Quantum existence testing gives extreme solutions to increase network speed

March 22 2007, By Lisa Zyga

Using a novel quantum computing algorithm, scientists have simplified the process for finding extreme values in a database compared with classical and earlier quantum computing methods. With its reduced time and minimal error probability, this quantum process could significantly increase the speed of computing in global and mobile networks.

Sándor Imre, an engineer at the Budapest University of Technology, calls this new computing process "quantum existence testing," which is a special case of quantum counting. The quantum existence testing algorithm searches unsorted databases to find extreme values, attesting to the intriguing powers of the quantum mechanical effects of parallel processing.

Imre's method combines elements from classical computing as well as the latest research in quantum computing. In today's classical computers, a binary search algorithm searches for values in a structured database, although this method's linear process can take long periods of time, especially with very large databases.

"While classical registers contain only one number from a large set, quantum registers are able to handle the entire large set of numbers at the same time," Imre explained to *PhysOrg.com*. "Quantum computing is much faster because any operation on a quantum register will perform a certain function evaluation on all the numbers stored in that register. Then, using quantum parallelism, one can compare many possible phase values to a reference value in a single step."

The first quantum searching algorithm, introduced in the mid-'90s by Lov Grover, takes advantage of parallel processing to search much more quickly than with a classical algorithm. (The number of calculations in Grover's algorithm is equal to the square root of the calculations in a classical algorithm.) Imre's new quantum existence testing is a special case of Shor's phase estimation algorithm applied on Grover's circuit, as it searches not for specific values, but values with special characteristics.

"Grover's algorithm is able to find a copy of a reference element in an unsorted database; however it cannot deal with relations, i.e. greater, smaller, etc," Imre explained. "Quantum existence testing decides whether any of the elements in the database is smaller (or larger) than a reference value. Classically, to make this decision efficiently, one has to sort the database in advance and keep this sorted status continuously. But by combining quantum existence testing with classical logarithmic searching, we can achieve efficient extreme value searching in an unsorted data base."

Finding extreme values is not only important for computer scientists searching large databases, but also for everyday applications. For example, global infocom networks use the shortest path (i.e. minimum) to transfer information. Likewise, mobile networks requiring optimal signal detection need to find the largest probability density (i.e. maximum) among 10^{30} (or a thousand billion billion billion) choices or more, Imre explained.

"Many problems emerging in telecom systems can be regarded as searching in a virtual data base or function," he said. "For example, to find an optimal route between two end-users located on different continents is nothing other than searching for the best solutions (an extreme value). Or detection in a 3G mobile terminal means that a received radio signal should be compared to all possible sent signals to decide which one has been really sent."

At its basic level, Imre's quantum existence testing algorithm consists of a recursive five-step code. The process begins with splitting the searching region into two subregions, and then checking for higher/lower values in that region. Depending on the answer, the code repeats with either the lower or upper subregion.

This algorithm, like the others, is probabilistic. In practical use, it would be programmed to run through a fixed number of steps, the number of which would scale with the error probability. The greatest advantage of the algorithm, as Imre explains, is that it decreases the computational complexity of the search. In other words, the algorithm requires fewer repetitions to produce the same results compared with other methods, translating to faster networks with stronger signals.

"Compared to classical solutions, the improvement with quantum existence testing is about the square root of N in the case of a database N entry of length," Imre explained. "For example, if you are able to classically find an extreme value in a database containing 1000 entries in 1 second, then the quantum alternative can handle 1000 such databases during the same time, or a database with 1 million entries."

The question that remains, however, is when quantum computers might be built. Imre noted that there are currently some promising manufacturers that predict quantum computers within a couple years.

"It depends on many things," he said. "There are many ways to build quantum computers theoretically. The question is how scalable is the given solution? I mean, to build a few-qbit computer is more or less easy, but a 1000-plus-qbit quantum PC proves to be a really hard job. However, there are some quantum-based communication solutions (for example, key distribution) that are already on the market."

Citation: Imre, Sándor. "Quantum Existence Testing and its Application

for Finding Extreme Values in Unsorted Databases." *IEEE Transactions on Computers*. To be published.