Computation in Quantum Space-Time Can Lead to a Super-Polynomial Speedup

Michael Zakharevich
Department of Mathematics
Stanford University
ymzakharevich@yahoo.com

Vladik Kreinovich
Department of Computer Science
University of Texas at El Paso
vladik@utep.edu

In theoretical computer science, researchers usually distinguish between problems that can be solved in polynomial time (i.e., in time that is bounded by a polynomial of the length n of the input) and problems that require more computation time. Problems solvable in polynomial time are usually called _feasible_, while others are called _intractable_. Of course, this association is not perfect -- for example, an algorithm that requires 10^100 * n steps is polynomial time but not feasible -- but this is the best available definition of feasibility.

A natural question is: can we use new physical processes, processes that have not been used in modern computers, to make computations drastically faster -- e.g., to make intractable problems feasible?
Such a possibility would occur if a physical process provides a super-polynomial (= faster than polynomial) speed-up.

In this direction, the most active research is undertaken in quantum computing. It is well known that quantum processes can speed up computations; see, e.g., (Nielsen and Chuang 2000). For example, Grover's algorithm enables us to reduce the computation time of many computations from 2^n to sqrt(2^n) = 2^(n/2). Some known quantum algorithms -- e.g., Shor's factorization algorithm -- are exponentially faster than the best known non-quantum ones; however, it is not clear whether a similar fast non-quantum algorithm is possible. In general, the only _proven_ quantum speed-ups are polynomial.

Parallelization is another potential source of speed-up. In Euclidean space-time, parallelization only leads to a polynomial speed-up; see, e.g., (Morgenstein and Kreinovich, 1995), (Kreinovich and Finkelstein 2004-06), and (Kreinovich and Margenstern 2008-09). The reason is that, since the speed of all the physical processes is bounded by the speed of light c, in time T, we can only reach computational units at a distance not exceeding R = c * T. In the Euclidean space, the volume of this area (inside of the sphere of radius R = c * T) is proportional to R^3 ~ T^3, so we can use no more than ~ T^3 computational elements.

In quantum space-time models (see, e.g., (Misner et al. 1975)), the corresponding volume grows super-polynomially with the radius R; see, e.g., (Finkelstein and Kreinovich 1987). Thus, we can fit a super-polynomial number of processors within a sphere of radius R = c * T. Hence, in quantum space-time, parallelization can potentially leads to super-polynomial speed-up of computations.

This is not (yet) a reduction from exponential time 2^n to polynomial time, but this is a solidly super-polynomial reduction from 2^n to 2^sqrt(n).

References

Andrei M. Finkelstein and Vladik Kreinovich. "The singularities in quantum cosmology," Astrophysics and Space Science, 1987, No. 1, pp. 73-76.

V. Kreinovich and A. M. Finkelstein, "Towards Applying Computational Complexity to Foundations of Physics", Notes of Mathematical Seminars of St. Petersburg Department of Steklov Institute of Mathematics, 2004, Vol. 316, pp. 63-110; reprinted in Journal of Mathematical Sciences, 2006, Vol. 134, No. 5, pp. 2358-2382.

V. Kreinovich and M. Margenstern, "In Some Curved Spaces, One Can Solve NP-Hard Problems in Polynomial Time", Notes of Mathematical Seminars of St. Petersburg Department of Steklov Institute of Mathematics, 2008, Vol. 358, pp. 224-250; reprinted in Journal of Mathematical Sciences, 2009, Vol. 158, No. 5, pp. 727-740.

C. W. Misner, K. S. Thorne, and J. A. Wheeler, Gravitation, Freeman, San Francisco, 1973.

D. Morgenstein and V. Kreinovich, "Which algorithms are feasible and which are not depends on the geometry of space-time", Geombinatorics, 1995, Vol. 4, No. 3, pp. 80-97.

M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, Massachusetts, 2000.