PHYSICAL REVIEW A **69**, 010302(R) (2004)

Efficient optical implementation of the Bernstein-Vazirani algorithm

P. Londero,[1] C. Dorrer,[2] M. Anderson,[3] S. Wallentowitz,[4] K. Banaszek,[1] and I. A. Walmsley[1,*]
[1]*Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, United Kingdom*
[2]*Bell Laboratories, Lucent Technologies, 101 Crawfords Corner Road, Holmdel, New Jersey 07733, USA*
[3]*Physics Department, San Diego State University, 5500 Campanile Drive, San Diego, California 92182-1233, USA*
[4]*Fachbereich Physik, Universität Rostock, Universitätsplatz 3, D-18051 Rostock, Germany*
(Received 24 January 2003; published 9 January 2004)

We implement the Bernstein-Vazirani algorithm on a 15-bit register encoding 2^{15} elements using optics. The algorithm provides a polynomial speed up for oracle queries. The apparatus is physically efficient in that its size (i.e., space-time volume) scales linearly with the size (i.e., number of digits) of the register. We demonstrate also that the algorithm may be performed not only without entanglement, but also with a computational basis that does not consist of orthogonal states, and that this coding is the source of the efficiency of the algorithm.

DOI: 10.1103/PhysRevA.69.010302 PACS number(s): 03.67.Lx, 42.50.−p

Quantum computers can execute certain important computational tasks with dramatically fewer resources than computers designed according to the laws of classical physics. In all cases, the key element missing from the classical machines is interference. For most algorithms, the speedup available from a quantum computer requires interference between correlated states of several particles, or entanglement. This feature of quantum computers is both the most enigmatic and the most difficult to achieve in practice.

Entanglement allows the physical size of the computer to scale logarithmically with the number of orthogonal logical states accessible to the register. Usually these are mapped onto orthogonal space-time modes and the computer is read out by measuring whether a particle occupies a particular mode or not. Thus a register of N modes, each containing a single particle in one of M possible states, can access a Hilbert space of dimension M^N. Readout of the register, however, requires only $M\times N$ detectors, and the volume of the processor itself (which implements the unitary transformations of the register that represent the algorithm itself) scales in the same way.

This ability to access a very large direct product Hilbert space has led a number of authors to claim that information-processing schemes based on single-particle interference alone can never be as efficient as those based on multiparticle interference [1,2]. According to the standard model of quantum computation, each physical basis state of the system represents one logical state. Therefore, an M^N dimensional Hilbert space for a single particle requires M^N orthogonal space-time modes for the processor, even though the readout of a system coded in this fashion still requires only $M\times N$ separate detectors in an M-ary tree. Because of the scaling of the processor volume with input size, this form of coding can never be efficient.

Optics provides a straightforward means to simulate quantum logical operations using interference [3,4], by means of a coding in which the states of the register correspond to different modes of the electromagnetic field. Coherent superpositions of register states are realized by intermodal interference, and consequently the readout probabilities are independent of the statistical properties of the injected light. A four-element database search was performed using phase-shifting optical elements by Kwiat *et al.* [5]. More recently, Battacharya *et al.* described a version of the Grover algorithm [6,7] with a database of more than 10 elements [8]. Another variation has been demonstrated by Ahn *et al.* using atoms [9]. In that experiment, phase information was encoded in the complex amplitudes of electronic Rydberg states and a readout pulse was used to convert this to populations of the states, allowing the ''marked'' element to be determined. Because it uses single-particle interference and unary coding, this procedure is no more efficient than a classical search implemented using optical waves [10]. The absence of entanglement in all of these experiments appears to confirm the Jozsa-Ekert hypothesis concerning scaling problems of quantum computers based entirely on interference. It was recently pointed out by Meyer [11], however, that at least one quantum algorithm uses interference solely without entanglement at any stage. The circuit is, by the standard measures, efficient, even with this restriction.

It is therefore worthwhile to consider how to implement such a circuit, and especially whether there exists a classical wave-based version that demonstrates the same scaling. In this paper, we demonstrate such an implementation, and show that extending the notion of classical computation to include classical fields, as opposed to particles, introduces the interference that provides the speedup shown by this algorithm.

The Bernstein-Vazirani quantum parity algorithm [12–14] uses an oracle to determine whether the parity of an input bit string is the same as that of a string encoded in the oracle. Meyer [11] has shown how to use this to execute a search of a database by setting a flag on an ancilla qubit if the target element of the database is relatively ''close'' to the element encoded in the register. Thus if x is an N-bit binary string, and b a binary digit, then the Bernstein-Vazirani quantum parity algorithm is defined by the transformation

$$|x\rangle|b\rangle \mapsto |x\rangle|b\oplus(x a)\rangle, \tag{1}$$

*Electronic address: walmsley@physics.ox.ac.uk

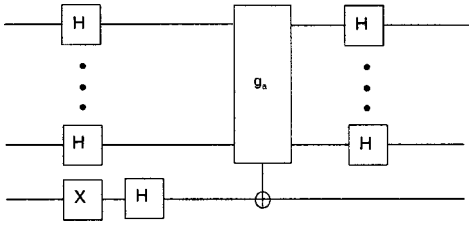

FIG. 1. Circuit implementing the Bernstein-Vazirani algorithm.

where $\oplus$ indicates addition modulo 2 and the parentheses around the scalar product indicate the parity of the product (i.e., whether the number of 1's is even or odd). A measurement of the ancilla that gives the result 1 indicates that when the register state and the oracle state are multiplied bitwise, the number of 1's in the resulting string is even. The circuit that executes this algorithm is shown in Fig. 1. At first sight, it would appear that this algorithm relies on entanglement, since it is clear that the controlled-NOT operation can certainly entangle the register and ancilla. For certain input states, however, the entanglement disappears.

When the circuit operates on the input state $|0_1,0_2,\ldots,0_N\rangle|0\rangle_b$, the first set of Hadamard gates transform this to

$$|\psi\rangle=\frac{1}{\sqrt{2}}\sum_{x=0}^{2^N-1}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle_b-|1\rangle_b). \tag{2}$$

The action of the oracle converts this to the state

$$|\psi'\rangle=\frac{1}{\sqrt{2}}\sum_{x=0}^{2^N-1}(-1)^{(xa)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle_b-|1\rangle_b). \tag{3}$$

upon which the final Hadamard gate converts the phase information to an amplitude that can be read easily by a particle-counting detector. This state can be written in the form

$$|\psi'\rangle=\frac{1}{\sqrt{2}}(|0\rangle_b-|1\rangle_b)\prod_{i=1}^{N}\frac{1}{\sqrt{2}}(|0\rangle_i+(-1)^{a_i}|1\rangle_i), \tag{4}$$

which illustrates the lack of entanglement. Moreover, the bit string encoded in the oracle appears as a phase shift of each of the qubits independently.

The algorithm has a classical analog that can be used to search for the oracle state. Since the oracle function is an N-bit controlled NOT, then encoding the register with the N-bit strings (0,...,0,0,1), (0,...,0,1,0), (0,...,1,0,0), etc. in sequence will give a series of ancilla bits that reveal exactly the oracle state. This classical approach requires N queries of the oracle, with N particles (representing N bits) per query. Meyer has shown how the quantum version can be used to perform a ''sophisticated search'' that yields the state of the oracle in a single query, using N particles encoding qubits. Thus there is a polynomial improvement in identifying the state of the oracle as compared to the classical search.

The complete absence of entanglement suggests the circuit can be implemented with a register and ancilla that contains only uncorrelated particles. Moreover, from the point of view of a search, there is no need to actually implement the controlled NOT, since the state of the register after the oracle is exactly the state encoded in the oracle. This simplifies considerably the experimental apparatus, though in an important sense it means that the algorithm no longer has a classical analog: the oracle cannot be queried classically in a way that would reveal its internal state in N attempts [15].

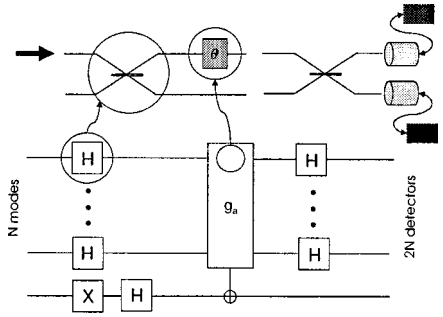

FIG. 2. Circuit of the Bernstein-Vazirani algorithm with $N+1$ two-state particles.

The circuit in Fig. 2 executes the Bernstein-Vazirani algorithm using $N+1$ two-state particles. The qubits are encoded using dual-rail logic. Each undergoes a Hadamard transformation. The logical 1 rail passes through the oracle, and the logical 0 state of each qubit bypasses the oracle. The oracle may or may not shift the phase of the logical 1 rail of each qubit depending on the bit string representing the marked element. Following a second Hadamard transformation, the register and ancilla are read out. The circuit therefore requires only $2(N+1)$ space-time modes and $N+1$ detectors in order to search a database with 2^N elements. Thus it is efficient even though it does not make use of entanglement at any point [16]. Moreover, because no entanglement is induced by the algorithm, the resources do not increase if each of the register elements does not contain exactly one qubit. Thus the algorithm can be executed with either mixed states of undetermined numbers of qubits per mode or even coherent superpositions of qubit number states.

The circuit illustrated in Fig. 2 can be translated to the optical arrangement shown in Fig. 3. In this apparatus, we used the two modes labeled by the wave vector and frequency (k_i,ω) as representing a logical 1 and 0. The distinct

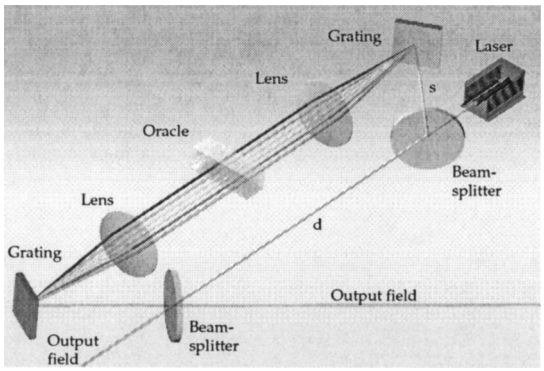

FIG. 3. Optical implementation of the circuit.

optical frequencies ω of a spectrally broadband optical pulse constitute distinct qubits, when each mode is occupied by a single photon. In our experiment, the light source was a 1-kHz repetition-rate chirped-pulse-amplified laser system delivering 50-fs duration pulses at a wavelength near 800 nm. Each mode of the pulse was therefore in a coherent state, with mean photon number greater than unity.

The pulses were incident on a broadband beamsplitter, which performed a Hadamard transformation on each pair of modes. For each frequency, one of the output modes, labeled, say, *s*, was directed to a zero-dispersion line with 1200 grooves per mm gratings and 50-cm focal length lenses. The combination of the first grating and lens created a Fourier plane, on which the spectral components of the pulse were spatially dispersed [17]. The other set of output modes, labeled *d*, bypassed this arrangement.

The oracle in this setup added a phase shift to a particular spectral component via a spatial light modulator located at the Fourier plane, in the same way as in an ultrafast pulse shaper [18]. In our case, the device that modifies the phases was an acousto-optic modulator [19]. A user-controlled acoustic waveform in a TeO_2 crystal induced both amplitude and phase modulations on the input optical waveform. The radiation diffracted from the acoustic wave is then sent to a symmetric lens and grating setup in order to recombine the spatially dispersed frequencies of the pulse.

The action of the apparatus on the input state of the qubits follows the analysis of the circuit in Fig. 2. However, we now show that classical fields can be used to implement the algorithm just as efficiently as unentangled quantum particles. To see this, it is instructive to consider its operation in terms of the field operators for each input mode $\hat{E}_{\text{“0/1”}}(\omega)$. The fields after the first Hadamard transformation are then $\hat{E}_{\text{“}s/d\text{”}}(\omega)=\hat{E}_{\text{“0”}}(\omega)\pm\hat{E}_{\text{“1”}}(\omega)$. In this case, the output field operators are related to those of the input field via $\hat{E}_{s'}^{(+)}(\omega)=\hat{E}_{s}(\omega)\exp[i\phi(\omega)+i\psi(\omega)]$, where the output phase is the sum of a static phase $\psi(\omega)$, which is independent of the state of the modulator, and the oracle-imposed phase $\phi(\omega)$. The shaped modes are mixed at a second beamsplitter with the unmodified modes. This performs a final Hadamard transformation, yielding the field operators $\hat{E}_{\text{“0′/1′”}}(\omega)=\hat{E}_{\text{“}s'\text{”}}(\omega)\pm\hat{E}_{\text{“}d'\text{”}}(\omega)$. This transformation converts the phase information imparted by the oracle to an amplitude suitable for detection via particle counting.

In our experiment, readout of the marked elements was performed using spectral interferometry [20]. The output field is sent to a spectrometer, at the exit port of which is an *N*-element detector array. The probability that the *j*th element of the detector array registers a photocount is $P_j=\langle\hat{E}^{(+)}(\omega_j)\hat{E}^{(-)}(\omega_j)\rangle$, where $\hat{E}^{(+)}(\omega_j)$ is the field operator at the detector. This is the sum of field operators of the two modes representing the different logical states of a single bit,

$$\hat{E}^{(+)}(\omega_j)=\hat{E}_{\text{“0”}}^{(+)}(\omega_j)(1-e^{i\pi a_j+i\omega_j\tau})+\hat{E}_{\text{“1”}}^{(+)}(\omega_j)(1+e^{i\pi a_j+i\omega_j\tau}),\qquad(5)$$

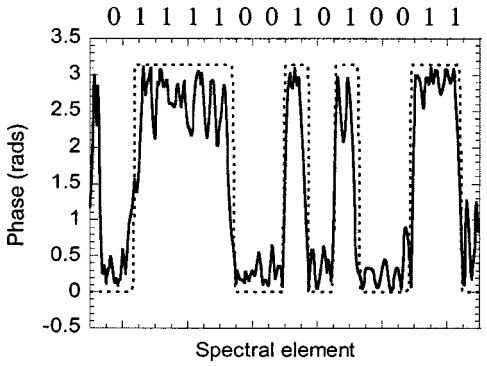

FIG. 4. Experimental result of a single run of the apparatus.

where a_j is the *j*th bit of the marked element, so that $\phi(\omega_j)=\pi a_j$, and τ is the temporal delay between the two paths.

Only the mean particle number contributes if the initial state is a coherent state in either set of modes and a vacuum in the other set, and this is the case most relevant to the classical fields used in our experiments. In both cases, information encoded in the oracle is revealed as modulations on the measured set of photocounts P_j.

A typical result of a single run of the apparatus is shown in Fig. 4. The encoded bits are labeled as 0 s or 1 s across the top of the figure, with the phase encoding of the oracle shown as the dashed line. The readout phases for each spectral element are shown as a solid line. Since the encoding is digital, the noise in the phase readout does not lead to any ambiguity in identifying the marked element of the database.

The physical resources required to implement this search scale efficiently with register size. The number of modes required to implement the search is $2N$, twice the number of slots in the oracle. Since these must be orthogonal in space-time, then a certain minimum volume of space, roughly $2N\lambda^3$, is required, and *N* detectors are needed. The number of records that can be encoded in the database and uniquely decoded in a single run of the apparatus is 2^N.

The number of particles per mode needed depends only on the noise floor of the detectors. If these are themselves quantum-limited, then at least $N\log_2 N$ photons are required per query.

Any information processor based solely on interference can be implemented using multiple copies of a single particle [21]. Consider a quantum particle with $2N$ states. These states can be grouped in pairs, each pair representing one bit of a binary coded string. Thus the particle can encode a single *N*-bit string as a superposition of *N* of the $2N$ states. With these states as the computational basis, the above circuit will perform in an identical fashion. Clearly, the readout will reveal just one bit of this *N*-bit string. Running the circuit with $N\log_2 N$ uncorrelated $2N$-state particles simultaneously means the entire bit string can be read with very high probability. Therefore, it is possible to use single-particle interference to implement the Bernstein-Vazirani algorithm with no increased overhead of the number of particles as compared to the qubit implementation. Note also that this is also more efficient than the classical particle implementation. The computational basis in this case clearly

consists of nonorthogonal states. Readout, however, only requires discrimination between the diagonal elements of the density matrices representing the different bit strings.

In conclusion, we have shown that the Bernstein-Vazirani quantum parity algorithm can be implemented efficiently using classical fields. The reason for this, as pointed out by Meyer, is that the register remains unentangled throughout the computation. This means that the speed up has no inherently quantum character. It remains an open question whether the coding scheme on which this algorithm is based can be extended to other circuits, and thus enable new ways in which single-particle interference can be used to improve the computational power of information processors.

Note added in proof. Recently, a similar work was published [25], using temporal rather than spectral encoding, as here. The conclusions of that paper are essentially the same as those of this paper.

We are grateful for enlightening conversations with J. H. Eberly, J. A. Jones, P. L. Knight, C. R. Stroud, Jr., and K. Wodkiewicz. This work was supported by the Center for Quantum Information, which is funded by ARO administered MURI Grant No. DAAG-19-99-1-0125. S.W. acknowledges the support of the Studienstiftung des Deutschen Volkes. When the experimental component of this work was performed, the authors were with The Institute of Optics, University of Rochester, Rochester, NY (C.D., M.A., K.B., I.A.W.) and The Department of Physics and Astronomy and the Rochester Theory Center, University of Rochester, Rochester, NY (S.W., K.B.).

[1] A. Ekert and R. Josza, Rev. Mod. Phys. **68**, 733 (1996).
[2] S. Lloyd, Phys. Rev. A **61**, 010301 (1999).
[3] N. J. Cerf, C. Adami, and P. G. Kwiat, Phys. Rev. A **57**, R1477 (1998).
[4] R. J. C. Spreeuw, Phys. Rev. A **63**, 062302 (2001).
[5] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White, J. Mod. Opt. **47**, 257 (2000).
[6] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[7] L. K. Grover, Phys. Rev. Lett. **79**, 4709 (1997).
[8] N. Bhattacharya, H. B. van Linden van den Heuvell, and R. J. C. Spreeuw, Phys. Rev. Lett. **88**, 137901 (2002).
[9] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum, Science **287**, 463 (2000).
[10] C. Dorrer, P. Londero, M. Anderson, S. Wallentowitz, and I. A. Walmsley, Paper QWB3, TOPS 57 QELS 2001 Technical Digest–Postconference Edition (Optical Society of America, Washington, D.C., 2001), pp. 149–150.
[11] D. A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).
[12] E. Bernstein and U. Vazirani, in *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing* (ACM, New York, 1993), p. 11.
[13] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).
[14] B. M. Terhal and J. A. Smolin, Phys. Rev. A **58**, 1822 (1998).
[15] Almost all of the previous implementations of quantum algorithms based on oracles fail this same test [5,8,9,22–24]. It is an important question whether it makes sense to claim an improvement for quantum mechanics in situations where there is no direct classical equivalent circuit.
[16] The comparison of efficiency is to previous search protocols using only interference, for which the experimental implementations required 2^N space-time modes to search a database with 2^N elements. From the point of view of complexity theory, all of the algorithms provide a polynomial speed up, reducing the number of queries to either $\sqrt{N}$ or 1 as compared with the classical value of N. However, statements of computational complexity cannot be divorced from statements about the physical size of the computer.
[17] A. M. Weiner, Rev. Sci. Instrum. **71**, 1929 (2000).
[18] C. Froehly, B. Colombeau, and M. Vampouille, in *Progress in Optics XX*, edited by E. Wolf (Elsevier, Amsterdam, 1983), pp. 63–153.
[19] J. X. Tull, M. A. Dugan, and W. S. Warren, Adv. Magn. Opt. Reson. **20**, 1 (1997).
[20] L. Lepetit, G. Cheriaux, and M. Joffre, J. Opt. Soc. Am. B **12**, 2467 (1995).
[21] S. Wallentowitz, I. A. Walmsley, and J. H. Eberly, e-print quant-ph/0009069.
[22] D. Collins, K. W. Kim, and W. C. Holton, Phys. Rev. A **58**, R1633 (1998).
[23] D. Collins, K. W. Kim, W. C. Holton, H. Sierzputowska-Gracz, and E. O. Stejskal, Phys. Rev. A **62**, 022304 (2000).
[24] K. Dorai, Arvind and A. Kurnar, e-print quant-ph/9909067.
[25] E. Brainis, L.-P. Lamoreux, N.J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, Phys. Rev. Lett. **90**, 157902 (2003).