

## Some Thoughts Regarding Practical Quantum Computing

Debabrata Ghoshal (dghoshal@gmu.edu)

Richard Gomez

School of Computational Sciences, George Mason University

Marco Lanzagorta

Advanced Engineering and Sciences, ITT Industries

Center for Computational Science, US Naval Research Laboratory

School of Computational Sciences, George Mason University

Jeffrey Uhlmann

Department of Computer Science

University of Missouri - Columbia

Author Summary of Paper W40.00015

Thursday, March 16, 2006, 5:18 PM, Rm 343

2006 APS March Meeting, Baltimore, MD

Quantum Computing (QC) indisputably offers a new model of computation that can allow certain problems to be solved more efficiently than is possible using Classical Computing (CC). This improved efficiency comes from the ability to apply operations in parallel to an entire dataset maintained in a quantum superposition. However, it is not the case that every classical operation can be applied to a superposition to exploit quantum parallelism. For example, the fundamental quantum no-cloning theorem prohibits the copying of information in a quantum superposition and hence does not allow us to store intermediate results. This severely restricts the class of algorithms for which QC can provide better complexity than CC.

Until recently, the class of algorithms for which QC improves CC has been defined only by a handful of special-case problems. In the past two years, however, the development of the semiclassical extraction algorithm by Lanzagorta and Uhlmann has demonstrated that quantum search algorithms (e.g., Grover's algorithm) can be generalized to solve an enormous class of practical problems more efficiently than is possible with CC. Thanks to this algorithm, QC can potentially be used to increase the performance of real practical software systems, including those for computer graphics, target tracking and guidance of autonomous vehicles.

The 2005 ACM SIGGRAPH conference in Los Angeles, CA, will likely be regarded as a significant historical event in that it recognized quantum computing as a serious emerging technology with important practical implications for mainstream applications. Specifically, SIGGRAPH 2005 included a course by Lanzagorta and Uhlmann on the applications of quantum computing to computer graphics, simulation, and search. The results presented in this course demonstrated to the large mainstream audience that quantum algorithms represent the only way to supercede classical lower bounds for many important classes of problems relating to computer

graphics and visualization. This presentation is regarded as a breakthrough in the serious consideration of quantum computation (as opposed to cryptography or communications) by a major mainstream technical organization (Siggraph is the largest and most important computer graphics conference in the world).

Overall, the semiclassical protocol provides some theoretical cause for optimism because it suggests that other classes of algorithms may similarly circumvent the apparent limitations imposed by the no-cloning theorem. Unfortunately, there remain many challenging practical issues that have the potential to represent bigger challenges than the no-cloning theorem. These issues include the storage of data in quantum memory for access by a superposition of indices; quantum memory devices and quantum memory addressing schemes; the input/output of classical information to/from quantum registers; logical debugging; the compilation of oracle functions on quantum hardware; the ability to dynamically change oracle functions, e.g., to support interactive manipulation of superpositions; and the ability to maintain superpositions for practical lengths of time.

In collaboration between George Mason University, the University of Missouri-Columbia, ITT Industries, and the US Naval Research Laboratory, we have been studying these types of problems that need to be solved if we want QC to become a general computational tool able to speed up real software systems, with clear and practical applications for the defense, scientific, financial and industrial establishments.