MAGAZINE

ISSUE NO: 146
November 27, 2023

Byte Quest

Department of
CSE

CRYPTOGRAPHY BREAKTHROUGH

AI CREATIVITY UNLEASHED

ALGORITHMIC PARADIGM SHIFT

UNRAVELING COMPUTATIONAL COMPLEXITY

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

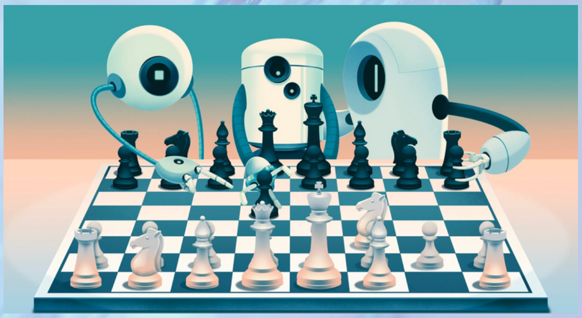
Byte Quest

CRYPTOGRAPHY BREAKTHROUGH

Researchers have made a breakthrough in solving a decades-old privacy problem in cryptography, bringing us closer to fully private internet searches. The challenge, known as private information retrieval (PIR), aims to access information from public databases without revealing the specific data accessed.

Traditional methods involved scanning entire databases during each search, becoming inefficient as databases grew larger. The new approach, developed by three researchers and recognized with a Best Paper Award, overcomes a major theoretical barrier. Initially skeptical, the researchers discovered a secure way to preprocess a single-server database, allowing users to pull information secretly. Although currently impractical for real-world use, the method lays the foundation for more efficient internet searches and programs requiring quick data access. The breakthrough offers hope for future optimizations in the field of cryptography, with potential applications in achieving private lookups from giant databases. The researchers believe their solution is a "magical building block" for advancing privacy-preserving applications.

AI CREATIVITY UNLEASHED



In 2020, computer scientist Tom Zahavy, inspired by chess puzzles, sought to enhance AI problem-solving beyond winning games. At Google DeepMind, Zahavy and colleagues combined the strengths of up to 10 diverse AI systems, including the powerful AlphaZero, to tackle challenges like Roger Penrose's intricate puzzles.

Unlike traditional AI programs, this collaborative system demonstrated improved creativity and adaptability, addressing puzzles more effectively. Zahavy identified a limitation in conventional reinforcement learning—systems lacked the ability to recognize and learn from failure, hindering creative problem-solving. To overcome this, the team introduced a diversified AlphaZero, incorporating various AI agents trained independently on diverse scenarios. The resulting system exhibited enhanced performance, creatively addressing challenges and outperforming the original AlphaZero. Zahavy believes this approach, emphasizing diversity and creativity, could revolutionize AI problem-solving beyond chess, marking a crucial step towards addressing generalization issues in machine learning. While computationally intensive, this approach holds promise for advancing AI's capacity to think creatively and find diverse solutions to complex problems.

Byte Quest

ALGORITHMIC PARADIGM SHIFT

Researchers have challenged a longstanding conjecture in computer science concerning online algorithms and their ability to handle the "k-server problem," which involves dispatching agents to fulfill requests in real-time without knowledge of future demands.

Traditionally, researchers believed there was a universal algorithmic performance level for this problem. However, a recent paper by three computer scientists, Sébastien Bubeck, Christian Coester, and Yuval Rabani, demonstrated that achieving a consistent algorithmic performance is not always possible. They constructed complex spaces and devised request sequences that proved challenging for any algorithm, leading them to disprove the randomized k-server conjecture. The study, recognized with a Best Paper Award, provides theoretical insights into algorithmic performance. While practical applications often exceed theoretical expectations, the research highlights the power of the employed technique and may influence future work in the field.

This groundbreaking study not only challenges established beliefs but also suggests potential shifts in algorithmic design and computational understanding.

Byte Quest

UNRAVELING COMPUTATIONAL COMPLEXITY

Computer scientists have grappled with the complex problem of vector addition systems' reachability for decades. Initially thought to be straightforward, this problem involves determining if a series of transitions within a system of vectors can reach a specific state without any vector component dropping below zero.

Despite its seemingly simple premise, the reachability problem's complexity has proven elusive to comprehension.

In 2019, a breakthrough revealed that the difficulty of the reachability problem escalates at an astonishing rate, surpassing previous expectations. The complexity is so profound that it outstrips even the Ackermann function, a mathematical monstrosity representing a hierarchy of operations. The lower and upper bounds established by researchers, particularly Wojciech Czerwiński and Jérôme Leroux, demonstrate that determining reachability can be as intricate as the Ackermann function's growth.

This revelation has implications for understanding fundamental aspects of computational theory. Despite recent advancements, there are still unanswered questions and unexplored variants of the reachability problem. Researchers aim to dissect its distinct effects, especially in cases with fixed dimensionality. Ultimately, this ongoing exploration is part of a broader quest to unravel the complexities of computability.

BROUGHT TO YOU BY

Department of Computer Science and Engineering

Vasavi College of Engineering