Abnormal detection of artificial intelligence based on hierarchical timing memory algorithms

Jianjun Huang¹,*, Xuemei Peng¹, He Zhou¹
¹Nanchang Institute of Technology, Nanchang 330044, Jiangxi, China

*Corresponding author e-mail: hjjun302@nut.edu.cn

Abstract. With the advent of the information age and the popularization of computers, computer technology has been greatly developed in this era. Many people began to take advantage of computers and develop computer performance, so a variety of algorithms were proposed. The main algorithm used in this paper is the newly proposed hierarchical timing memory algorithm. Because it is useful for detecting errors, we can use it to detect anomalies. Therefore, the purpose of this paper is to use the hierarchical timing memory algorithm to detect anomalies in artificial intelligence. After observing the possible anomalies of artificial intelligence, this paper records it, experiments it with strated timing memory algorithm and observes the advantages and disadvantages of strated timing memory algorithm and other algorithms for anomaly detection. The experimental results show that the abnormal detection efficiency of strated timing memory algorithm is better.

Keywords: Artificial Intelligence, Hierarchical Timing Memory Algorithm, Anomaly Detection, Comparative Analysis

1. Introduction

The present era is basically the era of artificial intelligence, all kinds of things about artificial intelligence are mentioned, and all things are expected to be replaced by artificial intelligence in the future (except for state secrets). Because compared with human, artificial intelligence has high processing performance, high accuracy and does not need rest, it is just a mechanized program [1]. So far, it has not been able to think and feel like a real person. At present, artificial intelligence is still just a program [2]. So now people can hold him in their hands. Artificial intelligence is a new discipline based on various disciplines. It mainly involves mathematics, computer science, graphics, statistics and other disciplines. This is because artificial intelligence mainly deals with data [3].

Artificial intelligence can use the computing resources provided by the computer to calculate some data. These data are usually very large and cannot be calculated by manpower[4]. Just like the previous major mathematical problems, it takes billions of years to complete the calculation by relying on the
ordinary computer, but it only takes more than ten seconds to complete the calculation by using the quantum computer, which is the progress of science and technology [5]. Artificial intelligence, as the most important link in the current progress of science and technology, was mentioned in the 1970s, and then there was a wave of upsurge. However, many people thought about what to do once they had their own emotions after the growth of artificial intelligence, just like the scene in the terminator. In the future, science and technology will wipe out human beings themselves, and human beings will die The species eventually died out. Therefore, there is a certain fear for the growth of artificial intelligence, which will eventually lead to the extinction of the whole human being [6]. But it's not. So far, artificial intelligence is still beneficial to human beings, the advantages outweigh the disadvantages. So we decided to use artificial intelligence [7].

But the current artificial intelligence, it will always appear some errors [8]. Sometimes it's due to self-designed program errors, sometimes it's due to self-protection program startup errors caused by too large data. These are all errors, and how to find them when they cause them is also a problem. Because it is generally too late to find a big problem in artificial intelligence, so our purpose is to establish an algorithm to detect the anomaly of artificial intelligence [9]. So, we choose hierarchical temporal memory algorithm to control it. Because the hierarchical temporal memory algorithm divides the data processing into multiple levels, and then uses different time periods to constrain them, records, and becomes a memory database from which data can be extracted at any time. Once it is found that the AI is abnormal, the database between them will have an abnormal connection, and the alarm center will be alerted by the algorithm to prompt the AI error [10].

2. Hierarchical timing algorithm

As can be achieved from the CSTR system, the expression that renders the exception state in a hierarchical form is:

\[ G_1(t)N_1 - [G_1(t) + G_2(t)]m_a = V \frac{dm_a}{dt} \]

1

The expression in which the sewage renders a normal state is:

\[ G_2(t)N_2 - [G_1(t) + G_2(t)]m_b = V \frac{dm_b}{dt} \]

2

According to the method (1) and the method (2), the dynamic control model of the number value can be expressed as:

\[ G_1(t)N_1 - V \frac{dm_a}{dt} = [G_1(t) + G_2(t)]m_a \]

3

\[ G_1(t)N_2 - V \frac{dm_b}{dt} = [G_1(t) + G_2(t)]m_b \]

4

To make y sm a-mb, the number of values in the control model can be simplified to:
\[
\frac{dV}{dt} = \left[ N_1 G_1(t) - N_2 G_2(t) \right] - \left[ G_1(t) + G_2(t) \right] y
\]

3. **Experiment**

3.1. *Three group controlled trials were established*

We selected several computers from the university and accepted several data groups at the same time, and then set up three groups, each of which used layered timing memory algorithms, expert algorithms, and artificial intelligence built by ant colony algorithms to analyze the rationality and classification of individual data sets in order to identify the advantages and disadvantages of the methods we use. In order to avoid errors in small probability events, we can avoid large experimental errors by analyzing two hundred sets of data sets to get the events generated by the larger probability and avoid the error of the small probability.

3.2. *Get experimental feedback*

We end up with a general experiment, then analyze all the statistics, get what we need, and then take the second step: have three groups of members work on the exchange system. Finally, step three: The questionnaire analyzes members' feelings and arrives at statistical results.

4. **Evaluation results**

4.1. *With regard to experimental data derived from two methods*

|                  | Calculate the probability of error/one millionth | Probability of classification error / one in a million | The overall situation |
|------------------|-----------------------------------------------|-------------------------------------------------------|----------------------|
| Hierarchical timing memory algorithm | 0.003                                         | 0.001                                                 | Excellent            |
| Expert algorithms | 0.011                                         | 0.004                                                 | Better               |
| Ant colony algorithm | 0.007                                         | 0.014                                                 | Better               |
Figure 1. The effect of different uses of algorithms on success rates

As you can see from Table 1 and Figure 1, expert algorithms and ant colony algorithms have more errors and large leaks, so we think it's better to use a hierarchical timing memory algorithm to look up errors.

4.2. Survey results

Table 2. Survey results on the use of different systems

| Evaluation attitude | Praise | Mid-review | Poor reviews | Total number of copies/servings |
|---------------------|--------|------------|--------------|--------------------------------|
| Number of copies / servings |
| Hierarchical timing memory algorithm | 42     | 14         | 4            | 60                             |
| Expert algorithms   | 23     | 28         | 9            | 60                             |
| Ant colony algorithm | 17     | 27         | 16           | 60                             |
| Total number of copies/servings | 82 | 69 | 29 | 180 |

![Bar chart showing survey results on the use of different systems](image_url)

**Figure 2.** Survey results on the use of different systems

We get the results from the student survey questionnaire, organize it as shown in Table 2, and then describe it more intuitively as shown in Figure 2. Figure 2 is based on the bar chart seen in Table 2, which shows how students feel about the systems built by the three algorithms. We sent out a total of 180 questionnaires, recovered 180 questionnaires, the recovery rate of 100%. Then divided into time series memory algorithm to build the system of the highest praise rate, the lowest rate of poor evaluation, indicating that the hierarchical timing memory algorithm to build a better system.

4.3. Technical support

The technology service platform requires a normal set of contract negotiations to implement the construction of distributed a pp. Any platform has a system whose data represents multiple collections. In order to be able to work together, the technical service platform must provide many groups of systems that are not of an unspecies type to communicate in different network systems, systems that can become different languages, and systems that make up systems that can use devices that communicate in different sizes. These agreements include:

**XMLXSD**

XML (a small collection in a wrote-down language that is not standard) is a good foundation for data formats in the Web services platform. In addition to being easy to build and handle different data, the main advantage of XML is that it has not only nothing to do with the platform but also nothing to do with the vendor. XML was created by the World Wide Web Society (W3C). XML schema sd developed by W3C defines a set of good common data types that cannot be standard and uses a language to augment this set of data types. The Web services platform uses XSD as a data base for a variety of usage and processing systems. When you create a Web service in a language such as V C, you need to convert, which is a protocol.

**SOAP**

5
SOAP is a non-complex object access protocol. It is a non-weight protocol for swapping XML, a small collection in a language that is not standardly used. It has three main aspects: XML describes a box that explains the content of the information and its unreasonable handling, describes the usage regulations and restrictions for XML objects in another language, and uses the Remote Procedure Call (RPC) contract. SOAP can run on numerous other declared transport contracts. For example, you can use SMTP (Internet e-mail protocol) to deliver SOAP messages, which is exciting. The headers between the transport layers are not right, but the total amount of information that XML can host remains the same. Web services hope that systems that are not the same can be transferred together in a "software conversation", breaking the state of a pp that cannot be used together between the Web and various devices, and achieving the goal of "seamless web-based integration".

WSDL

The Web Service Description Language (WSDL) is a description document that is provided in a way that the Internet can read, while XML-based languages (a small collection of wrote-down languages that are not standard) are used to describe web services and their functions, data, and returned data. Because it's based on XML, WSDL is machine-readable and human-understandable.

UDDI

The purpose of UDDI is to establish e-commerce standards; UDDI is a set of Web-based implementation standards and specifications that provide distributed web services and information registries, and also includes a set of implementation standards for access protocols that enable enterprises to register their own Web services so that other enterprises can develop their own access protocols.

Call RPC with messaging

The Web service itself is a conversation between different a pps. When using RPC, our primary purpose is to obscure the user's own ip address, apply a virtual and non-traceable ip address to process the information, and forward it. Because the ip address of the forwarding information is a virtual ip address established by servers around the world, it is not tracked.

4.4. Abnormal detection

In data mining, anomaly detection typically produces exception recognition for project events in individual patterns or datasets. Some of these anomalies are identified by system errors, while others are caused by hackers trespassing. It is usually presented in the form of text errors and structural defects. Abnormal detection is generally particularly obvious when large-scale hacking, because hackers mainly use system vulnerabilities to attack the system firewall to enter the system, to achieve the purpose of the control system. Exception monitoring is when the firewall monitors and reflects anomalies for these vulnerabilities. Abnormal monitoring is generally divided into three categories. The first category is unsealed anomaly monitoring methods, which generally identify an example that has nothing to do with detecting his anomalies. The second is the supervised anomaly monitoring method, which generally establishes a normal and abnormal data set, then divides it into training sets and data sets, and then monitors and judges it. The third category is the semi-supervisory anomaly monitoring method, which typically uses a normal data set and then gives the system a real example of self-learning to judge abnormal monitoring, which is then recorded.

5. Conclusion

To sum up, we detect anomalies in artificial intelligence by analyzing survey systems built by a variety of technologies. Finally, it is found that the system built by using hierarchical timing memory algorithm
is the most efficient and best for detecting anomalies in artificial intelligence. Because the hierarchical timing memory algorithm is the latest proposed algorithm, other algorithms may be proposed later than the hierarchical time series memory algorithm. So, let's wait and see.

Acknowledgments

"Science and technology research project of Jiangxi Provincial Department of education in 2019"(NO: GJJ191012).

References

[1] Aziz S. Artificial intelligence[J]. Defence journal, 2019, 22(1):28-29.
[2] A P A I , B X Z , Jacob Vanhouten , M C , et al. Artificial Intelligence for Diagnosis of Acute Coronary Syndromes: A Meta-analysis of Machine Learning Approaches[J]. Canadian Journal of Cardiology, 2020, 36(4):577-583.
[3] Yun D , Xiang Y , Liu Z , et al. Attitudes towards medical artificial intelligence talent cultivation: an online survey study[J]. Annals of Translational Medicine, 2020, 8(11):708-708.
[4] Wang Y , Liu Z , Qu A , et al. Study of tacrine derivatives for acetylcholinesterase inhibitors based on artificial intelligence[J]. LATIN AMERICAN JOURNAL OF PHARMACY, 2020, 39(6):1159-1170.
[5] Damova M. Neuromemrisitive architecture of HTM with on-device learning and neurogenesis[J]. Computing reviews, 2019, 60(12):474-474.
[6] Hasani Z , Krrabaj S. Survey and Proposal of an Adaptive Anomaly Detection Algorithm for Periodic Data Streams[J]. Journal of Computer and Communications, 2019, 07(8):33-55.
[7] Mackenzie J, Roddick J F , Zito R. An Evaluation of HTM and LSTM for Short-Term Arterial Traffic Flow Prediction[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(5):1847-1857.
[8] Park B E , Kim J S , Lee J K , et al. Anomaly detection in a hyper-compressor in low-density polyethylene manufacturing processes using WPCA-based principal component control limit[J]. Korean Journal of Chemical Engineering, 2020, 37(1):11-18.
[9] Matsui A , Asahi S , Tamura S , et al. Anomaly Detection in Mechanical Vibration Using Combination of Signal Processing and Autoencoder[J]. Journal of Signal Processing, 2020, 24(4):203-206.
[10] Hamedani S G , Moaiyeri M H. Comparative Analysis of the Crosstalk Effects in Multilayer Graphene Nanoribbon and MWCNT Interconnects in Sub-10 nm Technologies[J]. IEEE Transactions on Electromagnetic Compatibility, 2020, 62(2):561-570.