# Entanglement in Quantum Algorithms

**Richard Jozsa**
richard@cs.bris.ac.uk

Department of Computer Science, University of Bristol
Woodland Road, Bristol BS8 1UB, U.K.

It is often loosely stated that entanglement is the novel quantum feature that gives rise to computational speedup in quantum algorithms. We will discuss various aspects of this question. We show that the presence of multi-partite entanglement, with an unboundedly increasing number of parties, is necessary in any quantum algorithm operating on pure states, if the algorithm exhibits an exponential speedup over any classical algorithm for the same computational task.

For algorithms operating on general mixed states it is not known whether entanglement is necessary at all for an exponential speedup. However in special cases we can say more: if the mixed states have the form of the so-called pseudo-pure states and known quantum algorithms (such as Shor's or Grover's algorithms) are implemented in the standard manner on these states, then the presence of entanglement in the states is again necessary if the implementation uses physical resources that grow polynomially with input size.

Grover's searching algorithm is often regarded as fundamentally different in its quantum effects from Shor's algorithm (and its generalisation, the abelian hidden subgroup algorithm). We will discuss the role of entanglement in Grover's algorithm and argue that the origins of the quantum benefits in Shor's and Grover's algorithms are, in fact, essentially the same.