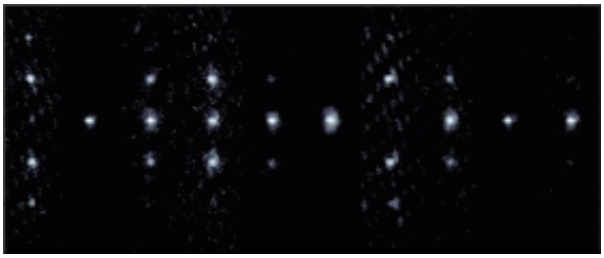
Physicists use Bose-Einstein condensates to enhance factoring algorithm

November 10 2008, By Lisa Zyga



An absorption image of the expanding Bose-Einstein condensate, demonstrating the diffraction pattern which constitutes the factoring signal. Image credit: Mark Sadgrove, et al.

(PhysOrg.com) -- Theoretically, quantum computing has the potential to work more efficiently and accurately than classical computing for certain processes, such as factoring. But quantum methods are experimentally challenging, since they often require tiny, fragile systems that are difficult to handle.

Recently, some approaches have suggested “rediscovering” old techniques such as analog computing, which usually lie outside the usual qubit architecture, in the hope of finding new pathways to experimentally realize quantum computation. For instance, using analog techniques and the quantum properties of atomic clusters called Bose-Einstein condensates, a team of researchers from Japan has recently improved upon a classical factoring algorithm.

“Any algorithm where the output is continuous rather than divided into bits (as on a digital computer) is analog,” Mark Sadgrove of the Japan Science and Technology Agency (JSTA) told *PhysOrg.com*. “In our case, we measure quantities which are continuous in principle. By this I mean that the energy or the probability to find an atom with a given momentum are continuous variables, in theory. In practice, we use a finite number of atoms, so in some sense the final outputs are discrete, but theoretically the result of the computation is analog in nature.”

Sadgrove and his colleagues Sanjay Kumar of the University of Electro Communications (UEC) in Chofushi, Chofugaoka, and Ken’ichi Nakagawa, who has affiliations with both JSTA and UEC, have demonstrated that, compared with the classical implementation, their method can distinguish more accurately between factors and non-factors of large numbers. Specifically, their quantum system could increase the accuracy of a classical algorithm called the Gauss sum algorithm, a technique pioneered by Wolfgang Shleich of Ulm University in Germany.

Their quantum system consists of thousands of rubidium-87 atoms that are cooled to near absolute zero to form a Bose-Einstein condensate (BEC). At such a low temperature, the atoms’ wavelengths increase and overlap, so that the cluster becomes a single quantum state and obeys quantum laws, yet has a relatively large size.

The physicists zapped the BEC with a brief light pulse composed of two counter-propagating beams. They programmed one beam to have phase jumps (to displace the beam’s wavelength), while the second beam had no phase jumps. Programming the first beam served as the input method, representing an integer to be factored.

The dynamics of the atoms subject to the pulse could then be used to perform factoring calculations. After applying the pulse, the researchers

allowed the BEC to expand freely for 14 ms. They then took an absorption image of the BEC, which showed that the pulse had separated the atoms in the BEC into different momentum orders. The atoms formed a diffraction pattern, based on the relative number of atoms in each momentum order, which the physicists could interpret as the "factoring signal." Specifically, high-momentum atoms represented factors, and low-momentum atoms represented non-factors.

"You can think of the laser beam as containing the software (encoded by phase jumps) and the atoms as providing the hardware (their natural dynamics in response to the light field is what actually calculates the Gauss sum)," Sadgrove explained.

In contrast to the usual Gauss sum, which is fundamentally limited in its accuracy, the quantum method significantly outperformed the classical method, in some cases doubling the atomic visibility and offering near-perfect factoring.

"In our case, our current method is still slow – it doesn't make factoring easy," Sadgrove said. "What we showed is that quantum mechanics offers an unexpected improvement to the Gauss sum method, overcoming a fundamental accuracy limit. If the atoms behaved classically, there would be no enhancement."

The researchers noted that the higher accuracy comes at a cost of requiring more atoms, so the quantum method's efficiency is about the same as that of the classical method. Nonetheless, as Sadgrove explained, the method offers a novel experiment in a field in which experiments are difficult to realize.

"You might know that everyone doing research in quantum information is excited about [Peter] Shor's algorithm for quantum factoring," Sadgrove said. "Shor found a remarkable way to factor numbers using

the quantum properties of interference and entanglement, which offers amazing savings in the time it takes for factoring a number. But Shor's algorithm is hard to implement. It's only been done successfully for up to the number 15 at the moment, and some people don't even consider that to be a real test due to some details about the way the algorithm works. So that's the current state of play regarding quantum factoring."

He added that researchers continue to investigate Shor's algorithm because of its potential impact on security: "In terms of applications, there's just one, but it's very important. If you could do real quantum factoring, then the RSA encryption used to do secure transactions in public situations would be no good anymore. That's because it relies on the fact that factoring large numbers is a hard problem. But quantum factoring makes it easy."

In the future, the physicists hope to use entangled systems as a factoring method, which they say the present scheme is ideally suited for. They also plan to investigate the use of multiple, correlated atomic ensembles to perform factoring of different integers simultaneously.

"We would also like to extend the method beyond factoring," Sadgrove said. "We can actually compute general 'exponential sums' with this method. A Gauss sum is a simple example of an exponential sum, as is a Fourier transform, which can be used to extract information about a signal. These so called 'exponential sums' are intricately tied to the most interesting parts of number theory, such as the distribution of prime numbers, which is still unknown. We think there may be other powerful applications of exponential sums apart from factoring."

More information: Sadgrove, Mark; Kumar, Sanjay; and Nakagawa, Ken'ichi. "Enhanced Factoring with a Bose-Einstein Condensate." *Physical Review Letters*, 101, 180502 (2008).