DOI 10.18699/sblai2023-04

О трех проблемах доверительного искусственного интеллекта

Нечесов А.В.
Институт математики им. С.Л. Соболева СО РАН, Новосибирск, Россия
nechesov@math.nsc.ru

На сегодняшний день проблема надежности и безопасности стоит очень остро в алгоритмах искусственного интеллекта (ИИ). Почти все существующие алгоритмы ИИ работают в централизованных средах. Это значит, что в любой момент тот, кто владеет доступом к этим алгоритмам, может изменить как сами алгоритмы, так и ту информацию и правила, с которыми они работают. Так же, как и для смарт-контрактов в децентрализованных средах [1], для алгоритмов ИИ существует проблема аудита. Очень часто код, который реализован, требует серьезных компетенций для их проверки и не всегда поддается тщательному анализу. Разработчик кода может оставить намеренно или непреднамеренно дырки в безопасности, что может привести к необратимым последствиям. Помимо этих двух проблем, существует еще одна важная проблема в ИИ – это проблема черного ящика ИИ. Когда интеллектуальное устройство представляет собой «черный ящик» и по входящим сигналам выдает только результат, но этот результат никак не объясняется. Все эти три проблемы очень сильно влияют на то, чтобы люди доверяли искусственному интеллекту.

В докладе исследуются вопросы применения методов семантического программирования [4, 5] в алгоритмах как объяснительного искусственного интеллекта (кратко XAI), так и в алгоритмах доверительного искусственного интеллекта (Trusted AI), которые исполняются в децентрализованных средах на основе блокчейн структур и смарт-контрактов [1]. Использование логического языка L* [2] позволяет нам полностью или частично заменять нейронные сети [3], работа которых не поддается человекопонятному объяснению, на специальные логико-вероятностные L*-программы, где каждый переход логически обоснован, прозрачен и понятен.

Литература

1. Nechesov A.V., Safarov R.A. Web 3.0 and Smart Cities // Proceedings of the International Conference “Current State and Development Perspectives of Digital Technologies and Artificial Intelligence”, Samarkand, Uzbekistan, 2022.

2. Goncharov S.S., Nechesov A.V. Semantic programming for AI and Robotics // IEEE International Multi-Conference on Engineering, Computer and Information Sciences. 2023;810-815. Doi 10.1109/SIBIRCON56155.2022.10017077.

3. Goncharov S.S., Nechesov A.V. Polynomial-Computable Representation of Neural Networks in Semantic Programming // J. 2023;6(1):48-57. Doi 10.3390/j6010004.

4. Goncharov S.S., Nechesov A.V. Solution of the problem P = L // Mathematics. 2022;10(1):113. Doi 10.3390/math10010113.

5. Goncharov S.S., Nechesov A.V. Polynomial analogue of Gandy's fixed point theorem // Mathematics. 2021;9(17):2102. Doi 10.3390/math9172102.

About three problems of trusted artificial intelligence

Nechesov A.V.
Sobolev Institute of Mathematics of SB RAS, Novosibirsk, Russia
nechesov@math.nsc.ru

Today the problem of reliability and security is very acute in artificial intelligence algorithms. Almost all existing AI algorithms work in centralized environments. This means that at any moment whoever has access to these algorithms can change both the algorithms themselves, and the information and rules with which they operate. As well as for smart contracts in decentralized environments [1] there is an audit problem for AI algorithms. Very often the code that is implemented requires serious competencies to verify and is not always amenable to careful analysis.

The code developer (intentionally or unintentionally) can leave holes in security, which can lead to irreversible consequences. In addition to these two problems, there is another important problem in AI: the AI Black Box Problem. When the intelligent device is a “black box” and the input signals give only the result, but this result is not explained. All three of these issues have a huge impact on how people can trust artificial intelligence.

The work explores the application of semantic programming methods [4, 5] in the algorithms of Explainable Artificial Intelligence (briefly XAI) and in the algorithms of Trusted Artificial Intelligence (Trusted AI) which are executed in decentralized environments based on blockchain structures and smart contracts [1]. The logical language L* [2] which is used allows us fully or partially to replace neural networks [3] whose operation is not amenable to human-understandable explanation, with special logical-probabilistic L*-programs where each transition is logical, transparent and understandable.

References

1. Nechesov A.V., Safarov R.A. Web 3.0 and Smart Cities // Proceedings of the International Conference “Current State and Development Perspectives of Digital Technologies and Artificial Intelligence”, Samarkand, Uzbekistan, 2022.

2. Goncharov S.S., Nechesov A.V. Semantic programming for AI and Robotics // IEEE International Multi-Conference on Engineering, Computer and Information Sciences. 2023;810-815. Doi 10.1109/SIBIRCON56155.2022.10017077.

3. Goncharov S.S., Nechesov A.V. Polynomial-Computable Representation of Neural Networks in Semantic Programming // J. 2023;6(1):48-57. Doi 10.3390/j6010004.

4. Goncharov S.S., Nechesov A.V. Solution of the problem P = L // Mathematics. 2022;10(1):113. Doi 10.3390/math10010113.

5. Goncharov S.S., Nechesov A.V. Polynomial analogue of Gandy's fixed point theorem // Mathematics. 2021;9(17):2102. Doi 10.3390/math9172102.

關於三個問題
值得信賴的人工智能

Nechesov A.V.
Sobolev 數學研究所，電子郵件：
nechesov@math.nsc.ru

今天，人工智能算法中的可靠性和安全性問題非常尖銳。
幾乎所有現有的人工智能算法都在集中式環境中工作。
這意味著任何時候有權訪問這些算法的人都可以更改算法本身，以及它們運行的信息和規則。
除了去中心化環境中的智能合約 [1] 之外，人工智能算法還存在審計問題。
通常，實施的代碼需要認真的能力來驗證，並不總是適合仔細分析。
代碼開發人員（有意或無意）可能會留下安全漏洞，從而導致不可逆轉的後果。
除了這兩個問題，AI中還有一個重要的問題：AI黑盒問題。
當智能設備是一個“黑盒子”，輸入信號只給出結果，但不解釋這個結果。
所有這三個問題都對人們如何信任人工智能產生了巨大影響。

這項工作探索了語義編程方法 [4,5] 在可解釋人工智能（簡稱 XAI）算法和可信人工智能（Trusted AI）算法中的應用，這些算法在基於區塊鏈結構和智能合約的去中心化環境中執行[1].
使用的邏輯語言 L* [2] 允許我們用特殊的邏輯概率 L* 程序完全或部分地替換其操作不符合人類可理解解釋的神經網絡 [3]，其中每個轉換都是邏輯的、透明的並且可以理解。

文學

1. Nechesov A.V., Safarov R.A. Web 3.0 and Smart Cities // Proceedings of the International Conference “Current State and Development Perspectives of Digital Technologies and Artificial Intelligence”, Samarkand, Uzbekistan, 2022.

2. Goncharov S.S., Nechesov A.V. Semantic programming for AI and Robotics // IEEE International Multi-Conference on Engineering, Computer and Information Sciences. 2023;810-815. Doi 10.1109/SIBIRCON56155.2022.10017077.

3. Goncharov S.S., Nechesov A.V. Polynomial-Computable Representation of Neural Networks in Semantic Programming // J. 2023;6(1):48-57. Doi 10.3390/j6010004.

4. Goncharov S.S., Nechesov A.V. Solution of the problem P = L // Mathematics. 2022;10(1):113. Doi 10.3390/math10010113.

5. Goncharov S.S., Nechesov A.V. Polynomial analogue of Gandy's fixed point theorem // Mathematics. 2021;9(17):2102. Doi 10.3390/math9172102.

DOI 10.18699/sblai2023-05

Non-MapReduce computing for intelligent analysis of Big Data

Huang Joshua Zhexue
Big Data Institute, Shenzhen University, China
zx.huang@szu.edu.cn

MapReduce is the most widely used programming model for distributed computing that runs on clusters and clouds. However, when a highly iterative intelligent algorithm implemented in MapReduce runs on a cluster to analyze a big dataset, say in terabytes, it will suffer from the problems of computing inefficiency and data unscalability due to the high costs of data communications between the nodes. To conquer these problems, we propose a Non-MapReduce distributed computing paradigm that can run an iterative algorithm on the nodes of a cluster independently and in parallel without the needs of data communication between the nodes. As a big benefit to industry, it removes the burden for reprogramming sequential algorithms in MapReduce. The Non-MapReduce distributed computing paradigm is enabled by the random sample partition (RSP) data model, the data analysis methods using multiple random samples, and the ensemble learning model. In this talk, I will introduce these new approaches which can make big data computing technologies computationally efficient, scalable to big data, directly execute sequential algorithms in parallel and distributed fashion, and analyze big data without memory limit.

非MapReduce計算大數據智能分析

Huang Joshua Zhexue
黃哲學博士
特聘教授
大數據研究所所長
中國深圳大學
zx.huang@szu.edu.cn

MapReduce 是在集群和雲上運行的分佈式計算使用最廣泛的編程模型。
然而，當MapReduce中實現的高度迭代的智能算法在集群上運行以分析大數據集時，例如TB級別的數據集，由於節點之間的數據通信成本高，它會遇到計算效率低下和數據不可擴展的問題。 為了克服這些問題，我們提出了一種非 MapReduce
分佈式計算範式，可以在集群的節點上獨立並行地運行迭代算法，而無需節點之間的數據通信。 作為對行業的一大好處，它消除了在 MapReduce 中重新編程順序算法的負擔。 非 MapReduce 分佈式計算範式由隨機樣本分區 (RSP)
數據模型、使用多個隨機樣本的數據分析方法和集成學習模型啟用。