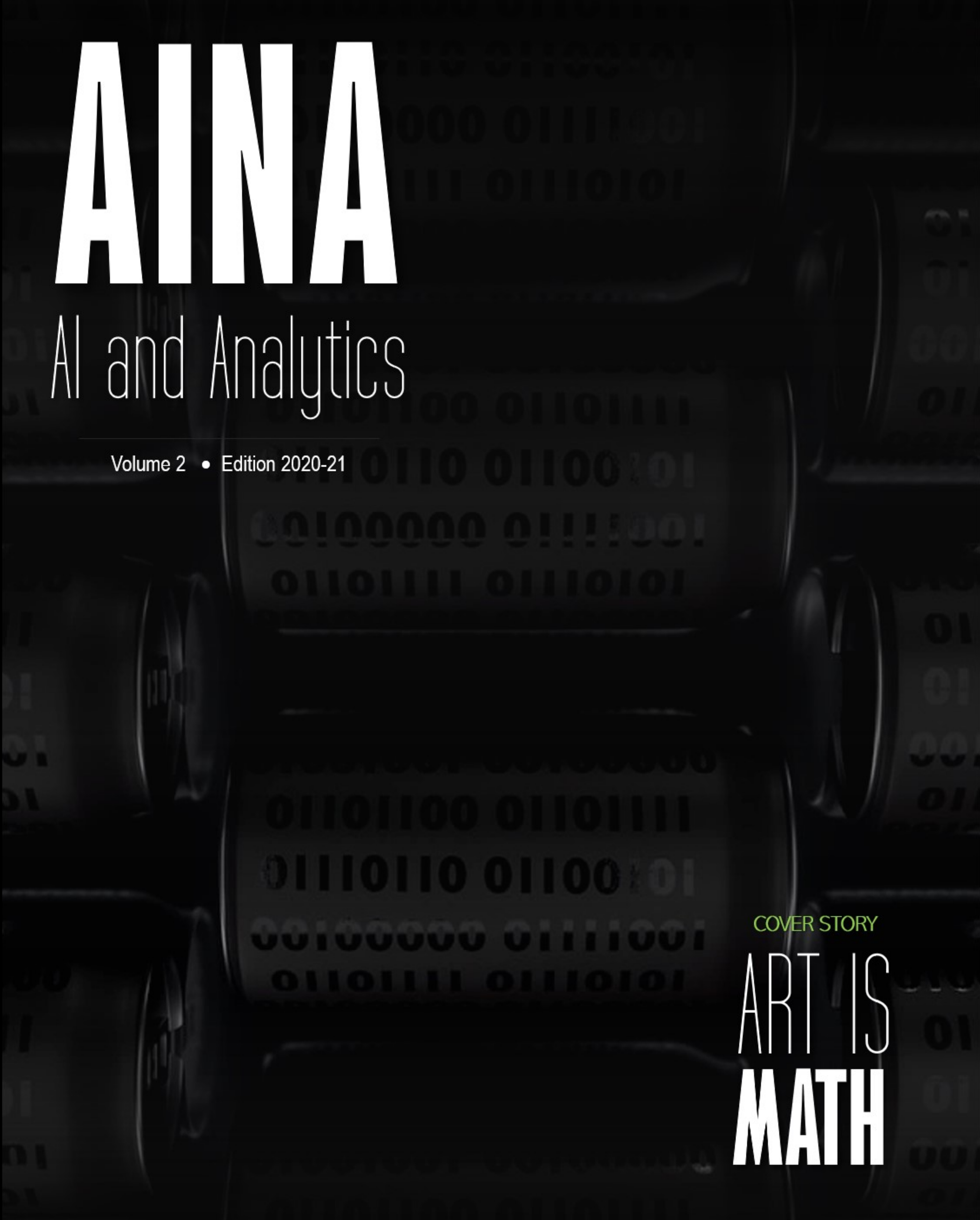
AINA

AI and Analytics

Volume 2 • Edition 2020-21



COVER STORY

ART IS MATH

Annual Analytics Magazine from the Students of PGDBA

Post Graduate Diploma in Business Analytics : Jointly offered by IIM Calcutta, ISI Kolkata & IIT Kharagpur

The Realm of Quantum Computing

Utkarsh Yadav

With each passing day, computers are becoming smaller and more powerful than ever before. There has been an exponential rise in computing power in recent decades. But as the size of transistors will reach their physical limits, the number of transistors in a dense integrated circuit cannot be increased further, violating Moore's law in the future. You might be thinking, why is there a physical limit on the size of a transistor? Let us try to understand this.

Transistors are the fundamental building blocks of classical computers. They are electrical switches that allow the passage of electrons. We already have transistors having the size of the order of 10 nanometres. As the transistors become smaller and their size approaches molecular levels, some very non-trivial problems can arise due to quantum effects. The electrons might exhibit quantum tunnelling, i.e., it just disappears from one side of the transistor and reappears on the other side, defeating the whole purpose of the electric switch! This physical limit puts a constraint on the computing power of classical computers, and to overcome it, scientists and researchers are trying to exploit quantum properties and create Quantum Computers.

A classical computer uses 'Bit', which takes a binary value of 0 or 1, as the smallest unit of information. Alternatively, a Quantum computer uses 'Qubit' instead of Bit. A qubit is a two-state quantum system that is a superposition or a mixture of 0 and 1 in a given proportion. One can think of it as a flipped coin that can either be head or tail with a specific pair of probabilities. An example of a qubit can be the polarization of a photon (vertical or horizontal) or the spin of an electron in a magnetic field (spin down or spin up). The state of a qubit collapses either to the values of 0 or 1 only when it is observed. Due to the superposition of states in qubits, quantum computers can represent far more data than a classical computer with bits. For example, 3 qubits represent 8 possible states while 3 bits represent only one among these 8 states. Hence with each unit increase in the number of qubits, we get an exponential increase in the data represented and processed in a quantum computer.

A quantum computer with N qubits can represent 2^N states, so with N=300, we have 2^{300} states which are already more than the number of particles in the observable universe! Another property of quantum physics that plays an essential role in quantum computing is entanglement. If two particles are in quantum entanglement, the state of one particle determines the state of another particle even if they are far apart.

Classical computers use logical gates to do one computation at a time. Similarly, quantum gates in quantum computers can manipulate the probabilities of qubits using the principles of superposition and entanglement to do multiple computations simultaneously. This way of simultaneous computation in quantum computers can prove to be exponentially more efficient when compared to classical computers.

Quantum computers hold a lot of promise for certain types of computation, which cannot be performed on classical computers. But, such systems require extremely low temperatures and the absence of even minute disturbances to exhibit quantum properties of superposition and entanglement. These conditions make the use of quantum systems very difficult for many practical applications. Another critical aspect of a quantum computer is that it is not universally faster as it does not perform an individual operation fast. Instead, it can perform several operations simultaneously, which is required for certain types of calculations. So, we can say quantum computers will not wholly replace classical computers, but they will coexist and complement each other.

To be or not to be?

Quantum computers could be used in an extensive range of applications. Its potential use cases could include drug discovery by simulating the interaction of drug molecules and modelling complex systems like climatic conditions or brain activity. They could also be used in computer security by creating a secure channel for communication over long distances by exploiting the principles of quantum entanglement.

Many tech companies like Google, IBM, Microsoft, etc., are already building quantum computers. Google in 2019 demonstrated quantum supremacy on a 54-qubit processor by running a target computation in 200 seconds which would have run on the world's fastest supercomputer in 10,000 years.

Research and applications in quantum computing are still in their inceptive stages, and we are anticipating many more breakthroughs in the coming years. Recent successes have motivated different nations and technology organizations to accelerate their efforts towards the quantum computing race. It would be fascinating to see what the future holds for this technology.