Speedup in quantum computation is associated with attenuation of processing probability

K. Svozil
Institut für Theoretische Physik
University of Technology Vienna
Wiedner Hauptstraße 8-10/136
A-1040 Vienna, Austria
e-mail: svozil@tph.tuwien.ac.at

January 17, 1995

kraft.tex

Abstract

Quantum coherence allows the computation of an arbitrary number of distinct computational paths in parallel. Based on quantum parallelism it has been conjectured that exponential or even larger speedups of computations are possible. Here it is shown that, although in principle correct, any speedup is accompanied by an associated attenuation of detection rates. Thus, on the average, no effective speedup is obtained relative to classical (nondeterministic) devices.

Recent findings in quantum complexity theory suggest an exponential speedup of discrete logarithms and factoring [1] and the travelling salesman problem [2] with respect to classical complexity. (The best classical estimate for the computing time for factoring is $e^{cn^{1/3}}$, where n is the number of bits in the number to be factored and c is a constant; the travelling salesman problem is *NP*-complete). At the heart of these types of speedups is quantum parallelism. Roughly stated, quantum parallelism assures that a single quantum bit, henceforth called *qbit,* can "branch off" into an arbitrary number of coherent states. A typical physical realization of a qbit is a single field mode of a photon (electron, neutron), with the empty and the one-photon state $\mid 0\rangle$ and $\mid 1\rangle$ representing the classical symbols 0 and 1, respectively. The qbit is representable by $a \mid 0\rangle + b \mid 1\rangle$ with $|a|^2 + |b|^2 = 1$. The branching process into coherent beam paths can be realized by an array of beam splitters such as semitransparent mirrors or a double slit. A typical cascade of branching process into n^k coherent beam paths is described by a successive array of k identical beam splitters with n slots and vanishing relative phases

$$\mid s_0\rangle \rightarrow \frac{1}{\sqrt{n}}\left(\mid s_0 s_{11}\rangle + \mid s_0 s_{12}\rangle + \cdots + \mid s_0 s_{1n}\rangle\right) \quad , \tag{1}$$

$$\frac{1}{\sqrt{n}} \mid s_0 s_{11}\rangle \rightarrow \frac{1}{n}\left(\mid s_0 s_{11} s_{21}\rangle + \mid s_0 s_{11} s_{22}\rangle + \cdots + \mid s_0 s_{11} s_{2n}\rangle\right) \tag{2}$$

$$\frac{1}{\sqrt{n}} \mid s_0 s_{12}\rangle \rightarrow \frac{1}{n}\left(\mid s_0 s_{12} s_{21}\rangle + \mid s_0 s_{12} s_{22}\rangle + \cdots + \mid s_0 s_{12} s_{2n}\rangle\right) \tag{3}$$

$$\vdots$$

$$\frac{1}{n^{-(k-1)/2}} \mid s_0 s_{1n} \cdots s_{(k-1)n}\rangle \rightarrow \frac{1}{n^{-k/2}}\left(\mid s_0 s_{1n} \cdots s_{kn}\rangle + \cdots + \mid s_0 s_{1n} \cdots s_{kn}\rangle\right) \ . \tag{4}$$

Notice that every beam splitter contributes a normalization factor of $1/\sqrt{n}$ to the amplitude of the process. The probability amplitude for a single quantum in state $\mid s_0\rangle$ to evolve into one particular beam path $s_0 s_{1i_1} s_{2i_2} s_{3i_3} \cdots s_{ki_k}$ therefore is

$$\langle s_0 s_{1i_1} s_{2i_2} s_{3i_3} \cdots s_{ki_k} \mid U \mid s_0\rangle = n^{-k/2} \quad , \tag{5}$$

where U stands for the unitary evolution operator corresponding to the array of beam splitters.

More generally, any one of the entangled qbits originating from the branching process can be processed in parallel. The beam path $s_0 s_{1i_1} s_{2i_2} s_{3i_3} \cdots s_{ki_k}$ can be interpreted as a *program code* [3, 4, 5, 6]. How many programs can be coded

into one beam path? Notice that, in order to maintain coherence, no code of a valid program can be the prefix of a code of another valid program. Therefeore, in order to maintain the parallel quality of quantum computation, only *prefix* or *instantaneous* codes are allowed. A straightforward proof using induction [3] shows that the instantaneous code of q programs $\{p_1, p_2, \ldots, p_q\}$ with length $l_1 \leq l_2 \leq \cdots \leq l_q$ satisfies the *Kraft inequality*

$$\sum_{i=1}^{q} n^{-l_i} \leq 1 \quad , \tag{6}$$

where n is the number of symbols of the code alphabet. In our case, n is identified with the number of slits in the beam splitters. Stated pointedly, instantaneous decodability restricts the number of legal programs due to the condition that to legal program can be the prefix of another legal program. The Kraft inequality then states that no more than maximally $q = n^k$ programs can be coded by a successive array of k identical beam splitters with n slots, corresponding to $l_1 = l_2 = \cdots = l_q$. The more general case $l_1 \leq l_2 \leq \cdots \leq l_q$ can be easily realized by allowing beams not to pass *all* k n-slit arrays.

By recalling equation (5), it is easy to compute the probability that a particular program p_j of length $l_j \leq k$ is executed. It is

$$\left|\langle s_0 s_{1i_1} s_{2i_2} s_{3i_3} \cdots s_{l_j i_{l_j}} \mid U \mid s_0 \rangle\right|^2 = n^{-l_j} \quad . \tag{7}$$

Therefore, there is an inevitable exponential decrease n^{-l_j} in the execution probability.

One possible way to circumvent attenuation would be to amplify the output signals from the beam splitter array. Classically, amplification and copying of bits is no big deal. In quantum mechanics, however, the no-cloning theorem [7] does not allow copying of quantum bits. Any attempt to copy qbits would result in the addition of noise (e.g., from spontaneous emmission processes) and, therefore, in errornous computations.

In summary, the price for speedups of computations originating in quantum parallelism is a corresponding attenuation of the computation probability. In order to compensate for an exponential decrease of execution probability, one would have to *exponentially increase* the number of (bosonic) quanta in the beam paths. This, however, is equivalent to the trivial solution of an arbitrarily complex problem by the introduction of an arbitrary number of classical parallel computers.

References

[1] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, in *Proc. 35th Annual Symposium of on Foundations of Computer Science* (IEEE Press, November 1994), in press. Notice that, in order to factorize a binary integer n with $N = O(\log_2 n)$ places, the dimension of the unitary matrix grows exponentially with N; more specifically, $q = O(n^2) = O(2^{2N})$.

[2] V. Černý, *Phys. Rev.* **A 48**, 116 (1993).

[3] R. W. Hamming, *Coding and Information Theory, Second Edition* (Prentice-Hall, Englewood Cliffs, New Jersey, 1980).

[4] G. J. Chaitin, *Information, Randomness and Incompleteness, Second edition* (World Scientific, Singapore, 1987, 1990); *Algorithmic Information Theory* (Cambridge University Press, Cambridge, 1987); *Information-Theoretic Incompleteness* (World Scientific, Singapore, 1992).

[5] C. Calude, *Information and Randomness — An Algorithmic Perspective* (Springer, Berlin, 1994).

[6] K. Svozil, *Randomness and Undecidability in Physics* (World Scientific, Singapore, 1993).

[7] W. K. Wooters and W. H. Zurek, *Nature* **299**, 802 (1982); L. Mandel, *Nature* **304**, 188 (1983); P. W. Milonni and M. L. Hardies, *Phys. Lett.* **92A**, 321 (1982); R. J. Glauber, *Amplifiers, Attenuators and the Quantum Theory of Measurement*, in *Frontiers in Quantum Optics*, ed. by E. R. Pikes and S. Sarkar (Adam Hilger, Bristol 1986); C. M. Caves, *Phys. Rev.* **D 26**, 1817 (1982).