

ISSUE NO: 143 October 16,2023

Byte Quest

Department of

CSE







THE CRYPTOGRAPHER WHO ENSURES WE CAN TRUST OUR COMPUTERS



SOLVE OPTIMIZATION PROBLEMS FASTER

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.

FACULTY COORDINATORS

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

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.

STUDENT COORDINATORS

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



Byte Quest

MATHEMATICIANS SOLVE LONG-STANDING COLORING PROBLEM

In a mathematical puzzle dating back to Leo Moser in the 1960s, researchers sought to color an infinite plane without any two points precisely one unit apart. Previous limits suggested the maximum coloring area was 27.91%, but Hungarian mathematicians, including Máté Matolcsi, challenged this, aiming to prove Erdős' conjecture of a bound below 25%. Collaborating with Alfréd Rényi Institute colleagues, they leveraged machine learning models inspired by AlphaGo and AlphaFold to identify a complex set of points solving the problem. The team tackled a linear optimization problem and used Fourier transforms to narrow down the potential point set. Using traditional search strategies surprisingly outperformed more advanced Al techniques.

After computational analysis on 128 CPUs, the team discovered that only 24.7% of the plane can be colored without forming unit-distance pairs, surpassing previous bounds and confirming Erdős' conjecture. Future efforts now focus on determining the chromatic number of the plane, exploring how many colors are needed for a complete unit-distance-avoiding coverage. This breakthrough adds a new dimension to mathematical explorations on infinite plane coloring.



TO MOVE FAST, QUANTUM MAZE SOLVERS MUST FORGET THE PAST

Quantum computers leverage superposition and interference to explore multiple options simultaneously, offering remarkable speed-ups for certain tasks like factoring large numbers or generic search problems. However, not all computational problems benefit from quantum enhancements.



Despite efforts to create memory-enhanced quantum walk algorithms like snake walks to maintain pathway information, proving their effectiveness remained a challenge. Coudron's team demonstrated that any fast quantum path-finding algorithm that retains knowledge of the entrance throughout the process is unattainable. This underscores the limitations of quantum algorithms in preserving pathway information.

While this discovery might not resolve the quest for a path-preserving quantum algorithm, it narrows down possibilities. Understanding quantum algorithms' limitations could inspire new cryptographic protocols or reveal applications for solving intricate problems.



Byte Quest

THE CRYPTOGRAPHER WHO ENSURES WE CAN TRUST OUR COMPUTERS

Yael Tauman Kalai, a pioneering theoretical computer scientist, transformed from a high school troublemaker to an award-winning researcher reshaping internet security. Despite a rebellious phase in her youth, she always harbored a love for math, which blossomed during her college years. Kalai's fascination with the elegance and counterintuitive nature of mathematics led her to delve into computer science and eventually cryptography, where she found a merging of abstract math and real-world applicability. Her groundbreaking work spans the development of ring signatures, ensuring message authenticity without revealing the sender's identity, to succinct non-interactive proofs that verify computations in cloud computing securely and efficiently.

Her contributions extend to the realm of quantum computing, where she explores challenges of ensuring security in a world where quantum computers vastly surpass classical ones. Kalai and her colleagues have achieved the remarkable feat of creating classical. computationally secure methods to verify quantum computations. This breakthrough holds promise for certifying the accuracy of quantum devices using classical computers, opening frontiers in secure computation verification in the quantum era.





Byte Quest

RISKY GIANT STEPS CAN SOLVE OPTIMIZATION PROBLEMS FASTER

Optimization problems are fundamental across fields, from GPS routing to machine learning, aiming to find the most efficient solutions. Gradient descent, a widely optimization technique, has been a staple for over 150 years, allowing systems to maneuver through complex cost functions toward the lowest point, representing the most favorable outcome. However, recent research by Ben Grimmer challenged a long-held belief about the ideal step sizes in gradient descent. Contrary to conventional wisdom that favored small steps, Grimmer's study revealed that including unexpectedly large step sizes in cyclic sequence can accelerate a convergence nearly threefold, a counterintuitive notion that reshapes understanding of this optimization method.

Grimmer's findings, while revolutionary in might not immediately alter applications practical like learning, which grapple with more intricate and multifaceted functions. The study's focus on smooth and convex functions limits its immediate impact on these complex real-world scenarios. Despite this, work has prompted reevaluation of how researchers perceive gradient descent, shedding light on the potential benefits of unconventional, cyclic step sequences and inviting exploration into the underlying symmetric patterns governing the most efficient solutions.



BROUGHT TO YOU BY



Department of Computer Science and Engineering

Vasavi College of Engineering