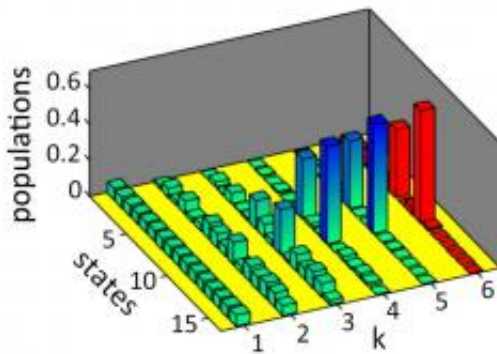


# 143 is largest number yet to be factored by a quantum algorithm

April 11 2012, by Lisa Zyga



Quantum factorization of 143 using the adiabatic quantum algorithm. As the system evolves to its ground state  $k = 6$ , it reaches a superposition of states 6 and 9, which denotes the answers 11 and 13. Image credit: Xu, et al. ©2012

American Physical Society

(Phys.org) -- While factoring an integer is a simple problem when the integer is small, the complexity of factorization greatly increases as the integer increases. When the integer grows to more than 100,000 or so digits, the problem reaches a point at which it becomes too complex to solve using classical computing methods. But quantum computers, with their use of entanglement and superposition, can theoretically factor a number of any size. However, the largest number that has been factored on a quantum processor so far is 21. Now in a new study, physicists have set a new record for quantum factorization by developing the first quantum algorithm that can factor a three-digit integer, 143, into its

prime factors, 11 and 13.

The [physicists](#), Nanyang Xu at the University of Science and Technology of China in Hefei, China, have published their study on the new quantum computation algorithm in a recent issue of [Physical Review Letters](#). They explain that, despite the potential for factoring any size number, quantum algorithms still face fundamental challenges.

“Quantum algorithms can theoretically solve the factoring problem; however, it is still challenging for today’s technologies to control a lot of qubits for a long enough time to factor a larger number,” Xu told *Phys.org*. “The environmental noises and other imperfections make the quantum system so fragile that decoherence could destroy everything stored in qubits in a short time.”

As the physicists note in their study, the first and most well-known [quantum algorithm](#) for factorization is Shor's algorithm, which was developed by mathematician Peter Shor in 1994. This algorithm, which involves quantum [entanglement](#), is based on a circuit model in which a sequence of operations is performed to solve the problem.

In the current study, Xu and coauthors use an alternative to Shor's algorithm called adiabatic quantum computation (AQC). Proposed by Edward Farhi, et al., in 2001, AQC was developed for optimization problems, in which the best value of many possible values is sought. Several computational problems, including factoring, have been formulated as optimization problems and then solved using AQC. Here, the scientists' algorithm builds on one of these formulations by Peng, et al., in 2008, which used AQC to factor the largest number before now, 21.

Unlike Shor's algorithm, AQC does not run through a sequence of operations, but instead relies on quantum adiabatic processes. More

specifically, the algorithm finds a mathematical function called the Hamiltonian in which all possible solutions are encoded as eigenstates, and the correct solution is encoded as the ground state. To solve a problem, the algorithm gradually evolves the Hamiltonian according to a mathematical equation, resulting in the system reaching its ground state and providing the correct answer. (In its physical implementation, the system consists of a liquid-crystal nuclear magnetic resonance (NMR) system like those used in magnetic resonance imaging (MRI), in which magnetic nuclei absorb and re-emit radiation at a specific frequency.)

While the adiabatic-based strategy works well in theory, in reality it still faces challenges when factoring large numbers because the Hamiltonian's spectrum of all possible eigenstates grows exponentially with the size of the integer. So Xu and coauthors developed a way to suppress the spectrum's growth by simplifying the mathematical equations governing the Hamiltonian. In the end, the physicists' simplified equations significantly decreased the growth rate of the spectrum to make it easier to factor larger numbers than before.

“We use a new method and reduce the qubits needed in the algorithm, which finally made the factorization of 143 available in realization,” Xu said. “Our work shows the practical importance of the adiabatic quantum algorithm.”

In the future, the strategies used here could lead to even larger integer factorization by quantum algorithms.

“It is possible to factor a larger number using the strategies in our current paper on current [quantum computing](#) platforms,” Xu said. “In this issue, we plan to improve our control ability towards the NMR quantum processor to factor a larger number, and the exact time complexity of the algorithm is still an open question.”

**More information:** Nanyang Xu, et al. “Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System.” *PRL* 108, 130501 (2012). [DOI: 10.1103/PhysRevLett.108.130501](https://doi.org/10.1103/PhysRevLett.108.130501)

*Copyright 2012 Phys.Org*

*All rights reserved. This material may not be published, broadcast, rewritten or redistributed in whole or part without the express written permission of PhysOrg.com.*

Citation: 143 is largest number yet to be factored by a quantum algorithm (2012, April 11) retrieved 20 March 2024 from <https://phys.org/news/2012-04-largest-factored-quantum-algorithm.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--