MAGAZINE

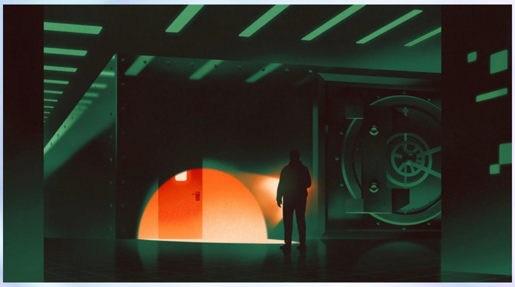
ISSUE NO: 138
August 7, 2023

Byte Quest

Department of
CSE

MATH MASTERY

MATH IN ML



CRYPTIC NEURAL THREATS

ML MAVERICK

Department Vision

To be a center for academic excellence in the field of Computer Science and Engineering education to enable graduates to be ethical and competent professionals.

Department Mission

To enable students to develop logic and problem solving approach that will help build their careers in the innovative field of computing and provide creative solutions for the benefit of society.

FACULTY COORDINATORS

DR. BHARGAVI PEDDIREDDY
(ASSOCIATE PROFESSOR)
S. KOMAL KAUR
(ASST. PROFESSOR)

STUDENT COORDINATORS

VAMSI (3/4) CSE C
SPOORTHI (3/4) CSE C

Byte Quest

MATH MASTERY

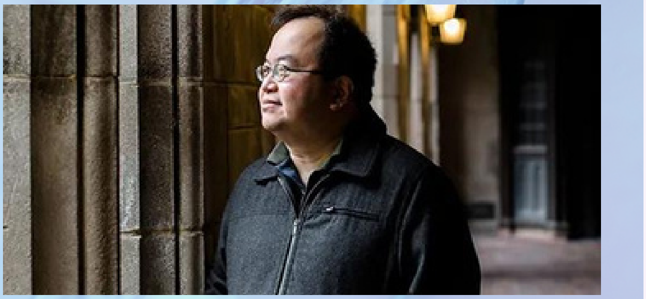
In recent breakthroughs, researchers explore how large language models (LLMs) like ChatGPT and Dall·E can grasp mathematical reasoning. Acknowledging the LLMs' impressive human-like responses and creativity, the papers highlight the challenge of their unreliability due to logical errors.

Two solutions emerge: autoformalization, translating natural language math problems into computer code, and training LLMs like Minerva to solve complex math queries. While Minerva's performance raises questions about verification, the researchers envision a future where autoformalization acts as a bridge. This approach combines the strengths of LLMs with reinforcement learning, offering a potential breakthrough in AI reasoning skills and applications.

These breakthroughs signal a transformative era where AI, honed through mathematical reasoning, could extend its capabilities to coding, medical diagnoses, and logical problem-solving, promising a more reliable and versatile future.

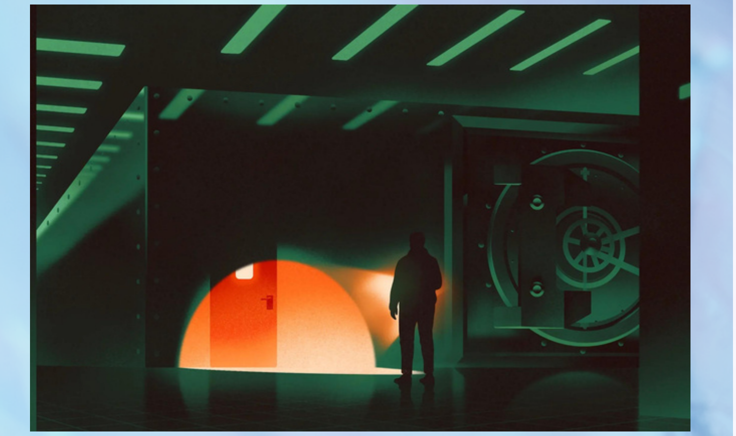
MATH IN MACHINE LEARNING

Lek-Heng Lim, a University of Chicago applied mathematician, blends pure and applied math, using algebra, geometry, and topology in machine learning. Advocating a return to the unified perspective of pioneers like Gauss and Hilbert, Lim applies these mathematical tools to delve into the intricacies of machine learning



His research, showcased in a 2020 paper, explores the topological facets of deep neural networks. Treating sets of cat and non-cat images as intertwined manifolds, Lim, along with his student Greg Naitzat, unveils the complex relationship between these categories. His approach, incorporating tools like persistent homology, reveals insights into neural network functioning and challenges conventional machine learning conjectures. In a collaborative effort with student Zehua Lai, Lim applies algebraic geometry tools to disprove a longstanding machine learning conjecture, showcasing the interdisciplinary nature of his contributions.

CRYPTIC NEURAL THREATS



In the realm of machine learning and neural networks, groundbreaking study has unveiled the potential for undetectable backdoors, akin to unbreakable locks, which could compromise the security of these systems.

The research, presented at the Foundations of Computer Science conference, establishes a theoretical link between cryptographic security and vulnerabilities in machine learning models. By leveraging mathematical rigor inspired by digital signatures, the study demonstrated the creation of "black-box undetectable" backdoors, allowing users with secret keys to manipulate output classifications without detection. Furthermore, the researchers explored "white-box undetectable" backdoors, remaining invisible even to scrutinizing defenders. The method involves tampering with the initial randomness of neural networks, posing a challenge for potential defenders in the field. The study's implications extend to potential real-world scenarios, emphasizing the need for ongoing research at the intersection of cryptography and machine learning to address emerging security challenges in this dynamic field.

In this dynamic landscape, the study advocates ongoing interdisciplinary collaboration to fortify machine learning systems against evolving security challenges.

Byte Quest

MACHINE LEARNING MAVERICK

Arvind Narayanan, a computer scientist at Princeton University, has been a driving force in shaping the understanding of privacy and fairness in machine learning. Beginning in 2006, he revealed the limitations of privacy measures by de-anonymizing supposedly anonymous Netflix user data.

He has been instrumental in exposing clandestine methods employed by websites for tracking and extracting user data, even uncovering implications for the National Security Agency's potential use of web browsing data. Shifting his focus to machine learning, Narayanan illuminates the technology's potential for unintended discrimination and underscores the importance of statistical intuition in navigating its pitfalls. His exploration of fairness in machine learning, marked by a 2017 course and a talk on diverse fairness definitions rooted in moral questions, addresses the misleading use of "personally identifiable information" in privacy debates. Narayanan's distinction between machine learning problem types emphasizes varying accuracies, dangers, and ethical implications. Despite recognizing challenges, particularly in social prediction problems, he enjoys interdisciplinary collaboration and maintains optimism regarding sustained activism's potential to positively influence new technology adoption.

BROUGHT TO YOU BY

Department of
Computer Science and Engineering

Vasavi College of Engineering