with a large number of classes usually requires the sequential use of the same model several times with different combinations of input data, which significantly complicates the process and increases computation time. This work separately considers an approach to building models based on the use of the concept of an ensemble of experts. A model based on the ensemble of experts paradigm provides a unique opportunity to effectively accumulate knowledge about a complex subject area in different, separate parts of the model, which act as individual experts, each specializing in a specific subset of data or aspect of the task.

Such models with distributed knowledge are much more flexible in terms of their further modification and/or expansion of the existing architecture (for example, in case of the need to add a new class of data to an already existing classification system). The models with distributed knowledge proposed in this work represent a universal approach that can be effectively applied to a wide range of tasks in various fields, such as computer vision, natural language (text) processing and analysis, and complex multimodal tasks that operate on data of various natures. The work separately demonstrates that effective integration of models with distributed knowledge allows successfully solving the complex task of multi-class classification in models trained on training datasets of limited size, using only a single forward pass of such models through the computational graph structure. In addition to this, the integration of models based on distributed knowledge, models designed for training based on small datasets, and an effective probabilistic approach to the training process made it possible to successfully solve the multi-class classification problem in difficult conditions of a limited amount of available data for training, as well as in conditions of the presence of certain errors and inaccuracies in the training data, and also in situations characterized by significant uncertainty and the presence of internal inconsistencies in the data.

Keywords: artificial neural networks, machine learning, deep learning, probabilistic modeling, few-shot learning techniques, distributed knowledge models, relational models, uncertainty modeling, computer vision, Bayesian neural networks, meta-learning, model adaptation, small sample.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. M. V. Baranov, S. A. Ivanov, D. V. Shvetsov, and Y. M. Shcherbyna, “Application of Super Resolution for Optical Character Recognition in Low Quality Images,” *Lecture Notes in Networks and Systems*, vol. 695, pp. 135–145, 2023, doi: 10.1007/978-981-99-3043-2_11 (**Scopus, Q4**).
2. M. V. Baranov, I. Borachok, S. A. Ivanov, M. Mandzak, and Y. M. Shcherbyna, “Residual Domain Expert Architecture for Few-Shot Learning Classification Task,” in *International Scientific and Technical Conference on Computer Sciences and Information Technologies*, 2023, pp. 1–6, doi: 10.1109/CSIT61576.2023.10324234 (**Scopus**).
3. М. В. Баранов, Ю. М. Щербина, “Техніки навчання на малому наборі даних для задач сегментації,” *Вісник Львівського університету. Серія прикладна математика та інформатика*, vol. 28, pp. 100–115, 2020, doi: 10.30970/vam.2020.28.10975.
4. М. В. Баранов, С. А. Іванов, Я. І. Соколовський, Ю. Р. Юрченко “Розробка прототипу системи оптичного розпізнавання тексту для зображень низької якості,” *Вісник Львівського університету. Серія прикладна математика та інформатика*, vol. 29, pp. 91–101, 2021, doi: 10.30970/vam.2021.29.11344.
5. М. В. Баранов, Д. В. Зарецька, С. А. Іванов, “Аудіо-аутентифікація користувача за голосом,” *Вісник Львівського університету. Серія прикладна математика та інформатика*, vol. 30, pp. 112–120, 2022, doi: 10.30970/vam.2022.30.11452.
6. M. V. Baranov and Y. M. Shcherbyna, “Comprehensive analysis of few-shot image classification method using triplet loss,” *Вісник Національного університету «Львівська політехніка», серія «Інформаційні системи та мережі»*, vol. 11, pp. 103–109, 2022, doi: 10.23939/sisn2022.11.103.

7. M. V. Baranov, Y. M. Shcherbyna, and O. V. Hodych, “Exploit computer vision inpainting approach to boost deep learning models,” *Вісник Національного університету «Львівська політехніка», серія «Інформаційні системи та мережі»*, vol. 12, pp. 1–6, 2022, doi: 10.23939/sisn2022.12.001

Наукові публікації, що засвідчують апробацію матеріалів

дисертації:

8. M. V. Baranov and Y. M. Scherbyna, “Application of Metric Learning to Large-Scale Image Classification Task,” *CEUR Workshop Proceedings*, vol. 3171, pp. 1097–1106, 2022 (**Scopus**).
9. М. В. Баранов, “Визначення цілей тренування нейронної мережі без змін цільової функції втрат”, *доповідь на конференції “Сучасні проблеми прикладної математики та комп’ютерних наук”*, 27 вересня 2021 р., Львів, Україна.
10. M. V. Baranov, “Application of Metric Learning to Large-scale Image Classification Task,” *доповідь на конференції “Main Conference (CoLInS 2022)”*, онлайн (Zoom), 1 травня 2022 р.
11. M. V. Baranov, “Application of Super Resolution for optical character recognition in low quality images,” *доповідь на конференції “8th International Congress on Information and Communication Technology (ICICT 2023)”*, 20–23 лютого 2023 р., Лондон, Велика Британія