25 January 2000
revised 22 June 2000
quant-ph/0007070

SOPHISTICATED QUANTUM SEARCH WITHOUT ENTANGLEMENT

David A. Meyer

Project in Geometry and Physics
Department of Mathematics
University of California/San Diego
La Jolla, CA 92093-0112
dmeyer@chonji.ucsd.edu

and Institute for Physical Sciences
Los Alamos, NM

ABSTRACT

Although entanglement is widely considered to be necessary for quantum algorithms to improve on classical ones, Lloyd has observed recently that Grover's quantum search algorithm can be implemented without entanglement, by replacing multiple particles with a single particle having exponentially many states. We explain that this maneuver removes entanglement from *any* quantum algorithm. But *all* physical resources must be accounted for to quantify algorithm complexity, and this scheme typically incurs exponential costs in some other resource(s). In particular, we demonstrate that a recent experimental realization requires exponentially increasing precision. There is, however, a quantum algorithm which searches a 'sophisticated' database (not unlike a Web search engine) with a single query, but which we show does not require entanglement even for multiparticle implementations.

1999 Physics and Astronomy Classification Scheme: 03.67.Lx, 32.80.Rm.
2000 American Mathematical Society Subject Classification: 81P68, 68Q15.

Key Words: quantum algorithms, entanglement, query complexity.

Quantum algorithms must exploit some physical resource unavailable to classical computers in order to solve problems in fewer steps [1,2,3,4,5]. Entanglement, which seems the "spookiest" [6] to many people, has been argued to be the crucial quantum mechanical resource [7]. This belief informs, for example, the criticism that NMR experiments performed to date [8] have not actually realized quantum algorithms because at each timestep the state of the system can be described as a probabilistic ensemble of unentangled quantum states [9]. Lloyd [10] and Ahn, Weinacht & Bucksbaum [11] have recently suggested, however, that entanglement is *not* necessary for Grover's quantum search algorithm [4]. In this Letter we clarify the situation by demonstrating that, contrary to their claims, the experimental realization of Ahn, Weinacht & Bucksbaum [11] requires an exponentially increasing amount of a resource—precision—replacing entanglement. But we do not conclude from this that entanglement (or some replacement resource) is required. Rather, we make the new and surprising observation that efficient quantum search of a 'sophisticated' database (not unlike a Web search engine) requires no entanglement at any timestep: a quantum-over-classical reduction in the number of queries is achieved using only interference, not entanglement, within the usual model of quantum computation.

The problem which forms the context for our discussion is database search—identifying a specific record in a large database. Formally, label the records $\{0, 1, \ldots, N-1\}$, where, for convenience when we write the numbers in binary, we take $N = 2^n$ for n a positive integer. Grover considered databases which when queried about a specific number, respond only that the guess is correct or not [4]. On a classical reversible computer we can implement a query by a pair of registers (x, b) where x is an n-bit string representing the guess, and b is a single bit which the database will use to respond to the query. If the guess is correct, the database responds by adding 1 (mod 2) to b; if it is incorrect, it adds 0 to b. That is, the response of the database is the operation: $(x, b) \to \big(x, b \oplus f_a(x)\big)$, where $\oplus$ denotes addition mod 2 and $f_a(x) = 1$ when $x = a$ and 0 otherwise. Thus if b changes, we know that the quess is correct. Classically, it takes $N - 1$ queries to solve this problem with probability 1.

Quantum algorithms work by supposing they will be realized in a quantum system, such as those described by Lloyd [10] and Ahn, Weinacht & Bucksbaum [11], which can be in a superposition of 'classical' states. These states form a basis for the Hilbert space whose elements represent states of the quantum system. The simplest such system is a *qubit* [12], which can be in a superposition of the states of a classical bit, *i.e.*, 0 and 1. More generally, Grover's algorithm works with quantum queries which are linear combinations $\sum c_{x,b}|x, b\rangle$, where the $c_{x,b}$ are complex numbers satisfying $\sum |c_{x,b}|^2 = 1$ and $|x, b\rangle$ is Dirac notation [13] for the quantum state which represents the classical state (x, b) of the two registers. The operations in quantum algorithms are unitary transformations, the quantum mechanical generalization of reversible classical operations. Thus the operation of the database Grover considered is implemented on superpositions of queries by a unitary transformation (f_a-controlled-NOT), which takes $|x, b\rangle$ to $|x, b \oplus f_a(x)\rangle$. Fig. 1 illustrates a quantum circuit implementation [14] of Grover's algorithm [4]. Using $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ quantum queries it identifies the answer with probability close to 1: the final vectors for the N possible answers a are nearly orthogonal.

This quantum circuit acts on an initial state $\psi_0 = |0\rangle \cdots |0\rangle|0\rangle = |0\ldots 0, 0\rangle$. The first set of gates transforms the state to $\psi_1 = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\cdots\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = \sum_{x=0}^{N-1}|x\rangle(|0\rangle-|1\rangle)/\sqrt{2N}$. Both these states, ψ_0 and ψ_1, are tensor products of the states of the individual qubits, so they are *unentangled* [16]. This is no longer true for subsequent states of the system (except when $N = 2$). The last qubit, however, is never entangled with the others—after the first timestep it remains in state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Lloyd's observation [10], which is exploited by Ahn, Weinacht & Bucksbaum [11], is that the absence of entanglement in the $N = 2$ case of Grover's algorithm (for which the guess register consists of a single qubit), generalizes to arbitrary N if the guess register is realized by one N state particle rather than by n qubits. In fact, Jozsa and Ekert [7] made exactly this observation several years ago: they wrote, "The state of n qubits is a 2^n dimensional space and can be isomorphically viewed as the state space of a *single* particle with 2^n levels. Thus we simply view certain states of a single 2^n level particle as 'entangled' via their correspondence under a chosen isomorphism between $\otimes^n\mathcal{H}_2$ and $\mathcal{H}_{2^n}$ (where $\mathcal{H}_k$ denotes a Hilbert space of dimension k.)". So despite the implication of Lloyd's [10] and Ahn, Weinacht & Bucksbaum's [11] papers, there is nothing special about Grover's algorithm: reformulating *any* quantum algorithm this way, *i.e.*, disregarding the tensor product structure of Hilbert space implicit in the use of qubits, removes entanglement from the system *by definition*. Nevertheless, one might hope that if a quantum algorithm—like Grover's—can be implemented naturally with a single particle, as Lloyd suggests [10] and as Ahn, Weinacht & Bucksbaum realized experimentally with N Rydberg levels of a cesium atom [11], there is some physical advantage to be gained.

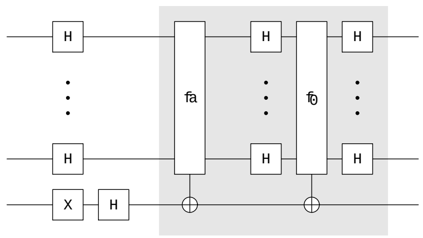

Figure 1. A (schematic) quantum circuit implementing Grover's algorithm. Each horizontal line represents a single qubit, which is initialized (on the left) in state $|0\rangle$. The portion of the circuit enclosed in the grey square is repeated $\lfloor\frac{\pi}{4}\sqrt{N}\rfloor$ times and then the top n qubits are measured. H is the Hadamard transformation $\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)/\sqrt{2}$, X is the Pauli matrix $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, and the 'gates' acting on all $n+1$ qubits are f_a- and f_0-controlled-NOT transformations, respectively. As was first noted by Brassard & Høyer, and subsequently by Grover, the $H^{\otimes n}$ $(\otimes I_2)$ transformation conjugating the f_0-controlled-NOT gate can be replaced by almost any unitary transformation [15]. Our discussion is independent of this choice.

But Jozsa and Ekert [7] continue, "However the physical implementation of this correspondence appears always to involve an exponential overhead in some physical resource so that the isomorphism is *not* a valid correspondence for considerations of complexity.", again anticipating Lloyd's discussion [10]. Although their data indicate that increasing N requires more repetitions of the experiment to extract the answer [11], Ahn, Weinacht & Bucksbaum neglect the exponential overhead required for measurement and for realization of $N \times N$ unitary transformations: They claim that extrapolation from their $N = 8$ experiments to $N = 20$ is straightforward and suggest that ultrafast shaped terahertz pulses [17] might realize more general unitary transformations than those used in their implementation of Grover's algorithm. But because the difference (detuning) between adjacent Rydberg energy levels converges to 0 polynomially in $1/N$ (for N labelling the energy levels) [13,17], both the laser pulses and the final measurements must be specified with exponentially increasing precision in n, the size of the problem [18]. This should be contrasted with the standard model for quantum computation using *poly-local* transformations implemented by polynomially many bounded size gates on Hilbert spaces with a tensor product decomposition [19];* these require specification of only polynomially many nontrivial amplitudes with constant precision. As Bernstein & Vazirani [2] and Shor [22] already emphasized in their original analyses of quantum models for computing, *all* physical resources must be accounted for to quantify algorithm complexity; it is a mistake to ignore some because the requirements for them do not overwhelm small N experiments.

Having identified an exponential cost associated with Ahn, Weinacht & Bucksbaum's realization [11] of Lloyd's suggestion for entanglement removal [10], we are now ready to demonstrate that it is also a mistake to infer, as Lloyd's presentation might lead one to [23], that quantum algorithms *require* entanglement—or an exponential amount of some resource replacing it—to improve on classical algorithms. Rather than Grover's 'naïve' database, let us consider a 'sophisticated' database which when queried about a specific number, responds with information about how close the guess is to the answer. This kind of response is more like that returned by, for example, Web search engines, which typically order pages by relevance [24]. A simple measure of relevance comes from the vector space model of information retrieval [25]: the records in the database and the guess are represented by vectors; then (the cosine of) the angle between a guess and any record measures their similarity and can be computed from the dot product of their vectors. In our setting the 'sophisticated' database acts on a query (x, b) by computing the dot product of the n-dimensional binary vectors $x \cdot a$ and adding it to b (mod 2). Thus $(x, b) \to \big(x, b \oplus g_a(x)\big)$, where $g_a(x) = x \cdot a$. Classically n queries suffice to identify a with probability 1.

Quantum mechanically, an underappreciated algorithm of Bernstein & Vazirani [2], rediscovered by Terhal & Smolin [5], searches this 'sophisticated' database with only a *single* quantum query.† The operation of the database is implemented by the unitary transformation (g_a-controlled-NOT) which takes $|x, b\rangle$ to $|x, b \oplus g_a(x)\rangle$. A quantum circuit for their algorithm (slightly improved [14]) is shown in Fig. 2. The first set of gates is the same as

* The tensor factors need not be two dimensional, *i.e.*, qubits. Higher dimensional factors have been considered in the context of error correction [20] and fault tolerance [21]. But in every case the dimension is bounded and scaling to larger problems is achieved using polynomially many tensor factors. Ahn, Weinacht & Bucksbaum have demonstrated single factor operations [11]; gate operations analogous to controlled-NOT on two Rydberg atoms would be required for such an atomic system to realize quantum computation.

† It should be noted that the algorithm realized by Ahn, Weinacht & Bucksbaum [11] is not Grover's first [4] which requires $O(\sqrt{N})$ queries, but rather, something like his second [26] which implements a single query on $O(N \log N)$ databases in parallel. This number of databases is required to achieve sufficient statistical power to identify the solution, and is reflected in the increasing number of times (commented on above) Ahn, Weinacht & Bucksbaum need to repeat their experiment to extract the answer as N increases [18]. This algorithm actually scales *worse* than the classical algorithm.

in Fig. 1, and takes $\psi_0 = |0\ldots 0, 0\rangle$ to $\psi_1 = \sum_{x=0}^{N-1} |x\rangle(|0\rangle - |1\rangle)/\sqrt{2N}$. After the database responds to this quantum query, the state is $\psi_2 = \sum_{x=0}^{N-1}(-1)^{x\cdot a}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2N}$. The final set of gates outputs $\psi_3 = |a\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, whereupon measuring the first (n-qubit) register identifies a with probability 1 (the output states for different as are orthogonal). Comparing with Grover's algorithm, we recognize that the last qubit still remains unentangled with the first register, so that we could again implement the latter with a single 2^n state particle and have no entanglement at any timestep. But this would be redundant: *there is no entanglement in Bernstein & Vazirani's algorithm*. To see this, observe that just as in Grover's algorithm there is no entanglement in ψ_0 or ψ_1, and there is none in ψ_3, since $|a\rangle$ is simply a tensor product of qubits each in state $|0\rangle$ or $|1\rangle$. But ψ_3 was obtained from ψ_2 by a unitary transformation acting on each of the $n+1$ qubits separately. Such a unitary transformation cannot change the entanglement of a state, so ψ_2 must also be unentangled.

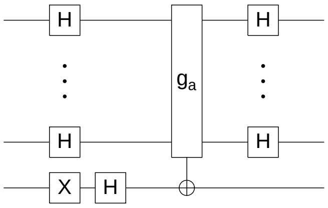

Figure 2. A (schematic) quantum circuit implementing Bernstein & Vazirani's algorithm. Each horizontal line again represents a qubit, which is initialized (on the left) in state $|0\rangle$. H and X are as in Fig. 1 and the "gate" acting on all $n+1$ qubits is the g_a-controlled-NOT transformation of the 'sophisticated' database. The top n qubits are measured at the end of the circuit.

To summarize: any quantum algorithm in the usual poly-local model for quantum computing can be rewritten to have no entanglement at any timestep, simply by disregarding the tensor product structure of the Hilbert space. Doing so physically incurs some exponential cost: in energy, in measurement precision, or in specification of the required unitary transformations. But one should not conclude that entanglement is *required* for quantum-over-classical complexity reduction. Without entanglement at any timestep, Bernstein & Vazirani's quantum algorithm for 'sophisticated' database search does not just reduce the number of queries required classically by a square root factor, but all the way from n to 1. Furthermore, we have shown for the first time that quantum interference alone suffices to reduce the query complexity of a problem within the standard model for quantum computation. Since implementing the g_a-controlled-NOT 'gate' with a subcircuit of *local* gates would introduce entanglement at intermediate timesteps, however, one might conclude that counting queries (or, more generally, nonlocal function calls) is a poor way to study the power of quantum algorithms [27]. But it was Simon's algorithm [3] (which exponentially reduces the number of nonlocal evaluations required to determine the period of a function) that led to Shor's quantum factoring algorithm [22], so it seems more productive to understand quantum search of a 'sophisticated' database as demonstrating the importance of interference and orthogonality, rather than entanglement, in quantum algorithms. This perspective may contribute to discovering the new algorithms necessary for quantum computing to become more generally useful.

Acknowledgements

I thank Thad Brown, Mike Freedman, Raymond Laflamme, Melanie Quong, John Smolin and Nolan Wallach for useful discussions. This work has been partially supported by Microsoft Research and the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) contract number DAAG55-98-1-0376.

References

[1] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proc. Roy. Soc. Lond. A* **400** (1985) 97–117;
D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation", *Proc. Roy. Soc. Lond. A* **439** (1992) 553–558.

[2] E. Bernstein and U. Vazirani, "Quantum complexity theory", in *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing*, San Diego, CA, 16–18 May 1993 (New York: ACM 1993) 11–20.

[3] D. R. Simon, "On the power of quantum computation", in S. Goldwasser, ed., *Proceedings of the 35th Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE 1994) 116–123.

[4] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, PA, 22–24 May 1996 (New York: ACM 1996) 212–219.

[5] B. M. Terhal and J. A. Smolin, "Single quantum querying of a database", *Phys. Rev. A* **58** (1998) 1822–1826.

[6] A. Einstein, in *The Born-Einstein Letters: Correspondence between Albert Einstein and Max and Hedwig Born from 1916 to 1955*, with commentaries by M. Born, transl. by I. Born (New York: Walker & Co. 1971) p. 158.

[7] R. Jozsa, "Entanglement and quantum computation", in S. A. Huggett, L. J. Mason, K. P. Tod, S. T. Tsou and N. M. J. Woodhouse, eds., *The Geometric Universe: Science, Geometry, and the Work of Roger Penrose* (Oxford: Oxford University Press 1998) 369–379;
A. Ekert and R. Jozsa, "Quantum algorithms: entanglement-enhanced information processing", *Phil. Trans. Roy. Soc. Lond. A* **356** (1998) 1769–1782.

[8] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung and S. Lloyd, "Experimental realization of a quantum algorithm", *Nature* **393** (1998) 143–146;
D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel and S. S. Somaroo, "Experimental quantum error correction", *Phys. Rev. Lett.* **81** (1998) 2152–2155;
J. A. Jones, M. Mosca and R. H. Hansen, "Implementation of a quantum search algorithm on a nuclear magnetic resonance computer", *Nature* **393** (1998) 344–346.

[9] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu and R. Schack, "Separability of very noisy mixed states and implications for NMR quantum computing", *Phys. Rev. Lett.* **83** (1999) 1054–1057;
For a response to this criticism, see R. Laflamme, "Review of 'Separability of very

noisy mixed states and implications for NMR quantum computing' ", *Quick Reviews in Quantum Computation and Information*, `http://quickreviews.org/qc/`.

[10] S. Lloyd, "Quantum search without entanglement", *Phys. Rev. A* **61** (1999) 010301.

[11] J. Ahn, T. C. Weinacht and P. H. Bucksbaum, "Information storage and retrieval through quantum phase", *Science* **287** (2000) 463–465.

[12] B. Schumacher, "Quantum coding (information theory)", *Phys. Rev. A* **51** (1995) 2738–2747.

[13] P. A. M. Dirac, *The Principles of Quantum Mechanics*, fourth edition (Oxford: Oxford University Press 1958).

[14] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, "Quantum algorithms revisited", *Proc. Roy. Soc. Lond. A* **454** (1998) 339–354.

[15] G. Brassard and P. Høyer, "An exact quantum polynomial-time algorithm for Simon's problem", in *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*, Ramat-Gan, Israel, 17–19 June 1997 (Los Alamitos, CA: IEEE 1997) 12–23;
L. K. Grover, "Quantum computers can search rapidly by using almost any transformation", *Phys. Rev. Lett.* **80** (1998) 4329–4332.

[16] E. Schrödinger, "*Die gegenwärtige Situation in der Quantenmechanik*", *Naturwissenschaften* **23** (1935) 807–812; 823–828; 844–849.

[17] N. E. Tielking and R. R. Jones, "Coherent population transfer among Rydberg states by subpicosecond, half-cycle pulses", *Phys. Rev. A* **52** (1995) 1371–1381.

[18] D. A. Meyer, "Rydberg state manipulation is not quantum computation", UCSD preprint (2000).

[19] M. H. Freedman, "Poly-locality in quantum computing", `quant-ph/0001077`.

[20] E. Knill, "Non-binary error bases and quantum codes", `quant-ph/9608048`;
E. M. Rains, "Nonbinary quantum codes", *IEEE Trans. Inform. Theory* **45** (1999) 1827–1832

[21] D. Aharonov and M. Ben-Or, "Fault tolerant quantum computation with constant error", `quant-ph/9611025`;
D. Gottesman, "Fault-tolerant quantum computation with higher-dimensional systems", *Chaos, Solitons and Fractals* **10** (1999) 1749–1758.

[22] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in S. Goldwasser, ed., *Proceedings of the 35th Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE 1994) 124–134.

[23] P. Knight, "Quantum information processing without entanglement", *Science* **287** (2000) 441–442.

[24] B. Yuwono and D. L. Lee, "Search and ranking algorithms for locating resources on the World Wide Web", in S. Y. W. Su, ed., *Proceedings of the Twelfth International Conference on Data Engineering*, New Orleans, LA, 26 February–1 March 1996 (Los Alamitos, CA: IEEE 1996) 164–171;
M. P. Courtois and M. W. Berry, "Results ranking in Web search engines", *Online* **23**:3 (1999) 39–46.

[25] G. Salton and M. McGill, *Introduction to Modern Information Retrieval* (New York: McGraw-Hill 1983);

M. W. Berry, Z. Drmač and E. R. Jessup, "Matrices, vector spaces, and information retrieval", *SIAM Rev.* **41** (1999) 335–362.

[26] L. K. Grover, "Quantum computers can search arbitrarily large databases by a single query", *Phys. Rev. Lett.* **79** (1997) 4709–4712.

[27] C. H. Bennett, E. Bernstein, G. Brassard and U. Vazirani, "Strengths and weaknesses of quantum computing", *SIAM J. Comput.* **26** (1997) 1510–1523.