Computation and Quantum Superposition

Richard Jozsa
Département IRO
Université de Montréal
C.P. 6128, Succursale A
Montréal, P.Q. Canada H3C 3J7

Abstract

We review recent work and some new results on the role of quantum superpositions in providing new modes of computation, not available to classical computers. For certain problems, these new modes can provide an exponential reduction in complexity over any classical computer demonstrating the importance of quantum processes for issues in complexity theory.

Introduction

Computation and information theory are well known to be fundamentally related to physics [1] - the operation of any computing machine is a physical process so that questions about the possibilities and limitations of computation must make reference to physical laws. On the other hand any act of measurement in physics may be viewed as an information gathering process, which may be analysed within the framework of information theory [4]. Wheeler and others [2,3] have suggested that the links between physics and computation may provide the key to understanding the origin of physical laws at the most fundamental level.

Despite these links, the standard mathematical theory of computational complexity rests firmly on *classical* (rather than quantum) physics. The fundamental concept of Turing machine [5] is clearly abstracted from classical considerations, disallowing quantum effects during a computation (e.g. writing a superposition of 0 and 1 on a tape square at some stage.)

The systematic consideration of computing processes in the context of quantum physics began in the early 1980's with the work of Benioff [6], followed by Feynman [7], Peres [8] and Deutsch [9,10]. Of these, Deutsch emphasised the novel implications of quantum interference, allowing the information bearing bits of the computer to begin in, end in or pass through states which are superpositions of the basic values 0 and 1. This gives rise to new modes of computation [9,11,12] not available to any classical computer. These modes affect the computational complexity of problems but no new functions (which are not already Turing computable) can be computed.

As will become clear below, the practical implementation of these new modes requires maintaining quantum coherence for many computational steps in potentially large systems (the joint state of many bits of memory). The number of degrees of freedom may even become unbounded in theoretical considerations, for example, of polynomial versus exponential complexity, which are essentially asymptotic concepts. Although the required level of coherence is probably impossible to achieve in practice, the present investigation may be expected to be of interest for fundamental theoretical issues in computation and quantum theory, e.g. possibly providing a new approach to the problem of whether quantum theory is valid in the macroscopic domain [17] or not. Also for some "small" computations (e.g. computing the XOR of two bits [9,12]) the quantum method does provide a new, plausibly implementable method of computation. The investigation of these new modes in the presence of restricted coherence remains a problem for future work.

We will describe two applications of quantum superpositions - computation by quantum parallelism and the solution of relational problems.

Computation by quantum parallelism

Let $\mathcal{U}_f$ be a device that computes a function $f : \mathbf{Z}_m \rightarrow \mathbf{Z}_n$ (i.e. a quantum computer [9] programmed to compute f) and let $\mathcal{H}_{mn}$ be a Hilbert space of dimension mn with a fixed orthonormal basis denoted $[i, j]$, $i \in \mathbf{Z}_m, j \in \mathbf{Z}_n$. Suppose that $\mathcal{U}_f$ operates by accepting an input state $[i, 0]$ and evolving it to the output state $[i, f(i)]$ from which $f(i)$ may be read with probability 1. Then by linearity of quantum evolution, $\mathcal{U}_f$ will evolve the input state $v_{in} = ([0,0] + \ldots + [m-1, 0])$ into the output state

$$v(f) = ([0, f(0)] + \ldots + [m-1, f(m-1)]) \qquad (1)$$

Thus by running $\mathcal{U}_f$ only *once*, we have computed *all* m values of f in superposition. The term "computation by quantum parallelism" refers to this process of using a superposed input to conduct parallel computations in quantum superposition. (We will consider here only the *equally* weighted superposition above but more general forms may also be considered [12].) Unfortunately the full information of the list of values

0-8186-3420-0/93 $03.00 © 1993 IEEE

$f(0), \ldots, f(m-1)$ cannot be extracted from the state $v(f)$ but certain joint properties $G(f(0), \ldots, f(m-1))$ (abbreviated $G(f)$) can, in a probabilistic sense described below.

The class of computational task we shall be considering involves being given $\mathcal{U}_f$ and then using it to determine some property $G(f)$ in an efficient way. On a classical computer we would generally need to repeatedly run $\mathcal{U}_f$, obtaining sufficiently many values $f(i)$ to determine $G(f)$. On a quantum computer we utilise the superposition $v(f)$ obtained after only one run, as follows.

Let $G(f)$ be a property taking values in the list $\gamma_1, \ldots, \gamma_k$. Then we will say that G is "computable by quantum parallelism" (abbreviated QPC) if there is a quantum observable $\mathcal{G}$ with eigenvalues $\gamma_1, \ldots, \gamma_k, fail$ (and corresponding eigenspaces denoted $E(\gamma_1), \ldots, E(\gamma_k), E(fail)$) satisfying (a) $proj_{E(\gamma)}(v(f)) = 0$ if $G(f) \neq \gamma$ and (b) $proj_{E(\gamma)}(v(f)) \neq 0$ if $G(f) = \gamma$. Hence if $\mathcal{G}$ is measured on any one of the vectors $v(f)$ the only possible results are the correct value $G(f)$ or the result *fail*. Furthermore the correct value is always seen with a *non-zero* probability, denoted $p(f)$. A wrong answer is never obtained.

Some examples of QPC G's are given in [9,12]. For $f : \mathbf{Z}_2 \to \mathbf{Z}_2$ the Boolean sum $G(f) = f(0) \oplus f(1)$ is QPC (with all probabilities $p(f)$ being $1/2$) but the Boolean product is not QPC.

These considerations raise the following questions: (a) How can we characterise the properties which are QPC? (b) How large can the probabilities $p(f)$ of successful computation be? Some results relating to (b) are given in the next section. The results below provide some answers to (a).

We first describe an alternative characterisation of G being QPC. Let $a_1 v(f_1) + \ldots + a_l v(f_l) = 0$ be a linear relation (with each a_i nonzero and each f_i occurring at most once.) We say that G "respects" the linear relation if the list $G(f_1), \ldots, G(f_l)$ contains each occurring value at least twice (i.e. no value occurs exactly once). Then it may be shown [12] that G is QPC if and only if G respects all linear relations amongst the n^m vectors $v(f)$. This result remains true for any choice of vectors $v(f)$ "representing " the functions f. Thus to increase the number of QPC G's we should arrange that the $v(f)$'s be as linearly independent as possible.

For our choice of equally weighted $v(f)$'s, all linear relations may be explicitly characterised [12] leading to results like the following: For the case of binary variables (i.e. $f : \mathbf{Z}_m \to \mathbf{Z}_2$ and $G : (\mathbf{Z}_2)^m \to \mathbf{Z}_2$), the only functions G which are QPC are (a) the constant function at 0 (b) the m projection functions (c) the $m(m-1)/2$ pairwise Boolean sums $G_{ij}(a_0, \ldots, a_{m-1}) = a_i \oplus a_j$, and the functions obtained by Boolean sum of 1 to each of these. This seems rather limiting but the class of QPC functions may be significantly increased by considering other natural constructions for the $v(f)$'s.

Probabilities of successful computation

If G is QPC then a successful computation can give the benefit of m computations of f for the price of one. This is computationally significant if the probabilities $p(f)$ can be made suitably large (e.g. if an average of them depending on the provided distribution of f's is larger than $1/m$.) We describe two results limiting the size of the probabilities.

Firstly, Deutsch [9] has shown that if G is QPC (for $f : \mathbf{Z}_m \to \mathbf{Z}_n$) then the smallest of the $p(f)$'s is always $\leq 1/m$.

Secondly, the decoding of a QPC property G may be thought of as the transmission of information through a quantum channel. The sender is transmitting the values $G(f)$ encoded as the state vectors $v(f)$. The receiver decodes the messages by applying the observable $\mathcal{G}$. The theorem of Kholevo [14] (also described in [15]) may be applied to this situation and used to derive the following result [13]. Consider the equation

$$(2-a)ln(2-a) - (1-a)ln(1-a) = 2ln(\frac{2m-1}{m}) - \frac{ln(2m-1)}{m} \tag{2}$$

Then (a) for each $m \in \mathbf{N}$ there is a unique solution $0 \leq a(m) \leq 1$ (b) $a(m)$ is monotonic decreasing in m with $a(m) \to 0$ as $m \to \infty$ and (c) for any QPC property G (on $f : \mathbf{Z}_m \to \mathbf{Z}_n$) *every* probability $p(f)$ is $\leq a(m)$.

Hence isolated probabilities can never remain large as m is increased. It may also be shown that $a(m) > 1/m$ for all m (in fact asymptotically $a(m) \sim (log_2 m)/m$) so this bound does not include Deutsch's result as a special case, nor does it settle the question of whether the average of the $p(f)$'s for some G can exceed $1/m$.[18]

Relational problems

So far we have been concerned with the computation of functions i.e. where the answer for a given input is unique. A more general class of problem involves the mathematical notion of a relation (which may be thought of as a "one-to-many" function). Given an input, the problem is to find any one of its relatives, e.g. given a composite number, find any one of its factors.

Deutsch has pointed out that in this context, a quantum computer offers another new mode of computation. A classical computer will always evaluate a function "subordinate" to the relation e.g a factorisation program will always find the *same* factor of a given input. However, a quantum computer may halt in an output state which represents a superposition of *all* the relatives (e.g. factors of a given number). Repeated computation on the same input followed by an observation of the output will generally yield different, but always correct, answers. This more general form of the output state implies less restriction on the computational evolution which may be exploited as a saving in computational complexity.

An example of such a problem has been given in [11] and reformulated in an elegant mathematical form in [16]. In contrast to the probabilistic nature of computation by quantum parallelism, this problem is always solved *with certainty* by the quantum computer. Furthermore, in a suitable context [11,16], the quantum computer offers an exponential saving in complexity over any classical computer. This provides clear evidence that the theory of computational complexity will need to be modified in the presence of quantum modes of computation.

References

[1] Zurek,W.H.(ed), Complexity, Entropy and the Physics of Information (Proceedings of the 1988 SantaFe Workshop) 530pp. Addison Wesley (1990)

[2] Wheeler, J.A. in Ref. [1] pp 3-28.

[3] Landauer, R. *Found.Phys.*,**16**, 551-564 (1986)

[4] Zurek, W.H. in Quantum Optics, Experimental Gravitation and Measurement Theory, ed. P. Meystre, M.O. Scully pp 87-116, NATO ASI Series B;Physics Vol 94 Plenum Press (1983)

[5] Garey, M.R. and Johnson, D.S. Computers and Intractibility. Freeman and Co. (1979)

[6] Benioff, P. *J. Stat. Phys.*, **22**, 563 (1980), **29**, 515 (1982), *Phys. Rev. Lett.*, **48**, 1581 (1982), *Int. J. Theor. Phys.*, **21**, 177 (1982)

[7] Feynman, R.P. *Int. J. Theor. Phys.*, **21**, 467-488 (1982) *Found. Phys.*, **16**, 507-531 (1986)

[8] Peres, A. *Phys.Rev.***A32**,3266-3276(1985)

[9] Deutsch, D. *Proc. Roy. Soc. Lond.* **A400**, 97-117 (1985)

[10] Deutsch, D. *Proc. Roy. Soc. Lond.* **A425**, 73-90 (1989)

[11] Deutsch, D. and Jozsa, R. "Rapid Solution of Problems by Quantum Computation",(to appear *Proc.Roy.Soc.Lond.* 1992)

[12] Jozsa, R. *Proc. Roy. Soc. Lond.* **A435**, 563-574 (1991)

[13] Jozsa, R. "An Entropic Bound on Probabilities in Quantum Computation"(preprint, in preparation, 1992)

[14] Kholevo, A.S. *Problemy Peredachi Informatsii*,**9**, 3-11(1973), (Translated by IEEE under title *Problems of Information Transfer.*)

[15] Schumacher, B. in Ref. [1] pp 29-37.

[16] Berthiaume, A. and Brassard, G. in Proceedings of 7th Annual IEEE Structures in Complexity Theory Meeting (1992)

[17] Leggett, A.J. pp 28-40 in Quantum Concepts in Space and Time, ed. R.Penrose and C. Isham, Clarendon Press,Oxford(1986)

[18] *Note added in proof:* More recent work (Jozsa 1992) has settled these questions (without any reference to Kholevo's theorem) showing that *every* $p(f)$ is $\leq 1/m$. This applies to the equally weighted superposition given in (1) and holds for G's which are nonconstant in at least two variables. (If G varies with only one of its arguments then input superpositions provide no benefit in its computation.)