A Survey of Quantum Algorithms

Peter Shor
AT&T Research

ABSTRACT

Quantum computers are hypothetical devices which use the principles of quantum mechanics to perform computations. For some difficult computational problems, including the cryptographically important problems of prime factorization and finding discrete logarithms, the best algorithms known for classical computers are exponentially slower than the algorithms known for quantum computers. Although they have not yet been built, quantum computers do not appear to violate any fundamental principles of physics. I will give a mathematical model of quantum computation, explain how quantum mechanics provides this extra computational power, and briefly describe some fundamental algorithms in quantum computation, including the algorithm for efficient prime factorization.