Most Cited Papers: Quantum Computers

Quantum computers perform calculations based on the probability of an object's state before it is measured - instead of just 1s or 0s - which means they have the potential to process exponentially more data compared to classical computers.

Contents

10. Holonomic Quantum Computation
11. Electron Spin Resonance Transistors for Quantum Computing in Silicon-Germanium Hetero-structures
12. Environmentally decoupled sds-wave Josephson junctions for quantum computing
13. Architecture for a large-scale ion-trap quantum computer
14. Geometric quantum computation using nuclear magnetic resonance
15. A One-Way Quantum Computer
16. Quantum computing in molecular magnets
17. A scheme for efficient quantum computation with linear optics
18. Fault-tolerant quantum computation by anyons

The Physical Implementation of Quantum Computation

David P. DiVincenzo

IBM T.J. Watson Research Center, Yorktown Heights, NY 10598 USA

(February 1, 2008)

After a brief introduction to the principles and promise of quantum information processing, the requirements for the physical implementation of quantum computation are discussed. These five requirements, plus two relating to the communication of quantum information, are extensively explored and related to the many schemes in atomic physics, quantum optics, nuclear and electron magnetic resonance spectroscopy, superconducting electronics, and quantum-dot physics, for achieving quantum computing.

I. INTRODUCTION

* The advent of quantum information processing, as an abstract concept, has given birth to a great deal of new thinking, of a very concrete form, about how to create physical computing devices that operate in the hitherto unexplored quantum mechanical regime. The efforts now underway to produce working laboratory devices that perform this profoundly new form of information processing are the subject of this book.

In this chapter I provide an overview of the common objectives of the investigations reported in the remainder of this special issue. The scope of the approaches, proposed and underway, to the implementation of quantum hardware is remarkable, emerging from specialties in atomic physics [1], in quantum optics [2], in nuclear [3] and electron [4] magnetic resonance spectroscopy, in superconducting device physics [5], in electron physics [6], and in mesoscopic and quantum dot research [7]. This amazing variety of approaches has arisen because, as we will see, the principles of quantum computing are posed using the most fundamental ideas of quantum mechanics, ones whose embodiment can be contemplated in virtually every branch of quantum physics.

The interdisciplinary spirit which has been fostered as a result is one of the most pleasant and remarkable features of this field. The excitement and freshness that has been produced bodes well for the prospect for discovery, invention, and innovation in this endeavor.

II. WHY *QUANTUM* INFORMATION PROCESSING?

The shortest of answers to this question would be, why not? The manipulation and transmission of information is today carried out by physical machines (computers, routers, scanners, etc.), in which the embodiment and transformations of this information can be described using the language of classical mechanics. But the final physical theory of the world is not Newtonian mechanics, and there is no reason to suppose that machines following the laws of quantum mechanics should have the same computational power as classical machines; indeed, since Newtonian mechanics emerges as a special limit of quantum mechanics, quantum machines can only have greater computational power than classical ones. The great pioneers and visionaries who pointed the way towards quantum computers, Deutsch [8], Feynman [9], and others, were stimulated by such thoughts. Of course, by a similar line of reasoning, it may well be asked whether machines embodying the principles of other refined descriptions of nature (perhaps general relativity or string theory) may have even more information processing capabilities; speculations exist about these more exotic possibilities, but they are beyond the scope of the present discussion.

But computing with quantum mechanics really deserves a lot more attention than wormhole computing or quantum-gravity computing; quantum computing, while far in the future from the perspective of CMOS roadmaps and projections of chip fab advances, can certainly be seen as a real prospect from the perspective of research studies in quantum physics. It does not require science fiction to envision a quantum computer; the proposals discussed later in this issue paint a rather definite picture of what a real quantum computer will look like.

So, how much is gained by computing with quantum physics over computing with classical physics? We do not seem to be near to a final answer to this question, which is natural since even the ultimate computing power of classical machines remains unknown. But the answer as we know it today has an unexpected structure; it is not that quantum tools simply speed up all information processing tasks by a uniform amount. By a standard complexity measure (i.e., the way in which the number of computational steps required to complete a task grows with the "size" n of the task), some tasks are not sped up at all [10] by using quantum tools (e.g., obtaining the nth iterate of a function $f(f(...f(x)...))$ [11]), some are sped up moderately (locating an entry in a database of n entries [12]), and some are apparently sped up exponen-

*Prepared for Fortschritte der Physik special issue, *Experimental Proposals for Quantum Computation*, eds. H.-K. Lo and S. Braunstein.

tially (Shor's algorithm for factoring an n-digit number [13]).

In other types of information processing tasks, particularly those involving communication [14], both quantitative and qualitative improvements are seen [15]: for certain tasks (choosing a free day for an appointment between two parties from out of n days) there is a quadratic reduction of the amount of communicated data required, if quantum states rather than classical states are transmitted [16]. For some tasks (the "set disjointness problem", related to allocating non-overlapping segments of a shared memory in a distributed computation) the reduction of required communication is exponential [17]. Finally, there are tasks that are doable in the quantum world that have no counterpart classically: quantum cryptography provides an absolute secrecy of communication between parties that is impossible classically [18]. And for some games, winning strategies become possible with the use of quantum resources that are not available otherwise [19,20].

This issue, and this chapter, are primarily concerned with the "hows" of quantum computing rather than the "whys," so we will leave behind the computer science after this extremely brief mention. There is no shortage of other places to obtain more information about these things; I recommend the recent articles by Aharonov [21] and by Cleve [22]; other general introductions [23] will give the reader pointers to the already vast specialized literature on this subject.

III. REALIZING QUANTUM COMPUTATION

Let me proceed with the main topic: the physical realization of quantum information processing. As a guide to the remainder of the special issue, and as a means of reviewing the basic steps required to make quantum computation work, I can think of no better plan than to review a set of basic criteria that my coworkers and I have been discussing over the last few years [24] for the realization of quantum computation (and communication), and to discuss the application of these criteria to the multitude of physical implementations that are found below.

So, without further ado, here are the

Five (plus two) requirements for the implementation of quantum computation

1. A scalable physical system with well characterized qubits

For a start, a physical system containing a collection of qubits is needed. A qubit (or, more precisely, the embodiment of a qubit) is [25] simply a quantum two-level system like the two spin states of a spin 1/2 particle, like the ground and excited states of an atom, or like the vertical and horizontal polarization of a single photon. The generic notation for a qubit state denotes one state as $|0\rangle$ and the other as $|1\rangle$. The essential feature that distinguishes a qubit from a bit is that, according to the laws of quantum mechanics, the permitted states of a single qubit fills up a two-dimensional complex vector space; the general state is written $a|0\rangle + b|1\rangle$, where a and b are complex numbers, and a normalization convention $|a|^2 + |b|^2 = 1$ is normally adopted. The general state of two qubits, $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, is a four-dimensional vector, one dimension for each distinguishable state of the two systems. These states are generically *entangled*, meaning that they cannot be written as a product of the states of two individual qubits. The general state of n qubits is specified by a 2^n-dimensional complex vector.

A qubit being "well characterized" means several different things. Its physical parameters should be accurately known, including the internal Hamiltonian of the qubit (which determines the energy eigenstates of the qubit, which are often, although not always, taken as the $|0\rangle$ and $|1\rangle$ states), the presence of and couplings to other states of the qubit, the interactions with other qubits, and the couplings to external fields that might be used to manipulate the state of the qubit. If the qubit has third, fourth, etc., levels, the computer's control apparatus should be designed so that the probability of the system ever going into these states is small. The smallness of this and other parameters will be determined by the capabilities of quantum error correction, which will be discussed under requirement 3.

Recognizing a qubit can be trickier than one might think. For example, we might consider a pair of one-electron quantum dots that share a single electron between them as a two-qubit system. It is certainly true that we can denote the presence or absence of an electron on each dot by $|0\rangle$ and $|1\rangle$, and it is well known experimentally how to put this system into the "entangled" state $1/\sqrt{2}(|01\rangle + |10\rangle)$ in which the electron is in a superposition of being on the left dot and the right dot. But it is fallacious to consider this as a two-qubit system; while the states $|00\rangle$ and $|11\rangle$ are other allowed physical states of the dots, superselection principles forbid the creation of entangled states involving different particle numbers such as $1/\sqrt{2}(|00\rangle + |11\rangle)$.

It is therefore false to consider this as a two-qubit system, and, since there are not two qubits, it is nonsense to say that there is entanglement in this system. It is correct to say that the electron is in a superposition of different quantum states living on the two different dots. It is also perfectly correct to consider this system to be the embodiment of a *single* qubit, spanned by the states (in the misleading notation above) $|01\rangle$ ("electron on the right dot") and $|10\rangle$ ("electron on the left dot"). Indeed, several of the viable proposals, including the ones by Schön, Averin, and Tanamoto in this special issue, use exactly this system as a qubit. However, false lines of reasoning like the one outlined here have sunk various proposals before they were properly launched (no such abortive proposals are represented in this book, but they

can be found occasionally in the literature).

An amazing variety of realizations of the qubit are represented in this volume. There is a very well developed line of work that began with the proposal of Cirac and Zoller [1] for an ion-trap quantum computer, in which, in its quiescent state, the computer holds the qubits in pairs of energy levels of ions held in a linear electromagnetic trap. Various pairs of energy levels (e.g., Zeeman-degenerate ground states, as are also used in the NMR approach [3] discussed by Cory) have been proposed and investigated experimentally. The many neutral-atom proposals (see chapters by Kimble [2], Deutsch [26], and Briegel [27]) use similar atomic energy levels of neutral species. These atomic-physics based proposals use other auxiliary qubits such as the position of atoms in a trap or lattice, the presence or absence of a photon in an optical cavity, or the vibrational quanta of trapped electrons, ions or atoms (in the Platzman proposal below [6] this is the primary qubit). Many of the solid-state proposals exploit the fact that impurities or quantum dots have well characterized discrete energy level spectra; these include the spin states of quantum dots (see chapters by Loss [7] and Imamoglu [2]), the spin states of donor impurities (see Kane [4]), and the orbital or charge states of quantum dots (see Tanamoto [7]). Finally, there are a variety of interesting proposals which use the quantized states of superconducting devices, either ones involving the (Cooper-pair) charge (see Schön, Averin), or the flux (see Mooij) [5].

2. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000...\rangle$

This arises first from the straightforward computing requirement that registers should be initialized to a known value before the start of computation. There is a second reason for this initialization requirement: quantum error correction (see requirement 3 below) requires a continuous, fresh supply of qubits in a low-entropy state (like the $|0\rangle$ state). The need for a continuous supply of 0s, rather than just an initial supply, is a real headache for many proposed implementations. But since it is likely that a demonstration of a substantial degree of quantum error correction is still quite some time off, the problem of continuous initialization does not have to be solved very soon; still, experimentalists should be aware that the speed with which a qubit can be zeroed will eventually be a very important issue. If the time it takes to do this initialization is relatively long compared with gate-operation times (see requirement 4), then the quantum computer will have to equipped with some kind of "qubit conveyor belt", on which qubits in need of initialization are carried away from the region in which active computation is taking place, initialized while on the "belt", then brought back to the active place after the initialization is finished. (A similar parade of qubits will be envisioned in requirement 5 for the case of low quantum-efficiency measurements [28].)

There are two main approaches to setting qubits to a standard state: the system can either be "naturally" cooled when the ground state of its Hamiltonian is the state of interest, or the standard state can be achieved by a measurement which projects the system either into the state desired or another state which can be rotated into it. These approaches are not fundamentally different from one another, since the projection procedure is a form of cooling; for instance, the laser cooling techniques used routinely now for the cooling of ion states to near their ground state in a trap [1] are closely connected to the fluorescence techniques used to measure the state of these ions. A more "natural" kind of cooling is advocated in many of the electron spin resonance based techniques (using quantum dots or impurities) [7,4] in which the spins are placed in a strong magnetic field and allowed to align with it via interaction with their heat bath. In this kind of approach the time scale will be a problem. Since the natural thermalization times are never shorter than the decoherence time of the system, this procedure will be too slow for the needs of error correction and a "conveyor belt" scheme would be required. Cooling by projection, in which the Hamiltonian of the system and its environment are necessarily perturbed strongly, will have a time scale dependent on the details of the setup, but potentially much shorter than the natural relaxation times. One cannot say too much more at this point, as the schemes for measurement have in many cases not been fully implemented (see requirement 5). In the NMR quantum computer implementations to date (see Cory below), cooling of the initial state has been foregone altogether; it is acknowledged [3] that until some of the proposed cooling schemes are implemented (a nontrivial thing to do), NMR can never be a scalable scheme for quantum computing.

3. Long relevant decoherence times, much longer than the gate operation time

Decoherence times characterize the dynamics of a qubit (or any quantum system) in contact with its environment. The (somewhat overly) simplified definition of this time is that it is the characteristic time for a generic qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$ to be transformed into the mixture $\rho = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|$. A more proper characterization of decoherence, in which the decay can depend on the form of the initial state, in which the state amplitudes may change as well, and in which other quantum states of the qubit can play a role (in a special form of state decay called "leakage" in quantum computing [29,30]), is rather more technical than I want to get here; but see Refs. [31] and [32] for a good general discussion of all these. Even the simplest discussion of decoherence that I have given here should also be extended to include the possibility that the decoherence of neighboring qubits is correlated. It seems safest to assume that they will be neither completely correlated nor completely uncorrelated, and the thinking about error correction has taken this into account.

Decoherence is very important for the fundamentals

of quantum physics, as it is identified as the principal mechanism for the emergence of classical behavior. For the same reason, decoherence is very dangerous for quantum computing, since if it acts for very long, the capability of the quantum computer will not be so different from that of a classical machine. The decoherence time must be long enough that the uniquely quantum features of this style of computation have a chance to come into play. How long is "long enough" is also indicated by the results of quantum error correction, which I will summarize shortly.

I have indicated that the "relevant" decoherence times should be long enough. This emphasizes that a quantum particle can have many decoherence times pertaining to different degrees of freedom of that particle. But many of these can be irrelevant to the functioning of this particle as a qubit. For example, the rapid decoherence of an electron's position state in a solid state environment does not preclude its having a very long spin coherence time, and it can be arranged that this is the only time relevant for quantum computation. Which time is relevant is determined by the choice of the qubit basis states $|0\rangle$ and $|1\rangle$; for example, if these two states correspond to different spin states but identical orbital states, then orbital decoherence will be irrelevant.

One might worry that the decoherence time necessary to do a successful quantum computation will scale with the duration of the computation. This would place incredibly stringent requirements on the physical system implementing the computation. Fortunately, in one of the great discoveries of quantum information theory (in 1995-6), it was found that error correction of quantum states is possible [33] and that this correction procedure can be successfully applied in quantum computation [34], putting much more reasonable (although still daunting) requirements on the needed decoherence times.

In brief, quantum error correction starts with coding; as in binary error correction codes, in which only a subset of all boolean strings are "legal" states, quantum error correction codes consist of legal states confined to a subspace of the vector space of a collection of qubits. Departure from this subspace is caused by decoherence. Codes can be chosen such that, with a suitable sequence of quantum computations and measurements of some ancillary qubits, the error caused by decoherence can be detected and corrected. As noted above, these ancillary qubits have to be continuously refreshed for use. I will not go much farther into the subject here, see [31] for more. It is known that quantum error correction can be made fully fault tolerant, meaning that error correction operations can be successfully intermingled with quantum computation operations, that errors occurring during the act of error correction, if they occur at a sufficiently small rate, do no harm, and that the act of quantum computation does not itself cause an unreasonable proliferation of errors.

These detailed analyses have indicated the magnitude of decoherence time scales that are acceptable for fault-tolerant quantum computation. The result is that, if the decoherence time is $10^4 - 10^5$ times the "clock time" of the quantum computer, that is, the time for the execution of an individual quantum gate (see requirement 4), then error correction can be successful. This is, to tell the truth, a rather stringent condition, quantum systems frequently do not have such long decoherence times. But sometimes they do, and our search for a successful physical implementation must turn towards these. At least this result says that the required decoherence rate does not become ever smaller as the size and duration of the quantum computation grows. So, once the desired threshold is attainable, decoherence will not be an obstacle to scalable quantum computation.

Having said this, it must be admitted that it will be some time before it is even possible to subject quantum error correction to a reasonable test. Nearly all parts of requirements 1-5 must be in place before such a test is possible. And even the most limited application of quantum error correction has quite a large overhead: roughly 10 ancillary qubits must be added for each individual qubit of the computation. Fortunately, this overhead ratio grows only logarithmically as the the size of the quantum computation is increased.

In the short run, it is at least possible to design and perform experiments which measure the decoherence times and other relevant properties (such as the correlation of decoherence of neighboring qubits) of candidate implementations of qubits. With such initial test experiments, caution must be exercised in interpreting the results, because decoherence is a very system-specific phenomenon, depending on the details of all the qubits' couplings to various environmental degrees of freedom. For example, the decoherence time of the spin of an impurity in the bulk of a perfect semiconductor may not be the same as its decoherence time when it is near the surface of the solid, in the immediate neighborhood of device structures designed to manipulate its quantum state. Test experiments should probe decoherence in as realistic a structure as is possible.

4. A "universal" set of quantum gates

This requirement is of course at the heart of quantum computing. A quantum algorithm is typically specified [8] as a sequence of unitary transformations U_1, U_2, U_3,..., each acting on a small number of qubits, typically no more than three. The most straightforward transcription of this into a physical specification is to identify Hamiltonians which generate these unitary transformations, viz., $U_1 = e^{iH_1 t/\hbar}$, $U_2 = e^{iH_2 t/\hbar}$, $U_3 = e^{iH_3 t/\hbar}$, etc.; then, the physical apparatus should be designed so that H_1 can be turned on from time 0 to time t, then turned off and H_2 turned on from time t to time $2t$, etc.

Would that life were so simple! In reality what can be done is much less, but much less can be sufficient. Understanding exactly how much less is still enough, is the main complication of this requirement. In all the physical implementations discussed in this volume, only particular

sorts of Hamiltonians can be turned on and off; in most cases, for example, only two-body (two-qubit) interactions are considered. This immediately poses a problem for a quantum computation specified with three-qubit unitary transformations; fortunately, of course, these can always be re-expressed in terms of sequences of one- and two-body interactions [35], and the two-body interactions can be of just one type [36], the "quantum XOR" or "cNOT". There are some implementations in which multi-qubit gates can be implemented directly [37].

However, this still leaves a lot of work to do. In some systems, notably in NMR (see Cory), there are two-body interactions present which cannot be turned *off*, as well as others which are switchable. This would in general be fatal for quantum computation, but the particular form of the fixed interactions permit their effects to be annulled by particular "refocusing" sequences of the controllable interactions, and it has recently been discovered [38] that these refocusing sequences can be designed and implemented efficiently.

For many other systems, the two-body Hamiltonian needed to generate directly the cNOT unitary transformation is not available. For example, in the quantum-dot proposal described by Loss below [7], the only two-body interaction which should be easily achievable is the exchange interaction between neighboring spins, $H \propto \vec{S}_i \cdot \vec{S}_{i+1}$; in the Imamoglu chapter [2], the attainable interaction is of the XY type, i.e., $H \propto S_{ix}S_{jx} + S_{iy}S_{jy}$. An important observation is that with the appropriate sequence of exchange or XY interactions, in conjunction with particular one-body interactions (which are assumed to be more easily doable), the cNOT transformation can be synthesized [39]. It is incumbent on each implementation proposal to exhibit such a sequence for producing the cNOT using the interactions that are naturally realizable.

Often there is also some sophisticated thinking required about the time profile of the two-qubit interaction. The naive description above uses a "square pulse" time profile, but often this is completely inappropriate; for instance, if the Hamiltonian can also couple the qubit to other, higher-lying levels of the quantum system, often the only way to get the desired transformation is to turn on and off the interaction smoothly and slowly enough that an adiabatic approximation is accurate [29,30] (in a solid-state context, see also [40]). The actual duration of the pulse will have to be sufficiently long that any such adiabatic requirement is satisfied; then typically only the time integral $\int dt H(t)$ is relevant for the quantum gate action. The overall time scale of the interaction pulse is also controlled by the attainable maximum size of the matrix elements of $H(t)$, which will be determined by various fundamental considerations, like the requirement that the system remains in the regime of validity of a linear approximation, and practical considerations, like the laser power that can be concentrated on a particular ion. Given these various constraints, the "clock time" of the quantum computer will be determined by the time interval needed such that two consecutive pulses have negligible overlap.

Another consideration, which does not seem to present a problem with any current implementation schemes, but which may be an issue in the future, is the classicality of the control apparatus. We say that the interaction Hamiltonian $H(t)$ has a time profile which is controlled externally by some "classical" means, that is, by the intensity of a laser beam, the value of a gate voltage, or the current level in a wire. But each of these control devices is made up themselves of quantum mechanical parts. When we require that these behave classically, it means that their action should proceed without any entanglement developing between these control devices and the quantum computer. Estimates indicate that this entanglement can indeed be negligible, but this effect needs to be assessed for each individual case.

In many cases it is impossible to turn on the desired interaction between a pair of qubits; for instance, in the ion-trap scheme, no direct interaction is available between the ion-level qubits [1]. In this and in other cases, a special quantum subsystem (sometimes referred to as a "bus qubit") is used which can interact with each of the qubits in turn and mediate the desired interaction: for the ion trap, this is envisioned to be the vibrational state of the ion chain in the trap; in other cases it is a cavity photon whose wavefunction overlaps all the qubits. Unfortunately, this auxiliary quantum system introduces new channels for the environment to couple to the system and cause decoherence, and indeed the decoherence occurring during gate operation is of concern in the ion-trap and cavity-quantum electrodynamics schemes.

Some points about requirement 4 are important to note in relation to the implementation of error correction. Successful error correction requires fully parallel operation, meaning that gate operations involving a finite fraction of all the qubits must be doable simultaneously. This can present a problem with some of the proposals in which the single "bus qubit" is needed to mediate each interaction. On the other hand, the constraint that interactions are only among nearest neighbors in a lattice, as in many of the solid-state proposals, does allow for sufficient parallelism [41].

Quantum gates cannot be implemented perfectly; we must expect both systematic and random errors in the implementation of the necessary Hamiltonians. Both types of errors can be viewed as another source of decoherence and thus error correction techniques are effective for producing reliable computations from unreliable gates, if the unreliability is small enough. The tolerable unreliability due to random errors is in the same vicinity as the decoherence threshold, that is, the magnitude of random errors should be $10^{-4} - 10^{-5}$ per gate operation or so. It might be hoped that systematic errors could be virtually eliminated by careful calibration; but this will surely not always be the case. It seems harder to give a good rule for how much systematic error is tolerable,

the conservative estimates give a very, very small number (the square of the above) [31], but on the other hand there seems to be some evidence that certain important quantum computations (e.g., the quantum Fourier transform) can tolerate a very high level of systematic error (over- or under-rotation). Some types of very large errors may be tolerable if their presence can be detected and accounted for on the fly (we are thinking, for example, about charge switching in semiconductors or superconductors).

Error correction requires that gate operations be done on coded qubits, and one might worry that such operations would require a new repertoire of elementary gate operations for the base-level qubits which make up the code. For the most important error correction techniques, using the so called "stabilizer" codes, this is not the case. The base-level toolkit is exactly the same as for the unencoded case: one-bit gates and cNOTs, or any gate repertoire that can produce these, are adequate. Sometimes the use of coding can actually *reduce* the gate repertoire required: in the work on decoherence free subspaces and subsystems, codes are introduced using blocks of three and four qubits for which two-qubit exchange interactions alone are enough to implement general quantum computation [42,43]. This simplification could be very useful in the quantum-dot [7] or semiconductor-impurity [4] implementations.

5. A qubit-specific measurement capability

Finally, the result of a computation must be read out, and this requires the ability to measure specific qubits. In an ideal measurement, if a qubit's density matrix is $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| + \alpha|0\rangle\langle 1| + \alpha^*|1\rangle\langle 0|$, the measurement should give outcome "0" with probability p and "1" with probability $1-p$ independent of α and of any other parameters of the system, including the state of nearby qubits, and without changing the state of the rest of the quantum computer. If the measurement is "nondemolition", that is, if in addition to reporting outcome "0" the measurement leaves the qubit in state $|0\rangle\langle 0|$, then it can also be used for the state preparation of requirement 2; but requirement 2 can be fulfilled in other ways.

Such an ideal measurement as I have described is said to have 100% quantum efficiency; real measurements always have less. While the fidelity of a quantum measurement is not captured by a single number, the single quantum-efficiency parameter is often a very useful way to summarize it, just as the decoherence time is a useful if incomplete summary of the damage caused to a quantum state by the environment.

While quantum efficiency of 100% is desirable, much less is needed for quantum computation; there is, in fact, a tradeoff possible between quantum efficiency and other resources which results in reliable computation. As a simple example, if the quantum efficiency is 90%, then, in the absence of any other imperfections, a computation with a single-bit output (a so-called "decision problem", common in computer science) will have 90% reliability. If 97% reliability is needed, this can just be achieved by rerunning the calculation three times. Much better, actually, is to "copy" the single output qubit to three, by applying two cNOT gates involving the output qubit and two other qubits set to $|0\rangle$, and measuring those three. (Of course, qubits cannot be "copied", but their value in a particular basis can.) In general, if quantum efficiency q is available, then copying to somewhat more than $1/q$ qubits and measuring all of these will result in a reliable outcome. So, a quantum efficiency of 1% would be usable for quantum computation, at the expense of hundreds of copies/remeasures of the same output qubit. (This assumes that the measurement does not otherwise disturb the quantum computer. If it does, the possibilities are much more limited.)

Even quantum efficiencies much, much lower than 1% can be and are used for successful quantum computation: this is the "bulk" model of NMR (see Cory and [3]), where macroscopic numbers of copies of the same quantum computer (different molecules in solution) run simultaneously, with the final measurement done as an ensemble average over the whole sample. These kinds of weak measurements, in which each individual qubit is hardly disturbed, are quite common and well understood in condensed-matter physics.

If a measurement can be completed quickly, on the timescale of 10^{-4} of the decoherence time, say, then its repeated application during the course of quantum computation is valuable for simplifying the process of quantum error correction. On the other hand, if this fast measurement capability is not available, quantum error correction is still possible, but it then requires a greater number of quantum gates to implement.

Other tradeoffs between the complexity and reliability of quantum measurement vs. those of quantum computation have recently been explored. It has been shown that if qubits can be initialized into pairs of maximally entangled states, and two-qubit measurements in the so-called Bell basis ($\Psi^{\pm} = |01\rangle \pm |10\rangle$, $\Phi^{\pm} = |00\rangle \pm |11\rangle$) are possible, then no two-qubit quantum gates are needed, one-bit gates alone suffice [44]. Now, often this tradeoff will not be useful, as in many schemes a Bell measurement would require two-bit quantum gates.

But the overall message, seen in many of our requirements, is that more and more, the theoretical study of quantum computation has offered a great variety of tradeoffs for the potential implementations: if X is very hard, it can be substituted with more of Y. Of course, in many cases both X and Y are beyond the present experimental state of the art; but a thorough knowledge of these tradeoffs should be very useful for devising a rational plan for the pursuit of future experiments.

IV. DESIDERATA FOR QUANTUM COMMUNICATION

For computation alone, the five requirements above suffice. But the advantages of quantum information pro-

cessing are not manifest solely, or perhaps even principally, for straightforward computation only. There are many kinds of information-processing tasks, reviewed briefly at the beginning, that involve more than just computation, and for which quantum tools provide a unique advantage.

The tasks we have in mind here all involve not only computation but also communication. The list of these tasks that have been considered in the light of quantum capabilities, and for which some advantage has been found in using quantum tools, is fairly long and diverse: it includes secret key distribution, multiparty function evaluation as in appointment scheduling, secret sharing, and game playing [14].

When we say communication we mean quantum communication: the transmission of intact qubits from place to place. This obviously adds more features that the physical apparatus must have to carry out this information processing. We formalize these by adding two more items to the list of requirements:

6. The ability to interconvert stationary and flying qubits

7. The ability faithfully to transmit flying qubits between specified locations

These two requirements are obviously closely related, but it is worthwhile to consider them separately, because some tasks need one but not the other. For instance, quantum cryptography [18] involves only requirement 7; it is sufficient to create and detect flying qubits directly.

I have used the jargon "flying qubits" [2], which has become current in the discussions of quantum communication. Using this term emphasizes that the optimal embodiment of qubits that are readily transmitted from place to place is likely to be very different from the optimal qubits for reliable local computation. Indeed, almost all proposals assume that photon states, with the qubit encoded either in the polarization or in the spatial wavefunction of the photon, will be the flying qubit of choice, and indeed, the well developed technology of light transmission through optical fibers provides a very promising system for the transmission of qubits. I would note, though, that my colleagues and I have raised the possibility that electrons traveling though solids could provide another realization of the flying qubit [14,45].

Only a few completely developed proposals exist which incorporate requirements 6 and 7. Of course, there are a number of quite detailed studies of 7, in the sense that experiments on quantum cryptography have been very concerned with the preservation of the photon quantum state during transmission through optical fibers or through the atmosphere. However, these studies are rather disconnected from the other concerns of quantum computing. Requirement 6 is the really hard one; to date the only theoretical proposal sufficiently concrete that experiments addressing it have been planned is the scheme produced by Kimble and coworkers [46] for unloading a cavity photon into a traveling mode via atomic spectroscopy, and loading it by the time-reversed process. Other promising concepts, like the launching of electrons from quantum dots into quantum wires such that the spin coherence of the electrons is preserved, need to be worked out more fully.

V. SUMMARY

So, what is the "winning" technology going to be? I don't think that any living mortal has an answer to this question, and at this point it may be counterproductive even to ask it. Even though we have lived with quantum mechanics for a century, our study of quantum effects in complex artificial systems like those we have in mind for quantum computing is in its infancy. No one can see how or whether all the requirements above can be fulfilled, or whether there are new tradeoffs, not envisioned in our present theoretical discussions but suggested by further experiments, that might take our investigations in an entirely new path.

Indeed, the above discussion, and the other chapters of this special issue, really do not cover all the foreseeable approaches. I will mention two of which I am aware: first, another computational paradigm, that of the cellular automaton, is potentially available for exploitation. This is distinguished from the above "general purpose" approach in that it assumes that every bit pattern throughout the computer will be subjected to the same evolution rule. It is known that general-purpose computation is performable, although with considerable overhead, by a cellular automaton. This is true as well for the quantum version of the cellular automaton, as Lloyd [47] indicated in his original work. New theoretical work by Benjamin [48] shows very explicitly how relatively simple local rules would permit the implementation of some quantum computations. This could point us perhaps towards some sort of polymer with a string of qubits on its backbone that can be addressed globally in a spectroscopic fashion. Experiments are not oriented towards this at the moment, but the tradeoffs are very different, and I don't believe it should be excluded in the future.

Second, even more speculative, but very elegant, is the proposal of Kitaev [49] to use quantum systems with particular kinds of topological excitations, for example nonabelian anyons, for quantum computing. It is hard to see at the moment how to turn this exciting proposal into an experimental program, as no known physical system is agreed to have the appropriate topological excitations. But further research in, for example, the quantum Hall effect might reveal such a system; more likely, perhaps, is that further understanding of this approach, and that of Freedman and his colleagues [50], will shed more light on doing quantum computing using the "standard" approach being considered in this book.

I am convinced of one thing: the ideas of quantum information theory will continue to exert a decisive in-

fluence on the further investigation of the fundamental quantum properties of complex quantum systems, and will stimulate many creative and exciting developments for many years to come.

ACKNOWLEDGMENTS

I gratefully acknowledge support from the Army Research Office under contract number DAAG55-98-C-0041. I thank Alec Maassen van den Brink for a careful reading of this manuscript.

---

[1] J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); T. Pellizzari, S.A. Gardiner, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **75**, 3788 (1995); C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," Phys. Rev. Lett. **75**, 4714 (1995); A. Sorensen and K. Molmer, Phys. Rev. Lett. **82**, 1971 (1999); S. Schneider, D. F. V. James, and G. J. Milburn, "Method of quantum computation with 'hot' trapped ions," quant-ph/9808012.

[2] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic," Phys. Rev. Lett. **75**, 4710 (1995); A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, Phys. Rev. Lett. **83**, 4204 (1999) (quant-ph/9904096).

[3] N. Gershenfeld and I. Chuang, Science **275**, 350 (1997); D. Cory, A. Fahmy, and T. Havel, Proc. Nat. Acad. Sci. **94** (5), 1634 (1997).

[4] B. Kane, Nature **393**, 133 (1998); R. Vrijen *et al.*, "Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures," Phys. Rev. A, in press (quant-ph/9905096).

[5] D. Averin, Solid State Commun. **105**, 659 (1998); A. Shnirman, G. Schön, and Z. Hermin, Phys. Rev. Lett. **79**, 2371 (1997); J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Wal, and S. Lloyd, Science **285**, 1036 (1999).

[6] P. M. Platzman and M. I. Dykman, Science **284**, 1967 (1999).

[7] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998) (cond-mat/9701055); M. Sherwin, A. Imamoglu, and T. Montroy, "Quantum computation with quantum dots and terahertz cavity quantum electrodynamics," Phys. Rev. A **60**, 3508 (1999) (quant-ph/9903065); T. Tanamoto, Phys. Rev. A **61**, 022305 (2000) (quant-ph/9902031).

[8] D. Deutsch Proc. R. Soc. London A **400**, 97 (1985); **425**, 73 (1989).

[9] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); Found. Phys. **16**, 507 (1986). See also *Feynman Lectures on Computation*, eds. A. J. G. Hey and R. Allen (Perseus Press, 1996).

[10] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum lower bounds by polynomials," *Proc. of the 39th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, 1998), p. 352; quant-ph/9802049.

[11] Y. Ozhigov, "Quantum computer cannot speed up iterated applications of a black box," quant-ph/9712051; B. Terhal, PhD Thesis, University of Amsterdam, 1999.

[12] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett. **79**, 325 (1997).

[13] P. W. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484 (1997), and references therein.

[14] D. P. DiVincenzo and D. Loss, "Quantum Computers and Quantum Coherence," J. Magnetism Magn. Matl. **200**, 202-218 (1999).

[15] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[16] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. Classical Communication and Computation," in *Proc. of the 30th Ann. ACM Symp. on the Theory of Computing* (ACM Press, 1998), p. 63; eprint quant-ph/9802040.

[17] A. Ambainis, L. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson, "The quantum communication complexity of sampling," in *Proc. of the 39th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, 1998); see http://www.icsi.berkeley.edu/~ amnon/Papers/qcc.ps.

[18] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[19] D. A. Meyer, "Quantum strategies," Phys. Rev. Lett. **82**, 1052 (1999) (quant-ph/9804010); J. Eisert, M. Wilkens, and M. Lewenstein, "Quantum games and quantum strategies," Phys. Rev. Lett. **83**, 3077 (1999) (quant-ph/9806088); L. Goldenberg, L. Vaidman, and S. Wiesner, "Quantum gambling," Phys. Rev. Lett. **82**, 3356 (1999) (quant-ph/9808001).

[20] A. M. Steane and W. van Dam, "Physicists Triumph at 'Guess my Number' ", Physics Today **53** (2), 35-39 (2000).

[21] D. Aharonov, "Quantum Computation," in *Annual Reviews of Computational Physics, vol. VI* (ed. Dietrich Stauffer, World Scientific, Singapore, 1998) (quant-ph/9812037).

[22] R. Cleve, "An Introduction to Quantum Complexity Theory," to appear in *Collected Papers on Quantum Computation and Quantum Information Theory* (eds. C. Macchiavello, G. M. Palma, and A. Zeilinger, World Scientific, 2000) (quant-ph/9906111).

[23] C. H. Bennett, Physics Today **48** (10), 24 (1995); D. P. DiVincenzo, Science **270**, 255 (1995); D. P. DiVincenzo, Proc. R. Soc. London A **454**, 261 (1998) (and quant-ph/9705009); A. Barenco, Contemp. Phys. **37**, 375 (1996); A. Steane, Rep. Prog. Phys. **61**, 117 (1998); C. H. Bennett and P. W. Shor, IEEE Trans. Info. Theory

44, 2724 (1998).
[24] D. P. DiVincenzo, in *Mesoscopic Electron Transport*, eds. L. Sohn, L. Kouwenhoven, and G. Schön (Vol. 345, NATO ASI Series E, Kluwer, 1997), p. 657 (cond-mat/9612126); D. P. DiVincenzo and D. Loss, Superlattices and Microstructures **23**, 419 (1998) (cond-mat/9710259); D. P. DiVincenzo and D. Loss, J. Magn. Mag. Matl. **200**, 202 (1999) (cond-mat/9901137).
[25] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[26] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch, Phys. Rev. Lett. **82**, 1060 (1999).
[27] D. Jaksch, H. J. Briegel, I. J. Cirac, C. Gardiner, and P. Zoller, Phys. Rev. Lett. **82**, 1975 (1999).
[28] I am grateful to R. Schoelkopf and M. Devoret for clarifying discussion on these points.
[29] M. B. Plenio and P. L. Knight, Phys. Rev. A **53**, 2986 (1996).
[30] M. B. Plenio and P. L. Knight, Proc. Roy. Soc. Lond. **A453**, 2017-2041 (1997).
[31] J. Preskill, Proc. R. Soc. Lond A **454**, 385 (1998) (quant-ph/9705031).
[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000); see also M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum, Proc. R. Soc. Lond. A **454**, 277-304 (1998) (quant-ph/9706064).
[33] P. Shor, Phys. Rev. A **52**, 2493 (1995); A. M. Steane, Phys. Rev. Lett. **77**, 793-797 (1996).
[34] P. Shor, in *Proceedings of the 37th Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, CA, 1996) (quant-ph/9605011); D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1997) (quant-ph/9611025); E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998). These results are reviewed in [31].
[35] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," Phys. Rev. A **51**, 1015 (1995), cond-mat/9407022.
[36] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," Phys. Rev. A **52**, 3457 (1995), quant-ph/9503016.
[37] K. Molmer and A. Sorensen, Phys. Rev. Lett. **82**, 1835 (1999).
[38] D. W. Leung, I. L. Chuang, F. Yamaguchi, and Y. Yamamoto, "Efficient implementation of selective recoupling in heteronuclear spin systems using Hadamard matrices," quant-ph/9904100.
[39] G. Burkard, D. Loss, D.P. DiVincenzo, and J.A. Smolin, Phys. Rev. B **60**, 11404 (1999); cond-mat/9905230.
[40] G. Burkard, D. Loss, D. P. DiVincenzo, Phys. Rev. B **59**, 2070 (1999); cond-mat/9808026.
[41] D. Gottesman, "Fault-Tolerant Quantum Computation with Local Gates," J. Mod. Optics **47**, 333 (2000); quant-ph/9903099.
[42] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley, "Universal fault-tolerant computation on decoherence-free subspaces," quant-ph/9909058.
[43] D. P. DiVincenzo, G. Burkard, D. Loss, and E. V. Sukhorukov, "Quantum computation and spin electronics," in *Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics*, eds. I. O. Kulik and R. Ellialtioglu (NATO Advanced Study Institute, Turkey, June 13-25, 1999), to be published; cond-mat/9911245.
[44] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).
[45] D. Loss and E. V. Sukhorukov, Phys. Rev. Lett. **84**, 1035 (2000).
[46] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997) (quant-ph/9611017).
[47] S. Lloyd, Science **261**, 1569 (1993); **263**, 695 (1994).
[48] S. Benjamin, Phys. Rev. A **61**, 020301(R) (2000) (quant-ph/9909007).
[49] A. Yu. Kitaev, "Fault-tolerant quantum computation with anyons," quant-ph/9707021; see also J. Preskill, in *Introduction to Quantum Computation and Information* (eds. H.-K. Lo, S. Popescu, and T. Spiller, World Scientific, Singapore, 1998) pp. 213-269 (quant-ph/9712048).
[50] M. H. Freedman, M. Larsen, and Z. Wang, "A modular functor which is universal for quantum computation," quant-ph/0001108; M. H. Freedman, "Poly-locality in quantum computing," quant-ph/0001077; M. H. Freedman, A. Yu. Kitaev, and Z. Wang, "Simulation of topological field theories by quantum computers," quant-ph/0001071.

Universal Quantum Computation with the Exchange Interaction

D. P. DiVincenzo[1], D. Bacon[2,3], J. Kempe[2,4,5], G. Burkard[6], and K. B. Whaley[2]

[1]*IBM Research Division, TJ Watson Research Center, Yorktown Heights, NY 10598 USA*

[2]*Department of Chemistry, University of California, Berkeley, CA 94720 USA*

[3]*Department of Physics, University of California, Berkeley, CA 94720 USA*

[4]*Department of Mathematics, University of California, Berkeley, CA 94720 USA*

[5]*École Nationale Superieure des Télécommunications, Paris, France*

[6]*Department of Physics and Astronomy, University of Basel, Klingelbergstrasse 82, CH-4056 Basel, Switzerland*

Experimental implementations of quantum computer architectures are now being investigated in many different physical settings. The full set of requirements that must be met to make quantum computing a reality in the laboratory [1] is daunting, involving capabilities well beyond the present state of the art. In this report we develop a significant simplification of these requirements that can be applied in many recent solid-state approaches, using quantum dots [2], and using donor-atom nuclear spins [3] or electron spins [4]. In these approaches, the basic two-qubit quantum gate is generated by a tunable Heisenberg interaction (the Hamiltonian is $H_{ij} = J(t)\vec{S}_i \cdot \vec{S}_j$ between spins i and j), while the one-qubit gates require the control of a local Zeeman field. Compared to the Heisenberg operation, the one-qubit operations are significantly slower and require substantially greater materials and device complexity, which may also contribute to increasing the decoherence rate. Here we introduce an explicit scheme in which the Heisenberg interaction alone suffices to exactly implement any quantum computer circuit, at a price of a factor of three in additional qubits and about a factor of ten in additional two-qubit operations. Even at this cost, the ability to eliminate the complexity of one-qubit operations should accelerate progress towards these solid-state implementations of quantum computation.

The Heisenberg interaction has many attractive features [2,5] that have led to its being chosen as the fundamental two-qubit interaction in a large number of recent proposals: Its functional form is very accurate — deviations from the isotropic form of the interaction, arising only from relativistic corrections, can be very small in suitably chosen systems. It is a strong interaction, so that it should permit very fast gate operation, well into the GHz range for several of the proposals. At the same time, it is very short ranged, arising from the spatial overlap of electronic wavefunctions, so that it should be possible to have an on-off ratio of many orders of magnitude. Unfortunately, the Heisenberg interaction by itself is not a universal gate [6], in the sense that it cannot generate any arbitrary unitary transformation on a collection of spin-1/2 qubits. So, every proposal has supplemented the Heisenberg interaction with some other means of applying independent one-qubit gates (which can be thought of as time-dependent local magnetic fields). But the need to add this capability to the device adds considerably to the complexity of the structures, by putting unprecedented demands on "g-factor" engineering of heterostructure materials [7,4], requiring that strong, inhomogeneous magnetic fields be applied [2,5], or involving microwave manipulations of the spins that may be slow and may cause heating of the device [4]. These added complexities may well exact a high cost, perhaps degrading the quantum coherence and clock rate of these devices by orders of magnitude.

The reason that the Heisenberg interaction alone does not give a universal quantum gate is that it has too much symmetry: it commutes with the operators $\hat{S}^2$ and $\hat{S}_z$ (for the total spin angular momentum and its projection on the z axis), and therefore it can only rotate among states with the same S, S_z quantum numbers. But by defining coded qubit states, ones for which the spin quantum numbers always remain the same, the Heisenberg interaction alone *is* universal [8–10], and single-spin operations and all their attendant difficulties can be avoided.

Recent work has identified the coding required to accomplish this. Starting with early work that identified techniques for suppressing phase-loss mechanisms due to coupling with the environment [11–13], more recent studies have identified encodings that are completely

immune from general collective decoherence, in which a single environmental degree of freedom couples in the same way to all the spins in a block. These codes are referred to both as decoherence-free subspaces (and their generalization, the decoherence-free subsystems) [14,8,10], and also as noiseless subspaces and subsystems [15,16,9]. The noiseless properties of these codes are not relevant to the present work; but they have the desired property that they consist of states with definite angular momentum quantum numbers.

So, in principle, the problem has been solved: the Heisenberg interaction alone is universal and can be used for quantum computation. However, a very practical question still remains: how great is the price that must be paid in return for eliminating single-spin operations? In particular, how many applications of the Heisenberg interaction are needed to complete some desired quantum gate operation? The only guidance provided by the existing theory [8–10] comes from a theorem of Solovay and Kitaev [17–19], which states that "efficient" approximations exist: given a desired accuracy parameter ϵ, the number N of exchange operations required goes like $N \approx K \log^c(1/\epsilon)$, where $c \approx 4$ and K is an unknown positive constant. However, this theorem provides very little useful practical guidance for experiment; it does not show how to obtain the desired approximating sequence of exchange operations, and, since K is unknown, it gives no clue of whether the number of operations needed for a practical accuracy parameter is 10 or 10000. In the following we remedy these inadequacies by showing that the desired quantum logic operations can be obtained exactly using sequences of exchange interactions short enough to be of practical significance for upcoming experiments.

In the scheme we analyze here, we use the smallest subspace with definite angular-momentum quantum numbers that can be used to encode a qubit; this subspace is made up of three spins. It should be noted [10] that in principle the overhead in spatial resources could be made arbitrarily small: asymptotically the rate of encoding into such noiseless subsystems converges to unity. The space of three-spin states with spin quantum numbers $S = 1/2$, $S_z = +1/2$ is two dimensional and will serve to represent our coded qubit. A good explicit

choice for the basis states of this qubit are $|0_L\rangle = |S\rangle|\uparrow\rangle$, $|1_L\rangle = \sqrt{2/3}|T_+\rangle|\downarrow\rangle - \sqrt{1/3}|T_0\rangle|\uparrow\rangle$. Here $|S\rangle = \sqrt{1/2}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ is the singlet state of spins 1 and 2 (see Fig. 1a) of the three-spin block, and $|T_+\rangle = |\uparrow\uparrow\rangle$ and $|T_0\rangle = \sqrt{1/2}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$ are triplet states of these two spins. For these states we have constructed an explicit exchange implementation of the basic circuit elements of quantum logic [6]; in particular, we discuss how one obtains any coded one-qubit gate, and a specific two-qubit gate, the controlled NOT (cNOT).

It is easy to understand how one-qubit gates are performed on a single three-spin block. We note that Hamiltonian H_{12} generates a rotation $U_{12} = \exp(i/\hbar \int J\vec{S}_1 \cdot \vec{S}_2 dt)$ which is just a z-axis rotation (in Bloch-sphere notation) on the coded qubit, while H_{23} produces a rotation about an axis in the x-z plane, at an angle of 120^o from the z-axis. Since simultaneous application of H_{12} and H_{23} can generate a rotation around the x-axis, three steps of 1D parallel operation (defined in Fig. 1a) permit any one-qubit rotation, using the classic Euler-angle construction. In serial operation, we find numerically that four steps are always adequate when only nearest-neighbor interactions are possible (eg, the sequence H_{12}-H_{23}-H_{12}-H_{23} shown in Fig. 2a, with suitable interaction strengths), while three steps suffice if interactions can be turned on between any pair of spins (eg, H_{12}-H_{23}-H_{13}, see Fig. 2b).

We have performed numerical searches for the implementation of two-qubit gates using a simple minimization algorithm. Much of the difficulty of these searches arises from the fact that while the four basis states $|0_L, 1_L\rangle|0_L, 1_L\rangle$ have total spin quantum numbers $S = 1$, $S_z = +1$, the complete space with these quantum numbers for six spins has nine states, and exchanges involving these spins perform rotations in this full nine-dimensional space. So, for a given sequence, eg the one depicted in Fig. 2c, one considers the resulting unitary evolution in this nine-dimensional Hilbert space as a function of the interaction times t_1, t_2, ... t_N. This unitary evolution can be expressed as a product $U(t_1, \ldots, t_N) = U_N(t_N) \cdots U_2(t_2) U_1(t_1)$, where $U_n(t_n) = \exp(i t_n H_{i(n),j(n)}/\hbar)$. The objective of the algorithm is to find a set of interaction times such that the total time evolution describes a cNOT gate in the four-dimensional logic subspace $U(t_1, \ldots, t_N) = U_{\rm cNOT} \oplus A_5$. The matrix A_5 can be any unitary

5×5 matrix (consistent with U having a block diagonal form). The efficiency of our search is considerably improved by the use of two invariant functions $m_{1,2}(U)$ identified by Makhlin [20], which are the same for any pair of two-qubit gates that are identical up to one-qubit rotations. It is then adequate to use an algorithm that searches for local minima of the function $f(t_1, \ldots, t_N) = \sum_i (m_i(U_{\rm cNOT}) - m_i(U(t_1, \ldots, t_N)))^2$ with respect to t_1, ...t_N (m_i is understood only to act on the 4×4 logic subspace of U). Finding a minimum for which $f = 0$ identifies an implementation of cNOT (up to additional one-qubit gates, which are easy to identify [20]) with the given sequence $(i(n), j(n))_n$, $i(n) \neq j(n)$ of exchange gates. If no minimum with $f = 0$ is found after many tries with different starting values (ideally mapping out all local minima), we have strong evidence (although not a mathematical proof) that the given sequence of exchange gates cannot generate cNOT.

The optimal serial-operation solution is shown in Fig. 2c. Note that by good fortune this solution happens to involve only nearest neighbors in the 1D arrangement of Fig. 1a. The circuit layout shown obviously has a high degree of symmetry; however, it does not appear possible to give the obtained solution in a closed form. (Of course, any gate sequence involving non-nearest neighbors can be converted to a local gate sequence by swapping the involved qubits, using the SWAP gate, until they are close; here however the *minimal* solution found does not require such manipulations.) We have also found (apparently) optimal numerical solutions for parallel operation mode. For the 1D layout of Fig. 1a, the simplest solution found involves 8 clock cycles with just 8*4 different interaction-time parameters (H_{12} can always be zero in this implementation). For the 2D parallel mode of Fig. 1b, a solution was found using just 7 clock cycles (7*7 interaction times).

It is worthwhile to give a complete overview of how quantum computation would proceed in the present scheme. It should begin by setting all the computational qubits to the $|0_L\rangle$ state. This state is easily obtained using the exchange interaction: if a strong H_{12} is turned on in each coded block and the temperature made lower than the strength J of the interaction, these two spins will equilibrate to their ground state, which is the singlet state. The third spin in the block should be in the $|\uparrow\rangle$ state, which can be achieved by also placing

the entire system in a moderately strong magnetic field B, such that $k_BT << g\mu_BB < J$. Then, computation can begin, with the one- and two-qubit gates implemented according to the schemes mentioned above. For the final qubit measurement, we note that determining whether the spins 1 and 2 of the block are in a singlet or a triplet suffices to perfectly distinguish [7] $|0_L\rangle$ from $|1_L\rangle$ (again, the state of the third spin does not enter). Thus, for example, the AC capacitance scheme for spin measurement proposed by Kane [3] is directly applicable to the coded-qubit measurement.

There are several issues raised by this work that deserve further exploration. The $S = 1/2$, $S_z = +1/2$ three-spin states that we use are a subspace of a decoherence-free subsystem that has been suggested for use in quantum computing by exchange interactions [10,16]. Use of this full subsystem, in which the coded qubit can be in any mixture of the $S_z = +1/2$ and the corresponding $S_z = -1/2$ states, would offer immunity from certain kinds of interactions with the environment, and would not require any magnetic field to be present, even for initialization of the qubits. In this modified approach, the implementation of one-qubit gates is unchanged, but the cNOT implementation must satisfy additional constraints – the action of the exchanges on both the $S = 1$ and the $S = 0$ six-spin subspaces must be considered. As a consequence, implementation of cNOT in serial operation is considerably more complex; our numerical studies have failed to identify an implementation (even a good approximate one) for sequences of up to 36 exchanges (cf. 19 in Fig. 2c). On the other hand, we have found implementations using 8 clock cycles for 1D and 2D parallel operation (again for the 1D case H_{12} can be zero), so use of this larger Hilbert space may well be advantageous in some circumstances.

Finally, we note that further work is needed on the performance of quantum error correction within this scheme. Our logical qubits can be used directly within the error correction codes that have been shown to produce fault tolerant quantum computation [21]. Spin decoherence will primarily result in "leakage" errors, which would take our logical qubits into states of different angular momentum (eg, $S = 3/2$). Our preliminary work indicates that, with small modifications, the conventional error correction circuits will not cause uncon-

trolled propagation of leakage error. In addition, the general theory [22,21,8,10] shows that there exist sequences of exchange interactions which directly correct for leakage by swapping a fresh $|0_L\rangle$ into the coded qubit if leakage has occurred, and doing nothing otherwise; we have not yet identified numerically such a sequence. If fast measurements are possible, teleportation schemes can also be used in leakage correction.

To summarize, the present results offer a new alternative route to the implementation of quantum computation. The tradeoffs are clear: for the price of a factor of three more devices, and about a factor of ten more clock cycles, the need for stringent control of magnetic fields applied to individual spins is dispensed with. We are hopeful that the new flexibility offered by these results will make easier the hard path to the implementation of quantum computation in the lab.

REFERENCES

[1] D. P. DiVincenzo, "The Physical Implementation of Quantum Computation," quant-ph/0002077, prepared for Fortschritte der Physik special issue, *Experimental Proposals for Quantum Computation*, to be published.

[2] D. Loss and D.P. DiVincenzo, "Quantum Computation with Quantum Dots," Phys. Rev. A **57**, 120-126 (1998).

[3] B.E. Kane, "A Silicon-Based Nuclear-Spin Quantum Computer," Nature **393**, 133-137 (1998).

[4] R. Vrijen *et al.*, "Electron-spin-resonance Transistors for Quantum Computing in Silicon-Germanium Heterostructures," Phys. Rev. A **62**, 012306 (2000) (10 pages).

[5] G. Burkard, D. Loss and D.P. DiVincenzo, "Coupled Quantum Dots as Quantum Gates," Phys. Rev. B **59**, 2070-2078 (1999).

[6] A. Barenco *et al.*, "Elementary Gates for Quantum Computation," Phys. Rev. A **52**, 3457-3467 (1995).

[7] D. P. DiVincenzo *et al.*, "Quantum Computation and Spin Electronics," cond-mat/9911245, prepared for *Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics* (eds. I. O. Kulik and R. Ellialtioglu, NATO ASI), to be published.

[8] D. Bacon, J. Kempe, D.A. Lidar and K.B. Whaley, "Universal Fault-Tolerant Computation on Decoherence-Free Subspaces," Phys. Rev. Lett. **85**, 1758-1761 (2000).

[9] L. Viola, E. Knill, and S. Lloyd, "Dynamical Generation of Noiseless Quantum Subsystems," quant-ph/0002072.

[10] J. Kempe, D. Bacon, D.A. Lidar and K.B. Whaley, "Theory of Decoherence-Free Fault-Tolerant Universal Quantum Compuation," submitted to Physical Review A, quant-ph/0004064.

[11] W.H. Zurek, "Environment-induced Superselection Rules," Phys. Rev. D **26**, 1862-1880 (1982).

[12] G.M. Palma, K.-A. Suominen and A.K. Ekert, "Quantum Computers and Dissipation," Proc. Roy. Soc. London Ser. A **452**, 567-584 (1996).

[13] L.-M Duan and G.-C. Guo, "Reducing Decoherence in Quantum-Computer Memory with all Quantum Bits Coupling to the Same Environment," Phys. Rev. A **57**, 737-741 (1998).

[14] D.A. Lidar, I.L. Chuang and K. B. Whaley, "Decoherence-Free Subspaces for Quantum Computation," Phys. Rev. Lett. **81**, 2594-2597 (1998).

[15] P. Zanardi and M. Rasetti, "Error Avoiding Quantum Codes," Mod. Phys. Lett. B **11**, 1085-1093 (1997).

[16] E. Knill, R. Laflamme and L. Viola, "Theory of Quantum Error Correction for General Noise," Phys. Rev. Lett. **84**, 2525-2528 (2000).

[17] R. Solovay, unpublished manuscript, 1995.

[18] A. Y. Kitaev, "Quantum Computations: Algorithms and Error Correction," Russ. Math. Surv., **52** (6), 1191-1249 (1997).

[19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000), Appendix 3, "The Solovay-Kitaev Theorem".

[20] Y. Makhlin, "Nonlocal properties of two-qubits Gates and Mixed States and Optimization of Quantum Computations," quant-ph/0002045 .

[21] J. Preskill, "Fault-Tolerant Quantum Computation," in *Introduction to Quantum Computation and Information* (eds. H.-K. Lo, S. Popescu, and T. Spiller, World Scientific, 1998), p. 213-269 (quant-ph/9712048).

[22] D.A. Lidar, D. Bacon, K.B. Whaley, "Concatenating Decoherence-Free Subspaces with Quantum Error Correcting Codes," Phys. Rev. Lett. **82**, 4556-4559 (1999).

Acknowledgments: DPD, DB, JK, and KBW acknowledge support from the National Security Agency (NSA) and the Advanced Research and Development Activity (ARDA). DPD also thanks the UCLA DARPA program on spin-resonance transistors for support, and is also grateful for the hospitality of D. Loss at the University of Basel, where much of this work was completed. JK also acknowledges support from the US National Science Foundation. The work of GB is supported in part by the Swiss National Science Foundation. Discussions with P. O. Boykin and B. M. Terhal are gratefully acknowledged.

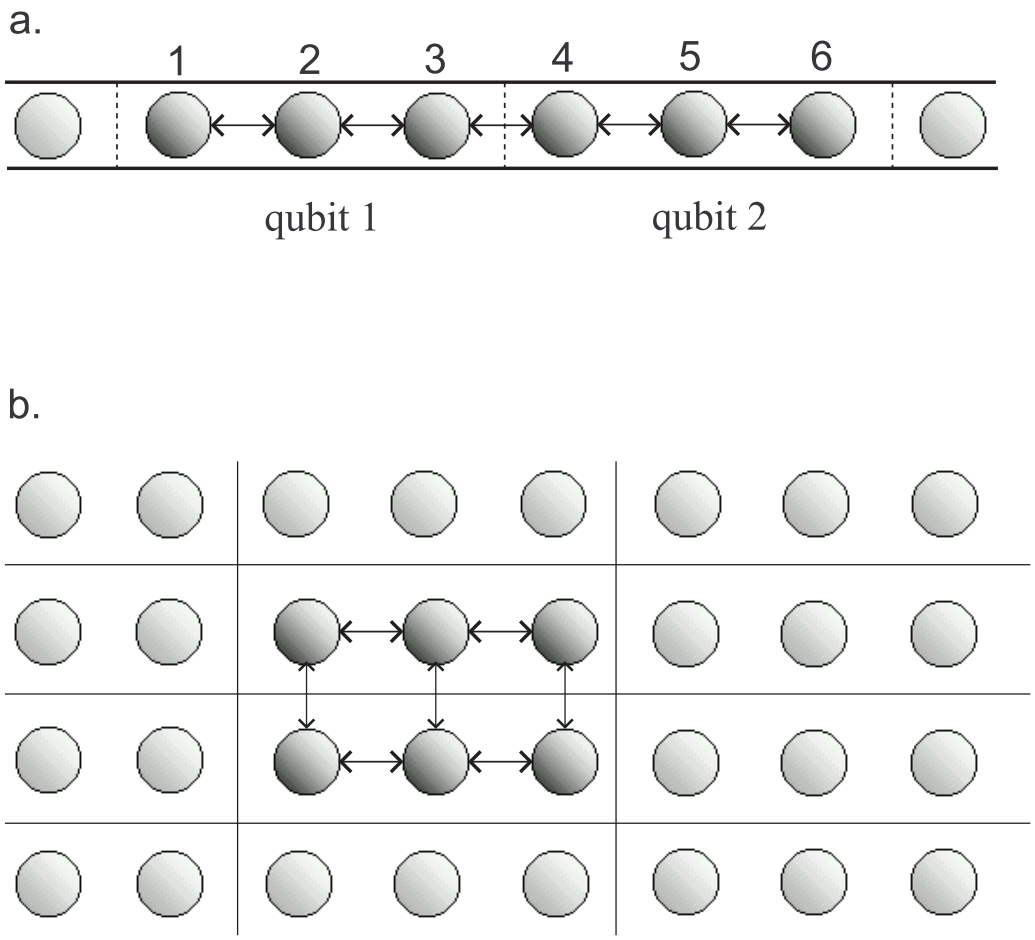
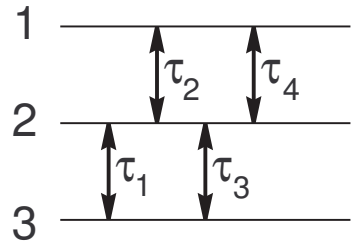
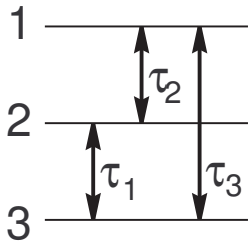


FIG. 1. Possible layouts of spin-1/2 devices. a) One-dimensional layout. We consider two different assumptions about how the exchange interactions can be turned on and off in this layout: 1) At any given time each spin can be exchange-coupled to at most one other spin (we refer to this as "serial operation" in the text), 2) All exchange interactions can be turned on simultaneously between any neighboring pair of spins in the line shown ("1D parallel operation"). b) Possible two-dimensional layout with interactions in a rectangular array. We imagine that any exchange interaction can be turned on between neighboring spins in this array ("2D parallel operation"). Of course other arrangements are possible, but these should be representative of the constraints that will be faced in actual device layouts.

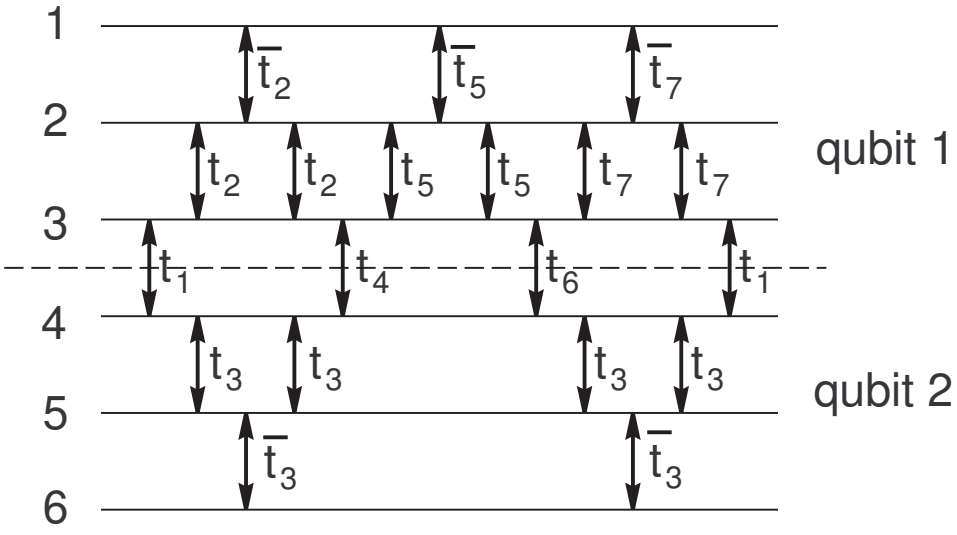
a.



b.



c.



t_1=0.410899(2) t_5=0.414720(10)

t_2=0.207110(20) t_6=0.147654(12)

t_3=0.2775258(12) t_7=0.813126(12)

t_4=0.640505(8) $\tan(\pi t_i)\tan(\pi \bar{t}_i) = -2$

FIG. 2. Circuits for implementing single-qubit and two-qubit rotations using serial operations. a) Single-qubit rotations by nearest-neighbor interactions. Four exchanges (double-headed arrows) with variable time parameters τ_i are always enough to perform any such rotation, one of the two possible layouts is shown. b) Non-nearest neighbor interactions. Only three interactions are needed, one of the possible layouts is shown. c) Circuit of 19 interactions that produce a cNOT between two coded qubits (up to one-qubit gates before and after). The durations of each interaction are given in units such that for $t = 1/2$ the rotation $U_{ij} = \exp(iJt\vec{S}_i \cdot \vec{S}_j/\hbar)$ is a SWAP, interchanging the quantum states of the two spins *i,j*. The $\bar{t}_i$ parameters are not independent, they are related to the t_is as indicated. The uncertainty of the final digits of these times are indicated in parentheses. With these uncertainties, the absolute inaccuracy of the matrix elements of the two-qubit gate rotations achieved is no greater than 6×10^{-5}. Further fine tuning of these time parameters would give the cNOT to any desired accuracy. In a practical implementation, the exchange couplings $J(t)$ would be turned on and off smoothly; then the time values given here provide a specification for the integrated value $\int J(t)dt$. The functional form of $J(t)$ is irrelevant, but its integral must be controlled to the precision indicated. The numerical evidence is very strong that the solution shown here is essentially unique, so that no other choices of these times are possible, up to simple permutations and replacements $t \to 1 - t$ (note that for the Heisenberg interaction adding any integer to t results in the same rotation). The results also strongly suggest that this solution is optimal: no one of these 19 interactions can be removed, and no other circuit layout with fewer than 19 has been found to give a solution. We have also sought, but not found, shorter implementations of other interesting two-qubit gates like $\sqrt{\text{SWAP}}$ [2,5].

Quantum computation with trapped polar molecules

D. DeMille
Department of Physics, P.O. Box 208120, Yale University, New Haven, CT 06520
(Dated: October 27, 2001)

We propose a novel physical realization of a quantum computer. The qubits are electric dipole moments of ultracold diatomic molecules, oriented along or against an external electric field. Individual molecules are held in a 1-D trap array, with an electric field gradient allowing spectroscopic addressing of each site. Bits are coupled via the electric dipole-dipole interaction. Using technologies similar to those already demonstrated, this design can plausibly lead to a quantum computer with $\gtrsim 10^4$ qubits, which can perform $\sim 10^5$ CNOT gates in the anticipated decoherence time of ~ 5 s.

PACS numbers: 03.67.Lx, 33.80.Ps, 33.55.Be

We describe a new technical approach to the design of a quantum computer (QC). The basic QC architecture is shown in Fig. 1. The qubits consist of the electric dipole moments of diatomic molecules, oriented along or against an external electric field. Bits are coupled by the electric dipole-dipole interaction. Individual molecules are held in a 1-D trap array, with an electric field gradient allowing spectroscopic addressing of each site. Loading with ultracold molecules makes it possible to use a weak trapping potential, which should allow long decoherence times for the system. This design bears various features in common with other recent proposals which employ electric dipole couplings [1, 2, 3]. However, the technical parameters of our design appear very favorable, and apparently only incremental improvements of demonstrated techniques are required in order to build a QC of unprecedented size.

We describe the molecular qubits as permanent electric dipoles oriented along ($|0\rangle$) or against ($|1\rangle$) an external electric field ($\vec{E}_{ext}$). (This model reproduces the exact behavior well in a certain regime.) Lattice sites are equally spaced in the x-direction and each contains one molecule, prepared initially in its ground state $|0\rangle$. The external field is perpendicular to the trap axis and

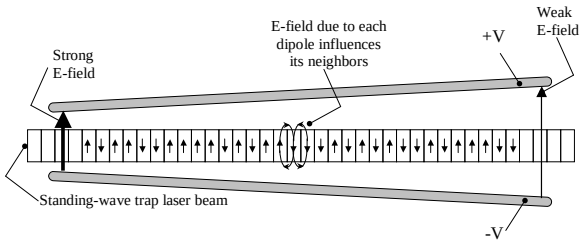


FIG. 1: Schematic depiction of the polar molecule quantum computer. Molecules are trapped in a 1-D optical lattice. Qubit states correspond to electric dipole moments up or down relative to the applied E-field. A field gradient makes the resonant frequency for each qubit unique. The electric field of each dipole changes the energy of its neighbors, according to their relative orientations.

consists of a constant bias field plus a linear gradient: $\vec{E}_{ext}(x) = [E_0 + x\,(\partial E/\partial x)]\,\hat{z}$. The Hamiltonian for bit a at position x_a is $H'_a = H^0 - \vec{d}_a \cdot \vec{E}_a$, where H^0 is the internal energy of a bit, $\vec{d}_a$ is the electric dipole moment of bit a, and $\vec{E}_a = \vec{E}_{ext}\,(x_a) + \vec{E}_{int}\,(x_a)$ is the total electric field at x_a. The internal field $\vec{E}_{int}$ is created by the electric dipole moments of neighboring bits: $\vec{E}_{int}\,(x_a) = \sum_{b\neq a} \frac{-\vec{d}_b}{|x_a - x_b|^3}$. For reasonable operating parameters, $E_{ext} \gg E_{int}$.

The scheme for gate operations is as outlined for the electric dipole moments of quantum dots in Ref. [1]. Transitions between qubit states can be driven by electric resonance, either directly in the microwave region or indirectly by an optical stimulated Raman process. Resonant drive pulses are tuned to frequency $\nu_a = \nu_0 + d_{eff}E_a/h$, where $h\nu_0$ is the difference in internal energies between states $|0\rangle$ and $|1\rangle$ in zero field; the effective dipole moment $d_{eff} = |\vec{d}_{|0\rangle} - \vec{d}_{|1\rangle}|$, where $\vec{d}_{|0\rangle(|1\rangle)}$ is the dipole moment in state $|0\rangle$ ($|1\rangle$); and h is Planck's constant. Pulses of sufficient temporal length to resolve the energy splitting due to E_{int} can be used for CNOT gates; shorter pulses suffice for one-bit rotations. Final-state readout can be accomplished by state-selective, resonant multiphoton ionization [4] and imaging detection of the resulting ions and electrons.

The efficient creation of ultracold diatomic molecules by photoassociation of laser cooled atoms was recently demonstrated [5, 6, 7, 8]. Electronically excited neutral molecules are produced by a laser-induced transition from the free state of two atoms; the excited state can subsequently decay into bound vibrational levels of the molecular ground state. The molecules are formed at a translational temperature similar to that of the constituent atoms; $T \approx 20$ μK has been demonstrated [7].

Production of ultracold atoms is most advanced for alkali atoms. Fortunately, heteronuclear bi-alkali molecules are well suited to our purposes. While no such species have yet been produced at ultracold temperatures, there seems to be no fundamental obstacle to making them. The rate-limiting Franck-Condon (FC) factors in the formation process in general should be more favorable for

hetero- than for homo-nuclear species, because of the better match between ground- and excited-state potential curves [9, 10]. Homonuclear bi-alkalis K_2, Rb_2, and Cs_2 have been formed, as well as heteronuclear molecular ions $NaCs^+$ [11]. Molecules formed by photoassociation are typically in the lowest rotational states ($J = 0 - 2$), but spread over many vibrational levels (v). High vibrational levels ($v > 100$) of Cs_2 were formed at a total rate of $> 10^6$/s [5, 7]; in a more complex scheme, K_2 molecules were produced at rates of up to 10^5/s/level, in low vibrational states ($v \sim 10$) [3]. Based on the calculated FC factors and the demonstrated production of homonuclear species, a production rate of $\gtrsim 10^5$/s ultracold heteronuclear molecules in individual rovibrational levels seems feasible. Molecules in any state with $J = 0$ or 2 and $v \gg 1$ can be transferred efficiently to the ground state ($v = 0, J = 0$) via a stimulated Raman transition [12].

For the bi-alkali molecules, there is some tradeoff between ease of production and the size of the molecular dipole moment. The FC factors for photoassociation are largest for pairs of atoms with similar excitation energies [9], while the dipole moments are largest for pairs where these are most different [13]. We specifically consider the KCs molecule, which has both a moderately large dipole moment and substantial FC factors; however, the other bi-alkali species have similar properties and one of them might prove ultimately more favorable.

An optical trap appears to be suitable for creating the desired 1-D array of molecules. For laser frequencies detuned to the red of any electronic transition, the dynamic polarizability gives rise to a force that attracts both atoms and molecules [14] to regions of high intensity. Far off-resonance traps are weak, but extremely non-perturbative [15]. Such traps are well developed for atoms, with demonstrated trap lifetimes $\gtrsim 300$ s [16], and internal state decoherence times $\gtrsim 4$ s [17]. Trapping of molecules in an off-resonant laser beam was recently demonstrated for ultracold Cs_2 [18].

Our proposed trap consists of a 1-D optical lattice, superposed with a crossed dipole trap [19] of cylindrically focused beams. This confines the molecules in sites spaced by $\lambda_t/2$ (where λ_t is the trap laser wavelength). The molecules will be well localized in these wells for trap depth $U_0 \gg kT$; we assume $U_0 = 100$ μK is sufficient. We take $\lambda_t \sim 1$ μm as a convenient compromise between small trap spacing and increased decoherence rates. For a homogeneous trap of length L, we require that the Rayleigh length $z_0 = \pi\omega_0^2/\lambda_t > L$, where ω_0 is the beam waist. We take $L = 5$ mm ($\sim 10^4$ trap sites) and $\omega_0 = 50$ μm. Transverse confinement is determined by the cylindrical beam waist ω_t; we assume diffraction-limited beams with f/1 focusing to achieve $\omega_t \sim \lambda_t$.

For given λ_t and laser power, the trap depth is determined by the KCs dynamic polarizability, which is not known in detail. However, it is possible to crudely estimate the required parameters. For moderate laser frequency detuning Δ, the polarizability will be dominated by the oscillator strength of the first excited $^1\Sigma$ level, which should couple to the ground state with a transition dipole moment comparable to that for the $6s - 6p$ transition of Cs [20]. For $\Delta \gg \omega_e$ (the molecular vibrational frequency), the FC structure is irrelevant. Thus, for the same detuning the trap depth for KCs should be similar to that for atomic Cs. We find that $\Delta \approx 2000$ cm^{-1} gives reasonable behavior. For KCs this corresponds to a trap wavelength $\lambda_t \approx 1.1$ μm, and requires only ≈ 1 W of laser power for the 1-D lattice (as for Cs [21]). The cross-sectional area of each transverse beam is $\sim 2\times$ that of the 1-D lattice beam, so the power in these must be comparable to achieve transverse confinement to $\sim \lambda_t/2$. The required lasers are commercially available.

K and Cs atoms can be loaded into such an optical trap from a standard magneto-optic trap. If necessary, the temperature of the atoms can be reduced in the trap by a variety of methods polarization gradient cooling [19, 22, 23]. The two-species sample in this trap should have $N \gtrsim 10^7$ atoms with density $n \gtrsim 10^{11}$ cm^{-3} and $T \lesssim 20$ μK. Photoassociation for ~ 1 s and stimulated Raman transfer should produce $\sim 10^5$ molecules in the ground molecular state. Remaining atoms (vibrationally-excited molecules) can be removed from the trap by resonant light pushing (selective photoionization [10]).

Remarkably, it may prove relatively easy to distribute the remaining molecules such that exactly one populates each lattice site. It has been argued that the repulsive interaction between atoms in a Bose condensate can lead to a Mott insulator-like phase transition, and thus unity filling of an optical lattice [24]. The interactions between polarized molecules are many orders of magnitude stronger than for atoms, and thus may facilitate reaching a similar phase transition even without Bose condensation. Detailed calculations are necessary to confirm this speculation, which does not take into account the anisotropy of the dipole-dipole interaction [25]. The large collision cross-sections for the polarized molecules [26] should also make it possible to achieve fast rates of evaporative cooling, and thus (if necessary) an even lower temperature than that of the original constituent atoms; the molecules can be held in their ground state in this phase, to avoid losses due to inelastic collisions. We note in passing that the final molecular temperature and density ($n \sim (2/\lambda_t)^3 \sim 10^{13}$ cm^{-3}) discussed here correspond to a phase-space density of $\sim 10^{-3}$, far from Bose condensation.

In the absence of an external field, even polar molecules have no net electric dipole moment. The application of an external field mixes rotational states; for low fields the mixed state which arises from the $J = 0$ ($J = 1, m_J = 0$) state corresponds to a dipolar charge distribution along (against) $\vec{E}_{ext}$. Calculations of the effect of E_{ext} on these two states are shown in Fig. 2. The energies for $E_{ext} = 0$ are $E_J = hBJ(J+1)$, where the rotational constant $B \approx$

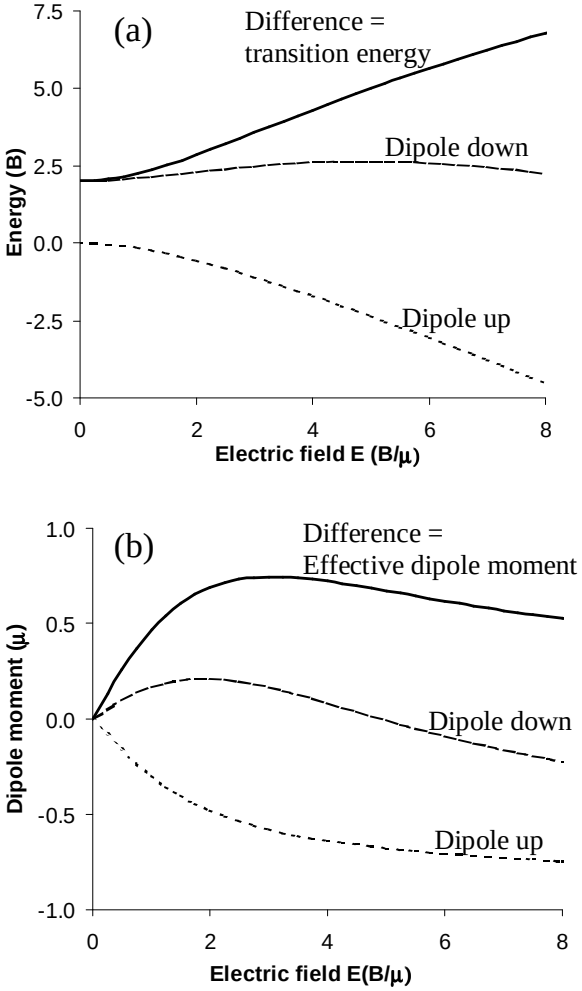


FIG. 2: Effect of an electric field on a polar molecule. a) Energy levels. b) Induced dipole moments.

1.0 GHz for KCs [13]. Stark matrix elements are taken from standard formulae [27], using the calculated value of the molecule-fixed dipole moment for KCs, $\mu = 1.92$ D [13]. In order to perform CNOT gates, it is necessary to resolve the transitions $|0\rangle|0\rangle \Leftrightarrow |0\rangle|1\rangle$ from $|1\rangle|0\rangle \Leftrightarrow |1\rangle|1\rangle$. These differ in energy by $h\delta\nu = d_{eff}^2/(\lambda_t/2)^3$. Over a wide range of electric field strengths $E_{ext} = (2-5)B/\mu$ ($\approx 2-5$ kV/cm for KCs), d_{eff} is within 10% of its maximum value (0.75 μ). The time required for CNOT gates is $\tau \gtrsim (2\pi\delta\nu)^{-1} \approx 50$ μs. The one-bit drive frequencies ν_a cover the range $3.5-6.0$ GHz over the array, with approximately equal steps of 250 kHz between sites. Direct microwave drive of a CNOT gate requires rf electric field strength $\approx$10 mV/cm for a π-pulse.

The final state of the register can be read out by rapidly (but adiabatically) turning off $\vec{E}_{ext}$, then applying a laser pulse to perform resonantly-enhanced multiphoton ionization [20]. Commercial pulsed lasers with $\sim$ns pulse widths have both sufficient energy for $\sim$100% ionization efficiency ($\sim$ mJ/pulse), and sufficient spectral resolution ($\ll 2B \approx 2$ GHz) to make contamination from the undesired logic state negligible. Molecules in each state can be detected by consecutive identical laser pulses, with an intervening rf π-pulse to transfer population between logic states. Simple ion optics can magnify the ionized array image 10-fold, so that the charges form a pattern 5 cm long, with spacing between ions of 5 μm. The magnified charge array can be detected on an imaging microchannel plate. Commercial detectors are available with sufficient size and resolution; detection of both ions and electrons from each logic state should lead to effective efficiencies $\gtrsim$90%.

The most important known source of decoherence is photon scattering from the trap laser. The total off-resonance photon scattering rate is dominated by inelastic (Raman) scattering to other rotational and vibrational levels [28]. For the chosen value of Δ, the scattering rate for KCs should be comparable to the elastic scattering rate R_s for Cs (much as for the trap depth). For the trap parameters discussed, $R_s \sim 0.2$ s^{-1} [21].

We have considered several technical noise issues, all of which appear controllable at the desired level. The trap laser shifts the values of ν_a, through coupling to the tensor polarizability of the molecule. Tensor shifts are typically several times smaller than the scalar shifts ($U_0 \approx 2$ MHz) responsible for the trapping potential [14]; we conservatively assume a tensor shift as large as U_0. We require that the 1-bit drive frequency have noise $\delta\nu_a \lesssim \sqrt{R_s} \sim 0.5$ Hz/$\sqrt{\text{Hz}}$ [29]; this implies laser intensity stability $\delta I/I \lesssim 3\times10^{-7}/\sqrt{\text{Hz}}$. This is $\sim 300\times$ the shot-noise limit, and should be achievable [30]. Electric field noise couples directly to the molecular dipole moments, and is also of concern. With field plate spacing of ~ 1 cm, we require broadband voltage noise $\delta V \lesssim 0.5$ μV/$\sqrt{\text{Hz}}$, the room-temperature Johnson noise on a 10 MΩ resistor. Noise from the high-voltage supply can be heavily filtered and should pose no problems. A variety of other possible decoherence sources seem to present no limitations. These include heating due to laser intensity, beam-pointing, or frequency fluctuations [16, 31]; dissociation of molecules by the trap laser [32]; spontaneous emission; coupling to blackbody radiation; collisions with background gas molecules; etc.

We have shown that a quantum computer based on ultracold KCs molecules can plausibly achieve $\sim 10^5$ CNOT gates on $\sim 10^4$ bits in the anticipated decoherence time of ~ 5 s. This may be sufficient for quantum error correction methods to ensure that arbitrarily long computations are stable [33]. We have also argued that this system requires no dramatic technical breakthroughs for its initial construction. The electric resonance techniques for the processor should be robust and easy to implement, by analogy with similar NMR methods. Creation of the trapped array of polar molecules appears to be a direct extension of recent work in laser cooling and trap-

ping, and the readout via resonance-enhanced ionization is standard. Unlike recent proposals for quantum computation using ultracold atoms, our technique requires neither mechanical motion [2, 34], nor coupling to short-lived excited states [2, 35], for gate operations.

There are a number of potentially serious issues that we have not considered. For example, the bit-bit interaction cannot be switched off, and thus operation will require techniques similar to the "refocusing" procedure used to control the couplings in NMR quantum computation [36]. We have ignored the motional states of the molecules; although the trap motional frequencies (~ 100 kHz) are well-separated from other frequency scales in the device, couplings of gate operations to the motion may cause additional decoherence or gate fidelity loss [35]. We have also ignored the hyperfine structure of the KCs molecules, which might complicate the initial state selection and/or gate operations. We plan to investigate these issues in the future. In the meantime, we have begun an experimental effort to implement these ideas (using RbCs rather than KCs for technical convenience).

On the other hand, the parameters discussed here might also be improved with other techniques that are currently less well developed. For example, buffer-gas cooling [37] or electric slowing and trapping [38], in combination with evaporative cooling [39], could yield larger and/or colder samples; the variety of molecules accessible to these techniques could enable the use of larger values of μ and/or smaller values of λ_t. Microfabricated traps based on low-frequency electromagnetic fields might prove advantageous [40], and non-destructive readout may be possible by direct pickup of the molecular dipole fields with nearby single-electron transistors [41]. Finally, in addition to our qubit states, there are $\sim 10^6$ long-lived rovibrational states available for each molecule [20]; these might allow each molecule to function as a quantum information unit containing $n \gg 1$ bits of information. Although entanglement between individual molecules is more difficult in this case, the massive parallelism involved may be useful in itself [42].

We thank M. Kasevich, P. Zoller, and A.J. Kerman for useful discussions. DD is an Alfred P. Sloan Research Fellow and a Packard Foundation Fellow. This work is supported by NSF ITR grant #EIA-0081332.

[1] A. Barenco *et al.*, Phys. Rev. Lett. **74**, 4083 (1995).
[2] G. Brennen *et al.*, Phys. Rev. Lett. **82**, 1060 (1999).
[3] P. Platzman and M. Dykman, Science **284**, 1967 (1999).
[4] W. Demtröder, *Laser Spectroscopy,* 2nd Ed. (Springer-Verlag, Berlin, 1996).
[5] Fioretti *et al.*, Phys. Rev. Lett. **80**, 4402 (1998).
[6] A. Nikolov *et al.*, Phys. Rev. Lett. **84**, 246 (2000).
[7] C. Drag *et al.*, IEEE J. Quant. El. **36**, 1378 (2000).
[8] C. Gabbanini *et al.*, Phys. Rev. Lett. **84**, 2814 (2000).
[9] H. Wang and W. Stwalley, J. Chem. Phys. **108**, 5767 (1998).
[10] C. M. Dion *et al.*, Phys. Rev. Lett. **86**, 2253 (2001).
[11] J. Shaffer, W. Chalupczak, and N. Bigelow, Phys. Rev. Lett. **82**, 6 (1999).
[12] See e.g. U. Gaubatz *et al.*, J. Chem. Phys. **92**, 5363 (1990).
[13] G. Igel-Mann *et al.*, J. Chem. Phys. **84**, 5007 (1986).
[14] B. Friedrich and D. Herschbach, Phys. Rev. Lett. **74**, 4623 (1995); see also P. Braun and A. Petelin, Sov. Phys. JETP **39**, 775 (1974).
[15] J. Miller, R. Cline, and D. Heinzen, Phys. Rev. A **47**, R4567 (1993).
[16] K. O'Hara *et al.*, Phys. Rev. Lett. **82**, 4204 (1999).
[17] N. Davidson *et al.*, Phys. Rev. Lett. **74**, 1311 (1995).
[18] T. Takekoshi, B. Patterson, and R. Knize, Phys. Rev. Lett. **81**, 5105 (1998).
[19] C. Adams *et al.*, Phys. Rev. Lett. **74**, 3577 (1995).
[20] Data on the typical electronic structure of bi-alkali molecules is taken from: A.A. Radzig and B.M. Smirnov, *Reference Data on Atoms, Molecules, and Ions* (Springer-Verlag, Berlin, 1980); K.P. Huber and G. Herzberg, *Molecular Spectra and Molecular Structure: IV. Constants of Diatomic Molecules* (Van Nostrand, New York, 1979); M. Korek *et al.*, Can. J. Phys. **78**, 977 (2000); A. Allouche *et al.*, J. Phys. B **33**, 2307 (2000); S. Magnier, M. Aubert-Frécon, and Ph. Millié, J. Mol. Spect. **200**, 96 (2000); and references therein.
[21] M.V. Romalis and E.N. Fortson, Phys. Rev. A **59**, 4547 (1999).
[22] S. Winoto *et al.*, Phys. Rev. A **59**, R19 (1999).
[23] See e.g. S. Hamann *et al.*, Phys. Rev. Lett. **80**, 4149 (1998).
[24] D. Jaksch *et al.*, Phys. Rev. Lett. **81**, 3108 (1998).
[25] L. Santos *et al.*, Phys. Rev. Lett. **85**, 1791 (2000).
[26] J.L. Bohn, Phys. Rev. A **63**, 052714 (2001).
[27] C. H. Townes and A. L. Schawlow, *Microwave Spectroscopy,* (McGraw-Hill, New York, 1955).
[28] R. Loudon, *The Quantum Theory of Light,* 2nd Ed. (Clarendon, Oxford, 1983).
[29] S. Lamoreaux, Phys. Rev. A **56**, 4970 (1997).
[30] J.L. Hall, in *International Conference on Quantum Optics,* ed. J. Harvey and D. Walls (Springer-Verlag, Berlin, 1986).
[31] T. Savard, K. O'Hara, and J. Thomas, Phys. Rev. A **56**, R1095 (1997).
[32] G. Askar'yan, Sov. Phys. JETP **21**, 439 (1965); V. Khersonskii, Opt. Spctrosc. (USSR) **43**, 19 (1977).
[33] J. Preskill, in *Introduction to Quantum Computation and Information,* ed. H.-K. Lo, S. Posescu, and T. Spiller (World Scientific, Singapore, 1998).
[34] D. Jaksch *et al.*, Phys. Rev. Lett. **82**, 1975 (1999).
[35] D. Jaksch *et al.*, Phys. Rev. Lett. **85**, 2208 (2000).
[36] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2000).
[37] J.D. Weinstein *et al.*, Nature **395**, 148 (1998).
[38] H.L. Bethlem *et al.*, Nature **406**, 491 (2000).
[39] J. M. Doyle *et al.*, Phys. Rev. A **52**, R2515 (1995).
[40] T. Calarco *et al.*, Phys. Rev. A **61**, 022304 (2000).
[41] R.J. Schoelkopf *et al.*, Science **280**, 1238 (1998); R. Schoelkopf, private communication (2001).
[42] J. Ahn, T. Weinacht, and P. Bucksbaum, Science **287**, 463 (2000); P. Knight, Science **287**, 441 (2000).

Measurement-based quantum computation on cluster states

Robert Raussendorf, Daniel E. Browne,* and Hans J. Briegel
Theoretische Physik, Ludwig-Maximilians-Universität München, Germany
(Dated: February 1, 2008)

We give a detailed account of the one-way quantum computer, a scheme of quantum computation that consists entirely of one-qubit measurements on a particular class of entangled states, the cluster states. We prove its universality, describe why its underlying computational model is different from the network model of quantum computation and relate quantum algorithms to mathematical graphs. Further we investigate the scaling of required resources and give a number of examples for circuits of practical interest such as the circuit for quantum Fourier transformation and for the quantum adder. Finally, we describe computation with clusters of finite size.

I. INTRODUCTION

Recently, we introduced the scheme of the one-way quantum computer ($QC_{\mathcal{C}}$) [1]. This scheme uses a given entangled state, the so-called cluster state [2], as its central physical resource. The entire quantum computation consists only of a sequence of one-qubit projective measurements on this entangled state. Thus it uses measurements as the central tool to drive a computation [3] - [6]. We called this scheme the "one-way quantum computer" since the entanglement in the cluster state is destroyed by the one-qubit measurements and therefore it can only be used once. To emphasize the importance of the cluster state for the scheme, we use the abbreviation $QC_{\mathcal{C}}$ for "one-way quantum computer".

The $QC_{\mathcal{C}}$ is universal since any unitary quantum logic network can be simulated on it efficiently. The $QC_{\mathcal{C}}$ can thus be explained as a simulator of quantum logic networks. However, the computational model that emerges for the $QC_{\mathcal{C}}$ [7] makes no reference to the concept of unitary evolution and it shall be pointed out from the beginning that the network model does not provide the most suitable description for the $QC_{\mathcal{C}}$. Nevertheless, the network model is the most widely used form of describing a quantum computer and therefore the relation between the network model and the $QC_{\mathcal{C}}$ must be clarified.

The purpose of this paper is threefold. First, it is to give the proof for universality of the $QC_{\mathcal{C}}$; second, to relate quantum algorithms to graphs; and third, to provide a number of examples for $QC_{\mathcal{C}}$-circuits which are characteristic and of practical interest.

In Section II we give the universality proof for the described scheme of computation in a complete and detailed form. The proof has already been presented to a large part in [1]. What was not contained in [1] was the explanation of why and how the gate simulations on the $QC_{\mathcal{C}}$ work. This omission seemed in order since the implementation of the gates discussed there (CNOT and arbitrary rotations) require only small clusters such that the functioning of the gates can be easily verified in a computer simulation. For the examples of gates and subcircuits given in Section IV this is no longer the case. Generally, we want an analytic explanation for the functioning of the gate simulations on the $QC_{\mathcal{C}}$. This explanation is given in Section II F and applied to the gates of a universal set in Section II G as well as to more complicated examples in Section IV.

In Section II H we discuss the spatial, temporal and operational resources required in $QC_{\mathcal{C}}$-computations in relation to the resources needed for the corresponding quantum logic networks. We find that overheads are at most polynomial. But there do not always need to be overheads. For example, as shown in Section III, all $QC_{\mathcal{C}}$-circuits in the Clifford group have unit logical depth.

In Section III we discuss non-network aspects of the $QC_{\mathcal{C}}$. In Section III A we state the reasons why the network model is not adequate to describe the $QC_{\mathcal{C}}$ in every respect. The network model is abandoned and replaced by a more appropriate model [7]. This model is described very briefly.

In Section III B we relate algorithms to graphs. We show that from every algorithm its Clifford part can be removed. The required algorithm-specific non-universal quantum resource to run the remainder of the quantum algorithm on the $QC_{\mathcal{C}}$ is then a graph state [9]. All that remains of the Clifford part is a mathematical graph specifying this graph state.

In Section IV we give examples of larger gates and subcircuits which may be of practical relevance, among them the $QC_{\mathcal{C}}$-circuit for quantum Fourier transformation and for the n-qubit adder.

In Section V we discuss the $QC_{\mathcal{C}}$ computations on finite (small) clusters and in the presence of decoherence. We describe a variant of the scheme consisting of repeated steps of (re-)entangling a cluster via the Ising interaction, alternating with rounds of one-qubit measurements. Using this modified scheme it is possible to split long computations such that they fit piecewise on a small cluster.

II. UNIVERSALITY OF QUANTUM COMPUTATION VIA ONE-QUBIT-MEASUREMENTS

In this section we prove that the $QC_{\mathcal{C}}$ is a universal quantum computer. The technique to accomplish this is to show that any quantum logic network can be simulated

efficiently on the $\mathrm{QC}_{\mathcal{C}}$. Before we go into the details, let us state the general picture.

For the one-way quantum computer, the entire resource for the quantum computation is provided initially in the form of a specific entangled state –the cluster state [2]– of a large number of qubits. Information is then written onto the cluster, processed, and read out from the cluster by one-particle measurements only. The entangled state of the cluster thereby serves as a universal "substrate" for any quantum computation. It provides in advance all entanglement that is involved in the subsequent quantum computation. Cluster states can be created efficiently in any system with a quantum Ising-type interaction (at very low temperatures) between two-state particles in a lattice configuration.

It is important to realize here that information processing is possible even though the result of every measurement in any direction of the Bloch sphere is completely random. The mathematical expression for the randomness of the measurement results is that the reduced density operator for each qubit in the cluster state is $\frac{1}{2}\mathbf{1}$. The individual measurement results are random but correlated, and these correlations enable quantum computation on the $\mathrm{QC}_{\mathcal{C}}$.

For clarity, let us emphasize that in the scheme of the $\mathrm{QC}_{\mathcal{C}}$ we distinguish between cluster qubits on $\mathcal{C}$ which are measured in the process of computation, and the logical qubits. The logical qubits constitute the quantum information being processed while the cluster qubits in the initial cluster state form an entanglement resource. Measurements of their individual one-qubit state drive the computation.

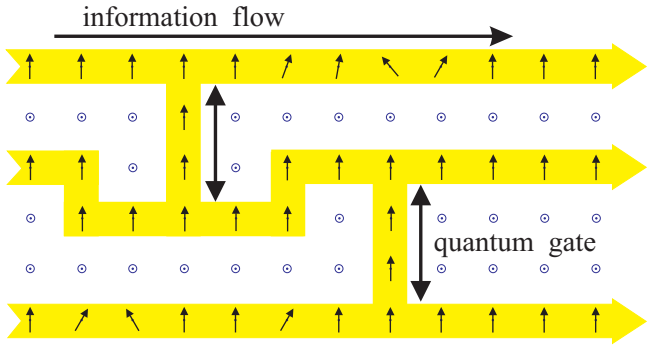


FIG. 1: Simulation of a quantum logic network by measuring two-state particles on a lattice. Before the measurements the qubits are in the cluster state $|\phi\rangle_{\mathcal{C}}$ of (1). Circles $\odot$ symbolize measurements of σ_z, vertical arrows are measurements of σ_x, while tilted arrows refer to measurements in the x-y-plane.

To process quantum information with this cluster, it suffices to measure its particles in a certain order and in a certain basis, as depicted in Fig. 1. Quantum information is thereby propagated through the cluster and processed. Measurements of σ_z-observables effectively remove the respective lattice qubit from the cluster. Measurements in the σ_x- (and σ_y-) eigenbasis are used for "wires", i.e. to propagate logical quantum bits through the cluster, and for the CNOT-gate between two logical qubits. Observables of the form $\cos(\varphi)\,\sigma_x \pm \sin(\varphi)\,\sigma_y$ are measured to realize arbitrary rotations of logical qubits. For these cluster qubits, the basis in which each of them is measured depends on the results of preceding measurements. This introduces a temporal order in which the measurements have to be performed. The processing is finished once all qubits except a last one on each wire have been measured. The remaining unmeasured qubits form the quantum register which is now ready to be read out. At this point, the results of previous measurements determine in which basis these "output" qubits need to be measured for the final readout, or if the readout measurements are in the σ_x-, σ_y- or σ_z-eigenbasis, how the readout measurements have to be interpreted. Without loss of generality, we assume in this paper that the readout measurements are performed in the σ_z-eigenbasis.

A. Cluster states and their quantum correlations

Cluster states are pure quantum states of two-level systems (qubits) located on a cluster $\mathcal{C}$. This cluster is a connected subset of a simple cubic lattice $\mathbb{Z}^d$ in $d \geq 1$ dimensions. The cluster states $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ obey the set of eigenvalue equations

$$K^{(a)}|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} = (-1)^{\kappa_a}|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}, \tag{1}$$

with the correlation operators

$$K^{(a)} = \sigma_x^{(a)} \bigotimes_{b\in \mathrm{nbgh}(a)} \sigma_z^{(b)}. \tag{2}$$

Therein, $\{\kappa_a \in \{0,1\} |\, a \in \mathcal{C}\}$ is a set of binary parameters which specify the cluster state and $\mathrm{nbgh}(a)$ is the set of all neighboring lattice sites of a. All states $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ are equally good for computation. A cluster state is completely specified by the eigenvalue equations (1). To see this, first note that two states $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ and $|\phi_{\{\tilde{\kappa}\}}\rangle_{\mathcal{C}}$ which obey a set of equations (1) but differ in at least one eigenvalue are orthogonal. This holds because if there exists an $a \in \mathcal{C}$ such that, say, $K^{(a)}|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} = |\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ and $K^{(a)}|\phi_{\{\tilde{\kappa}\}}\rangle_{\mathcal{C}} = -|\phi_{\{\tilde{\kappa}\}}\rangle_{\mathcal{C}}$, then ${}_{\mathcal{C}}\langle\phi_{\{\tilde{\kappa}\}}|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} = {}_{\mathcal{C}}\langle\phi_{\{\tilde{\kappa}\}}|K^{(a)}|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} = -{}_{\mathcal{C}}\langle\phi_{\{\tilde{\kappa}\}}|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} = 0$. From the set of states which obey (1) with the eigenvalues specified by $\{\kappa\}$ a representative $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ is taken. There are $2^{|\mathcal{C}|}$ such classes of states, and hence $2^{|\mathcal{C}|}$ mutually orthogonal representatives $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$. Therefore, the representative cluster states form a basis $\{|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} \,|\, \{\kappa\} \in \{0,1\}^{|\mathcal{C}|}\}$ of the $|\mathcal{C}|$-qubit Hilbert space. To that end, let us now consider a state $|\phi'_{\{\kappa\}_0}\rangle_{\mathcal{C}}$ that obeys (1) with the same $\{\kappa\}_0$ as $|\phi_{\{\kappa\}_0}\rangle_{\mathcal{C}}$, and expand it into the above basis. One finds $|\phi'_{\{\kappa\}_0}\rangle_{\mathcal{C}} = \sum_{\{\kappa\}} {}_{\mathcal{C}}\langle\phi_{\{\kappa\}}|\phi'_{\{\kappa\}_0}\rangle_{\mathcal{C}}\, |\phi_{\{\kappa\}}\rangle_{\mathcal{C}} = {}_{\mathcal{C}}\langle\phi_{\{\kappa\}_0}|\phi'_{\{\kappa\}_0}\rangle_{\mathcal{C}}\; |\phi_{\{\kappa\}_0}\rangle_{\mathcal{C}}$. Hence, two states $|\phi'_{\{\kappa\}_0}\rangle_{\mathcal{C}}$ and $|\phi_{\{\kappa\}_0}\rangle_{\mathcal{C}}$ which obey (1) with the same set $\{\kappa\}_0$ are the same modulo a possible global phase. Consequently, any

method that creates a state obeying equations (1) with a specific set $\{\kappa_a | a \in \mathcal{C}\}$ creates the same state.

The eigenvalue equations (1) and the quantum correlations they imply are central for the described scheme of computation. Also, they represent a very compact way of characterizing the cluster states. To reflect this in the presentation, the discussion in this paper will be based entirely on these eigenvalue equations and we will never need to work out some cluster state in any specific basis. In fact, to write down a cluster state in its explicit form would be quite space-consuming since the minimum number of required terms scales exponentially with the number of qubits [2], and for computation we will be going to consider rather large cluster states. Nevertheless, for illustration we give a few examples of cluster states with a small number of qubits. The cluster states on a chain of 2, 3 and 4 qubits, fulfilling the eigenvalue equations (1) with all $\kappa_a = 0$, are

$$\begin{aligned} |\phi\rangle_{\mathcal{C}_2} &= \frac{1}{\sqrt{2}}\left(|0\rangle_1|+\rangle_2 + |1\rangle_1|-\rangle_2\right), \\ |\phi\rangle_{\mathcal{C}_3} &= \frac{1}{\sqrt{2}}\left(|+\rangle_1|0\rangle_2|+\rangle_3 + |-\rangle_1|1\rangle_2|-\rangle_3\right), \\ |\phi\rangle_{\mathcal{C}_4} &= \frac{1}{2}|+\rangle_1|0\rangle_2|+\rangle_3|0\rangle_4 + \frac{1}{2}|+\rangle_1|0\rangle_2|-\rangle_3|1\rangle_4, \\ &\quad + \frac{1}{2}|-\rangle_1|1\rangle_2|-\rangle_3|0\rangle_4 + \frac{1}{2}|-\rangle_1|1\rangle_2|+\rangle_3|1\rangle_4, \end{aligned} \tag{3}$$

with the notations

$$\begin{aligned} |0\rangle_a &:= |0\rangle_{a,z} = \sigma_z^{(a)}|0\rangle_{a,z}, \\ |1\rangle_a &:= |1\rangle_{a,z} = -\sigma_z^{(a)}|1\rangle_{a,z}, \\ |\pm\rangle_a &:= \tfrac{1}{\sqrt{2}}(|0\rangle_a \pm |1\rangle_a). \end{aligned} \tag{4}$$

The state $|\phi\rangle_{\mathcal{C}_2}$ is local unitary equivalent to a Bell state and $|\phi\rangle_{\mathcal{C}_3}$ to the Greenberger-Horne-Zeilinger (GHZ) state. $|\phi\rangle_{\mathcal{C}_4}$ is not equivalent to a 4-particle GHZ state. In particular, the entanglement in $|\phi\rangle_{\mathcal{C}_4}$ cannot be destroyed by a single local operation [2].

Ways to create a cluster state in principle are to measure all the correlation operators $K^{(a)}$, $a \in \mathcal{C}$ of (2) on an arbitrary $|\mathcal{C}|$-qubit state or to cool into the ground state of a Hamiltonian $H_K = -\hbar g \sum_{a\in\mathcal{C}} \kappa_a K^{(a)}$.

Another way –likely to be more suitable for realization in the lab– is as follows. First, a product state $|+\rangle_{\mathcal{C}} = \bigotimes_{a\in\mathcal{C}} |+\rangle_a$ is prepared. Second, the unitary transformation $S^{(\mathcal{C})}$,

$$S^{(\mathcal{C})} = \prod_{a,b\in\mathcal{C}|b-a\in\gamma_d} S^{ab}, \tag{5}$$

is applied to the state $|+\rangle$. Often we will write S in short for $S^{(\mathcal{C})}$. In (5), for the cases of dimension $d = 1, 2, 3$, we have $\gamma_1 = \{1\}$, $\gamma_2 = \{(1,0)^T, (0,1)^T\}$ and $\gamma_3 = \{(1,0,0)^T, (0,1,0)^T, (0,0,1)^T\}$, and the two-qubit transformation S^{ab} is such that the state $|1\rangle_a \otimes |1\rangle_b$ acquires a phase of π under its action while the remaining states $|0\rangle_a \otimes |0\rangle_b$, $|0\rangle_a \otimes |1\rangle_b$ and $|1\rangle_a \otimes |0\rangle_b$ acquire no phase. Thus, S^{ab} has the form

$$S^{ab} = \frac{1}{2}\left(\mathbf{1} + \sigma_z^{(a)} + \sigma_z^{(b)} - \sigma_z^{(a)} \otimes \sigma_z^{(b)}\right). \tag{6}$$

The state $|+\rangle_{\mathcal{C}}$ obviously obeys the eigenvalue equations $\sigma_x^{(a)}|+\rangle_{\mathcal{C}} = |+\rangle_{\mathcal{C}}$ $\forall a \in \mathcal{C}$ and thus the cluster state $|\phi\rangle_{\mathcal{C}}$ generated via S obeys

$$|\phi\rangle_{\mathcal{C}} = S\sigma_x^{(a)}S^\dagger |\phi\rangle_{\mathcal{C}}, \quad \forall a \in \mathcal{C}. \tag{7}$$

To obtain $S\sigma_x^{(a)}S^\dagger$, observe that

$$\begin{aligned} S^{ab}\sigma_x^{(a)}S^{ab\dagger} &= \sigma_x^{(a)} \otimes \sigma_z^{(b)}, \\ S^{ab}\sigma_x^{(b)}S^{ab\dagger} &= \sigma_z^{(a)} \otimes \sigma_x^{(b)}, \end{aligned} \tag{8}$$

and

$$S^{ab}\sigma_x^{(c)}S^{ab\dagger} = \sigma_x^{(c)}, \quad \forall c \in \mathcal{C}\backslash\{a,b\}. \tag{9}$$

Further, the Pauli phase flip operators $\sigma_z^{(d)}$ commute with all S^{ab}, i.e.

$$S^{ab}\sigma_z^{(d)}S^{ab\dagger} = \sigma_z^{(d)}, \quad \forall d \in \mathcal{C}. \tag{10}$$

Now, from (8), (9) and (10) it follows that

$$S\sigma_x^{(a)}S^\dagger = \sigma_x^{(a)} \bigotimes_{b\in\mathrm{nbgh}(a)} \sigma_z^{(b)}. \tag{11}$$

Thus, the state $|\phi\rangle_{\mathcal{C}}$ generated from $|+\rangle_{\mathcal{C}}$ via the transformation S as defined in (5) does indeed obey eigenvalue equations of form (1), with

$$\kappa_a = 0, \quad \forall a \in \mathcal{C}. \tag{12}$$

Note that all operations S^{ab} in S mutually commute and that they can therefore be carried out at the same time. Initial individual preparation of the cluster qubits in $|+\rangle_{a\in\mathcal{C}}$ can also be done in parallel. Thus, the creation of the cluster state is a two step process. *The temporal resources to create the cluster state are constant in the size of the cluster.*

If a cluster state is created as described above this leads to the specific set of eigenvalues in (1) specified by the parameters κ_a in (12). As the eigenvalues are fixed in this case, we drop them in the notation for the cluster state $|\phi\rangle_{\mathcal{C}}$. Cluster states specified by different sets $\{\kappa_a\}$ can be obtained by applying Pauli phase flip operators $\sigma_z^{(a)}$. To see this, note that

$$\sigma_z^{(a)}K^{(b)}{\sigma_z^{(a)}}^\dagger = (-1)^{\delta_{a,b}} K^{(b)}. \tag{13}$$

Therefore,

$$\bigotimes_{a\in\mathcal{C}} \left(\sigma_z^{(a)}\right)^{\Delta\kappa_a} |\phi_{\{\kappa_a\}}\rangle_{\mathcal{C}} = |\phi_{\{\kappa_a+\Delta\kappa_a\}}\rangle_{\mathcal{C}}, \tag{14}$$

where the addition for the κ_a is modulo 2.

The transformation S defined in (5) is generated by the Hamiltonian

$$H = \hbar g \sum_{a,b\in\mathcal{C}|b-a\in\gamma_d} \frac{1-\sigma_z^{(a)}}{2}\frac{1-\sigma_z^{(b)}}{2}, \tag{15}$$

and S is of the form

$$S = \exp\left(-i\pi \sum_{a,b\in\mathcal{C}|b-a\in\gamma_d} \frac{1-\sigma_z^{(a)}}{2}\frac{1-\sigma_z^{(b)}}{2}\right). \quad (16)$$

Expanding the exponent in (16), one obtains

$$S = \left[\prod_{a,b\in\mathcal{C}|b-a\in\gamma_d} e^{-i\frac{\pi}{4}} \exp\left(i\frac{\pi}{4}\sigma_z^{(a)}\right)\exp\left(i\frac{\pi}{4}\sigma_z^{(b)}\right)\right] \times \exp\left(-i\frac{\pi}{4}\sum_{a,b\in\mathcal{C}|b-a\in\gamma_d}\sigma_z^{(a)}\sigma_z^{(b)}\right). \quad (17)$$

We find that the interaction part H_I of the Hamiltonian H generating S is of Ising form,

$$H_I = \hbar\frac{g}{4}\sum_{a,b\in\mathcal{C}|b-a\in\gamma_d}\sigma_z^{(a)}\sigma_z^{(b)}, \quad (18)$$

and, since the local part H_{local} of the Hamiltonian commutes with the Ising Hamiltonian H_I, the interaction S generated by H is local unitary equivalent to the unitary transformation generated by a Ising Hamiltonian.

For matter of presentation, the interaction S^{ab} in (6) and, correspondingly, the local part of the Hamiltonian H in (15) has been chosen in such a way that the eigenvalue equations (1) take the particularly simple form with $\kappa_a = 0$ for all $a \in \mathcal{C}$, irrespective of the shape of the cluster.

Concerning the creation of states that are useful as a resource for the $\text{QC}_{\mathcal{C}}$, i.e. cluster- or local unitary equivalent states, all systems with a tunable Ising interaction and a local σ_z-type Hamiltonian, i.e. with a Hamiltonian

$$H' = \sum_{a\in\mathcal{C}}\Delta E_a\,\sigma_z^{(a)} + \hbar\frac{g(t)}{4}\sum_{a,b\in\mathcal{C}|b-a\in\gamma_d}\sigma_z^{(a)}\sigma_z^{(b)} \quad (19)$$

are suitable, provided the coupling $g(t)$ can be switched between zero and at least one nonzero value.

Even this condition can be relaxed. A permanent Ising interaction instead of a globally tunable one is sufficient, if the measurement process is much faster than the characteristic time scale for the Ising interaction, i.e. if the measurements are stroboscopic. If it takes the Ising interaction a time T_{Ising} to create a cluster state $|\phi\rangle_{\mathcal{C}}$ from a product state $|+\rangle_{\mathcal{C}}$, then the Ising interaction acting for a time $2T_{\text{Ising}}$ performs the identity operation, $S^{(\mathcal{C})}S^{(\mathcal{C})} = \mathbb{1}^{(\mathcal{C})}$. Therefore, starting with a product state $|+\rangle_{\mathcal{C}}$ at time $t = 0$ evolving under permanent Ising interaction, stroboscopic measurements may be performed at times $(2k+1)\,T_{\text{Ising}}$, $k \in \mathbb{N}$.

Some basic notions of graph theory will later, in the universality proof, simplify the formulation of our specifications. Therefore let us, at this point, establish a connection between quantum states such as the cluster state of (1) and graphs. The treatment here follows that of [9], adapted to our notation.

First let us recall the definition of a graph. A graph $G(V, E)$ is a set V of vertices connected via edges e from the set E. The information of which vertex $a \in V$ is connected to which other vertex $b \in V$ is contained in a symmetric $|V| \times |V|$ matrix Γ, the adjacency matrix. The matrix Γ is such that $\Gamma_{ab} = 1$ if two vertices a and b are connected via an edge $e \in E$, and $\Gamma_{ab} = 0$ otherwise. We identify the cluster $\mathcal{C}$ with the vertices $V_{\mathcal{C}}$ of a graph, $\mathcal{C} = V_{\mathcal{C}}$, and in this way establish a connection to the notion introduced earlier.

To relate graphs to quantum mechanics, the vertices of a graph can be identified with local quantum systems, in this case qubits, and the edges with two-particle interactions [9],[10], in the present case $\sigma_z\sigma_z$-interactions. If one initially prepares each individual qubit a in the state $(\sigma_z^{(a)})^{\kappa_a}|+\rangle_a$ and subsequently switches on, for an appropriately chosen finite time span, the interaction

$$H_{G(V,E)} = \hbar g\sum_{(a,b)\in E}\frac{1-\sigma_z^{(a)}}{2}\frac{1-\sigma_z^{(b)}}{2}, \quad (20)$$

with $(a, b) \in E$ denoting an edge between qubits a and b, then one obtains quantum states that are graph code words as introduced in [9]. Henceforth we will refer to these graph code words as graph states and use them in a context different from coding. The graph states $|\phi\{\kappa\}\rangle_G$ are defined by a set of eigenvalue equations which read

$$\sigma_x^{(a)}\bigotimes_{b\in V}\left(\sigma_z^{(b)}\right)^{\Gamma_{ab}}|\phi\{\kappa\}\rangle_G = (-1)^{\kappa_a}|\phi\{\kappa\}\rangle_G, \quad (21)$$

with $\kappa_a \in \{0, 1\}\ \forall\, a \in V$. Here we use G instead of V as an index for the state $|\phi\rangle$ as the set $E \subset V \times V$ of edges is now independent and no longer implicitly specified by V as was the case in (1).

Note that cluster states (1) are a particular case of graph states (21). The graph $G(\mathcal{C}, E_{\mathcal{C}})$ which describes a cluster state is that of a square lattice in 2D and that of a simple cubic lattice in 3D, i.e. the set $E_{\mathcal{C}}$ of edges is given by

$$E_{\mathcal{C}} = \big\{(a,b)|\, a, b \in \mathcal{C}, b \in \text{nbgh}(a)\big\}. \quad (22)$$

Let us at the end of this section mention how cluster states may be created in practice. One possibility is via cold controlled collisions in optical lattices, as described in [2]. Cold atoms representing the qubits can be arranged on a two- or three dimensional lattice and state-dependent interaction phases may be acquired via cold collisions between neighboring atoms [12] or via tunneling [13]. For a suitable choice of the collision phases φ, $\varphi = \pi \bmod 2\pi$, the state resulting from a product state $|+\rangle_{\mathcal{C}}$ after interaction is a cluster state obeying the eigenvalue equations (1), with the set $\{\kappa_a, a \in \mathcal{C}\}$ specified by the filling pattern of the lattice.

B. A universal set of quantum gates

To provide something definite to discuss right from the beginning, we now give the procedures of how to realize a CNOT-gate and a general one-qubit rotation via one-qubit measurements on a cluster state. The explanation of why and how these gates work will be given in Section II G.

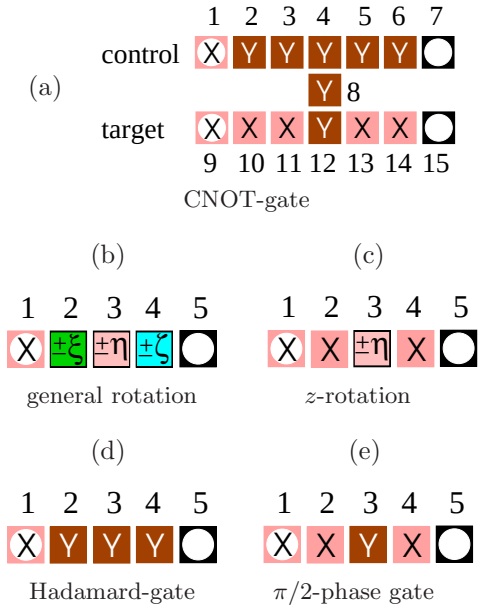


FIG. 2: Realization of elementary quantum gates on the QC_C. Each square represents a lattice qubit. The squares in the extreme left column marked with white circles denote the input qubits, those in the right-most column denote the output qubits.

A CNOT-gate can be realized on a cluster state of 15 qubits, as shown in Fig. 2. All measurements can be performed simultaneously. The procedure to realize a CNOT-gate on a cluster with 15 qubits as displayed in Fig. 2 is

Procedure 1 Realization of a CNOT-gate acting on a two-qubit state $|\psi_{\rm in}\rangle$.

1. Prepare the state $|\Psi_{\rm in}\rangle_{\mathcal{C}_{15}} = |\psi_{\rm in}\rangle_{1,9} \otimes \left(\bigotimes_{i\in\mathcal{C}_{15}\setminus\{1,9\}} |+\rangle_i\right)$.

2. Entangle the 15 qubits of the cluster $\mathcal{C}_{15}$ via the unitary operation $S^{(\mathcal{C}_{15})}$.

3. Measure all qubits of $\mathcal{C}_{15}$ except for the output qubits 7, 15 (following the labeling in Fig. 2). The measurements can be performed simultaneously. Qubits 1, 9, 10, 11, 13, 14 are measured in the σ_x-eigenbasis and qubits 2-6, 8, 12 in the σ_y-eigenbasis.

Dependent on the measurement results, the following gate is thereby realized:

$$U'_{CNOT} = U_{\Sigma,CNOT}\, CNOT(c,t). \tag{23}$$

Therein the byproduct operator $U_{\Sigma,CNOT}$ has the form

$$\begin{aligned} U_{\Sigma,CNOT} &= {\sigma_x^{(c)}}^{\gamma_x^{(c)}} {\sigma_x^{(t)}}^{\gamma_x^{(t)}} {\sigma_z^{(c)}}^{\gamma_z^{(c)}} {\sigma_z^{(t)}}^{\gamma_z^{(t)}}, \text{ with} \\ \gamma_x^{(c)} &= s_2+s_3+s_5+s_6 \\ \gamma_x^{(t)} &= s_2+s_3+s_8+s_{10}+s_{12}+s_{14} \\ \gamma_z^{(c)} &= s_1+s_3+s_4+s_5+s_8+s_9+s_{11}+1 \\ \gamma_z^{(t)} &= s_9+s_{11}+s_{13}. \end{aligned} \tag{24}$$

Therein, the s_i represent the measurement outcomes s_i on the qubits i. The expression (24) is modified if redundant cluster qubits are present and/or if the cluster state on which the CNOT gate is realized is specified by a set $\{\kappa_a\}$ different from (12), see Section II C. This concludes the presentation of the CNOT gate, the proof of its functioning is given in Section II G.

An arbitrary rotation $U_{Rot} \in SU(2)$ can be realized on a chain of 5 qubits. Consider a rotation in its Euler representation

$$U_{Rot}[\xi,\eta,\zeta] = U_x[\zeta]U_z[\eta]U_x[\xi], \tag{25}$$

where the rotations about the x- and z-axis are

$$\begin{aligned} U_x[\alpha] &= \exp\left(-i\alpha\frac{\sigma_x}{2}\right) \\ U_z[\alpha] &= \exp\left(-i\alpha\frac{\sigma_z}{2}\right). \end{aligned} \tag{26}$$

Initially, the first qubit is prepared in some state $|\psi_{\rm in}\rangle$, which is to be rotated, and the other qubits are prepared in $|+\rangle$. After the 5 qubits are entangled by the unitary transformation S, the state $|\psi_{\rm in}\rangle$ can be rotated by measuring qubits 1 to 4. At the same time, the state is also swapped to site 5. The qubits $1\,..\,4$ are measured in appropriately chosen bases

$$\mathcal{B}_j(\varphi_j) = \left\{\frac{|0\rangle_j + e^{i\varphi_j}|1\rangle_j}{\sqrt{2}}, \frac{|0\rangle_j - e^{i\varphi_j}|1\rangle_j}{\sqrt{2}}\right\}, \tag{27}$$

whereby the measurement outcomes $s_j \in \{0,1\}$ for $j = 1\,..\,4$ are obtained. Here, $s_j = 0$ means that qubit j is projected into the first state of $\mathcal{B}_j(\varphi_j)$. In (27) the basis states of all possible measurement bases lie on the equator of the Bloch sphere, i.e. on the intersection of the Bloch sphere with the x-y-plane. Therefore, the measurement basis for qubit j can be specified by a single parameter, the measurement angle φ_j. The measurement direction of qubit j is the vector on the Bloch sphere which corresponds to the first state in the measurement basis $\mathcal{B}_j(\varphi_j)$. Thus, the measurement angle φ_j is the angle between the measurement direction at qubit j and the positive x-axis. In summary, the procedure to realize an arbitrary rotation $U_{Rot}[\xi,\eta,\zeta]$, specified by its Euler angles ξ,η,ζ, is this:

Procedure 2 Realization of general one-qubit rotations $U_{Rot} \in SU(2)$.

1. Prepare the state $|\Psi_{\rm in}\rangle_{\mathcal{C}_5} = |\psi_{\rm in}\rangle_1 \otimes \left(\bigotimes_{i=2}^{5} |+\rangle_i\right)$.
2. Entangle the five qubits of the cluster $\mathcal{C}_5$ via the unitary operation $S^{(\mathcal{C}_5)}$.
3. Measure qubits 1 - 4 in the following order and basis

$$\begin{array}{ll} 3.1 & \text{measure qubit 1 in } \mathcal{B}_1(0) \\ 3.2 & \text{measure qubit 2 in } \mathcal{B}_2\left(-\xi\,(-1)^{s_1}\right) \\ 3.3 & \text{measure qubit 3 in } \mathcal{B}_3\left(-\eta\,(-1)^{s_2}\right) \\ 3.4 & \text{measure qubit 4 in } \mathcal{B}_4\left(-\zeta\,(-1)^{s_1+s_3}\right) \end{array} \qquad (28)$$

Via Procedure 2 the rotation U'_{Rot} is realized:

$$U'_{Rot}[\xi,\eta,\zeta] = U_{\Sigma,Rot}\, U_{Rot}[\xi,\eta,\zeta]. \qquad (29)$$

Therein, the random byproduct operator has the form

$$U_{\Sigma,Rot} = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}. \qquad (30)$$

It can be corrected for at the end of the computation, as will be explained in Section II E.

There is a subgroup of rotations for which the realization procedure is somewhat simpler than Procedure 2. These rotations form the subgroup of local operations in the Clifford group. The Clifford group is the normalizer of the Pauli group.

Among these rotations are, for example, the Hadamard gate and the $\pi/2$-phase gate. These gates can be realized on a chain of 5 qubits in the following way:

Procedure 3 Realization of a Hadamard- and $\pi/2$-phase gate.

1. Prepare the state $|\Psi_{\rm in}\rangle_{\mathcal{C}_5} = |\psi_{\rm in}\rangle_1 \otimes \left(\bigotimes_{i=2}^{5} |+\rangle_i\right)$.
2. Entangle the five qubits of the cluster $\mathcal{C}_5$ via the unitary operation $S^{(\mathcal{C}_5)}$.
3. Measure qubits 1 - 4. This can be done simultaneously. For the Hadamard gate, measure individually the observables $\sigma_x^{(1)}$, $\sigma_y^{(2)}$, $\sigma_y^{(3)}$, $\sigma_y^{(4)}$. For the $\pi/2$-phase gate measure $\sigma_x^{(1)}$, $\sigma_x^{(2)}$, $\sigma_y^{(3)}$, $\sigma_x^{(4)}$.

The difference with respect to Procedure 2 for general rotations is that in Procedure 3 no measurement bases need to be adjusted according to previous measurement results and therefore the measurements can all be performed at the same time.

As in the cases before, the Hadamard- and the $\pi/2$-phase gate are performed only modulo a subsequent byproduct operator which is determined by the random measurement outcomes s_k

$$\begin{array}{rcl} U_{\Sigma,H} & = & \sigma_x^{s_1+s_3+s_4}\,\sigma_z^{s_2+s_3} \\ U_{\Sigma,U_z(\pi/2)} & = & \sigma_x^{s_2+s_4}\,\sigma_z^{s_1+s_2+s_3+1}. \end{array} \qquad (31)$$

Before we explain the functioning of the above gates, we would like to address the following questions: First,"How does one manage to occupy only those lattice sites with cluster qubits that are required for a particular circuit but leaves the remaining ones empty?". The answer to this question is that redundant qubits will not have to be removed physically. It is sufficient to measure each of them in the σ_z-eigenbasis, as will be described in Section II C.

Second, "How can the described procedures for gate simulation be concatenated such that they represent a measurement based simulation of an entire circuit?". It seems at first sight that the described building blocks would only lead to a computational scheme consisting of repeated steps of entangling operations and measurements. This is not the case. As will be shown in Section II D, the three procedures stated are precisely of such a form that the described measurement-based scheme of quantum computation can be decomposed into them.

The third question is: "How does one deal with the randomness of the measurement results that leads to the byproduct operators (24), (30) and (31)?". The appearance of byproduct operators may suggest that there is a need for local correction operations to counteract these unwanted extra operators. However, there is neither a possibility for such counter rotations within the described model of quantum computation, nor is there a need. The scheme works with unit efficiency despite the randomness of the individual measurement results, as will be discussed in Section II E.

C. Removing the redundant cluster qubits

A cluster state on a two-dimensional cluster of rectangular shape, say, is a resource that allows for any computation that fits on the cluster. If one realizes a certain quantum circuit on this cluster state, there will always be qubits on the cluster which are not needed for its realization. Such cluster qubits we call redundant for this particular circuit.

In the description of the $\mathrm{QC}_{\mathcal{C}}$ as a quantum logic network, the first step of each computation will be to remove these redundant cluster qubits. Fortunately, the situation is not such that we have to remove the qubits (or, more precisely, the carriers of the qubits) physically from the lattice. To make them ineffective to the realized circuit, it suffices to measure each of them in the σ_z-eigenbasis. In this way, one is left with an entangled quantum state on the cluster $\mathcal{C}_N$ of the unmeasured qubits and a product state on $\mathcal{C}\backslash\mathcal{C}_N$,

$$|\phi_{\{\kappa\}}\rangle_{\mathcal{C}} \longrightarrow |Z\rangle_{\mathcal{C}\backslash\mathcal{C}_N} \otimes |\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}, \qquad (32)$$

with $|Z\rangle_{\mathcal{C}\backslash\mathcal{C}_N} = \left(\bigotimes_{i\in\mathcal{C}\backslash\mathcal{C}_N} |s_i\rangle_{i,z}\right)$ and s_i the results of the σ_z-measurements. The resulting entangled state $|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}$ on the sub-cluster $\mathcal{C}_N$ is again a cluster state

obeying the set of equations (11). This can be seen as follows. First, by definition we have

$$|Z\rangle_{\mathcal{C}\setminus\mathcal{C}_N}\otimes|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}=\left(\bigotimes_{i\in\mathcal{C}\setminus\mathcal{C}_N}\frac{1+(-1)^{s_i}\sigma_z^{(i)}}{2}\right)|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}. \tag{33}$$

Using the eigenvalue equations (11), we now insert a correlation operator $K^{(a)}$ with $a\in\mathcal{C}_N$ into the r.h.s of (33) between the projector and the state, and obtain

$$|Z\rangle_{\mathcal{C}\setminus\mathcal{C}_N}\otimes|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}=(-1)^{\kappa'_a}K'^{(a)}|Z\rangle_{\mathcal{C}\setminus\mathcal{C}_N}\otimes|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}, \tag{34}$$

with the correlation operators

$$K'^{(a)}=\sigma_x^{(a)}\bigotimes_{c\in\mathrm{nbgh}(a)\cap\mathcal{C}_N}\sigma_z^{(c)}, \tag{35}$$

and the set $\{\kappa'_a\}$ specifying the eigenvalues

$$\kappa'_a=\left(\kappa_a+\sum_{b\in\mathrm{nbgh}(a)\cap(\mathcal{C}\setminus\mathcal{C}_N)}s_b\right)\ \mathrm{mod}\ 2. \tag{36}$$

As the new correlation operators $K'^{(a)}$ in (34) only act on the cluster qubits in $\mathcal{C}_N$, the states $|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}$ again obey eigenvalue equations of type (11), i.e.

$$K'^{(a)}|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}=(-1)^{\kappa'_a}|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N},\ \forall\ a\in\mathcal{C}_N. \tag{37}$$

There are $|\mathcal{C}_N|$ such eigenvalue equations for a state of $|\mathcal{C}_N|$ qubits. Thus, the state $|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}$ is specified by (37) up to a global phase.

From (36) we find that the redundant qubits have some remaining influence on the process of computation. After they have been measured, the random measurement results enter into the eigenvalues that specify the residual cluster state $|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}$ on the cluster $\mathcal{C}_N$. However, any cluster state $|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}$ is equally good for computation as stated in Section II A. From (14) it follows that

$$|\phi_{\{\kappa'\}}\rangle_{\mathcal{C}_N}=\bigotimes_{a\in\mathcal{C}_N}\left(\sigma_z^{(a)}\right)^{\kappa'_a}|\phi\rangle_{\mathcal{C}_N}. \tag{38}$$

The Pauli phase flip operators that appear on the r.h.s. of equation (38) may be absorbed into the subsequent measurements. This allows us to adopt the following two rules in the further discussion

1. *The redundant cluster qubits are discarded. We only consider the sub-cluster* $\mathcal{C}_N$.
2. *We assume that* $\kappa'_a=0$ *for all* $a\in\mathcal{C}_N$. (39)

This reduction will make a number of expressions such as those for the byproduct operators more transparent and it will also simplify the remaining part of the universality proof.

D. Concatenation of gate simulations

A quantum circuit on the $\mathrm{QC}_{\mathcal{C}}$ is a spatial and temporal pattern of measurements on individual qubits which have previously been entangled to form a cluster state. To better understand its functioning we would like –as in the network model of quantum computation– to decompose the circuit into basic building blocks. These building blocks should be such that out of them any circuit can be assembled. In explaining the $\mathrm{QC}_{\mathcal{C}}$ in a network language, we can relate the building blocks of a quantum logic network –the quantum gates– to building blocks of $\mathrm{QC}_{\mathcal{C}}$-circuits.

The fact that quantum gates can be combined to quantum logic networks is obvious. But the statement that, for a $\mathrm{QC}_{\mathcal{C}}$-computation, measurement patterns which simulate gates can simply be patched together to give the measurement pattern for the whole circuit requires a proof. This proof is given next.

We begin by stating the general form of the procedures to realize gates and sub-circuits. The reason why these procedures work is explained in subsequent sections. To realize a gate g on the $\mathrm{QC}_{\mathcal{C}}$ consider a cluster $\mathcal{C}(g)$. This cluster has an input section $\mathcal{C}_I(g)$, a body $\mathcal{C}_M(g)$ and an output section $\mathcal{C}_O(g)$, with

$$\begin{aligned}\mathcal{C}_I(g)\cup\mathcal{C}_M(g)\cup\mathcal{C}_O(g)&=\mathcal{C}(g)\\ \mathcal{C}_I(g)\cap\mathcal{C}_M(g)&=\emptyset\\ \mathcal{C}_I(g)\cap\mathcal{C}_O(g)&=\emptyset\\ \mathcal{C}_M(g)\cap\mathcal{C}_O(g)&=\emptyset.\end{aligned} \tag{40}$$

The measurement bases of the qubits in $\mathcal{C}_M(g)$, the body of the gate g, encode g. The general scheme for procedures to realize a gate g on a cluster $\mathcal{C}(g)$ is

Scheme 1 Simulation of the gate g on $\mathcal{C}(g)$, acting on the input state $|\psi\rangle_{\mathrm{in}}$.

1. Prepare the input state $|\psi_{\mathrm{in}}\rangle$ on $\mathcal{C}_I(g)$ and the qubits in $\mathcal{C}_M(g)\cup\mathcal{C}_O(g)$ individually in the state $|+\rangle=|0\rangle_x$ such that the quantum state of all qubits in $\mathcal{C}(g)$ becomes
$$|\Psi_{\mathrm{in}}\rangle_{\mathcal{C}(g)}=|\psi_{\mathrm{in}}\rangle_{\mathcal{C}_I(g)}\otimes\bigotimes_{k\in\mathcal{C}_M(g)\cup\mathcal{C}_O(g)}|+\rangle_k. \tag{41}$$
2. Entangle $|\Psi_{\mathrm{in}}\rangle_{\mathcal{C}(g)}$ by the interaction
$$S^{(\mathcal{C}(g))}=\prod_{a,b\in\mathcal{C}(g)|\ b-a\in\gamma_d}S^{ab}, \tag{42}$$
such that the resulting quantum state is $|\Psi_\varepsilon\rangle_{\mathcal{C}_N}=S^{(\mathcal{C}(g))}|\Psi_{\mathrm{in}}\rangle_{\mathcal{C}(g)}$.
3. Measure the cluster qubits in $\mathcal{C}_I(g)\cup\mathcal{C}_M(g)$, i.e. choose measurement bases specified by $\vec{r}_k\in S^2$, $k\in\mathcal{C}_I(g)\cup\mathcal{C}_M(g)$ and obtain the random measurement results s_k such that the projector
$$P^{(\mathcal{C}_I(g)\cup\mathcal{C}_M(g))}=\bigotimes_{k\in\mathcal{C}_I(g)\cup\mathcal{C}_M(g)}\frac{1+(-1)^{s_k}\vec{r}_k\cdot\vec{\sigma}^{(k)}}{2} \tag{43}$$

is applied. The resulting state is $|\Psi_{\rm out}\rangle_{\mathcal{C}_N} = P^{(\mathcal{C}_I(g)\cup\mathcal{C}_M(g))}|\Psi_\varepsilon\rangle_{\mathcal{C}_N}$.

Putting all three steps of Scheme 1 together, the relation between $|\Psi_{\rm in}\rangle_{\mathcal{C}_N}$ and $|\Psi_{\rm out}\rangle_{\mathcal{C}_N}$ is

$$|\Psi_{\rm out}\rangle_{\mathcal{C}_N} = P^{(\mathcal{C}_I(g)\cup\mathcal{C}_M(g))}\, S^{(\mathcal{C}(g))}\, |\Psi_{\rm in}\rangle_{\mathcal{C}_N}. \qquad (44)$$

As we will show later, the state $|\Psi_{\rm out}\rangle_{\mathcal{C}_N}$ has the form

$$|\Psi_{\rm out}\rangle_{\mathcal{C}_N} = \left(\bigotimes_{k\in\mathcal{C}_I(g)\cup\mathcal{C}_M(g)} |s_k\rangle_{k,\vec{r}_k}\right) \otimes |\psi_{\rm out}\rangle_{\mathcal{C}_O(g)}, \qquad (45)$$

where $|s_k\rangle_{k,\vec{r}_k}$ denotes the state of the qubit k after the observable $\vec{r}_k\cdot\vec{\sigma}^{(k)}$ has been measured and the measurement outcome was s_k, and

$$|\psi_{\rm out}\rangle = U_{\Sigma,g}U_g|\psi_{\rm in}\rangle. \qquad (46)$$

Therein, U_g is the desired unitary operation and $U_{\Sigma,g}$ an extra multi-local rotation that depends on the measurement results $\{s_k \mid k \in \mathcal{C}_I(g)\cup\mathcal{C}_M(g)\}$. The extra rotations $U_{\Sigma,g}$ are always in the Pauli group, i.e.

$$U_{\Sigma,g} = \bigotimes_{i=1}^{n} \left(\sigma_x^{[i]}\right)^{x_i} \left(\sigma_z^{[i]}\right)^{z_i} \qquad (47)$$

modulo a possible global phase, and $n = |I| = |O|$. In (47) the $\sigma^{[i]}$ denote Pauli operators acting on the *logical* qubit i, not cluster qubit. The values $x_i, z_i \in \{0,1\}$ are computed from the measurement outcomes $\{s_k \mid k \in \mathcal{C}_I(g)\cup\mathcal{C}_M(g)\}$.

We now have all prerequisites at hand to explain why measurement patterns of basic gates can be combined to form the measurement pattern of the whole circuit which is obtained by combining the gates. The scheme of quantum computation with the $\mathrm{QC}_\mathcal{C}$ consists of a single entangling operation which creates the resource cluster state and, subsequently, of a series of one-qubit measurements on that state. We want to view the measurement pattern of a quantum circuit as being composed of basic blocks from whose function the function of the whole circuit can be deduced. To do so, we will explain computation on the $\mathrm{QC}_\mathcal{C}$ as a sequential process of performing the circuit gate by gate. Then we have to demonstrate that the computational scheme as it is practically carried out, i.e. entangle once and afterwards only measure, and the sequential scheme that we use to explain the functioning of the circuit are mathematically equivalent.

The sequential scheme is this. Consider a circuit $U = \prod_{i=1}^{|\mathcal{N}|} U_{g_i}$ that consists of a succession of gates $g_1, .., g_{|\mathcal{N}|} \in \mathcal{N}$ applied to some input state $|\psi_{\rm in}\rangle$, leading to an output state $|\psi_{\rm out}\rangle = U|\psi_{\rm in}\rangle$ which is then measured. $\mathcal{N}$ denotes the network, i.e. the set of gates plus a description of their relation. For simplicity let us first assume that each gate g_i acts on all of the logical qubits. Subsequently we will drop this assumption.

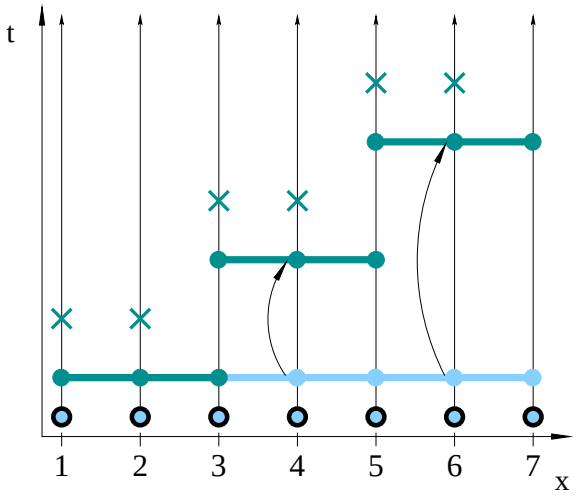


FIG. 3: Here the exchange of the order of the measurements and the entanglement operations is shown. The crosses "×" denote the one-qubit measurements and the horizontal lines between adjacent cluster qubits denote the unitary transformations $S^{a,a+1}$.

First, a quantum state $|\psi_{\rm in}\rangle_I \otimes |+\rangle_{\mathcal{C}_N\setminus I}$ is prepared. Then each gate, one after another, is realized on a subcluster $\mathcal{C}(g) \subset \mathcal{C}_N$ according to Scheme 1. Finally, the output is measured as usual.

In the step of carrying out the gate g_i the state of the quantum register is, besides being processed, also teleported from $\mathcal{C}_I(g_i) = \mathcal{C}_O(g_{i-1})$ to $\mathcal{C}_O(g_i) = \mathcal{C}_I(g_{i+1})$. In this way, by carrying out the gate g_i the input for the successor gate g_{i+1} is provided. To proceed with the realization of gate g_{i+1}, in accordance with Scheme 1, the sub-cluster $\mathcal{C}(g_{i+1})$ is entangled via $S^{(\mathcal{C}(g_{i+1}))}$and subsequently the cluster qubits in $\mathcal{C}_I(g_{i+1})\cup\mathcal{C}_M(g_{i+1})$ are measured. This completes the realization of gate g_{i+1} and at the same time writes the input for g_{i+2}, and so on.

The reason why the sequential scheme just described is equivalent to the entangle-once-and-then-only-measure scheme is the following. The entanglement operations at the various stages of the sequential scheme commute with all the measurements carried out earlier. This holds because both operations, entangling operation and earlier measurement, act on different particles. Thus, the operations may be reordered in such a way that in a first step all entangling operations $S^{(\mathcal{C}(g_i))}$ act on the initial state and afterwards all the measurements are performed.

The exchange of the order of the one-particle measurements and the two-particle Ising interactions is shown in Fig. 3 for a 1D cluster. In one dimension the decomposition of a cluster into sub-clusters, as displayed in Fig. 3, is clear. However, the interesting cases for $\mathrm{QC}_\mathcal{C}$-computations are clusters in 2D and 3D; and there we must state more precisely what "decomposition of a cluster into sub-clusters" means. The use of basic notions from graph theory will prove helpful for this purpose.

To decompose a cluster into sub-clusters means in

more precise terms to decompose the associated graph $G(\mathcal{C}_N, E_{\mathcal{C}_N})$ into subgraphs. That is, we have to decompose both the vertices and the edges of the graph. Each vertex $a \in \mathcal{C}_N$ has to belong to a subset $\mathcal{C}(g_i)$, where

$$\mathcal{C}_N = \bigcup_{i=1}^{|\mathcal{N}|} \mathcal{C}(g_i), \tag{48}$$

and the sets $\mathcal{C}(g_i)$ of vertices corresponding to the gates g_i may overlap on their input- and output vertices.

Correspondingly, the set $E_{\mathcal{C}_N}$ of edges, defined in the same way as $E_{\mathcal{C}}$ in (22), is decomposed into subsets

$$E_{\mathcal{C}_N} = \bigcup_{i=1}^{|\mathcal{N}|} E(g_i), \tag{49}$$

but the subsets $E(g_i)$ of edges are not allowed to overlap,

$$\forall i, j = 1\,..\,|\mathcal{N}|, i \neq j: \; E(g_i) \cap E(g_j) = \emptyset. \tag{50}$$

The rules for the decomposition of edges (49) and (50) are, as we shall see, central for the universality proof.

Further, for the decomposition to be useful, the subsets $\mathcal{C}(g_i)$ and $E(g_i)$ must fulfill a number of constraints. The first of these is that each pair $(\mathcal{C}(g_i), E(g_i))$ is again a graph, $G(\mathcal{C}(g_i), E(g_i))$. This requires, in particular, that the endpoints of all the edges in $E(g_i)$ are in $\mathcal{C}(g_i)$,

$$\forall i = 1, .., |\mathcal{N}| : E(g_i) \subset \mathcal{C}(g_i) \times \mathcal{C}(g_i). \tag{51}$$

For details on the graph decomposition, in particular for conditions on the subgraphs imposed to guarantee (49) and (50) see Appendix A.

Now consider the concatenation $g_2 \circ g_1$ of the two gates g_1, realized on a cluster $\mathcal{C}(g_1)$, and g_2, realized on a cluster $\mathcal{C}(g_2)$, each of them by a procedure according to scheme II. The composite circuit $g = g_2 \circ g_1$ is realized on the cluster

$$\mathcal{C}(g) = \mathcal{C}(g_1) \cup \mathcal{C}(g_2), \tag{52}$$

with

$$\begin{aligned} \mathcal{C}_I(g) &= \mathcal{C}_I(g_1) \cup (\mathcal{C}_I(g_2) \backslash \mathcal{C}_O(g_1)) \\ \mathcal{C}_O(g) &= \mathcal{C}_O(g_2) \cup (\mathcal{C}_O(g_1) \backslash \mathcal{C}_I(g_2)). \end{aligned} \tag{53}$$

Now, the procedure to perform the two gates g_1, g_2 sequentially is

1. Prepare the state $|\Psi_{\text{in}}\rangle_{\mathcal{C}(g)} = |\psi_{\text{in}}\rangle_{\mathcal{C}_I(g)} \otimes |+\rangle_{\mathcal{C}(g)\backslash\mathcal{C}_I(g)}$.

2. Entangle the qubits on the sub-cluster $\mathcal{C}(g_1)$ via

$$S_1 := S^{(\mathcal{C}(g_1))} = \prod_{a,b \in \mathcal{C}(g_1) \,|\, b-a \in \gamma_d} S^{ab}. \tag{54}$$

3. Measure the qubits in $\mathcal{C}_I(g_1) \cup \mathcal{C}_M(g_1)$, resulting in the projector $P_{\mathcal{C}_I(g_1)\cup\mathcal{C}_M(g_1)} =: P_1$,

$$P_1 = \bigotimes_{k \in \mathcal{C}_I(g_1)\cup\mathcal{C}_M(g_1)} \frac{1 + (-1)^{s_k} \vec{r}_k \cdot \vec{\sigma}^{(k)}}{2}. \tag{55}$$

Therein s_k is the outcome of the measurement of qubit k and $\vec{r}_k$ the respective measurement direction.

4. Entangle the qubits on the sub-cluster $\mathcal{C}(g_2)$ via

$$S_2 := S^{(\mathcal{C}(g_2))} = \prod_{a,b \in \mathcal{C}(g_2) \,|\, b-a \in \gamma_d} S^{ab}. \tag{56}$$

5. Measure the qubits in $\mathcal{C}_I(g_2) \cup \mathcal{C}_M(g_2)$, resulting in the projector $P_{\mathcal{C}_I(g_2)\cup\mathcal{C}_M(g_2)} =: P_2$,

$$P_2 = \bigotimes_{k \in \mathcal{C}_I(g_2)\cup\mathcal{C}_M(g_2)} \frac{1 + (-1)^{s_k} \vec{r}_k \cdot \vec{\sigma}^{(k)}}{2}. \tag{57}$$

The procedure results in an output state

$$|\Psi_{\text{out}}\rangle_{\mathcal{C}(g)} = P_2\, S_2\, P_1\, S_1 |\Psi_{\text{in}}\rangle_{\mathcal{C}(g)} \tag{58}$$

that has the form

$$|\Psi_{\text{out}}\rangle_{\mathcal{C}(g)} = \left(\bigotimes_{\mathcal{C}_I(g)\cup\mathcal{C}_M(g)} |s_k\rangle_{k,\vec{r}_k} \right) \otimes |\psi_{\text{out}}\rangle_{\mathcal{C}_O(g)}, \tag{59}$$

with

$$|\psi_{\text{out}}\rangle = U_{\Sigma,g_2}\, U_{g_2} U_{\Sigma,g_1}\, U_{g_1} |\psi_{\text{in}}\rangle, \tag{60}$$

according to (46).

As will be shown next, the above procedure is equivalent to a procedure of Scheme II applied to the cluster $\mathcal{C}(g) = \mathcal{C}(g_1) \cup \mathcal{C}(g_2)$, i.e. when, first, all qubits in $\mathcal{C}(g)$ are entangled and, second, all but the output qubits of $\mathcal{C}_O(g)$ are measured.

The procedure according to Scheme II yields the state

$$|\Psi'_{\text{out}}\rangle_{\mathcal{C}(g)} = P^{(\mathcal{C}_I(g)\cup\mathcal{C}_M(g))}\, S^{(\mathcal{C}(g))}\, |\Psi_{\text{in}}\rangle_{\mathcal{C}(g)}, \tag{61}$$

and we now have to show that the output states $|\Psi_{\text{out}}\rangle_{\mathcal{C}(g)}$ in (58) and $|\Psi'_{\text{out}}\rangle_{\mathcal{C}(g)}$ in (61) are the same for all input states $|\Psi_{\text{in}}\rangle_{\mathcal{C}(g)}$.

First note that the operations P_1 and S_2 commute since they act on different particles. P_1 acts on the qubits in $\mathcal{C}_I(g_1) \cup \mathcal{C}_M(g_1)$ while S_2 acts on $\mathcal{C}(g_2)$. The sub-clusters associated with the gates may overlap only via their input- and output qubits. This is intuitively clear, and also follows from the decomposition constraint (A5). As the gate g_1 is applied before g_2, of $\mathcal{C}(g_1)$ only the qubits in $\mathcal{C}_O(g_1)$ may overlap with the qubits in $\mathcal{C}_I(g_2)$. Thus, $(\mathcal{C}_I(g_1) \cup \mathcal{C}_M(g_1)) \cap \mathcal{C}(g_2) = \emptyset$. Therefore

$$P_2\, S_2\, P_1\, S_1 = P_2\, P_1\, S_2\, S_1. \tag{62}$$

Now note that as a direct consequence of (53) the union of the input- and body section of the composite gate g on the cluster $\mathcal{C}(g)$ are made up by the union of the input- and body sections of the two individual gates g_1 and g_2, i.e.

$$\mathcal{C}_I(g_1)\cup\mathcal{C}_M(g_1)\cup\mathcal{C}_I(g_2)\cup\mathcal{C}_M(g_2)=\mathcal{C}_I(g)\cup\mathcal{C}_M(g). \quad (63)$$

Further, from the decomposition constraint (A5) and from the fact that g_1 is applied before g_2 it follows that the input- and body sections of gates g_1 and g_2 do not intersect,

$$(\mathcal{C}_I(g_1)\cup\mathcal{C}_M(g_1))\cap(\mathcal{C}_I(g_2)\cup\mathcal{C}_M(g_2))=\emptyset. \quad (64)$$

Therefore,

$$\begin{aligned} P_2\,P_1 &= \bigotimes_{\mathcal{C}_I(g_2)\cup\mathcal{C}_M(g_2)} \frac{1+(-1)^{s_k}\vec{r}_k\cdot\vec{\sigma}^{(k)}}{2} \\ &\quad \bigotimes_{\mathcal{C}_I(g_1)\cup\mathcal{C}_M(g_1)} \frac{1+(-1)^{s_k}\vec{r}_k\cdot\vec{\sigma}^{(k)}}{2} \\ &= \bigotimes_{\mathcal{C}_I(g)\cup\mathcal{C}_M(g)} \frac{1+(-1)^{s_k}\vec{r}_k\cdot\vec{\sigma}^{(k)}}{2} \\ &= P^{(\mathcal{C}_I(g)\cup\mathcal{C}_M(g))}, \end{aligned} \quad (65)$$

where the second line holds by (63) and (64). We find that measurement patterns corresponding to the projections P_1 and P_2 can be patched together to form the measurement pattern on the cluster $\mathcal{C}(g)$.

The same holds for the entangling operations. The entangling operation S_1 on $\mathcal{C}(g_1)$ and S_2 on $\mathcal{C}(g_2)$ combined give the entangling operation $S^{(\mathcal{C}(g))}$ on $\mathcal{C}(g)$,

$$S_2\,S_1=S^{(\mathcal{C}(g))}, \quad (66)$$

because of the central rule (50).

Inserting (65) and (66) into (62) yields

$$P_2\,S_2\,P_1\,S_1=P^{(\mathcal{C}_I(g)\cup\mathcal{C}_M(g))}\,S^{(\mathcal{C}(g))}, \quad (67)$$

and therefore, if we compare (58) and (61) we find that $|\Psi_{\rm out}\rangle_{\mathcal{C}(g)}$, the output state of the sequential realization of the two gates g_1 and g_2, and $|\Psi'_{\rm out}\rangle_{\mathcal{C}(g)}$, the output state of the standard procedure applied to the composite circuit, are indeed the same for all inputs $|\Psi_{\rm in}\rangle_{\mathcal{C}(g)}$. Thus both realizations, the sequential and the non-sequential, are equivalent.

This composition can be iterated so that the entire circuit can be realized via the standard procedure of Scheme 1. The measurement pattern of the circuit is thereby obtained by patching together the measurement patterns of the gates the circuit is composed of.

From (60) it follows that the quantum input $|\psi_{\rm in}\rangle$ and the quantum output $|\psi_{\rm out}\rangle$ of the unitary evolution are related via

$$|\psi_{\rm out}\rangle=\left(\prod_{i=1}^{|\mathcal{N}|}U_{\Sigma,g_i}\,U_{g_i}\right)|\psi_{\rm in}\rangle. \quad (68)$$

The random but known byproduct operators U_{Σ,g_i} that appear in (68) are dealt with in Section III F. The gates $g_i\in\mathcal{N}$ are labeled corresponding to the order of their action.

Now, we want to specify to the case where the quantum input is *known* and where the quantum output is measured. This is the situation which interests us most in this paper. Examples of such a situation are Shor's factoring algorithm and Grover's search algorithm. In both cases, the quantum input is $|\psi_{\rm in}\rangle=\bigotimes_{i=1}^{n}|+\rangle_i$.

Let us denote the input section of the whole cluster $\mathcal{C}$, comprising the input qubits of the network simulation, as I; and the output section, comprising the qubits of the readout quantum register, as O. As long as the quantum input is known it is sufficient to consider the state $|+\rangle_I=\bigotimes_{i\in I}|+\rangle_i$. For different but known input states $|\psi_{\rm in}\rangle_I$ one can always find a transformation $U_{\rm in}$ such that $|\psi_{\rm in}\rangle_I=U_{\rm in}|+\rangle_I$ and instead of realizing some unitary transformation U on $|\psi_{\rm in}\rangle_I$ one realizes $U\,U_{\rm in}$ on $|+\rangle_I$.

Preparing an input state $|+\rangle_I$ and entangling it via $S^{(\mathcal{C})}$ is the same as creating a cluster state $|\phi\rangle_{\mathcal{C}}$, $S^{(\mathcal{C})}|+\rangle_I\otimes|+\rangle_{\mathcal{C}\setminus I}=S^{(\mathcal{C})}|+\rangle_{\mathcal{C}}=|\phi\rangle_{\mathcal{C}}$. This holds because the state $S^{(\mathcal{C})}|+\rangle_{\mathcal{C}}$ obeys the eigenvalue equations (11) and, as we have stated earlier, these eigenvalue equations determine the state completely. Thus the created state is a cluster state $|\phi\rangle_{\mathcal{C}}$ that could as well have been prepared by any other means.

Once the quantum output is read then all cluster qubits have been measured. Therefore, the entire procedure of realizing a quantum computation on the $\mathrm{QC}_{\mathcal{C}}$ amounts to

Scheme 2 Performing a computation on the $\mathrm{QC}_{\mathcal{C}}$.

1. Prepare a cluster state $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ of sufficient size.

2. Perform a sequence of measurements on $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}}$ and obtain the result of the computation from all the measurement outcomes.

The link between the network model and the $\mathrm{QC}_{\mathcal{C}}$ is established by Scheme 1. The elementary constituents of the quantum logic network are mapped onto the corresponding basic blocks of the $\mathrm{QC}_{\mathcal{C}}$. In this way, Scheme 1 helps to understand why the $\mathrm{QC}_{\mathcal{C}}$ works.

However, a $\mathrm{QC}_{\mathcal{C}}$-computation is more appropriately described by Scheme 2 than by Scheme 1. Scheme 2 does not use the notion of quantum gates, but only of a spatial and temporal measurement pattern. Once universality of the $\mathrm{QC}_{\mathcal{C}}$ is established, to demonstrate the functioning of specific $\mathrm{QC}_{\mathcal{C}}$-algorithms one would prefer decomposing a measurement pattern directly into subpatterns rather than decomposing a network simulation into simulations of gates. A tool for the direct approach is provided by Theorem 1 in Section III E.

E. Randomness of the measurement results

We will now show that the described scheme of quantum computation with the $\mathrm{QC}_{\mathcal{C}}$ works with unit efficiency despite the randomness of the individual measurement results.

First note that a byproduct operator U_Σ that acts after the final unitary gate $U_{g_{|\mathcal{N}'|}}$ does not jeopardize the scheme. Its only effect is that the results of the readout measurements have to be reinterpreted. The byproduct operator U_Σ that acts upon the logical output qubits $1\,..\,n$ has the form

$$U_\Sigma = \prod_{i=1}^{n} \left(\sigma_x^{[i]}\right)^{x_i} \left(\sigma_z^{[i]}\right)^{z_i}, \tag{69}$$

where $x_i, z_i \in \{0,1\}$ for $1 \leq i \leq n$. Let the qubits on the cluster which are left unmeasured be labeled in the same way as the readout qubits of the quantum logic network.

The qubits on the cluster which take the role of the readout qubits are, at this point, in a state $U_\Sigma|\mathrm{out}\rangle$, where $|\mathrm{out}\rangle$ is the output state of the corresponding quantum logic network. The computation is completed by measuring each qubit in the σ_z-eigenbasis, thereby obtaining the measurement results $\{s_i'\}$, say. In the $\mathrm{QC}_{\mathcal{C}}$-scheme, one measures the state $U_\Sigma|\mathrm{out}\rangle$ directly, whereby outcomes $\{s_i\}$ are obtained and the readout qubits are projected into the state $|\mathcal{M}\rangle = \prod_{i=1}^{n} \frac{1+(-1)^{s_i}\sigma_z^{(i)}}{2}\, U_\Sigma|\mathrm{out}\rangle$. Depending on the byproduct operator U_Σ, the set of measurement results $\{s\}$ in general has a different interpretation from what the network readout $\{s_i'\}$ would have. The measurement basis is the same. From (69) one obtains

$$\begin{aligned} |\mathcal{M}\rangle &= \prod_{i=1}^{n} \frac{1+(-1)^{s_i}\sigma_z^{(i)}}{2}\, U_\Sigma|\mathrm{out}\rangle \\ &= U_\Sigma \left(U_\Sigma^\dagger \prod_{i=1}^{n} \frac{1+(-1)^{s_i}\sigma_z^{(i)}}{2} U_\Sigma \right) |\mathrm{out}\rangle \\ &= U_\Sigma \prod_{i=1}^{n} \frac{1+(-1)^{s_i+x_i}\sigma_z^{(i)}}{2} |\mathrm{out}\rangle \end{aligned} \tag{70}$$

From (70) we see that a σ_z-measurement on the state $U_\Sigma\,|\mathrm{out}\rangle$ with results $\{s\}$ represents the same algorithmic output as a σ_z-measurement of the state $|\mathrm{out}\rangle$ with the results $\{s_i'\}$, where the sets $\{s\}$ and $\{s_i'\}$ are related by

$$s_i' \equiv s_i + x_i \bmod 2. \tag{71}$$

The set $\{s_i'\}$ represents the result of the computation. It can be calculated from the results $\{s_i\}$ of the σ_z-measurements on the "readout" cluster qubits, and the values $\{x_i\}$ which are determined by the byproduct operator U_Σ.

Thus we find that one can cope with the randomness of the measurement results provided the byproduct operators U_{Σ,g_i} in (68) can be propagated forward through the subsequent gates such that they act on the cluster qubits representing the output register. This can be done. To propagate the byproduct operators we use the propagation relations

$$\begin{aligned} \mathrm{CNOT}(c,t)\sigma_x^{(t)} &= \sigma_x^{(t)}\mathrm{CNOT}(c,t) \\ \mathrm{CNOT}(c,t)\sigma_x^{(c)} &= \sigma_x^{(c)}\sigma_x^{(t)}\mathrm{CNOT}(c,t) \\ \mathrm{CNOT}(c,t)\sigma_z^{(t)} &= \sigma_z^{(c)}\sigma_z^{(t)}\mathrm{CNOT}(c,t) \\ \mathrm{CNOT}(c,t)\sigma_z^{(c)} &= \sigma_z^{(c)}\mathrm{CNOT}(c,t) \end{aligned} \tag{72}$$

for the CNOT gate,

$$\begin{aligned} U_{Rot}[\xi,\eta,\zeta]\sigma_x &= \sigma_x U_{Rot}[\xi,-\eta,\zeta] \\ U_{Rot}[\xi,\eta,\zeta]\sigma_z &= \sigma_z U_{Rot}[-\xi,\eta,-\zeta] \end{aligned} \tag{73}$$

for general rotations $U_{Rot}[\xi,\eta,\zeta]$ as defined in (25), and

$$\begin{aligned} H\sigma_x &= \sigma_z H \\ H\sigma_z &= \sigma_x H \\ U_z[\pi/2]\sigma_x &= \sigma_y U_z[\pi/2] \\ U_z[\pi/2]\sigma_z &= \sigma_z U_z[\pi/2] \end{aligned} \tag{74}$$

for the Hadamard- and $\pi/2$-phase gate. The propagation relations (73) apply to general rotations realized via Procedure 2 –including Hadamard- and $\pi/2$-phase gates– while the propagation relations (74) apply to Hadamard- and $\pi/2$-phase gates as realized via Procedure 3.

Note that the propagation relations (72) - (74) are such that Pauli operators are mapped onto Pauli operators under propagation and thus the byproduct operators remain in the Pauli group when being propagated. Further note that there is a difference between the relations for propagation through gates which are in the Clifford group and through those which are not. For CNOT-, Hadamard- and $\pi/2$-phase gates the byproduct operator changes under propagation while the gate remains unchanged. This holds for all gates in the Clifford group, because the propagation relations for Clifford gates are of the form $U_g U_\Sigma = (U_g U_\Sigma U_g^{-1}) U_g$ as (72) and (74), i.e. the byproduct operator U_Σ is conjugated under the gate, and the Clifford group by its definition as the normalizer of the Pauli group maps Pauli operators onto Pauli operators under conjugation. For gates which are not in the Clifford group this would in general not work and therefore, for rotations which are not in the Clifford group, the propagation relations are different. There, the gate is conjugated under the byproduct operator; and thus the byproduct operator remains unchanged in propagation while the gate is modified. In both cases, the forward propagation leaves the byproduct operators in the Pauli group. In particular, their tensor product structure is maintained.

Let us now discuss how byproduct operator propagation affects the scheme of computation with the $\mathrm{QC}_{\mathcal{C}}$. In Section III D we arrived at the conclusion (68) that by patching the measurement patterns of individual gates together and keeping the measurement bases fixed, we can realize a composite unitary evolution on some input

state $|\psi_{\rm in}\rangle$,

$$|\psi_{\rm out}\rangle \;=\; \left(\prod_{i=1}^{|\mathcal{N}|} U_{\Sigma,g_i}\, U_{g_i}\right) |\psi_{\rm in}\rangle,$$

where U_{g_i} is the i-th unitary gate in the circuit and U_{Σ,g_i} the byproduct operator resulting from the realization of that gate. Now using the above propagation relations, (68) can be rewritten in the following way

$$|\psi_{\rm out}\rangle = \left(\prod_{i=1}^{|\mathcal{N}|} U_{\Sigma,g_i}|_{\Omega}\right) \left(\prod_{i=1}^{|\mathcal{N}|} U'_{g_i}\right) |\psi_{\rm in}\rangle. \qquad (75)$$

Therein, $U_{\Sigma,g_i}|_{\Omega}$ are forward propagated byproduct operators resulting from the byproduct operators U_{Σ,g_i} of the gates g_i. They accumulate to the total byproduct operator U_Σ whose effect on the result of the computation is contained in (71),

$$U_\Sigma = \prod_{i=1}^{|\mathcal{N}|} U_{\Sigma,g_i}|_{\Omega}\,. \qquad (76)$$

Further, the U'_{g_i} are the gates modified under the propagation of the byproduct operators. As discussed above, for gates in the Clifford group we have

$$U'_g = U_g,\ \forall\ g \in \text{Clifford group}, \qquad (77)$$

as can be seen from (72) and (74).

Gates which are not in the Clifford group are modified by byproduct operator propagation. Specifically, the general rotations (25) are conjugated as can be seen from (73). From the structure of (68) we see that only the byproduct operators of gates g_k earlier than g_i in the network may have an effect on U_{g_i}, i.e. those with $k < i$. To give an explicit expression, let us define $U_{\Sigma,g_k}|_{\mathcal{O}_i}$, which are byproduct operators U_{Σ,g_k} propagated forward by the propagation relations (72) - (74) to the vertical cut $\mathcal{O}_i$ through the network, see Fig. 4. A vertical cut through a network is a cut which intersects each qubit line exactly once and does not intersect gates. The vertical cut $\mathcal{O}_i$ has the additional property that it intersects the network just before the input of gate g_i. The relation between a rotation U'_{g_i} modified by the byproduct operators and the non-modified rotation U_{g_i} is

$$U'_{g_i} \;=\; \left(\prod_{k|k<i} U_{\Sigma,g_k}|_{\mathcal{O}_i}\right) U_{g_i} \left(\prod_{k|k<i} U_{\Sigma,g_k}|_{\mathcal{O}_i}\right)^{\dagger}, \qquad (78)$$

$$\forall\ U_{g_i} \in SU(2).$$

Now that we have investigated the effect of byproduct operator propagation on the individual gates let us return to equation (75). There, we find that the operations which act on the input state $|\psi_{\rm in}\rangle$ group into two

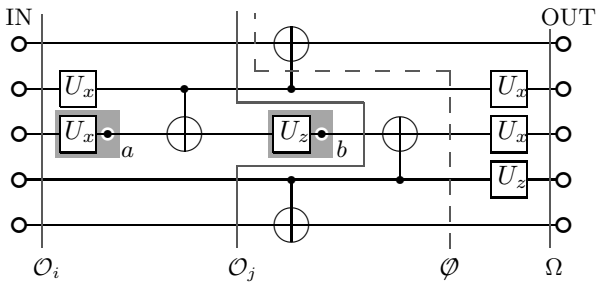


FIG. 4: Vertical cuts. The vertical cuts intersect each qubit line exactly once but do not intersect gates. Thus, $\mathcal{O}_i$, $\mathcal{O}_j$ and Ω are vertical cuts, but $\not\mathcal{O}$ is not. The cut $\mathcal{O}_i$ intersects the rotation U_x just before its input. For two of the rotations in the displayed network, the sub-clusters on which these gates are realized are symbolically displayed in gray underlay. Via the measurement of the cluster qubits a and b (displayed as black dots with white border), the rotation angles of the respective rotations U_x and U_z are set.

factors. The first is composed of the modified gate operations U'_{g_i} and the second of the forward propagated byproduct operators. The second factor gives the accumulated byproduct operator U_Σ and is absorbed into the result of the computation via (71). It does not cause any complication.

So what remains is the first factor, and we find that the unitary evolution of the input state $|\psi_{\rm in}\rangle$ that is realized is composed of the modified gates U'_{g_i}. The gates we will realize are thus the U'_{g_i}, not U_{g_i}. However, the standard procedures 1 - 3 in Section II B are for the operations U_{g_i}. Thus we have to read (78) in reverse. We need to deduce U_{g_i} from U'_{g_i}. Once the gates g_k for all $k < i$ have been realized, this can be done for each gate g_i since the byproduct operators $U_{\Sigma,k}$ are then known for all $k < i$. Finally, with U_{g_i} determined from U'_{g_i}, Procedure 2 gives the measurement bases required for the realization of the gate g_i. Please note that it is a sufficient criterion for the realization of the gate g_i that all gates g_k with $k < i$ must have been realized before, but not a necessary one.

Let us, at this point, address the question of temporal ordering more explicitly. For proper discussion of the temporal ordering we have to step out of the network frame for a moment. First note that in case of the $\mathrm{QC}_\mathcal{C}$ the basic primitive are measurements. Thus, the temporal complexity will be determined by the temporal ordering of these measurements, unlike in quantum logic networks, where it depends on the ordering of gates. The most efficient ordering of measurements that simulates a quantum logic network is not pre-described by the temporal ordering of the gates in this network.

A temporal ordering among the measurements is inferred from the requirement to keep the computation on the $\mathrm{QC}_\mathcal{C}$ deterministic in spite of of the randomness introduced by the measurements. This randomness is accounted for by the byproduct operators. The key to obtain the temporal ordering of measurements is eq. (78).

There, the byproduct operators $U_{\Sigma,g_k}|_{\mathcal{O}_i}$ may modify Euler angles of the one-qubit rotations in the network and consequently change measurement bases. The temporal ordering thus arises due to the fact that bases for one-qubit measurements must be chosen in accordance with outcomes obtained from the measurements of other qubits.

For each cluster qubit q that needs to be measured in a non-trivial basis, i.e. not in the eigenbasis of σ_x, σ_y or σ_z, a set of cluster qubits p_i can be identified, whose measurement outcomes influence the choice of the measurement basis for qubit q. We say that q is in the forward cone [7] of p_i, $q \in \mathrm{fc}(p_i)$. Each cluster qubit has a forward cone, and in no forward cone there appears a qubit which is measured in a trivial basis.

The rule is that a cluster qubit q can only be measured once all cluster qubits p_i for which $q \in \mathrm{fc}(p_i)$ have been measured earlier. The forward cones thereby generate an anti-reflexive partial ordering among the measurements from which the most efficient measurement strategy can be inferred, see [7]. Gates in the Clifford group do not contribute to the temporal complexity of a $\mathrm{QC}_{\mathcal{C}}$-algorithm, see Section III.

F. Using quantum correlations for quantum computation

In this section we give a criterion which allows do demonstrate the functioning of the $\mathrm{QC}_{\mathcal{C}}$-simulations of unitary gates in a compact way.

Before we state the theorem, let us make the notion of a measurement pattern more precise. In a $\mathrm{QC}_{\mathcal{C}}$-computation one can only choose the measurement bases, while the measurement outcomes are random. This is sufficient for deterministic computation. Thus one can perform measurements specified by a spatial and temporal pattern of measurement bases but one cannot control into which of the two eigenstates the qubits are projected.

Definition 1 *A measurement pattern $\mathcal{M}^{(\mathcal{C})}$ on a cluster $\mathcal{C}$ is a set of vectors*

$$\mathcal{M}^{(\mathcal{C})} = \left\{ \vec{r}_a \in S^2 \mid a \in \mathcal{C} \right\}, \tag{79}$$

defining the measurement bases of the one-qubit measurements on $\mathcal{C}$.

If this pattern $\mathcal{M}^{(\mathcal{C})}$ of measurements is applied on an initial state $|\Psi_{\mathcal{E}}\rangle_{\mathcal{C}}$ and thereby the set of measurement outcomes

$$\{s\}_{\mathcal{C}} = \{ s_a \in \{0,1\} \mid a \in \mathcal{C} \} \tag{80}$$

is obtained, then the resulting state $|\Psi_{\mathcal{M}}\rangle_{\mathcal{C}}$ is, modulo norm factor, given by $|\Psi_{\mathcal{M}}\rangle_{\mathcal{C}} = P^{(\mathcal{C})}_{\{s\}}(\mathcal{M})\,|\Psi_{\mathcal{E}}\rangle_{\mathcal{C}}$, where

$$P^{(\mathcal{C})}_{\{s\}}(\mathcal{M}) = \bigotimes_{k\in\mathcal{C}} \frac{1+(-1)^{s_k}\vec{r}_k\cdot\vec{\sigma}^{(k)}}{2}. \tag{81}$$

Besides, let us introduce some conventions for labeling. Be $\mathcal{C}_I(g)$ and $\mathcal{C}_O(g)$ such that $|\mathcal{C}_I(g)| = |\mathcal{C}_O(g)| = n$ where n is the number of logical qubits processed by g. Operators acting on qubits $p \in \mathcal{C}_I(g)$ and $q \in \mathcal{C}_O(g)$ are labeled by upper indices $(\mathcal{C}_I(g), i)$ and $(\mathcal{C}_O(g), i')$, $1 \le i, i' \le n$, respectively. The qubits $p \in \mathcal{C}_I(g)$ and $q \in \mathcal{C}_O(g)$ are ordered from 1 to n in the same way as the logical qubits that they represent.

We make a distinction between the gate g and the unitary transformation U it realizes. The gate $g \in \mathcal{N}$ does, besides specifying the unitary transformation U, also comprise the information about the location of the gate within the network.

After these definitions and conventions we can now state the following theorem

Theorem 1 *Be $\mathcal{C}(g) = \mathcal{C}_I(g) \cup \mathcal{C}_M(g) \cup \mathcal{C}_O(g)$ with $\mathcal{C}_I(g) \cap \mathcal{C}_M(g) = \mathcal{C}_I(g) \cap \mathcal{C}_O(g) = \mathcal{C}_M(g) \cap \mathcal{C}_O(g) = \emptyset$ a cluster for the simulation of a gate g, realizing the unitary transformation U, and $|\phi\rangle_{\mathcal{C}(g)}$ the cluster state on the cluster $\mathcal{C}(g)$.*

Suppose, the state $|\psi\rangle_{\mathcal{C}(g)} = P^{(\mathcal{C}_M(g))}_{\{s\}}(\mathcal{M})\,|\phi\rangle_{\mathcal{C}(g)}$ obeys the $2n$ eigenvalue equations

$$\begin{aligned} \sigma_x^{(\mathcal{C}_I(g),i)} \left(U\sigma_x^{(i)}U^\dagger\right)^{(\mathcal{C}_O(g))} |\psi\rangle_{\mathcal{C}(g)} &= (-1)^{\lambda_{x,i}} |\psi\rangle_{\mathcal{C}(g)} \\ \sigma_z^{(\mathcal{C}_I(g),i)} \left(U\sigma_z^{(i)}U^\dagger\right)^{(\mathcal{C}_O(g))} |\psi\rangle_{\mathcal{C}(g)} &= (-1)^{\lambda_{z,i}} |\psi\rangle_{\mathcal{C}(g)}, \end{aligned} \tag{82}$$

with $\lambda_{x,i}, \lambda_{z,i} \in \{0,1\}$ and $1 \le i \le n$.

Then, on the cluster $\mathcal{C}(g)$ the gate g acting on an arbitrary quantum input state $|\psi_{\mathrm{in}}\rangle$ can be realized according to Scheme 7 with the measurement directions in $\mathcal{C}_M(g)$ described by $\mathcal{M}^{(\mathcal{C}_M(g))}$ and the measurements of the qubits in $\mathcal{C}_I(g)$ being σ_x-measurements. Thereby, the input- and output state in the simulation of g are related via

$$|\psi_{\mathrm{out}}\rangle = U U_\Sigma\, |\psi_{\mathrm{in}}\rangle, \tag{83}$$

where U_Σ is a byproduct operator given by

$$U_\Sigma = \bigotimes_{(\mathcal{C}_I(g)\ni i)=1}^{n} (\sigma_z^{[i]})^{s_i+\lambda_{x,i}} (\sigma_x^{[i]})^{\lambda_{z,i}}. \tag{84}$$

The significance of the above theorem is that it provides a comparatively simple criterion for the functioning of gate simulations on the $\mathrm{QC}_{\mathcal{C}}$.

In Scheme 1, after read-in of the input state and the entangling operation $S^{(\mathcal{C}(g))}$, i.e. before the measurements that realize the gate are performed, the resulting state carries the quantum input in an encoded form. This state is in general not a cluster state. It is therefore not clear a priori that cluster state correlations alone are sufficient to explain the functioning of the gate. However, this is what Theorem 1 states. To prove the functioning of a gate g realized via Scheme 1 it is sufficient to demonstrate that a cluster state on $\mathcal{C}(g)$ exhibits certain quantum correlations. About the variable input one does not need to worry.

This is convenient in two ways. First, we can base the explanation of the gates directly on the eigenvalue equations (11) which were also used to define the cluster states in a compact way. The quantum correlations required to explain the functioning of the gates are derived from the basic correlations (2) rather easily and thus the use of Theorem 1 makes the explanation of the gates compact.

Second, Theorem 1 is a tool to demonstrate the functioning of $\mathrm{QC}_{\mathcal{C}}$-circuits without having to repeat the whole universality proof for each particular circuit under consideration. Scheme 2 describes the computation as a series of one-qubit measurements on a cluster state. An accordance with this, instead of decomposing a circuit simulation into gate simulations as done in Scheme 1, a measurement pattern is decomposed into sub-patterns. The effect of these measurement sub-patterns is tested via the criterion (82) in Theorem 1.

Before we turn to the proof of Theorem 1 let us note that the measurements described by $P_{\{s\}}^{(\mathcal{C}_M(g))}(\mathcal{M}(g))$, as they have full rank, project the initial cluster state $|\phi\rangle_{\mathcal{C}(g)}$ into a tensor product state, $|\psi\rangle_{\mathcal{C}(g)} = |m\rangle_{\mathcal{C}_M(g)} \otimes |\psi\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)}$. Thereof only the second factor, $|\psi\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)}$, is of interest. This state alone satisfies the eigenvalue equations (82), and is uniquely determined by these equations. To see this, consider the state $|\psi'\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)} = U^\dagger|\psi\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)}$. It satisfies the $2n$ eigenvalue equations

$$\begin{aligned} \sigma_x^{(i,\mathcal{C}_I(g))}\sigma_x^{(i,\mathcal{C}_O(g))}|\psi'\rangle &= (-1)^{\lambda_{x,i}}|\psi'\rangle, \\ \sigma_z^{(i,\mathcal{C}_I(g))}\sigma_z^{(i,\mathcal{C}_O(g))}|\psi'\rangle &= (-1)^{\lambda_{z,i}}|\psi'\rangle, \end{aligned} \tag{85}$$

where we have written in short $|\psi'\rangle$ for $|\psi'\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)}$. The state $|\psi'\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)}$ is uniquely defined by the above set of commuting observables, it is a product of Bell states. Therefore, $|\psi\rangle_{\mathcal{C}_I(g)\cup\mathcal{C}_O(g)}$ is uniquely defined as well.

Proof of Theorem 1. We will discuss the functioning of the gates for two cases of inputs. First, for all input states in the computational basis. This leaves relative phases open which have to be determined. To fix them, we discuss second the input state with all qubits individually in $|+\rangle$. As we will see, from these two cases it can be concluded that the gate simulation works for all input states of the computational basis. This is sufficient because of the linearity of the applied operations; if the gate simulations work for states of the computational basis then they work for superpositions of such inputs as well.

Case 1: The input $|\psi_{\mathrm{in}}\rangle$ is one of the states of the computational basis, i.e. $|\psi_{\mathrm{in}}\rangle = |\mathbf{z}\rangle := \bigotimes_{i=1}^n |z_i\rangle_{z,i}$ with $z_i \in \{0,1\}$, $i = 1..n$. Then the state $|\Psi_{\mathrm{out}}(\mathbf{z})\rangle_{\mathcal{C}(g)}$ of the qubits in $\mathcal{C}$ [after performing a procedure according to Scheme 1, using a measurement pattern $\mathcal{M}^{(\mathcal{C}_M(g))}$ on the body $\mathcal{C}_M(g)$ of the gate g, and applying σ_x-measurements on $\mathcal{C}_I(g)$] is

$$\begin{aligned} &n_O(\mathbf{z})\,|\Psi_{\mathrm{out}}(\mathbf{z})\rangle_{\mathcal{C}(g)} = \\ &P_{\{s\}}^{(\mathcal{C}_I(g))}(X)P_{\{s\}}^{(\mathcal{C}_M(g))}(\mathcal{M})S^{(\mathcal{C}(g))}\,|\mathbf{z}\rangle_{\mathcal{C}_I(g)}\otimes|+\rangle_{\mathcal{C}_M(g)\cup\mathcal{C}_O(g)}, \end{aligned} \tag{86}$$

with norm factors $n_O(\mathbf{z})$ that are nonzero for all $\mathbf{z}$, as we shall show later.

The input $|\mathbf{z}\rangle$ in (86) satisfies the equation

$$n_I(\mathbf{z})\,|\mathbf{z}\rangle = P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}\bigotimes_{i=1}^n|+\rangle_i, \tag{87}$$

with $P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))} = \bigotimes_{i=1}^n \frac{1+(-1)^{z_i}\sigma_z^{[i]}}{2}$, and $n_I(\mathbf{z}) = 1/2^{n/2}$ for all $\mathbf{z}$. Now note that $S^{(\mathcal{C}(g))}$ and $P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}$, as well as $P_{\{s\}}^{(\mathcal{C}_M(g))}(\mathcal{M})$ and $P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}$, commute. Thus, $|\Psi_{\mathrm{out}}(\mathbf{z})\rangle_{\mathcal{C}(g)}$ can be written as

$$\begin{aligned} &n'_O(\mathbf{z})\,|\Psi_{\mathrm{out}}(\mathbf{z})\rangle_{\mathcal{C}(g)} = \\ &\quad= P_{\{s\}}^{(\mathcal{C}_I(g))}(X)\,P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}\,P_{\{s\}}^{(\mathcal{C}_M(g))}(\mathcal{M})\,|\phi\rangle_{\mathcal{C}(g)} \\ &\quad= P_{\{s\}}^{(\mathcal{C}_I(g))}(X)\,P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}\,|\psi\rangle_{\mathcal{C}(g)}, \end{aligned} \tag{88}$$

where $|\psi\rangle_{\mathcal{C}(g)}$ is specified by the eigenvalue equations (82) in Theorem 1.

Let us, at this point, emphasize that the projections $P_{\{s\}}^{(\mathcal{C}_I(g))}(X)$ and $P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}$ in (88) are of very different origin. The projector $P_{\{s\}}^{(\mathcal{C}_I(g))}(X)$ describes the action of the σ_x-measurements on the qubits in $\mathcal{C}_I(g)$. These measurements are part of the procedure to realize some gate g on the cluster $\mathcal{C}(g)$. One has no control over the thereby obtained measurement outcomes $\{s\}$ specifying $P_{\{s\}}^{(\mathcal{C}_I(g))}(X)$. In contrast, the projector $P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}$ does not correspond to measurements that are performed in reality. Instead, it is introduced as an auxiliary construction that allows one to relate the processing of quantum inputs to quantum correlations in cluster states. The parameters $\mathbf{z}$ specifying the quantum input $|\mathbf{z}\rangle$ and thus the projector $P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}$ in (87) can be chosen freely.

The goal is to find for the state $|\Psi_{\mathrm{out}}(\mathbf{z})\rangle_{\mathcal{C}(g)}$ an expression involving the transformation U acting on the input $|\mathbf{z}\rangle$. To accomplish this, first observe that for the state on the r.h.s of (88) via (82) the following eigenvalue equations hold

$$\begin{aligned} &\left(U\sigma_z^{[i]}U^\dagger\right)^{(\mathcal{C}_O)}\left[P_{\{s\}}^{(\mathcal{C}_I(g))}(X)\,P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}\,|\psi\rangle_{\mathcal{C}(g)}\right] = \\ &\qquad(-1)^{\lambda_{z,i}+z_i}\left[P_{\{s\}}^{(\mathcal{C}_I(g))}(X)\,P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}\,|\psi\rangle_{\mathcal{C}(g)}\right], \end{aligned} \tag{89}$$

with $i = 1..n$.

To make use of the equations (89) we need to prove that $P_{\{s\}}^{(\mathcal{C}_I(g))}(X)\,P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}\,|\psi\rangle_{\mathcal{C}(g)} \neq 0$ for all $\mathbf{z}$ under the assumptions of theorem 1.

For this, we consider the scalar ${}_{\mathcal{C}(g)}\langle\psi|P_{Z,\mathbf{z}}^{(\mathcal{C}_I(g))}|\psi\rangle_{\mathcal{C}(g)}$

and write $P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}$ in the form

$$P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}} = \frac{1}{2^n}\left(1+\sum_{k=1}^{2^n}\bigotimes_{i\in I_k}(-1)^{z_i}\sigma_z^{(i)}\right)^{(\mathcal{C}_I(g))}, \quad (90)$$

where $I_k \subset \mathcal{C}_I \neq \emptyset\ \forall k = 1..2^n$. For each I_k we choose an $i \in I_k$ and insert the respective eigenvalue equation from the upper line of (82) into ${}_{\mathcal{C}(g)}\langle\psi|\bigotimes_{j\in I_k}\sigma_z^{(j)}|\psi\rangle_{\mathcal{C}(g)}$. Since $\bigotimes_{j\in I_k}\sigma_z^{(j)}$ and $\sigma_x^{(i,\mathcal{C}_I(g))}\left(U\sigma_x^{(i)}U^\dagger\right)^{(\mathcal{C}_O(g))}$ anti-commute, ${}_{\mathcal{C}(g)}\langle\psi|\bigotimes_{j\in I_k}\sigma_z^{(i)}|\psi\rangle_{\mathcal{C}(g)} = 0$ for all I_k. Thus, with (90), one finds ${}_{\mathcal{C}(g)}\langle\psi|P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}|\psi\rangle_{\mathcal{C}(g)} = 1/2^n$, such that $P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}|\psi\rangle_{\mathcal{C}(g)} \neq 0$ and therefore also

$$P^{(\mathcal{C}_I(g))}_{\{s\}}(X)\,P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}\,|\psi\rangle_{\mathcal{C}(g)} \neq 0, \quad (91)$$

or, in other words, $n'_O(\mathbf{z}) \neq 0$ for all $\mathbf{z}$.

Due to the fact that the projections $P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}$ and $P^{(\mathcal{C}_M(g))}_{\{s\}}(\mathcal{M})$ are of full rank the above state has the form

$$P^{(\mathcal{C}_I(g))}_{\{s\}}(X)\,P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}\,|\psi\rangle_{\mathcal{C}(g)} = n'_O(\mathbf{z})\,|\mathbf{s}\rangle_{x,\mathcal{C}_I(g)}\otimes|m\rangle_{\mathcal{C}_M(g)}\otimes|\psi_{\rm out}(\mathbf{z})\rangle_{\mathcal{C}_O(g)}, \quad (92)$$

where $|\mathbf{s}\rangle_{x,\mathcal{C}_I} = \bigotimes_{(\mathcal{C}_I\ni i)=1}^{n}|s_i\rangle_{x,i}$, and $|m\rangle_{\mathcal{C}_M(g)}$ is some product state with $\||m\rangle_{\mathcal{C}_M(g)}\| = 1$. Elaborating the argument that leads to (91) one finds that $n'_O(\mathbf{z}) = 1/2^n$ and $n_O(\mathbf{z}) = 1/2^{n/2}$, but at this point the precise values of the normalization factors are not important as long as they are nonzero.

In (92) only the third factor of the state on the r.h.s. is interesting, and this factor is determined by the eigenvalue equations (89):

$$|\psi_{\rm out}(\mathbf{z})\rangle = e^{i\eta(\mathbf{z})}UU_\Sigma|\mathbf{z}\rangle, \quad (93)$$

where U_Σ is given by (84). Now, because of (88) with $n'_O(\mathbf{z}) \neq 0\ \forall\,\mathbf{z}$, a solution (92) with (93) for the state $P^{(\mathcal{C}_I(g))}_{\{s\}}(X)\,P^{(\mathcal{C}_I(g))}_{Z,\mathbf{z}}\,|\psi\rangle_{\mathcal{C}(g)}$ is also a solution for the state $|\Psi_{\rm out}(\mathbf{z})\rangle_{\mathcal{C}(g)}$, and one finally obtains

$$|\Psi_{\rm out}(\mathbf{z})\rangle_{\mathcal{C}(g)} = e^{i\eta(\mathbf{z})}|\mathbf{s}\rangle_{x,\mathcal{C}_I(g)}\otimes|m\rangle_{\mathcal{C}_M(g)}\otimes[UU_\Sigma|\mathbf{z}\rangle]_{\mathcal{C}_O(g)}. \quad (94)$$

There appear no additional norm factors in (94) because the states on the l.h.s. and the r.h.s. are both normalized to unity.

The solution (94) still allows for one free parameter, the phase factor $e^{i\eta(\mathbf{z})}$. Note that, a priori, the phase factors for different $\mathbf{z}$ can all be different.

This concludes the discussion of case 1. We have found in (94) that the realized gate acts as

$$\tilde{U} = U\,U_\Sigma\,D \quad (95)$$

where the gate D is diagonal in the computational basis and contains all the phases $e^{i\eta(\mathbf{z})}$. What remains is to show that $D = \mathbf{1}$ modulo a possible global phase.

Case 2. Now the same procedure is applied for the input state $|\psi_{\rm in}\rangle = |+\rangle := \bigotimes_{i=1}^{n}|+\rangle_i$. Then, the state $|\Psi_{\rm out}(+)\rangle_{\mathcal{C}(g)}$ that results from the gate simulation is

$$n_O(+)\,|\Psi_{\rm out}(+)\rangle_{\mathcal{C}(g)} = P^{(\mathcal{C}_I(g))}_{\{s\}}(X)\,P^{(\mathcal{C}_M(g))}_{\{s\}}(\mathcal{M})\,|\phi\rangle_{\mathcal{C}(g)}, \quad (96)$$

with a nonzero norm factor $n_O(+)$. Using the upper line of eigenvalue equations (82), the state $|\Psi_{\rm out}(+)\rangle_{\mathcal{C}(g)}$ is found to obey the eigenvalue equations

$$\left(U\sigma_x^{[i]}U^\dagger\right)^{(\mathcal{C}_O(g))}|\Psi_{\rm out}(+)\rangle_{\mathcal{C}(g)} = (-1)^{\lambda_{x,i}+s_i}|\Psi_{\rm out}(+)\rangle_{\mathcal{C}(g)}. \quad (97)$$

The eigenvalue equations (97) in combination with (96) imply that

$$|\Psi_{\rm out}(+)\rangle_{\mathcal{C}(g)} = e^{i\chi}|\mathbf{s}\rangle_{x,\mathcal{C}_I(g)}\otimes|m\rangle_{\mathcal{C}_M(g)}\otimes[UU_\Sigma|+\rangle]_{\mathcal{C}_O(g)}, \quad (98)$$

with χ being a free parameter. Therefore, on the input state $|+\rangle$ the gate simulation acts as

$$\tilde{U} = e^{i\chi}\,U\,U_\Sigma. \quad (99)$$

This observation concludes the discussion of case 2.

The fact that (94) and (98) hold simultaneously imposes stringent conditions on the phases $\eta(\mathbf{z})$. To see this, let us evaluate the scalar product

$$c_\chi = {}_{\mathcal{C}(g)}\langle\Psi_{\rm out}(+)|UU_\Sigma|\mathbf{s}\rangle_{x,\mathcal{C}_I(g)}\otimes|m\rangle_{\mathcal{C}_M(g)}\otimes|+\rangle_{\mathcal{C}_O(g)}. \quad (100)$$

From (98) it follows immediately that

$$c_\chi = e^{-i\chi}. \quad (101)$$

On the other hand, since $|+\rangle = 1/2^{n/2}\sum_{\mathbf{z}\in\{0,1\}^n}|\mathbf{z}\rangle$ and, by linearity, $|\Psi_{\rm out}(+)\rangle = 1/2^{n/2}\sum_{\mathbf{z}\in\{0,1\}^n}|\Psi_{\rm out}(\mathbf{z})\rangle$, from (94) it follows that

$$c_\chi = \frac{1}{2^n}\sum_{\mathbf{z}\in\{0,1\}^n}e^{-i\eta(\mathbf{z})}. \quad (102)$$

The sum in (102) runs over 2^n terms. Thus, with $|e^{-i\eta(\mathbf{z})}| = 1$ for all $\mathbf{z}$, it follows from the triangle inequality that $|c_\chi| \leq 1$. The modulus of c_χ can be unity only if all $e^{-i\eta(\mathbf{z})}$ are equal. As (101) shows, $|c_\chi|$ is indeed equal to unity. Therefore, the phase factors $e^{i\eta(\mathbf{z})}$ must all be the same, and with (101) and (102),

$$e^{i\eta(\mathbf{z})} = e^{i\chi},\ \forall\,\mathbf{z}. \quad (103)$$

If we now insert (103) into (94) we find that the gate simulation acts upon every input state in the computational basis, and thus upon every input state, as $\tilde{U}_g = e^{i\chi}U\,U_\Sigma$. Therein, the global phase factor $e^{i\chi}$ has no effect. Thus we find that the gate simulation indeed acts as stated in (83) and (84). □

We would like to acknowledge that a similar theorem restricted to gates in the Clifford group has been obtained in [14].

Let us conclude this section with some comments on how to use this theorem. First, note that *Theorem 1 does not imply anything about the temporal order of measurements within a gate simulation.* In particular it should be understood that a procedure according to Scheme 1 is not such that first the measurements on the cluster qubits in $\mathcal{C}_M(g)$ and thereafter the measurements in $\mathcal{C}_I(g)$ are performed.

Instead, first all those cluster qubits $q \in \mathcal{C}_I(g) \cup \mathcal{C}_M(g)$ are measured whose measurement basis is the eigenbasis of either σ_x or σ_y (remember that, after the removal of the redundant cluster qubits as described in Section II C, we are dealing with clusters $\mathcal{C}_N$ such that, apart from the readout, no measurements in the σ_z-eigenbasis occur). Second, possibly in several subsequent rounds, the remaining measurements are performed in bases which are chosen according to previous measurement results.

Let us now discuss how to choose the appropriate measurement bases. First note that the unitary operations U_Σ and U in (83) both depend on measurement results of qubits in $\mathcal{C}(g)$,

$$\begin{aligned} U_\Sigma &= U_\Sigma\left(\{s_i|\, i \in \mathcal{C}_I(g) \cup \mathcal{C}_M(g)\}\right), \\ U &= U\left(\mathcal{M}^{(\mathcal{C}_M(g))}, \{s_i|\, i \in \mathcal{C}_M(g)\}\right). \end{aligned} \tag{104}$$

The dependence of U_Σ on $\{s_i|\, i \in \mathcal{C}_M(g)\}$ arises through the $\{\lambda_{x,i}, \lambda_{z,i}|\, i = 1\,..\,n\}$ of (82).

Now note that in (83) the order of the unitary gate U and the byproduct operator U_Σ is the opposite of what is required in (68). Therefore, the order of these operators has to be interchanged, which is achieved by propagating the byproduct operator U_Σ through the gate U. For gates or sub-circuits given as a quantum logic network composed of CNOT-gates and one-qubit rotations, this task can be performed using the propagation relations (72), (73) and (74). The result is

$$\begin{aligned} \tilde{U} = U\left(\mathcal{M}^{(\mathcal{C}_M(g))}, \{s\}_{\mathcal{C}_M}\right) U_\Sigma\left(\{s\}_{\mathcal{C}_I \cup \mathcal{C}_M}\right) = \\ U'_\Sigma\left(\{s\}_{\mathcal{C}_I \cup \mathcal{C}_M}\right) U'\left(\mathcal{M}^{(\mathcal{C}_M(g))}, \{s\}_{\mathcal{C}_I \cup \mathcal{C}_M}\right). \end{aligned} \tag{105}$$

Now, the choice of measurement bases in $\mathcal{M}^{(\mathcal{C}_M(g))}$ is allowed to be adaptive, that is the measurement bases may depend on measurement outcomes at other cluster qubits, $\mathcal{M}^{(\mathcal{C}_M(g))} = \mathcal{M}^{(\mathcal{C}_M(g))}(\{s\})$. For the realization of the gate U_g, the measurement bases must be chosen in such a way that

$$U'\left(\mathcal{M}^{(\mathcal{C}_M(g))}, \{s\}\right) = U_g. \tag{106}$$

This induces the identification,

$$U'_\Sigma\left(\{s\}_{\mathcal{C}_{IM}}\right) = U_{\Sigma,g} \tag{107}$$

of the byproduct operators. Now, the order of the desired unitary operation U_g and the byproduct operator $U_{\Sigma,g}$ is as required in (68). With adaptive measurement bases the effect of the randomness introduced by the measurements can be counteracted. What remains is a random byproduct operator which does not affect the deterministic character of a $\mathrm{QC}_\mathcal{C}$-computation and which is accounted for in the post-processing of the measurement results.

In subsequent sections we will illustrate in a number of examples how Theorem 1 is used to demonstrate the functioning of quantum gate simulations on the $\mathrm{QC}_\mathcal{C}$, and how the strategies for adapting the measurement bases are found.

G. Function of CNOT-gate and general one-qubit rotations

In this section, we demonstrate that the measurement patterns which we have introduced do indeed realize the desired quantum logic gates.

The basis for all our considerations is the set (11) of eigenvalue equations fulfilled by the cluster states. Therefore let us, before we turn to the realization of the gates in the universal set, describe how the eigenvalue equations can be manipulated. Equations (11) are not the only eigenvalue equations satisfied by the cluster state. Instead, a vast number of other eigenvalue equations can be derived from them.

The operators $K^{(a)}$ may for example be added, multiplied by a scalar and multiplied with each other. In this way, a large number of eigenvalue equations can be generated from equations (11). Note, however, that not all operators generated in this way are correlation operators. Non-Hermitian operators can be generated which do not represent observables, yet will prove to be useful for the construction of new correlation operators.

Furthermore, if quantum correlation operator K for state $|\phi\rangle$ commutes with measured observable $\vec{r}_i \cdot \vec{\sigma}^{(i)}$, the correlation will still apply to the measured state. More specifically, if the state $|\phi\rangle$ satisfies the eigenvalue equation $K|\phi\rangle = \lambda|\phi\rangle$ and $[K, \vec{r}_i \cdot \vec{\sigma}] = 0$, then the state resulting from the measurement, $P^{(i)}_{s_i}|\phi\rangle$, where $P^{(i)}_{s_i} = \frac{1+(-1)^{s_i}\vec{r}_i\cdot\vec{\sigma}^{(i)}}{2}$, satisfies the same eigenvalue equation since $\lambda[P^{(i)}_{s_i}|\phi\rangle] = [P^{(i)}_{s_i}K|\phi\rangle] = K[P^{(i)}_{s_i}|\phi\rangle]$. Thus the correlation K is inherited to the resultant state, $P^{(i)}_{s_i}|\phi\rangle$.

To demonstrate and explain the measurement patterns realizing certain quantum gates, the program is as follows. First, from the set of eigenvalue equations which define the cluster state $|\phi\rangle_{\mathcal{C}(g)}$, we derive a set of eigenvalue equations which is compatible with the measurement pattern on $\mathcal{C}_M$. Then, we use these to deduce the set of eigenvalue equations which define the state $|\psi\rangle_{\mathcal{C}(g)}$, where the qubits in $\mathcal{C}_M$ have been measured. Thus we demonstrate that the assumptions for Theorem 1, that is the set of equations (82), are satisfied with the appropriate unitary transformation U. Third, U_Σ is obtained from equation (84) as a function of the measurement re-

sults. The order of U and U_Σ is then interchanged and, in this way, the temporal ordering of the measurements becomes apparent.

1. Identity gate

As a simple example, let us first consider a gate which realizes the identity operation $\mathbb{1}$ on a single logical qubit.

For the identity gate $\mathcal{C}_I$, $\mathcal{C}_M$ and $\mathcal{C}_O$ each consist of a single qubit, so labeling the qubits 1, 2 and 3, $1 \in \mathcal{C}_I$, $2 \in \mathcal{C}_M$ and $3 \in \mathcal{C}_O$. The pattern $\mathcal{M}(\mathbb{1})$ corresponds to a measurement of qubit 2 in the σ_x basis.

Let $|\phi\rangle_{\mathcal{C}(\mathbb{1})}$ be the cluster state on these three qubits. The state is defined by the following set of eigenvalue equations.

$$\sigma_x^{(1)}\sigma_z^{(2)} \quad |\phi\rangle_{\mathcal{C}(\mathbb{1})} = |\phi\rangle_{\mathcal{C}(\mathbb{1})}, \tag{108a}$$
$$\sigma_z^{(1)}\sigma_x^{(2)}\sigma_z^{(3)} \quad |\phi\rangle_{\mathcal{C}(\mathbb{1})} = |\phi\rangle_{\mathcal{C}(\mathbb{1})}, \tag{108b}$$
$$\sigma_z^{(2)}\sigma_x^{(3)} \quad |\phi\rangle_{\mathcal{C}(\mathbb{1})} = |\phi\rangle_{\mathcal{C}(\mathbb{1})}. \tag{108c}$$

After the measurement of qubit 2, the resulting state of the cluster is

$$|\psi\rangle_{\mathcal{C}(\mathbb{1})} = P_{x,s_2}^{(2)}|\phi\rangle_{\mathcal{C}(\mathbb{1})}, \tag{109}$$

where $s_2 \in \{0,1\}$, and $P_{x,s_2}^{(2)} = \frac{1+(-1)^{s_2}\sigma_x^{(2)}}{2}$.

$P_{x,s_2}^{(2)}$ and $\sigma_x^{(2)}$ obey the following relation,

$$P_{x,s_2}^{(2)}\sigma_x^{(2)} = (-1)^{s_2}P_{x,s_2}^{(2)}. \tag{110}$$

Applying $P_{x,s_2}^{(2)}$ to both sides of equation (108b), and using equation (110), one obtains for $|\psi\rangle_{\mathcal{C}(\mathbb{1})}$, defined in equation (109),

$$\sigma_z^{(1)}\sigma_z^{(3)} \quad |\psi\rangle_{\mathcal{C}(\mathbb{1})} = (-1)^{s_2}|\psi\rangle_{\mathcal{C}(\mathbb{1})}. \tag{111}$$

Also from equations (108a) and (108c) we have

$$\sigma_x^{(1)}\sigma_x^{(3)} \quad |\phi\rangle_{\mathcal{C}(\mathbb{1})} = |\phi\rangle_{\mathcal{C}(\mathbb{1})}. \tag{112}$$

Applying $P_{x,s_2}^{(2)}$ to both sides of this equation gives

$$\sigma_x^{(1)}\sigma_x^{(3)} \quad |\psi\rangle_{\mathcal{C}(\mathbb{1})} = |\psi\rangle_{\mathcal{C}(\mathbb{1})}. \tag{113}$$

Now, since qubits 1 and 3 represent the input and output qubits respectively, the assumption of Theorem 1, equation (82), is satisfied for $U = \mathbb{1}$. The byproduct operator U_Σ is obtained from equation (84), and we find that the full unitary operation realized by the gate is $\tilde{U} = \mathbb{1}\,\sigma_x^{s_2}\,\sigma_z^{s_1} = \sigma_x^{s_2}\,\sigma_z^{s_1}\,\mathbb{1}$.

Also note that a wire with length one ($\mathcal{C}_I(H) = 1$, $\mathcal{C}_M(H) = \emptyset$, $\mathcal{C}_O(H) = 2$), i.e. half of the above elementary wire, implements a Hadamard transformation. As in this construction the input- and output qubits lie on different sub-lattices of $\mathcal{C}$, one on the even and one on the odd sub-lattice, we do not use it in the universal set of gates. Nevertheless, this realization of the Hadamard transformation can be a useful tool in gate construction. For example, we will use it in Section II G 4 to construct the realization of the z-rotations out of the realization of x-rotations.

2. Removing unnecessary measurements

In larger measurement patterns, whenever pairs of adjacent σ_x- qubits in a wire are surrounded above and below by either vacant lattice sites or σ_z-measurements, they can be removed from the pattern without changing the logical operation of the gate. This is simple to show in the case of a linear cluster. Consider six qubits, labelled a to f, which are part of a longer line of qubits, prepared in a cluster state. Four of the eigenvalue equations which define the state are

$$\begin{aligned}
\sigma_z^{(a)}\sigma_x^{(b)}\sigma_z^{(c)}|\psi\rangle_{\mathcal{C}} &= |\psi\rangle_{\mathcal{C}},\\
\sigma_z^{(b)}\sigma_x^{(c)}\sigma_z^{(d)}|\psi\rangle_{\mathcal{C}} &= |\psi\rangle_{\mathcal{C}},\\
\sigma_z^{(c)}\sigma_x^{(d)}\sigma_z^{(e)}|\psi\rangle_{\mathcal{C}} &= |\psi\rangle_{\mathcal{C}},\\
\sigma_z^{(d)}\sigma_x^{(e)}\sigma_z^{(f)}|\psi\rangle_{\mathcal{C}} &= |\psi\rangle_{\mathcal{C}}.
\end{aligned} \tag{114}$$

Suppose, a measurement pattern $\mathcal{M}$ on these qubits contains measurements of the observable σ_x on qubits c and d. Measurements in the σ_x basis can be made before any other measurements in $\mathcal{M}$. If these two measurements alone are carried out, the new state fulfills the following eigenvalue equations, derived from equation (114) in the usual way,

$$\begin{aligned}
\sigma_z^{(a)}\sigma_x^{(b)}\sigma_z^{(e)}|\psi\rangle_{\mathcal{C}} &= (-1)^{s_d}|\psi\rangle_{\mathcal{C}},\\
\sigma_z^{(b)}\sigma_x^{(e)}\sigma_z^{(f)}|\psi\rangle_{\mathcal{C}} &= (-1)^{s_c}|\psi\rangle_{\mathcal{C}}.
\end{aligned} \tag{115}$$

The resulting state is therefore a cluster state from which qubits c and d have been removed, and b and e play the role of adjacent qubits. Thus, the two measurements have mapped a cluster state onto a cluster state and thus do not contribute to the logical operation realized by $\mathcal{M}$, which, in the case where both s_c and s_d equal 0, is completely equivalent to the reduced measurement pattern $\mathcal{M}'$, from which these adjacent σ_x measurements have been removed.

3. One-qubit rotation around x-axis

A one-qubit rotation through an angle α about the x-axis $U_x[\alpha] = \exp[-i\alpha/2\sigma_x]$ is realized on the same three qubit layout as the identity gate. Labeling the qubits 1, 2 and 3 as in the previous section, $1 = \mathcal{C}_I$, $2 = \mathcal{C}_M$ and $3 = \mathcal{C}_O$. The measurement pattern $\mathcal{M}(U_x)$ consists of a measurement, on qubit 2, of the observable represented by the vector $\vec{r}_{xy}(\eta) = (\cos(\eta), \sin(\eta), 0)$,

$$\vec{r}_{xy}(\eta)\cdot\vec{\sigma} = \cos\eta\,\sigma_x + \sin\eta\,\sigma_y = U_z[\eta]\sigma_x U_z[-\eta], \tag{116}$$

whose eigenstates lie in the x-y-plane of the Bloch sphere at an angle of η to the x-axis.

The cluster state $|\phi\rangle_{\mathcal{C}(U_x)}$ is defined by equations (1108). After the measurement of $\mathcal{M}(U_x)$, the resulting state is $|\psi\rangle_{\mathcal{C}(U_x)} = P^{(2)}_{xy(\eta)}|\phi\rangle_{\mathcal{C}(U_x)}$ where $P^{(2)}_{xy(\eta)} = \frac{1+(-1)^{s_2}\vec{r}_{xy}(\eta)\cdot\vec{\sigma}}{2}$. To generate an eigenvalue equation whose operator commutes with $\vec{r}_{xy}(\eta)\cdot\vec{\sigma}$ we manipulate equation (1108d) in the following way,

$$\sigma^{(2)}_z\sigma^{(3)}_x|\phi\rangle_{\mathcal{C}(U_x)} = |\phi\rangle_{\mathcal{C}(U_x)} \quad (117)$$

$$\text{i.e.} \quad \sigma^{(2)}_z|\phi\rangle_{\mathcal{C}(U_x)} = \sigma^{(3)}_x|\phi\rangle_{\mathcal{C}(U_x)}$$

$$\text{i.e.} \quad [\sigma^{(2)}_z - \sigma^{(3)}_x]|\phi\rangle_{\mathcal{C}(U_x)} = 0$$

$$\therefore \quad \exp[-\mathrm{i}(\theta/2)[\sigma^{(2)}_z - \sigma^{(3)}_x]|\phi\rangle_{\mathcal{C}(U_x)} = |\phi\rangle_{\mathcal{C}(U_x)} \quad (118)$$

where the last equation is true for all $\theta \in [0, 2\pi]$. This takes a more useful form, if we write it in terms of one-qubit rotations,

$$U^{(2)}_z[\theta]\, U^{(3)}_x[-\theta]|\phi\rangle_{\mathcal{C}(U_x)} = |\phi\rangle_{\mathcal{C}(U_x)}. \quad (119)$$

We use this and equation (1108b) to construct the following eigenvalue equation for $|\phi\rangle_{\mathcal{C}(U_x)}$,

$$\begin{aligned}|\phi\rangle_{\mathcal{C}(U_x)} =& \sigma^{(1)}_z\, U^{(2)}_z[\eta]\, \sigma^{(2)}_x\, U^{(2)}_z[-\eta] \\ & U^{(3)}_x[-\eta]\, \sigma^{(3)}_z\, U^{(3)}_x[\eta]\, |\phi\rangle_{\mathcal{C}(U_x)}.\end{aligned} \quad (120)$$

Applying $P_{xy(\eta),2}$ to both sides, we obtain the following eigenvalue equation for $|\psi\rangle_{\mathcal{C}(U_x)}$,

$$\sigma^{(1)}_z U^{(3)}_x[-\eta]\, \sigma^{(3)}_z\, U^{(3)}_x[\eta]\, |\psi\rangle_{\mathcal{C}(U_x)} = (-1)^{s_2}|\psi\rangle_{\mathcal{C}(U_x)}. \quad (121)$$

In the same way as for the identity gate we also apply the projector to an eigenvalue equation generated from equations (1108a) and (1108d) to obtain

$$\begin{aligned}|\psi\rangle_{\mathcal{C}(U_x)} &= \sigma^{(1)}_x\sigma^{(3)}_x|\psi\rangle_{\mathcal{C}(U_x)} \\ &= \sigma^{(1)}_x\, U^{(3)}_x[-\eta]\, \sigma^{(3)}_x\, U^{(3)}_x[\eta]\, |\psi\rangle_{\mathcal{C}(U_x)}\end{aligned} \quad (122)$$

and thus we see that equation (82) is satisfied for $U = U_x(-\eta)$ and $U_\Sigma = \sigma^{s_1}_z\sigma^{s_2}_x$. Interchanging the order of these operators is not as trivial here as for the identity gate. When σ_z is propagated through $U_x(\eta)$ the sign of the angle is reversed, so we find that the gate operation realized by this $\mathcal{M}(U_x)$ in the $\mathrm{QC}_\mathcal{C}$ is

$$U_g = U_x\left[(-1)^{s_1}(-\eta)\right]. \quad (123)$$

The sign of the rotation realized by this gate is a function of s_1, the outcome of the measurement on qubit 1. This is an example of the temporal ordering of measurements in the $\mathrm{QC}_\mathcal{C}$. In order to realize $U_x[\alpha]$ deterministically, the angle of the measurement, η, on qubit 2 must be $\eta = (-1)^{s_1}(-\alpha)$, thus this measurement can only be realized after the measurement of qubit 1.

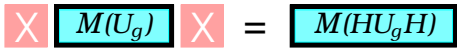


FIG. 5: Useful identity for the realization of the rotation $U_z[\alpha]$ as the sequence $H\, U_x[\alpha]\, H$.

4. *Rotation around z-axis*

The measurement pattern for a rotation around the z-axis $U_z[\beta] = \exp[-\mathrm{i}\beta/2\sigma_z]$ is illustrated in Fig. 2. It requires 5 qubits for its realization.

The measurement layout $\mathcal{M}(U_z)$ is similar to the rotation about the x-axis, except for two additional σ_x measurements on either side of the central qubit. The simplest way to understand this gate is regard it as the concatenation $U_z[\alpha] = H\, U_x[\alpha]\, H$. The Hadamard transformations may be realized as wires of length one, see Section II G 1. Thus, the measurement pattern of the z-rotation is that of the x-rotation plus one cluster qubit on either side measured in the eigenbasis of σ_x, as displayed in Fig 5.

The explanation in terms of eigenvalue equations obeyed by cluster states is as follows. Let us label the qubits 1 to 5. The cluster state $|\phi\rangle_{\mathcal{C}(U_z)}$ is defined by eigenvalue equations of the usual form. If qubits 2 and 4 are measured in the σ_x basis, the resulting state $|\phi'\rangle_{\mathcal{C}(U_z)} = P^{(2)}_{x,s_2}P^{(4)}_{x,s_4}|\phi\rangle_{\mathcal{C}(U_z)}$ fulfills the following set of eigenvalue equations

$$\sigma^{(1)}_x\sigma^{(3)}_x\sigma^{(5)}_x|\phi'\rangle_{\mathcal{C}(U_z)} = |\phi'\rangle_{\mathcal{C}(U_z)}, \quad (124a)$$

$$\sigma^{(1)}_z\sigma^{(3)}_z \quad |\phi'\rangle_{\mathcal{C}(U_z)} = (-1)^{s_2}|\phi'\rangle_{\mathcal{C}(U_z)}, \quad (124b)$$

$$\sigma^{(3)}_z\sigma^{(5)}_z|\phi'\rangle_{\mathcal{C}(U_z)} = (-1)^{s_4}|\phi'\rangle_{\mathcal{C}(U_z)}. \quad (124c)$$

This set of equations is analogous to equations (1108), except for the different eigenvalues and that the input and output qubits x- and z-bases have been exchanged. From here on the analysis of the measurement pattern runs parallel to the previous section.

One finds $\mathcal{M}(U_z)$ realizes the operation $U_z(\beta)$ if the basis of the measurement on qubit 3 is chosen to be the eigenbasis of $\vec{r}_{xy}((-1)^{s_2}(-\beta))\cdot\vec{\sigma}$, where $\vec{r}_{xy}(\eta)$ is defined in equation (1116). Qubit 2 must thus be measured prior to qubit 3. The byproduct operator for this gate is $U_{\Sigma,U_z} = \sigma^{s_2+s_4}_x\sigma^{s_1+s_3}_z$.

5. *Arbitrary Rotation*

The arbitrary Euler rotation can be realized by combining the measurement patterns of rotations around x- and z-axes by overlaying input and output qubits of adjacent patterns, as described in section II D. This creates a measurement pattern of 7 qubits plus input and output qubits, labelled as in Fig. 6, with measurements of σ_x on qubits 3, 4, 6 and 7, and measurements in the x-y-plane at angles α, β and γ on qubits 2, 5 and 8, respectively.

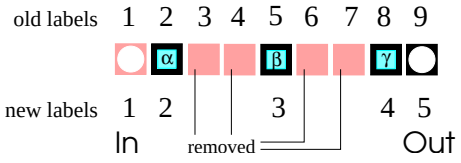


FIG. 6: General rotation composed of two x-rotations and a z-rotation in between (Euler representation). In the $QC_{\mathcal{C}}$-realization pairs of adjacent cluster qubits measured in the σ_x-eigenbasis may be removed from the measurement pattern.

The unitary operation realized by these connected measurement patterns is,

$$\begin{aligned} U_\Sigma U_{Rot}[\xi,\eta,\zeta] =& \sigma_z^{s_7}\sigma_x^{s_8}U_x[(-1)^{s_7}(-\gamma)]\sigma_z^{s_3+s_5}\sigma_x^{s_4+s_6} \\ & U_z[(-1)^{s_4}(-\beta)]\sigma_z^{s_1}\sigma_x^{s_2} \\ & U_x[(-1)^{s_1}(-\alpha)] \end{aligned} \tag{125}$$

As we have shown above, adjacent pairs of σ_x measurements can be removed from the pattern without changing the operation realized by the gate. The operation realized by this reduced measurement pattern is obtained by setting the measurement results from the removed qubits to zero, $s_3, s_4, s_6, s_7 = 0$. After relabelling the remaining qubits in the measurement pattern 1 to 5, we obtain

$$\begin{aligned} U_\Sigma U_{Rot}[\xi,\eta,\zeta] =& \sigma_x^{s_4}U_x[-\gamma]\sigma_z^{s_3}U_z[(-\beta)] \\ & \sigma_z^{s_1}\sigma_x^{s_2}U_x[(-1)^{s_1}(-\alpha)] \end{aligned} \tag{126}$$

Propagating all byproduct operators to the left hand side we find the unitary operation realized by the measurement pattern is

$$\begin{aligned} U_{Rot}[\xi,\eta,\zeta] =& U_x[-(-1)^{s_1+s_3}\gamma]U_z[-(-1)^{s_2}\beta] \\ & U_x[-(-1)^{s_1}\alpha] \end{aligned} \tag{127}$$

with byproduct operator $U_\Sigma = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}$. One finds that, to realize a specific rotation $U_{Rot}[\xi,\eta,\zeta] = U_x[\zeta]U_z[\eta]U_x[\xi]$, the angles α, β, γ specifying the measurement bases of the qubits 2,3, and 4 are again dependent on the measurement results of other qubits. We see that $\alpha = (-1)^{s_1}(-\xi)$, $\beta = (-1)^{s_2}(-\eta)$, $\gamma = (-1)^{s_1+s_3}(-\zeta)$. To realize a specific rotation deterministically, qubit 2 must thus be measured before qubits 3 and 4, and qubit 3 before qubit 4, in the bases specified in Section II B.

6. *Hadamard- and π/2-phase gate*

The Hadamard- and the $\pi/2$-phase gate have the property that under conjugation with these gates Pauli operators are mapped onto Pauli operators,

$$\begin{aligned} H\sigma_x H^\dagger &= \sigma_z, \\ H\sigma_z H^\dagger &= \sigma_x, \end{aligned} \tag{128}$$

and

$$\begin{aligned} U_z[\pi/2]\sigma_x U_z[\pi/2]^\dagger &= \sigma_y, \\ U_z[\pi/2]\sigma_z U_z[\pi/2]^\dagger &= \sigma_z, \end{aligned} \tag{129}$$

from which the propagation relations (74) follow. Related to this property is the fact that these two special rotations may be realized via σ_x- and σ_y-measurements. Such measurement bases need not be adapted to previously obtained measurement results and therefore, while these rotations might be realized in the same way as any other rotation, there is a more advantageous way to do so.

To realize either of the gates we use again a cluster state of 5 qubits in a chain $\mathcal{C}(H)$. Let the labeling of the qubits be as in Fig. 2d and e, i.e. qubit 1 is the input- and qubit 5 the output qubit.

A cluster state $|\phi\rangle_{\mathcal{C}(H)}$ obeys the two eigenvalue equations

$$\begin{aligned} |\phi\rangle_{\mathcal{C}(H)} &= K^{(1)}K^{(3)}K^{(4)}|\phi\rangle_{\mathcal{C}(H)} \\ &= \sigma_x^{(1)}\sigma_y^{(3)}\sigma_y^{(4)}\sigma_z^{(5)}|\phi\rangle_{\mathcal{C}(H)}, \\ |\phi\rangle_{\mathcal{C}(H)} &= K^{(2)}K^{(3)}K^{(5)}|\phi\rangle_{\mathcal{C}(H)} \\ &= \sigma_z^{(1)}\sigma_y^{(2)}\sigma_y^{(3)}\sigma_x^{(5)}|\phi\rangle_{\mathcal{C}(H)}. \end{aligned} \tag{130}$$

When the qubits 2, 3 and 4 of this state are measured in the σ_y-eigenbasis and thereby the measurement outcomes s_2, s_3, $s_4 \in \{0,1\}$ are obtained, the resulting state $|\psi\rangle_{\mathcal{C}(H)}$ obeys the eigenvalue equations

$$\begin{aligned} \sigma_x^{(1)}\sigma_z^{(5)}|\phi\rangle_{\mathcal{C}(H)} &= (-1)^{s_3+s_4}|\phi\rangle_{\mathcal{C}(H)}, \\ \sigma_z^{(1)}\sigma_x^{(5)}|\phi\rangle_{\mathcal{C}(H)} &= (-1)^{s_2+s_3}|\phi\rangle_{\mathcal{C}(H)}. \end{aligned} \tag{131}$$

From equation (128) we see that the correlations (131) are precisely those we need to explain the realization of the Hadamard gate. Using Theorem 1 we find that by procedure 3 with measurement of the operators $\sigma_x^{(1)}$, $\sigma_y^{(2)}$, $\sigma_y^{(3)}$ and $\sigma_y^{(4)}$ a Hadamard gate with a byproduct operator as given in (31) is realized.

A cluster state $|\phi\rangle_{\mathcal{C}(U_z[\pi/2])}$ of a chain of 5 qubits obeys the eigenvalue equations

$$\begin{aligned} |\phi\rangle_{\mathcal{C}(U_z[\pi/2])} &= K^{(1)}K^{(3)}K^{(4)}K^{(5)}|\phi\rangle_{\mathcal{C}(U_z[\pi/2])}, \\ &= -\sigma_x^{(1)}\sigma_y^{(3)}\sigma_x^{(4)}\sigma_y^{(5)}|\phi\rangle_{\mathcal{C}(U_z[\pi/2])} \\ |\phi\rangle_{\mathcal{C}(U_z[\pi/2])} &= K^{(2)}K^{(4)}|\phi\rangle_{\mathcal{C}(U_z[\pi/2])} \\ &= \sigma_z^{(1)}\sigma_x^{(2)}\sigma_x^{(4)}\sigma_z^{(5)}|\phi\rangle_{\mathcal{C}(U_z[\pi/2])}. \end{aligned} \tag{132}$$

When the qubits 2, and 4 of this state are measured in the σ_x- and qubit 3 is measured in the σ_y-eigenbasis, with the measurement outcomes s_2, s_3, $s_4 \in \{0,1\}$ obtained, the resulting state $|\psi\rangle_{\mathcal{C}(U_z[\pi/2])}$ obeys the eigenvalue equations

$$\begin{aligned} \sigma_x^{(1)}\sigma_y^{(5)}|\psi\rangle_{\mathcal{C}(U_z[\pi/2])} &= (-1)^{s_3+s_4+1}|\psi\rangle_{\mathcal{C}(U_z[\pi/2])}, \\ \sigma_z^{(1)}\sigma_z^{(5)}|\psi\rangle_{\mathcal{C}(U_z[\pi/2])} &= (-1)^{s_2+s_4}|\psi\rangle_{\mathcal{C}(U_z[\pi/2])}. \end{aligned} \tag{133}$$

Using Theorem 1 we find that by procedure 3 with measurement of the operators $\sigma_x^{(1)}$, $\sigma_x^{(2)}$, $\sigma_y^{(3)}$ and $\sigma_x^{(4)}$ a $\pi/2$-phase gate is realized, where the byproduct operator is given by (31).

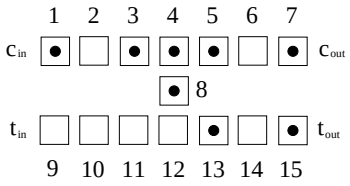


FIG. 7: Pattern of correlation centers representing the eigenvalue equation (134a).

7. The CNOT gate

A measurement pattern which realizes a CNOT gate is illustrated in Fig. 2. Labeling the qubits as in Fig. 2, we use the same analysis as above to show that this measurement pattern does indeed realize a CNOT gate in the $\mathrm{QC}_{\mathcal{C}}$.

Of the cluster $\mathcal{C}(CNOT)$ on which the gate is realized, qubits 1 and 9 belong to $\mathcal{C}_I$, qubits 7 and 15 belong to $\mathcal{C}_O$ and the remaining qubits belong to $\mathcal{C}_M$. Let $|\phi\rangle$ be a cluster state on $\mathcal{C}(CNOT)$, which obeys the set of eigenvalue equations (11).

From these basic eigenvalue equations there follow the equations

$$\begin{aligned}
|\phi\rangle &= K^{(1)}K^{(3)}K^{(4)}K^{(5)}K^{(7)}K^{(8)}K^{(13)}K^{(15)}\,|\phi\rangle \\
&= -\sigma_x^{(1)}\sigma_y^{(3)}\sigma_y^{(4)}\sigma_y^{(5)}\sigma_x^{(7)}\sigma_y^{(8)}\sigma_x^{(13)}\sigma_x^{(15)}\,|\phi\rangle, \qquad (134a)\\
|\phi\rangle &= K^{(2)}K^{(3)}K^{(5)}K^{(6)}\,|\phi\rangle \\
&= \sigma_z^{(1)}\sigma_y^{(2)}\sigma_y^{(3)}\sigma_y^{(5)}\sigma_y^{(6)}\sigma_z^{(7)}\,|\phi\rangle, \qquad (134b)\\
|\phi\rangle &= K^{(9)}K^{(11)}K^{(13)}K^{(15)}\,|\phi\rangle \\
&= \sigma_x^{(9)}\sigma_x^{(11)}\sigma_x^{(13)}\sigma_x^{(15)}\,|\phi\rangle, \qquad (134c)\\
|\phi\rangle &= K^{(5)}K^{(6)}K^{(8)}K^{(10)}K^{(12)}K^{(14)}\,|\phi\rangle \\
&= \sigma_y^{(5)}\sigma_y^{(6)}\sigma_z^{(7)}\sigma_y^{(8)}\sigma_z^{(9)}\sigma_x^{(10)}\sigma_y^{(12)}\sigma_x^{(14)}\sigma_z^{(15)}\,|\phi\rangle. \qquad (134d)
\end{aligned}$$

Subsequently we will often use a graphic representation of eigenvalue equations like (134a) - (134d). Each of these equations is specified by the set of correlation centers q for which the basic correlation operators $K^{(q)}$ (2) enter the r.h.s. of the equation. While the information content is the same, it is often more illustrative to display the pattern of correlation centers than to write down the corresponding cluster state eigenvalue equation. As an example, the pattern of correlation centers which represents the eigenvalue equation (134a) is given in Fig. 7.

If the qubits 10, 11, 13 and 14 are measured in the σ_x- and the qubits 2, 3, 4, 5, 6, 8 and 12 are measured in the σ_y-eigenbasis, whereby the measurement results s_2 - s_6, s_8, s_{10} - s_{14} are obtained, then the cluster state eigenvalue equations (134a) - (134d) induce the following eigenvalue equations for the projected state $|\psi\rangle$

$$\begin{aligned}
\sigma_x^{(1)}\,\sigma_x^{(7)}\,\sigma_x^{(15)}\,|\psi\rangle &= (-1)^{1+s_3+s_4+s_5+s_8+s_{13}}|\psi\rangle, \qquad (135a)\\
\sigma_z^{(1)}\,\sigma_z^{(7)}\,|\psi\rangle &= (-1)^{s_2+s_3+s_5+s_6}|\psi\rangle \qquad (135b)\\
\sigma_x^{(9)}\,\sigma_x^{(15)}\,|\psi\rangle &= (-1)^{s_{11}+s_{13}}|\psi\rangle, \qquad (135c)\\
\sigma_z^{(9)}\,\sigma_z^{(7)}\,\sigma_z^{(15)}\,|\psi\rangle &= (-1)^{s_5+s_6+s_8+s_{10}+s_{12}+s_{14}}|\psi\rangle. \qquad (135d)
\end{aligned}$$

Therein, qubits 1 and 7 represent the input and output for the control qubit and qubits 9 and 15 represent the input and output for the target qubit. Writing the CNOT unitary operation on control and target qubits $CNOT(c,t)$, we find

$$\begin{aligned}
CNOT(c,t)\sigma_x^{(c)}CNOT(c,t) &= \sigma_x^{(c)}\sigma_x^{(t)}, \qquad (136a)\\
CNOT(c,t)\sigma_z^{(c)}CNOT(c,t) &= \sigma_z^{(c)}, \qquad (136b)\\
CNOT(c,t)\sigma_x^{(t)}CNOT(c,t) &= \sigma_x^{(t)}, \qquad (136c)\\
CNOT(c,t)\sigma_z^{(t)}CNOT(c,t) &= \sigma_z^{(c)}\sigma_z^{(t)}. \qquad (136d)
\end{aligned}$$

Comparing these equations to the eigenvalue equations (135a) to (135d), one sees that $\mathcal{M}$ does indeed realize a CNOT gate. Furthermore, after reading off the operator U_Σ using equations (82) and (84) and propagating the byproduct operators through to the output side of the CNOT gate, one finds the expressions for the byproduct operators, reported in equation (24).

H. Upper bounds on resource consumption

Here we discuss the spatial, temporal and operational resources required for the $\mathrm{QC}_{\mathcal{C}}$ and compare with resource requirements of a network quantum computer.

To run a specific quantum algorithm, the $\mathrm{QC}_{\mathcal{C}}$ requires a cluster of a certain size. Therefore the $\mathrm{QC}_{\mathcal{C}}$-*spatial resources* S are the number of cluster qubits in the required cluster state $|\phi\rangle_{\mathcal{C}}$, i.e. $S = |\mathcal{C}|$. The computation is driven by one-qubit measurement only. Thus, a single one-qubit measurement is one unit of operational resources, and the $\mathrm{QC}_{\mathcal{C}}$-*operational resources* O are defined as the total number of one-qubit measurements involved. The operational resources O are always smaller or equal to the spatial resources S,

$$O \leq S, \qquad (137)$$

since each cluster qubit is measured at most once. As for the temporal resources, the $\mathrm{QC}_{\mathcal{C}}$-*logical depth* T is the minimum number of measurement rounds to which the measurements can be parallelized.

Let us briefly recall the definition of these resources in the network model. The temporal resources are specified by the network logical depth T_{qln}, which is the minimal number of steps to which quantum gates and readout measurements can be parallelized. The spatial resources S_{qln} count the number of logical qubits on which an algorithm runs. Finally, the operational resources O_{qln} are

the number of elementary operations required to carry out an algorithm, i.e. the number of gates and measurements.

The construction kit for the simulation of quantum logic networks on the $QC_{\mathcal{C}}$ shall contain a universal set of gates, in our case the CNOT gate between arbitrary qubits and the one qubit rotations. Already the next-neighbor CNOT with general rotations is universal since a general CNOT can be assembled of a next-neighbor CNOT and swap gates which can themselves be composed of next-neighbor CNOTs. However, in the following we would like to use for the general CNOT the less cumbersome construction described in Section IV C. For this gate, the distance between logical qubits, i.e. between parallel qubit wires, is 4. The virtue of this gate is that it can always be realized on a vertical slice of width 6 on the cluster, no matter how far control and target qubit are separated. A slice of width 6 means that the distance between an input qubit of the gate and the corresponding input of the consecutive gate is 6 lattice spacings. This general CNOT gate determines the spatial dimensions of a unit cell in the measurement patterns. The size of this unit cell is 4×6. The other elementary gates, the next-neighbor CNOT and the rotations are smaller than a unit cell and therefore have to be stretched. This is easily accomplished. The next-neighbor CNOT as displayed in Fig. 2a has a size of 2×6 and is extended to size 4×6 by inserting two adjacent cluster qubits into the vertical bridge connecting the horizontal qubit lines. The general rotation as in Fig. 2b has width 4 and is stretched to width 6 by inserting two cluster qubits just before the output.

Concerning the temporal resources we first observe that we can realize the gates in the same temporal order as in the network model. To realize a general CNOT on the $QC_{\mathcal{C}}$ takes one step of measurements, to realize a general rotation takes at most three. For the network model we do not assume that a general rotation has to be Euler-decomposed. Rather we assume that in the network model a rotation can be realized in a single step. Thus the temporal resources of the $QC_{\mathcal{C}}$ and in the network model are related via

$$T \leq 3T_{\rm qln}. \tag{138}$$

As for the spatial resources, let us consider a rectangular cluster of height h and width w on which the qubit wires are oriented horizontally, with the network register state propagating from left to right. As the logical qubits have distance 4, the height of the cluster has to be $h = 4S_{\rm qln} - 3$ where $S_{\rm qln}$ is equal to the number n of logical qubits. Further, the number of gates in the circuit is at most $S_{\rm qln}T_{\rm qln}$ because, in the network model, in each step at most $S_{\rm qln}$ gates can be realized. On each vertical slice of width 6 on the cluster there fits at least one gate such that –taking into account an extra slice of width 1 for the readout cluster qubits– for the width holds $w \leq 6S_{\rm qln}T_{\rm qln} + 1$. With $S = h\,w$ one finds that

$$S \leq 24\,S_{\rm qln}{}^2T_{\rm qln}. \tag{139}$$

In a similar way, a bound involving the network operational resources can be obtained. The spatial overhead S and the operational overhead O per elementary network operation is $\leq 24S_{\rm qln}$ if this operation is a unitary gate from the universal set described before, and is equal to one if this operation is a readout measurement. Thus, we also have

$$\begin{aligned} S &\leq 24\,O_{\rm qln}S_{\rm qln}, \\ O &\leq 24\,O_{\rm qln}S_{\rm qln}. \end{aligned} \tag{140}$$

The purpose of this section was to demonstrate that the scaling of spatial and temporal resources is at worst polynomial as compared to the network model. In [7] it has been shown, as stated in Section III A, that the required classical processing increases the computation time only marginally (logarithmically in the number n of logical qubits) and thus there is no exponential overhead in either classical or quantum resources.

The upper bounds in (138), (139) and (140) should not be taken for estimates. For algorithms of practical interest the required resources usually scale much more favorably and there do not even have to be overheads at all. This is illustrated for the temporal complexity of Clifford circuits in Section III I and in the examples of Section IV. A spatial overhead always exists. However, this is compensated by the fact that the operational effort to create a cluster state is independent of the cluster size.

I. Quantum circuits in the Clifford group can be realized in a single step

The measurement bases to realize the Hadamard- and the $\pi/2$-phase gate need not be adapted since only operators σ_x and σ_y are measured. The same holds for the realization of the CNOT gate, see Fig. 2. Thus, all the Hadamard-, $\pi/2$-phase- and CNOT-gates of a quantum circuit can be realized simultaneously in the first measurement round, regardless of their location in the network. In particular, quantum circuits which consist only of such gates, i.e. circuits in the Clifford group, can be realized in a single time step. As an example, many circuits for coding and decoding are in the Clifford group.

The fact that quantum circuits in the Clifford group can be realized in a single time step has previously not been known for networks. The best upper bound on the logical depth that was known previously scales logarithmically with the number of logical qubits [17].

Note that, as stated by the Gottesman-Knill-Theorem [19], there is no need for fast Clifford circuits if the quantum output is measured in a Pauli basis because these circuits can be simulated efficiently classically. However, the purpose of this section is to point out that the whole Clifford part of *any* quantum circuit can be performed in a single time step. We will discuss this point further in Section III B.

Here we find a first aspect of $QC_{\mathcal{C}}$-computation which is not adequately described within the network model,

and with this observation we conclude the discussion of the $\mathrm{QC}_{\mathcal{C}}$ as a simulator of quantum logic networks.

III. COMPUTATIONAL MODEL UNDERLYING THE $\mathrm{QC}_{\mathcal{C}}$

A. Processing of information

In the network model of quantum computation one usually regards a quantum register as the carrier of information. The quantum register is prepared in some input state and processed to some output state by applying a suitable unitary transformation composed of quantum gates. Finally, the output state of the quantum register is measured by which the classical readout is obtained.

For the $\mathrm{QC}_{\mathcal{C}}$ the notions of "quantum input" and "quantum output" have no genuine meaning if we restrict ourselves to the situation where the input state is known. As stated before, Shor's factoring algorithm [15] and Grover's search algorithm [16] are both examples of such a situation. In these cases the final result of any computation –including quantum computations– is a classical number. In a $\mathrm{QC}_{\mathcal{C}}$-computation this number is extracted from the outcomes of all the one-qubit measurements. The entire computation amounts to just measurements of the cluster qubits in a certain order and basis.

We have divided the set $\mathcal{C}$ of cluster qubits into subsets I, M and O to describe the $\mathrm{QC}_{\mathcal{C}}$ in terms of the network model. Such a terminology is not required for the $\mathrm{QC}_{\mathcal{C}}$ a priori. It is true that when a quantum logic network is realized on a cluster state there is a subset of cluster qubits which play the role of the output register. However, these qubits are not the final ones to be measured, but among the first (!). The measurement outcomes from all the cluster qubits contribute to the result of the computation. The qubits of $O \subset \mathcal{C}$ simulate the output state of the quantum register and thus contribute obviously to the computational result. The cluster qubits in the set $I \subset \mathcal{C}$ simulate the fiducial input state of the quantum register and their measurement contributes via the accumulated byproduct operator on O. Finally, the qubits in the section $M \subset \mathcal{C}$ of the cluster whose measurements simulate the quantum gates also contribute via the byproduct operator.

Naturally there arises the question whether there is any difference in the way how measurements of cluster qubits in I, O or M contribute to the final result of the computation. As shown in [7], it turns out that there is none. This is why we can abandon the notions of quantum input, quantum output and quantum register altogether from the description of the $\mathrm{QC}_{\mathcal{C}}$. Furthermore, quantum gates are not constitutive elements of the $\mathrm{QC}_{\mathcal{C}}$; these are instead one-qubit measurements performed in a certain temporal order and in a spatial pattern of adaptive measurement bases. In fact, the most efficient temporal order of the measurements does not follow from the temporal order of the simulated gates in the network model.

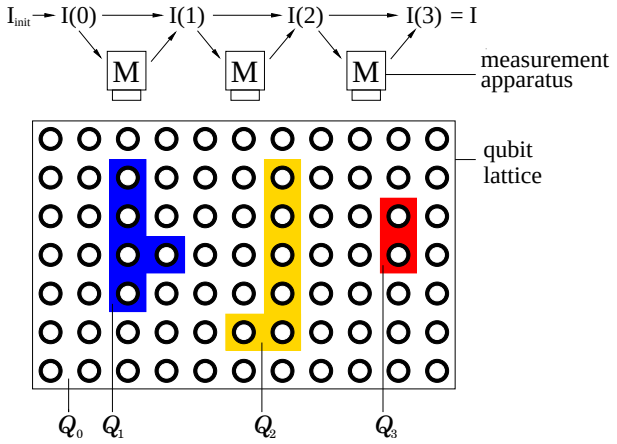


FIG. 8: General scheme of the quantum computer via one-qubit measurements. The sets Q_t of lattice qubits are measured one after the other. The results of earlier measurements determine the measurement bases of later ones. All classical information from the measurement results needed to steer the $\mathrm{QC}_{\mathcal{C}}$ is contained in the information flow vector $\mathbf{I}(t)$. After the last measurement round $t_{\max}$, $\mathbf{I}(t_{\max})$ contains the result of the computation.

The general view of a $\mathrm{QC}_{\mathcal{C}}$-computation is as follows. The cluster $\mathcal{C}$ is divided into disjoint subsets $Q_t \subset \mathcal{C}$ with $0 \leq t \leq t_{\max}$, i.e. $\bigcup_{t=0}^{t_{\max}} Q_t = \mathcal{C}$ and $Q_s \cap Q_t = \emptyset$ for all $s \neq t$. The cluster qubits within each set Q_t can be measured simultaneously and the sets are measured one after another. The set Q_0 consists of all those qubits for which no measurement bases have to be adjusted, i.e. those of which the operator σ_x, σ_y or σ_z is measured. In the subsequent measurement rounds only operators of the form $\cos\varphi\,\sigma_x \pm \sin\varphi\,\sigma_y$ are measured where $|\varphi| < \pi/2$, $\varphi \neq 0$. The measurement bases are adaptive in these rounds, i.e. they are adapted to measurement results obtained in previous rounds. The measurement outcomes from the qubits in Q_0 determine the measurement bases for the qubits in Q_1, which are measured in the second round, those from Q_0 and Q_1 together determine the bases for the measurements of the qubits in Q_2 which are measured in the third round, and so on. Finally, the result of the computation is calculated from the measurement outcomes obtained in all the measurement rounds.

Now there arises the question of how complex the required classical processing is. In principle it could be that all the obtained measurement results had to be stored separately and the functions to compute the measurement bases were so complicated that one would gain no advantage over the classical algorithm for the considered problem. This is not at all the case. If the network algorithm runs on n qubits then the classical data that the $\mathrm{QC}_{\mathcal{C}}$ has to keep track of is entirely contained in a $2n$-component binary valued vector, which we have called the information flow vector $\mathbf{I}(t)$ [7]. The update of $\mathbf{I}(t)$ is a classical computation that is needed to adapt the

measurement bases of cluster qubits according to previous measurement outcomes. These updates and the final identification of the computational result from $\mathbf{I}(t_{\max})$ are all elementary.

Concerning the resources for the classical processing of the measurement outcomes in a $\mathrm{QC}_{\mathcal{C}}$-computation, we point out that this processing increases the total time of computation only marginally [7].

In summary, the formal description of the $\mathrm{QC}_{\mathcal{C}}$ is based on primitive quantities of which the most important ones are the sets $Q_t \subset \mathcal{C}$ of cluster qubits defining the temporal ordering of measurements on the cluster state, and the binary valued information flow vector $\mathbf{I}(t)$ which is the carrier of the algorithmic information. The reader who is interested in how this computational model arises and in its detailed description is referred to [7].

B. Algorithms and graphs

In this section we relate $\mathrm{QC}_{\mathcal{C}}$-algorithms to graphs. We do this by considering non-universal graph states suited for the specific algorithm in question. For the $\mathrm{QC}_{\mathcal{C}}$, the Clifford part of each algorithm can be removed. A mathematical graph comprises all the information that needs to be kept the Clifford part.

While the network formulation of a quantum algorithm is given as a sequence of quantum gates applied to a fiducial input state, the $\mathrm{QC}_{\mathcal{C}}$-version of a quantum algorithm is specified by a measurement pattern on the universal cluster state plus the structure [7] for the processing of the measurement outcomes.

The measurement pattern is, in the simplest case, just a copy of the network layout to the substrate cluster state, imprinted by the measurements. As such it contains information about the precise location of the gate simulations and about the way the "wires" connecting the gates are bent around. These are all details of the realization of an algorithm but do not belong to the description of the algorithm itself. Thus, the measurement pattern introduces a large amount of redundancy into the description of a $\mathrm{QC}_{\mathcal{C}}$-algorithm. This redundancy may be reduced to a large extent by allowing for non-universal, algorithm-specific quantum resources.

Clearly, at this point one has to specify how special the algorithm-specific resource is allowed to be. Obviously it would make no sense to take the quantum output of the entire network as the required quantum resource and to regard the subsequent readout measurements as the algorithm. Here, we allow for any *graph state* [9], (21) as the quantum resource. Graph states are both easy to create and to describe. Every algorithm may be run with a graph state as the quantum resource since the cluster state is a particular graph state.

To allow for an algorithm-specific graph state as the quantum resource of a $\mathrm{QC}_{\mathcal{C}}$-computation reduces the redundancy of both the description and the realization of a quantum algorithm. This can easily be seen from the material presented in Section II C. All the cluster qubits $q \in \mathcal{C}\backslash\mathcal{C}_N$ can be get rid of either by measuring them in the σ_z-eigenbasis or equivalently by not placing them initially into their positions at all. The remaining state on the sub-cluster $\mathcal{C}_N$ is again a cluster state. Hence it is also a graph state. It is less redundant and no longer universal.

But we can go further. Not only the qubits measured in the σ_z-eigenbasis may be removed from the cluster but instead all those qubits of which one of the Pauli operators σ_x, σ_y or σ_z is measured, i.e. all the qubits which form the set Q_0. The state of the unmeasured qubits that emerges after the measurement of the cluster qubits in Q_0 is again (local equivalent to) a graph state.

This may be seen as follows. First note that the operators $\sigma_x^{(a)} \bigotimes_{b\in V} \left(\sigma_z^{(b)}\right)^{\Gamma_{ab}}$ which appear in (21) form a stabilizer of the state $|\phi\{\kappa\}\rangle_G$. The generator of the stabilizer contains $|\mathcal{C}|$ elements for a state of $|\mathcal{C}|$ qubits. After all the qubits $q \in Q_0$ have been measured, the resulting state $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ of the $|\mathcal{C}\backslash Q_0|$ unmeasured qubits is again described by a stabilizer of the form

$$\bigotimes_{i=1}^{|\mathcal{C}\backslash Q_0|} \left(\sigma_x^{(i)}\right)^{X_{a,i}} \left(\sigma_z^{(i)}\right)^{Z_{a,i}} |\Psi\rangle_{\mathcal{C}\backslash Q_0} = \pm|\Psi\rangle_{\mathcal{C}\backslash Q_0} \quad \forall a = 1\,..\,|\mathcal{C}\backslash Q_0|, \tag{141}$$

with two $|\mathcal{C}\backslash Q_0| \times |\mathcal{C}\backslash Q_0|$-matrixes X and Z, for which $X_{a,i}, Z_{a,i} \in \{0,1\}$. The $|\mathcal{C}\backslash Q_0| \times 2|\mathcal{C}\backslash Q_0|$-compound matrix $(X|Z)$ is called the generator matrix of the stabilizer for $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$. The state $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ is uniquely determined by the generator of its stabilizer.

The state $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ can thus be regarded as a $[|\mathcal{C}\backslash Q_0|, 0, d]$-stabilizer code, with the distance d not specified. Whether a code with only one code word that encodes 0 qubits should be regarded as a code in the sense of coding shall not concern us here. For the present purpose, it is important to note that the state $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ fulfills the assumptions of Theorem 1 in [20]. The cited theorem states that any stabilizer code over the alphabet $A = \mathbb{F}_{p^m}$ is [local unitary] equivalent to a graph code. If we specialize to our case, $A = \mathbb{F}_{2^2}$, we find that the state $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ specified in (141) is local unitary equivalent to a graph state $|\phi\{\kappa\}\rangle_{G(\mathcal{C}\backslash Q_0, E_{\mathcal{C}\backslash Q_0})}$ (21).

That is, the state $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ needed for the computation can be obtained from a graph state $|\phi\{\kappa\}\rangle_{G(\mathcal{C}\backslash Q_0, E_{\mathcal{C}\backslash Q_0})}$ via local unitary transformations. Subsequently in the process of computation, the qubits of $|\Psi\rangle_{\mathcal{C}\backslash Q_0}$ are measured in their given temporal order and in the appropriate adapted bases. An alternative way to proceed is to use the graph state $|\phi\{\kappa\}\rangle_{G(\mathcal{C}\backslash Q_0, E_{\mathcal{C}\backslash Q_0})}$ directly, only modifying the measurement bases instead of performing the local rotations prior to the measurements. Thus, in a $\mathrm{QC}_{\mathcal{C}}$-computation with a special graph state as the quantum resource and the first measurement round omitted, the way of processing the classical information is the same as in a $\mathrm{QC}_{\mathcal{C}}$-computation with a universal resource and the first measurement round performed.

The graphs associated with states (141) are in general not unique [20]. A constructive way to obtain graphs on $\mathcal{C}\backslash Q_0$ from $G(\mathcal{C}, E_\mathcal{C})$ and the measurement bases of the qubits in Q_0 has been described in [21].

Now note that the measurement of the qubits in Q_0 realize the Clifford part of a quantum circuit. The fact that we can reduce the quantum resource by these qubits means that *we can remove from each quantum algorithm its Clifford part*. This represents, in a way, an extension to the Knill-Gottesman-Theorem [19], stating that a quantum computation that consist only of quantum input state preparation in the computational basis, unitary gates in the Clifford group, measurement of observables in the Pauli group, and gates in the Clifford group conditioned on the outcomes of such measurements, may be simulated efficiently classically and thus requires no quantum resources at all.

With only a single non-Clifford operation in the circuit, such as a one-qubit rotation about most axes and angles, the efficient classical formalism upon which the Gottesman-Knill theorem rests can no longer be applied. The $\mathrm{QC}_\mathcal{C}$-construction, on the other hand, is not affected by this. Each quantum network algorithm in question may be reduced by its Clifford part. Only the non-Clifford gates require quantum resources. The price is that the universal quantum resource, the cluster state, is changed into a non-universal, algorithm-specific resource –a graph state (121)– on fewer qubits. The Clifford part of the network algorithm specifies the corresponding graph.

In conclusion, instead of describing a quantum algorithm as a network of gates applied to some fiducial input state, a quantum algorithm may (arguably more effectively) be characterized by a graph specifying the quantum resource and the structure [7] for the processing of the measurement outcomes.

IV. EXAMPLES OF PRACTICAL INTEREST

A. Multi-qubit swap gate

A multi-qubit swap gate is an n-qubit generalization of the two-qubit swap gate. It reverses the order of the n-qubits, interchanging qubit i with $n+1-i$, $i = 1, 2, .., N$. This can be realized in a simple way on the $\mathrm{QC}_\mathcal{C}$, as shown in Fig. 9a. The measurement pattern $\mathcal{M}$ on $\mathcal{C}_M$ consists of a square of σ_x measurements, with sides of $2n-1$ cluster qubits. The input qubits are, simultaneously with the qubits in $\mathcal{C}_M$, also measured in the σ_x-eigenbasis.

It can be verified using the methods introduced above that realizing $\mathcal{M}$ leads to correlations between the ith input qubit and the $n+1-i$th output qubit. Here, we discuss the four-qubit swap as a particular example.

After the σ_x-measurements of the qubits in $\mathcal{C}_M$ we obtain for the projected state $|\psi\rangle_{\mathcal{C}(\mathrm{swap})}$ the eigenvalue

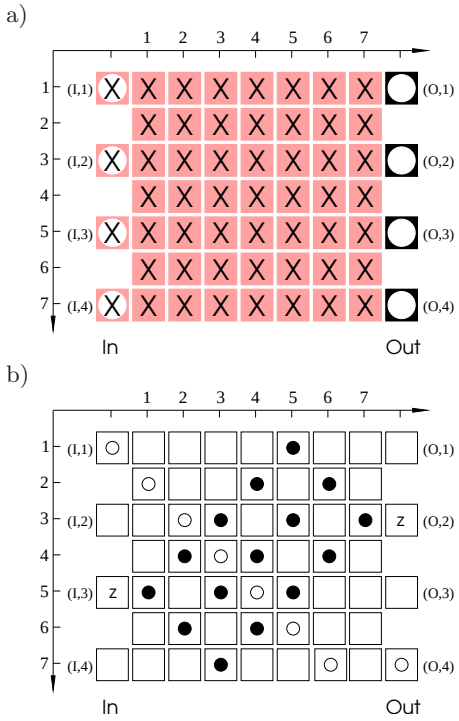


FIG. 9: The multi-qubit swap gate. a) measurement pattern to realize the swap gate. b) Correlation centers for two correlations of the projected state $|\psi\rangle_{\mathcal{C}(\mathrm{swap})}$ as inherited from correlations of $|\phi\rangle_{\mathcal{C}(\mathrm{swap})}$. The correlation $\sigma_x^{(I,1)}\sigma_x^{(O,4)}$ of $|\psi\rangle_{\mathcal{C}(\mathrm{swap})}$ stems from the product correlation for $|\phi\rangle_{\mathcal{C}(\mathrm{swap})}$ with the centers a of basic correlation operators $K^{(a)}$ denoted by "$\circ$". The centers of the initial correlation, which after the measurements induces the correlation $\sigma_z^{(I,3)}\sigma_z^{(O,2)}$ of $|\psi\rangle_{\mathcal{C}(\mathrm{swap})}$, are denoted by "$\bullet$".

equations

$$
\begin{aligned}
\sigma_x^{(I,1)}\sigma_x^{(O,4)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{x,1}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_x^{(I,2)}\sigma_x^{(O,3)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{x,2}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_x^{(I,3)}\sigma_x^{(O,2)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{x,3}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_x^{(I,4)}\sigma_x^{(O,1)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{x,4}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_z^{(I,1)}\sigma_z^{(O,4)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{z,1}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_z^{(I,2)}\sigma_z^{(O,3)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{z,2}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_z^{(I,3)}\sigma_z^{(O,2)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{z,3}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},\\
\sigma_z^{(I,4)}\sigma_z^{(O,1)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} &= (-1)^{\lambda_{z,4}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})}.
\end{aligned}
\tag{142}
$$

Therein, the parameters $\lambda_{k,x}, \lambda_{k,z} \in \{0,1\}$ depend linearly on the measurement outcomes $\{s_{(i,j)}\}$. Therein, i is the value of the x- and j the value of the y-coordinate of the respective qubit site. For example, $\lambda_{x,1} = s_{(1,2)} + s_{(2,3)} + s_{(3,4)} + s_{(4,5)} + s_{(5,6)} + s_{(6,7)} \bmod 2$.

The eigenvalue equations (142) can be derived from corresponding eigenvalue equations for the cluster state $|\phi\rangle_{\mathcal{C}(\mathrm{swap})}$ on the cluster $\mathcal{C}(\mathrm{swap})$. The required initial correlations are products of the basic correlation oper-

ators (2). The way to obtain the equations (142) is rather straightforward and therefore we omit the detailed derivations. In Fig. 9b two examples for the composition of product correlation operators from basic correlation operators $K^{(a)}$ are illustrated. The first line of (142),

$$\sigma_x^{(I,1)}\sigma_x^{(O,4)}\,|\psi\rangle_{\mathcal{C}(\mathrm{swap})} = (-1)^{\lambda_{x,1}}|\psi\rangle_{\mathcal{C}(\mathrm{swap})},$$

for example, is derived from the eigenvalue equation

$$|\phi\rangle_{\mathcal{C}(\mathrm{swap})} = K^{(\mathcal{C}_{x,1})}|\phi\rangle_{\mathcal{C}(\mathrm{swap})}, \tag{143}$$

with

$$K^{(\mathcal{C}_{x,1})} = \prod_{a\in\mathcal{C}_{x,1}} K^{(a)}, \tag{144}$$

and $\mathcal{C}_{x,1} = \{(I,1),(1,2),(2,3),(3,4),(4,5),(5,6),\ (6,7),\ (O,4)\}$. Multiplying it out we find that all operators σ_z cancel and that

$$K^{(\mathcal{C}_{x,1})} = \prod_{a\in\mathcal{C}_{x,1}} \sigma_x^{(a)}. \tag{145}$$

It is now easy to see that after the σ_x measurements of the qubits in $\mathcal{C}_M$ there remains a strict $\sigma_x^{(I,1)}\sigma_x^{(O,4)}$-correlation for the state $|\psi\rangle_{\mathcal{C}(\mathrm{swap})}$. A similar construction can be given to obtain the $\sigma_z^{(I,1)}\sigma_z^{(O,4)}$-correlation.

With the eigenvalue equations (142) the assumptions of theorem 1 are fulfilled and thus via the described measurement pattern a unitary operation $U = SWAP$ is realized modulo a byproduct operator as specified in (84). To exchange the order of the swap-gate U_{swap} and the byproduct operator U_Σ the byproduct operator is conjugated under U_{swap}, as usual for gates in the Clifford group.

B. Simulating multi-qubit Hamiltonians

Here we display a gate which simulates the unitary evolution with $U = \exp(-iH_4t)$ of the quantum input for the multi-particle Hamiltonian

$$H_4 = g\,\sigma_z^{(1)}\sigma_z^{(2)}\sigma_z^{(3)}\sigma_z^{(4)} \tag{146}$$

and *arbitrary* times t. In addition, the gate performs a swap which can be corrected for by a subsequent swap gate as described in Section IV A.

The procedure to realize the measurement pattern $\mathcal{M}$ for Hamiltonian simulation, as shown in Fig. 10, requires two rounds of measurements. In the first round all the σ_x-measurements are performed. In the second measurement round, of the qubit $(3,4)$ the operator

$$\vec{r}_{(3,4)}\cdot\vec{\sigma} = U_z[(-1)^{\lambda_M}2\varphi]\,\sigma_x\,U_z^\dagger[(-1)^{\lambda_M}2\varphi] \tag{147}$$

is measured, where $U_z[\alpha] = \exp(-i\alpha\sigma_z/2)$. Therein, the angle φ is given by

$$\varphi = gt, \tag{148}$$

and $\lambda_M \in \{0,1\}$, which depends linearly on outcomes of measurements in the first round, will be specified below.

To understand the functioning of the Hamiltonian simulator let us first discuss the state $|\psi'\rangle$ on the cluster $\mathcal{C}(\mathrm{sim})$ after the first round of measurements. By arguments analogous to those used in Section IV A, the state $|\psi'\rangle$ obeys the following eigenvalue equations:

$$\begin{aligned}
\sigma_x^{(3,4)}\sigma_x^{(I,1)}\sigma_x^{(O,4)}\,|\psi'\rangle &= (-1)^{\lambda_{x,1}}|\psi'\rangle,\\
\sigma_x^{(3,4)}\sigma_x^{(I,2)}\sigma_x^{(O,3)}\,|\psi'\rangle &= (-1)^{\lambda_{x,2}}|\psi'\rangle,\\
\sigma_x^{(3,4)}\sigma_x^{(I,3)}\sigma_x^{(O,2)}\,|\psi'\rangle &= (-1)^{\lambda_{x,3}}|\psi'\rangle,\\
\sigma_x^{(3,4)}\sigma_x^{(I,4)}\sigma_x^{(O,1)}\,|\psi'\rangle &= (-1)^{\lambda_{x,4}}|\psi'\rangle,\\
\sigma_z^{(I,1)}\sigma_z^{(O,4)}\,|\psi'\rangle &= (-1)^{\lambda_{z,1}}|\psi'\rangle,\\
\sigma_z^{(I,2)}\sigma_z^{(O,3)}\,|\psi'\rangle &= (-1)^{\lambda_{z,2}}|\psi'\rangle,\\
\sigma_z^{(I,3)}\sigma_z^{(O,2)}\,|\psi'\rangle &= (-1)^{\lambda_{z,3}}|\psi'\rangle,\\
\sigma_z^{(I,4)}\sigma_z^{(O,1)}\,|\psi'\rangle &= (-1)^{\lambda_{z,4}}|\psi'\rangle.
\end{aligned} \tag{149}$$

Further, the state $|\psi'\rangle$ obeys the eigenvalue equation

$$\sigma_z^{(3,4)}\,\sigma_z^{(O,1)}\sigma_z^{(O,2)}\sigma_z^{(O,3)}\sigma_z^{(O,4)}\,|\psi'\rangle = (-1)^{\lambda}|\psi'\rangle, \tag{150}$$

with $\lambda \in \{0,1\}$ linear in the measurement outcomes of the first round. Equation (150) can be easily verified with the pattern of correlation centers displayed in Fig. 10b. From (150) it follows that

$$\exp\left(i\theta\,\sigma_z^{(3,4)}\right)U_4[(-1)^{\lambda}\theta]\,|\psi'\rangle = |\psi'\rangle \tag{151}$$

for arbitrary angles θ, with

$$U_4[\alpha] = \exp\left(-i\alpha\,\sigma_z^{(O,1)}\sigma_z^{(O,2)}\sigma_z^{(O,3)}\sigma_z^{(O,4)}\right). \tag{152}$$

Equation (151) is now inserted in both the l.h.s. and r.h.s. of the equations (149). For example, with the first equation from (149) one obtains

$$\begin{aligned}
(-1)^{\lambda_{x,1}}\,|\psi'\rangle \;=\; &\left(U_z[2\theta]\sigma_x U_z^\dagger[2\theta]\right)^{(3,4)}\sigma_x^{(I,1)}\\
&\left(U_4[-(-1)^{\lambda}\theta]\sigma_x^{[4]}U_4^\dagger[-(-1)^{\lambda}\theta]\right)^{(O)}|\psi'\rangle.
\end{aligned} \tag{153}$$

In the second measurement round the qubit $(3,4)$ is the only one left to be measured. As can be seen from (153), if of the operator $U_z[2\theta]\sigma_x U_z^\dagger[2\theta]$ of qubit (3,4) is measured then the state $|\psi\rangle$, into which the cluster qubits are projected after the second measurement round, obeys the eigenvalue equation

$$\begin{aligned}
&(-1)^{\lambda_{x,1}+s_{(3,4)}}\,|\psi\rangle =\\
&\sigma_x^{(I,1)}\left(U_4[-(-1)^{\lambda}\theta]\sigma_x^{[4]}U_4^\dagger[-(-1)^{\lambda}\theta]\right)^{(O)}|\psi\rangle.
\end{aligned} \tag{154}$$

If we carry out this procedure for all equations in (149) we find that the state $|\psi\rangle$ that emerges after the second measurement round obeys the eigenvalue equations

$$\begin{aligned}
&\sigma_x^{(I,i)}\left(U_4U_{\mathrm{swap}}\sigma_x^{[i]}U_{\mathrm{swap}}{}^\dagger U_4^\dagger\right)^{(O)}|\psi\rangle = (-1)^{\lambda_{x,i}+s_{(3,4)}}\,|\psi\rangle,\\
&\sigma_z^{(I,i)}\left(U_4U_{\mathrm{swap}}\sigma_z^{[i]}U_{\mathrm{swap}}{}^\dagger U_4^\dagger\right)^{(O)}|\psi\rangle = (-1)^{\lambda_{z,i}}\,|\psi\rangle,
\end{aligned} \tag{155}$$

for $i = 1..4$ and with U_4 written in short for $U_4[-(-1)^\lambda\theta]$.

With the set of equations (155) the assumptions (82) of theorem 1 are fulfilled. With theorem 1 it follows that the measurement pattern displayed in Fig. 10 realizes a unitary transformation

$$U_{\rm sim} = U_4[-(-1)^\lambda\theta]U_{\rm swap}U_\Sigma, \tag{156}$$

where the byproduct operator is given by

$$U_\Sigma = \bigotimes_{i=1}^{4}\left(\sigma_z^{[i]}\right)^{s_{(I,i)}+\lambda_{x,i}+s_{(3,4)}}\left(\sigma_x^{[i]}\right)^{\lambda_{z,i}}. \tag{157}$$

Finally, the order of the operators has to be exchanged. Note that $U_{\rm swap}$ and U_4 commute. From (156) one finds

$$U_{\rm sim} = U'_\Sigma U_{\rm swap}U_4[-(-1)^{\lambda+\sum_{i=1}^4\lambda_{z,i}}\theta], \tag{158}$$

with

$$U'_\Sigma = U_{\rm swap}\,U_\Sigma\,{U_{\rm swap}}^\dagger. \tag{159}$$

Thus, in order to realize $U_4[\varphi]$ with φ specified in (148) we must choose

$$\theta = (-1)^{1+\lambda+\sum_{i=1}^4\lambda_{z,i}}\varphi. \tag{160}$$

That is, in the second measurement round we measure on the qubit $(3,4)$ the operator given in (147), where

$$\lambda_M = \left(1+\lambda+\sum_{i=1}^{4}\lambda_{z,i}\right) \bmod 2. \tag{161}$$

The $\{\lambda_{x,i}\}$, $\{\lambda_{z,i}\}$ and λ depend linearly on the measurement outcomes $\{s_{(i.j)}\}$ obtained in the first measurement round.

The sub-circuit we have described in this section simulates the unitary evolution according to a particular four-particle Hamiltonian in a two-step process of measurements. The time for which the simulated Hamiltonian acts is encoded in the basis of the measurement in the second round.

The generalization of the simulation of the 4-particle Hamiltonian H_4, shown in Fig. 10, to an arbitrary number n of qubits, i.e. the simulation of the Hamiltonian $H_n = \bigotimes_{i=1}^n \sigma_z^{[i]}$, is straightforward.

C. CNOT between non-neighbouring qubits

The CNOT gate described in Section II G 7 operates on two logical qubits whose input qubits are adjacent to each other on the cluster. However, for universal quantum computation, one must be able to realize a CNOT gate between any two logical qubits. While this could be achieved using a combination of the CNOT gate, introduced above, and the swap gate, the width of the measurement pattern needed to realize this would grow linearly with the separation of the two logical qubits. There

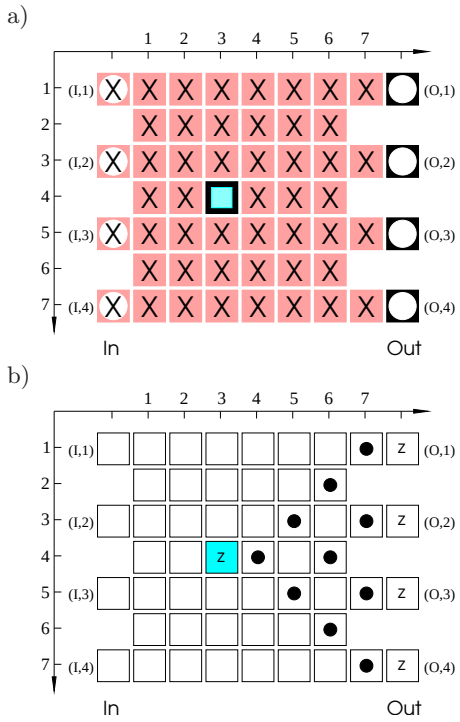


FIG. 10: Simulation of the Hamiltonian H_4 as specified in eq. (146). a) measurement pattern. b) Correlation centers for additional correlation. Shaded squares (in b)) represent cluster qubits measured in adaptive bases.

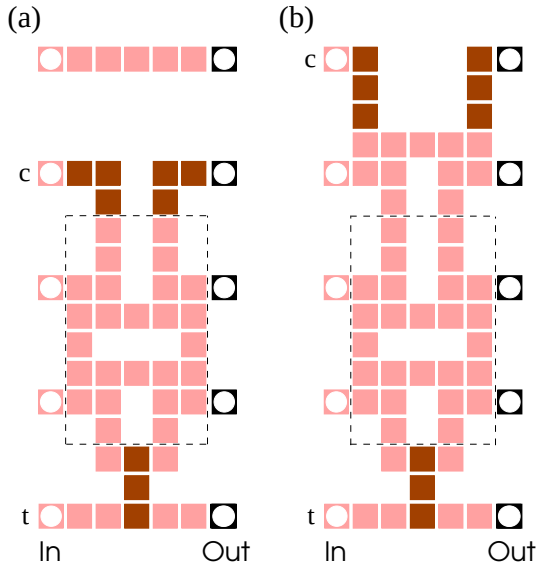


FIG. 11: Measurement pattern for a CNOT gate between two logical qubits whose input and output qubits are not neighbors. Squares in light gray denote cluster qubits measured in the eigenbasis of σ_x, in dark gray of σ_y. Pattern (a) is for the case where the two qubits are separated by an odd number of logical qubits. Pattern (b) is for an even numbered separation. The patterns can be adapted to any separation by repeating the section enclosed by the dashed line. The width of the pattern remains the same for all separations.

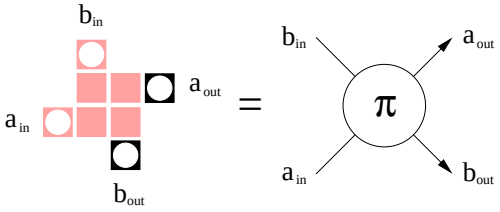


FIG. 12: This measurement pattern is one of the key components of the measurement pattern in Fig. 11. It performs a conditional π-phase-gate and a swap-gate.

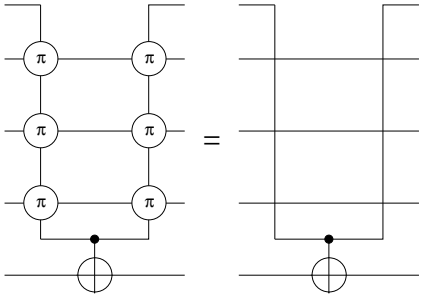


FIG. 13: The measurement pattern in Fig. 11 realizes the quantum logic circuit on the left hand side of this figure. This network is equivalent to the one on the right hand side, where the only gate realized is the CNOT between the two desired non-adjacent qubits.

is, however, an alternative measurement pattern, which, at the cost of doubling the spacing between the input qubits on the cluster, has a fixed width. The measurement pattern is illustrated in Fig. 11 for qubits separated by an odd and even number of logical qubits, respectively.

This layout can be understood within the quantum logic network model. The "wires" for the logical qubits in between the target- and the control qubit are crossed using the measurement sub-pattern illustrated in Fig. 12a. However, as well as swapping the qubits, this pattern also realizes the a controlled π-phase gate, also known as a controlled σ_z gate, illustrated in Fig. 12b.

The quantum logic circuit realized by the whole measurement pattern, illustrated on the left-hand side of Fig. 13 uses these sub-patterns to swap the positions of adjacent qubits. This brings non-neighboring qubits together so that a CNOT operation may be performed on them.

The networks on the left and on the right of Fig. 13 act identically, and thus the measurement pattern displayed in Fig. 11 realizes a distant CNOT-gate.

D. Controlled Phase Gate

Here, we give an example of another two-qubit gate which can be realized without decomposing it into CNOTs and rotations, the controlled phase gate

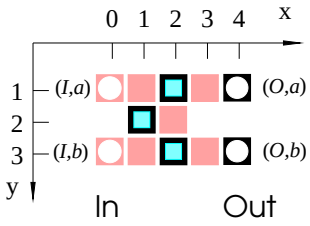


FIG. 14: Controlled phase gate with additional swap.

$U_{\rm CPG}(\theta)$. This gate realizes the unitary operation

$$U_{\rm CPG}[\theta] = \mathbb{1}^{(ab)} + (e^{i\theta} - 1)\,|11\rangle_{ab}\langle 11|, \tag{162}$$

applied to the two qubits a and b.

We can write this in terms of the following one- and two-qubit rotations,

$$U_{\rm CPG}[\theta] = e^{i\frac{\theta}{4}} U_{zz}^{(ab)}[-\theta/2] U_z^{(a)}[\theta/2] U_z^{(b)}[\theta/2], \tag{163}$$

where the two-qubit rotation is

$$U_{zz}^{(ab)}[\theta] = \exp\left(-\mathrm{i}\theta/2 \sigma_z^{(a)}\sigma_z^{(b)}\right). \tag{164}$$

This representation is particularly convenient for finding the measurement pattern that realizes the gate, since rotations $U_z[\theta/2]$ and $U_{zz}[-\theta/2]$ are realized on the $\mathrm{QC}_{\mathcal{C}}$ in a simple natural way. The measurement pattern is illustrated in Fig. 14, in which the labelling of the qubits is also defined.

We follow the same method as above, beginning with the eigenvalue equations of the cluster state $|\phi\rangle_{\mathcal{C}}$ on the qubits shown. The σ_x-measurements can be considered first, using the methods already illustrated in this paper. The resultant state of the remaining qubits $|\psi'\rangle$, after this sub-set of the measurements has been carried out, is defined by the following set of eigenvalue equations.

$$\sigma_x^{(a,I)}\sigma_x^{(1,2)}\sigma_x^{(2,3)}\sigma_x^{(b,O)}|\psi'\rangle = |\psi'\rangle, \tag{165a}$$
$$\sigma_x^{(b,I)}\sigma_x^{(1,2)}\sigma_x^{(2,1)}\sigma_x^{(a,O)}|\psi'\rangle = |\psi'\rangle, \tag{165b}$$
$$\sigma_z^{(a,I)}\sigma_z^{(b,O)}|\psi'\rangle = (-1)^{s_{(1,1)}+s_{(2,2)}+s_{(3,3)}}|\psi'\rangle, \tag{165c}$$
$$\sigma_z^{(b,I)}\sigma_z^{(a,O)}|\psi'\rangle = (-1)^{s_{(1,3)}+s_{(2,2)}+s_{(3,1)}}|\psi'\rangle, \tag{165d}$$

and

$$\sigma_z^{(2,1)}\sigma_z^{(a,O)}|\psi'\rangle = (-1)^{s_{(3,1)}}|\psi'\rangle, \tag{166a}$$
$$\sigma_z^{(2,3)}\sigma_z^{(b,O)}|\psi'\rangle = (-1)^{s_{(3,3)}}|\psi'\rangle, \tag{166b}$$
$$\sigma_z^{(1,2)}\sigma_z^{(a,O)}\sigma_z^{(b,O)}|\psi'\rangle = (-1)^{s_{(3,1)}+s_{(2,2)}+s_{(3,3)}}|\psi'\rangle. \tag{166c}$$

As in section II C 3, eigenvalue equations are now generated which commute with the remaining measurements in $\mathcal{M}$, namely the measurements of $\sigma_{xy}^{(i)}(\alpha_i)$ on qubits

$i \in \{(2,1),(1,2),(2,3)\}$. First, we manipulate the equations (166)such that, for example, the eigenvalue equation (166c) attains the form

$$U_z^{(1,2)}[\xi]\, U_{zz}^{((O,a),(O,b))}\left[-(-1)^{s_{(3,1)}+s_{(2,2)}+s_{(3,3)}}\xi\right]\,|\psi'\rangle = |\psi'\rangle. \tag{167}$$

Similar equations containing one-qubit rotations on qubits $(2,1)$ and (O,a), and $(2,3)$ and (O,b) are derived from the other equations of (166) in the same way. These equations are inserted into both sides of the eigenvalue equations (165) so that, using the method introduced above, we obtain a set of four eigenvalue equations for $|\psi'\rangle$ which induce a set of four eigenvalue equations for the state $|\psi\rangle$ that one obtains after the remaining measurements have been carried out.

Specifically, in the second measurement round the qubits $(1,2)$, $(2,1)$ and $(2,3)$ are measured. Of these qubits one measures the observables

$$\vec{r}_a \cdot \vec{\sigma}^{(a)} = \left(U_z[\alpha_a]\sigma_x U_z[\alpha_a]^\dagger\right)^{(a)}, \tag{168}$$

for $a \in \{(1,2),(2,1),(2,3)\}$ and the $\{\alpha_a\}$ specified below.

The induced eigenvalue equations for the state $|\psi\rangle$ are of the form of equation (82), and the unitary operation realized by the gate can be read off from them using theorem 1. The full unitary operation realized by the measurement pattern is

$$\begin{aligned} U'U'_\Sigma \;=\; & U_{zz}^{(a,b)}\left[-(-1)^{s_{(3,1)}+s_{(2,2)}+s_{(3,3)}}\alpha_{(1,2)}\right]U_z^{(a)}\left[-(-1)^{s_{(3,1)}}\alpha_{(2,1)}\right]U_z^{(b)}\left[-(-1)^{s_{(3,3)}}\alpha_{(2,3)}\right]U_{\rm swap}^{(a,b)} \\ & \left(\sigma_x^{(a)}\right)^{s_{(1,1)}+s_{(2,2)}+s_{(3,3)}}\left(\sigma_x^{(b)}\right)^{s_{(1,3)}+s_{(2,2)}+s_{(3,1)}}\left(\sigma_z^{(a)}\right)^{s_{(I,a)}+s_{(1,2)}+s_{(2,3)}}\left(\sigma_z^{(b)}\right)^{s_{(I,b)}+s_{(2,1)}+s_{(1,2)}} \end{aligned} \tag{169}$$

such that after the order of the gate and the byproduct operator is reversed, $U'U'_\Sigma = U_\Sigma U$, one obtains

$$\begin{aligned} U_\Sigma U \;=\; & \left(\sigma_x^{(a)}\right)^{s_{(1,3)}+s_{(2,2)}+s_{(3,1)}}\left(\sigma_x^{(b)}\right)^{s_{(1,1)}+s_{(2,2)}+s_{(3,3)}}\left(\sigma_z^{(a)}\right)^{s_{(2,1)}+s_{(1,2)}+s_{(I,b)}}\left(\sigma_z^{(b)}\right)^{s_{(I,a)}+s_{(1,2)}+s_{(2,3)}} \\ & U_{zz}^{(a,b)}\left[-(-1)^{s_{(1,1)}+s_{(2,2)}+s_{(1,3)}}\alpha_{(1,2)}\right]U_z^{(a)}\left[-(-1)^{s_{(2,2)}+s_{(1,3)}}\alpha_{(2,1)}\right]U_z^{(b)}\left[-(-1)^{s_{(1,1)}+s_{(2,2)}}\alpha_{(2,3)}\right]U_{\rm swap}^{(a,b)}. \end{aligned} \tag{170}$$

Using (170) one finds the following result: To realize the controlled phase gate (162) together with a swap-gate, the observables (168) measured in the second round have to be chosen with the angles $\alpha_{(2,1)} = (-1)^{1+s_{(2,2)}+s_{(1,3)}}\,\theta/2$, $\alpha_{(1,2)} = (-1)^{s_{(1,1)}+s_{(2,2)}+s_{(1,3)}}\theta/2$ and $\alpha_{(2,3)} = (-1)^{s_{(1,1)}+s_{(2,2)}+1}\,\theta/2$. This realizes the gate $U_\Sigma U_{CPG}[\theta]$, where the byproduct operator U_Σ generated by the measurements may be read off from equation (170).

E. Quantum Fourier transformation

To realize the quantum Fourier transform we simulate the quantum logic network given in Fig. 15a. The arrangement of the gates in this network is taken from [22]. Note that in [22] it was demonstrated that the setup to perform a quantum Fourier transformation simplifies considerably in a situation where the output state is measured right after the transformation. Here, however, the quantum Fourier transformation may constitute part of a larger quantum circuit and we do not measure its output state.

As can be seen from Fig. 15, the quantum Fourier transform consists of Hadamard gates and combined gates which perform a conditional phase shift and a swap. These gates have been discussed in Sections II B and IV D. All that remains to do is put the measurement patterns simulating these gates together, using the network-like composition principle described in Section II D.

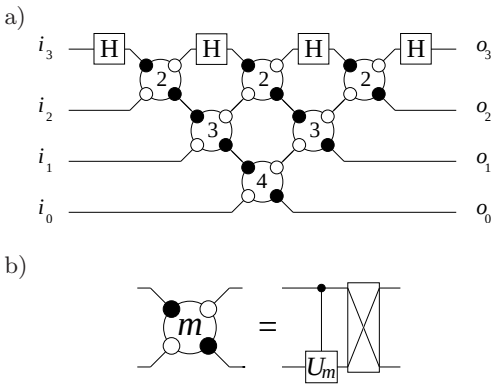


FIG. 15: Quantum Fourier Transformation. a) Network for quantum Fourier transformation on four qubits, taken from [22]. b) Component of the network shown in a) which performs a conditional phase- and a swap-gate. Specifically, the gate shown is $U_{CPG}[2\pi/2^m]$, i.e. $U_m = |0\rangle\langle 0| + e^{i2\pi/2^m}|1\rangle\langle 1|$.

In this way we obtain a measurement pattern in which there are adjacent cluster qubits in "wires" that are measured in the σ_x-eigenbasis. As described in Section II G 2, such pairs of cluster qubits may be removed from the measurement pattern. Note, that by removing adja-

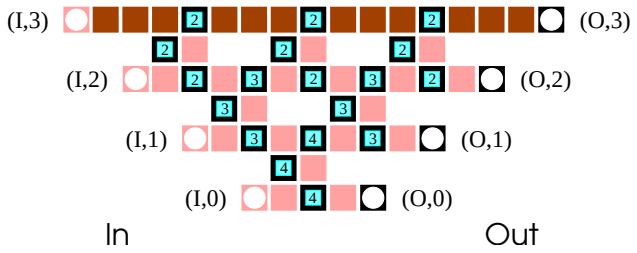


FIG. 16: QC$_{\mathcal{C}}$-realization of a quantum Fourier transformation on four qubits. The cluster qubits displayed as framed squares are measured in adapted bases. For the labels see text.

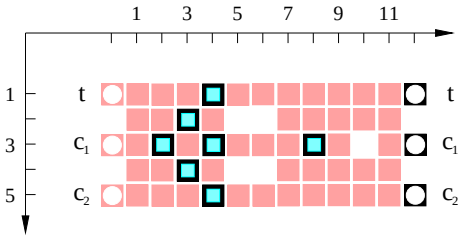


FIG. 17: A measurement layout to realize a Toffoli phase gate with phase ϕ. The qubits marked by black boxes are simultaneously measured in adapted bases depending on previous measurement outcomes.

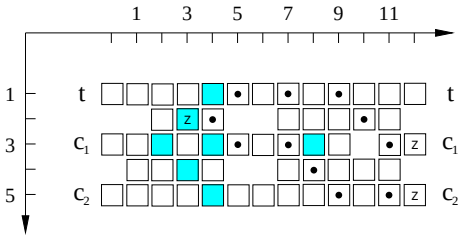


FIG. 18: Cluster state quantum correlations for the realization of $U_{zz}^{(c_1,c_2)}[\phi/4]$, used in the Toffoli phase gate.

cent pairs of σ_x-measured cluster qubits we have moved the σ_y-measurements of the Hadamard transformations "into" the subsequent conditional phase gates, i.e. we removed a cluster qubit which was not from a wire. It can be easily verified that this is an allowed extension of the method described in Section II G 2. Finally, one obtains the QC$_{\mathcal{C}}$-circuit displayed in Fig. 16.

In this circuit, as in all the others, the adaptive measurements are of observables

$$U_z[\pm\eta]\sigma_x U_z[\pm\eta]^\dagger, \tag{171}$$

with $\eta = \pi/4$ for cluster qubits marked with "2" in Fig. 16, $\eta = \pi/8$ for qubits marked with "3" and $\eta = \pi/16$ for the qubits marked with "4". The sign factors of the angles in (171) depend on the results of previous measurements.

The QC$_{\mathcal{C}}$-circuit, shown in Fig. 16 for the case of four qubits, is straightforwardly generalized to an arbitrary number n of logical qubits. The temporal spatial and operational resources T, S and O are, to leading order

$$T = n, \quad S, O = 2n^2. \tag{172}$$

The corresponding network resources are $T_{\rm qln} = 2n$, $S_{\rm qln} = n$ and $O_{\rm qln} = n^2/2$. Thus, the scaling of the QC$_{\mathcal{C}}$ spatial resources is worse than in the network model, but the temporal and operational resources scale in the same way as the corresponding resources for the network. The QC$_{\mathcal{C}}$-simulation of the network displayed in Fig. 15 requires half as many time steps and four times as many operations, albeit only one-qubit operations.

F. Multi-qubit controlled gates

In this section we describe the realization of the Toffoli phase gate and the three-qubit controlled gate *CARRY* which we will both need for the construction of the QC$_{\mathcal{C}}$-adder circuit described in Section IV G.

The Toffoli phase gate is a three-qubit generalization of the two-qubit controlled phase gate. If all three qubits are in the state $|1\rangle$, the state gains a phase of $\exp(i\phi)$, while all other logical basis states remain unchanged by the gate,

$$U_{\rm Toffoli}^{(c_1,c_2,t)}[\phi] = \mathbb{1}^{(c_1,c_2,t)} + (e^{i\phi} - 1)\,|111\rangle_{c_1,c_2,t}\langle 111|. \tag{173}$$

Like the controlled phase gate it can be represented as a product of multi-qubit rotations,

$$\begin{aligned} U_{\rm Toffoli}^{(c_1,c_2,t)}[\phi] = {} & U_{zzz}^{(c_1,c_2,t)}\left[\frac{\phi}{4}\right] U_{zz}^{(c_1,c_2)}\left[-\frac{\phi}{4}\right] U_{zz}^{(c_1,t)}\left[-\frac{\phi}{4}\right] \\ & U_{zz}^{(c_2,t)}\left[-\frac{\phi}{4}\right] U_{z}^{(c_1)}\left[\frac{\phi}{4}\right] U_{z}^{(c_2)}\left[\frac{\phi}{4}\right] U_{z}^{(t)}\left[\frac{\phi}{4}\right]. \end{aligned} \tag{174}$$

where we have dropped the global phase, and $U_{zzz}^{(c_1,c_2,t)}[\alpha] = \exp\left(-i\alpha/2\sigma_z^{(c_1)}\sigma_z^{(c_2)}\sigma_z^{(t)}\right)$ is a three qubit generalized rotation. The two-qubit rotations U_{zz} are as defined in (164).

The way to convert the sequence (174) of generalized rotations into a measurement pattern is as in the examples before. The measurement layout for the Toffoli phase gate is illustrated in Fig. 17. Each of the generalized rotations that make up the gate is directly associated with of one of the measurements made in the eigenbasis of $U_z[\pm\phi/4]\sigma_x U_z[\pm\phi/4]^\dagger$. An initial cluster-state correlations which is used for the realization of a generalized rotation is shown in Fig. 18: the rotation $U_{zz}^{(c_1,c_2)}[\phi/4]$ is realized via the measurement of the cluster qubit at the lattice site $(3,1)$ in the appropriate basis.

The sign factors of the angles that specify the measurement bases depend on the outcome of σ_x-measurements only. Thus, after all σ_x- measurements have been performed, the measurement bases for the remaining qubits

can be deduced and the Toffoli phase-gate is realized in a single further time-step. The measurement pattern realizes the generalized rotations directly and is not derived from a quantum logic network.

Now we describe the realization of a four-qubit gate $CARRY$, which has one target and three control qubits. It performs a phase-flip σ_z on the target if at least two of the control qubits are in state $|1\rangle$ and otherwise does nothing, i.e.

$$U_{CARRY} = \exp\left(-i\pi \sum_{i=000_d \,|\, w(i)\geq 2}^{111_d} |i\rangle_{c_1c_2c_3}\langle i| \otimes |1\rangle_t\langle 1|\right), \tag{175}$$

Expanding the projectors on the control qubits into products of Pauli operators one obtains

$$\begin{aligned} U_{CARRY} \;=\; e^{-i\frac{\pi}{4}} & \underbrace{\exp\left(-i\frac{\pi}{8}\sigma_z^{(t)}\sigma_z^{(c_3)}\right)}_{U_i} \underbrace{\exp\left(-i\frac{\pi}{8}\sigma_z^{(t)}\sigma_z^{(c_2)}\right)}_{U_h} \underbrace{\exp\left(i\frac{\pi}{8}\sigma_z^{(c_3)}\right)}_{U_g} \underbrace{\exp\left(i\frac{\pi}{8}\sigma_z^{(c_2)}\right)}_{U_f} \underbrace{\exp\left(i\frac{\pi}{8}\sigma_z^{(c_1)}\right)}_{U_e} \\ & \underbrace{\exp\left(i\frac{\pi}{4}\sigma_z^{(t)}\right)}_{U_d} \underbrace{\exp\left(-i\frac{\pi}{8}\sigma_z^{(t)}\sigma_z^{(c_1)}\right)}_{U_c} \underbrace{\exp\left(-i\frac{\pi}{8}\sigma_z^{(c_1)}\sigma_z^{(c_2)}\sigma_z^{(c_3)}\right)}_{U_b} \underbrace{\exp\left(i\frac{\pi}{8}\sigma_z^{(t)}\sigma_z^{(c_1)}\sigma_z^{(c_2)}\sigma_z^{(c_3)}\right)}_{U_a}. \end{aligned} \tag{176}$$

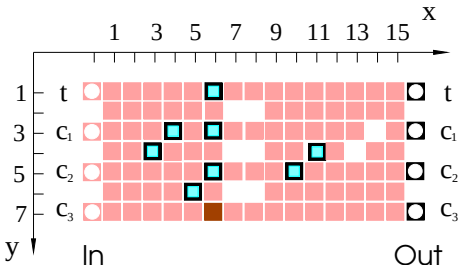


FIG. 19: The three qubit controlled gate. Qubits displayed as squares in light gray are measured in the σ_x-eigenbasis, the qubit displayed in dark gray is measured in the σ_y-eigenbasis, and the measurement bases of the qubits displayed as framed squares are adaptive.

The global phase is henceforth discarded.

The unitary transformation is now subdivided into two parts,

$$U_{CARRY} = U_{h,i}\, U_{a-g}, \tag{177}$$

with $U_{a-g} = U_g U_f U_e U_d U_c U_b U_a$ and $U_{h,i} = U_i U_h$. Correspondingly, the cluster on which U_{CARRY} is realized is divided into two sub-clusters. On the first sub-cluster the transformations U_a to U_g are realized, on the second sub-cluster $U_{h,i}$. The measurement pattern to realize U_{CARRY} is displayed in Fig. 19. The first sub-cluster stretches from $x = 0$ to $x = 8$, with the input at $x = 0$ and the intermediate output at $x = 8$. The qubits with $8 \leq x \leq 16$ belong to the second sub-cluster.

Let us now explain the sub-gate U_{a-g}. The conversion of the sequence (176) of generalized rotations is as in the previous examples. For each generalized rotation there is one cluster qubit in $\mathcal{C}_M(U_{a-g})$ whose measurement basis specifies the respective rotation angle. Specifically, the measurement of the cluster qubit $(3,4)$ sets the rotation angle of U_a, the measurement of qubit $(4,3)$ sets the angle for U_b, $(5,6)$ sets U_c, $(6,7)$ sets U_d, $(6,5)$ sets U_e, $(6,3)$ sets U_f and qubit $(6,1)$ sets U_g. The quantum correlations of the initial cluster state which induce via the measurements of the cluster qubits in $\mathcal{C}_M(U_{a-g})$ the quantum correlations associated with the generalized rotations are displayed in Fig. 20.

The realization of the gate requires two measurement rounds. In the first round the standard measurements of σ_x and σ_y are performed. Note that the rotation angle of U_d is twice as big as for the other rotations. To realize U_d of the cluster qubit $(6,7)$ the observable

$$U_z\left[\pm\frac{\pi}{4}\right]\, \sigma_x U_z\left[\mp\frac{\pi}{4}\right] = \pm\sigma_y \tag{178}$$

is measured. Thus, the realization of U_d belongs to the first round of measurements. Strictly speaking, this measurement round does not belong to the gate but to the circuit as a whole since all standard measurements are performed simultaneously.

In the second measurement round, of the remaining qubits in $\mathcal{C}_M(U_{a-g})$ one measures the observables

$$U_z\left[\pm\frac{\pi}{8}\right]\, \sigma_x U_z\left[\mp\frac{\pi}{8}\right]. \tag{179}$$

The procedure to infer the sign factors in (179) and (178) is explained in Section 11.E.

The reason why the measurements in the tilted bases may all be performed simultaneously in the second round can be seen as follows. Be $Q_\nearrow$ the set of qubits measured in tilted bases. The contribution $U_{\Sigma,Q_\nearrow}$ of the cluster qubits measured in tilted bases to the byproduct operator U_Σ in (84) contains only a z-part but no x-part. That is, it has the form

$$U_{\Sigma,Q_\nearrow} = \bigotimes_{i\in I\subset\{t,c_1,c_2,c_3\}} \sigma_z^{[i]}. \tag{180}$$

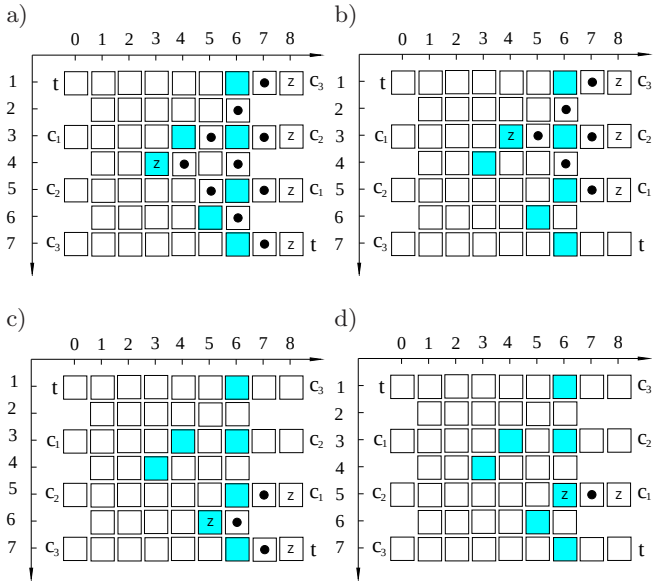


FIG. 20: Quantum correlations of the initial cluster state $|\phi\rangle_{\mathcal{C}(U_{a-g})}$ on the cluster $\mathcal{C}(U_{a-g})$. These correlations induce via the σ_x-measurements the quantum correlations for the state $|\psi'\rangle$ which act only on the output qubits and one cluster qubit in $\mathcal{C}_M(U_{a-g})$. The pattern of correlation centers in a) displays the correlation required to realize U_a; b),c) and d) display the correlations for U_b, U_c and U_e, respectively. The correlations used for the realization of U_d, U_f and U_g are not shown. They are analogous to the one in d) used for the realization of U_e.

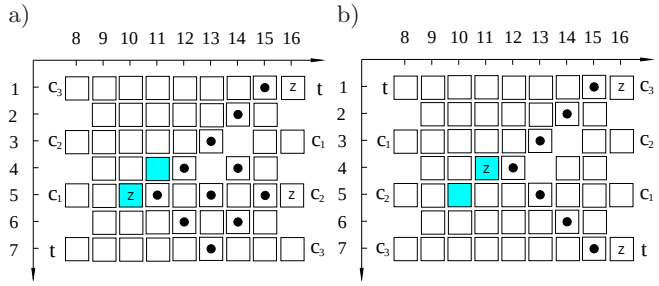


FIG. 21: Quantum correlations of the initial cluster states on $\mathcal{C}(U_h)$ and $\mathcal{C}(U_i)$. These correlations induce, via the σ_x-measurements, the quantum correlations for the states $|\psi'\rangle_{\mathcal{C}(U_h)}$ and $|\psi'\rangle_{\mathcal{C}(U_i)}$ that involve only the respective output qubits and one qubit in the gate body. The pattern of correlation centers in a) displays the correlation required to realize U_h and b) the correlation for U_i.

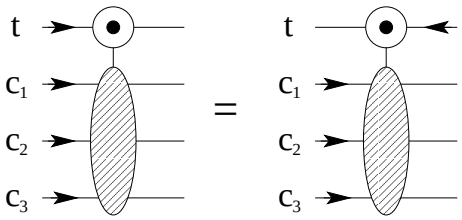


FIG. 22: In the three-qubit controlled gate $CARRY$, the target qubit may travel either back or forth.

In (83) the byproduct operator appears "on the wrong side" of U_{a-g} as does the contribution $U_{\Sigma,Q_\nearrow}$. When the order of the gate and the byproduct operator is exchanged, the byproduct operator may modify the gate. While this is, not surprisingly, indeed the case for the whole U_Σ, it is not so for the contribution $U_{\Sigma,Q_\nearrow}$ coming from the measurements in the tilted bases. Because $U_{\Sigma,Q_\nearrow}$ has only a z-part it commutes with U_{a-g}. Therefore, the results of measurements in a tilted basis do not mutually affect the choice of their measurement bases.

The fact that hat the byproduct operator $U_{\Sigma,Q_\nearrow}$ is indeed of form (180) we do not show here explicitly. For the byproduct operator created in the measurement of qubit $(3,4)$ realizing the transformation U_a it may be verified from equation (157) in Section IV B.

The explanation of the second sub-gate, $U_{h,i}$, is analogous. Fig. 21 displays the quantum correlations of the initial cluster state which, via the measurements in $\mathcal{C}_M(U_{h,i})$, induce the required quantum correlations associated with U_h and U_i.

Two further points we would like to address in this section. The first is to note that the whole gate U_{CARRY} can be performed on the $\mathrm{QC}_\mathcal{C}$ in two measurement rounds. The first measurement round is that of the σ_x-, σ_y- and σ_z-measurements which, strictly speaking, does not belong to the gate but to the circuit as a whole. The second measurement round is that of the simultaneous measurements in tilted measurement bases.

We have already seen that the measurements that realize the unitary transformations $U_a, .., U_g$ may be realized simultaneously, and this argument may be extended to the entire gate U_{CARRY}. All the byproduct operators created with the measurements in tilted bases have only a z- but no x-part. Therefore they all commute with U_{CARRY}. Thus, to choose the right measurement bases neither of the measurements in a tilted basis that realizes one of the rotations $U_a, .., U_i$ needs to wait for another measurement in a tilted basis.

Second, note that the for U_{CARRY} the target-input and the target-output can be interchanged, see Fig. 22. This holds because the (conditional) phase-flip on the target qubit is its own inverse. Thus, the target qubit may travel through the gate backwards. This property also holds for the Toffoli phase gate. We will make use of it in the construction of the quantum adder in the next section.

G. Circuit for addition

The $\mathrm{QC}_\mathcal{C}$-version of the quantum adder corresponds to the quantum logic network as given in [23], see Fig. 23. In this paper we use the three-qubit controlled phase gate

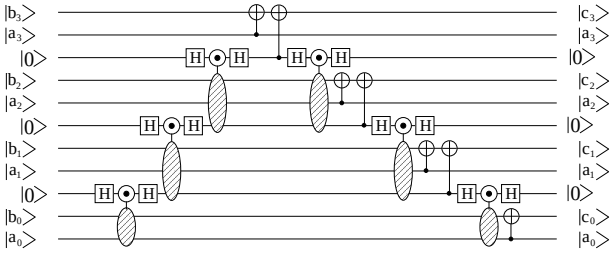


FIG. 23: Quantum logic network for 4-qubit adder, $c = a + b \bmod 2^4$. The adder network is taken from [23]. The two-qubit controlled gate in this network is the Tofolli phase gate as discussed in Section IV F. A straightforward simulation of this network on the $\mathrm{QC}_\mathcal{C}$ would result in a quadratic scaling of spatial resources. However, the more compact realization discussed below requires only a linear overhead.

CARRY together with a prior and subsequent Hadamard gate on the target qubit while in [23] the equivalent three-qubit controlled spin-flip gate is used directly.

At first sight it appears as if the horizontal dimension of the cluster to realize the adder circuit would grow linearly with the number of logical qubits n. This is, however, not the case. The $\mathrm{QC}_\mathcal{C}$-circuit may be formed in such a way that the horizontal size of the required cluster is constant such that the cluster size increases only linearly with the number n of logical qubits. To see what the $\mathrm{QC}_\mathcal{C}$-realization of the quantum adder will look like, the network displayed in Fig. 23 may be bent in a way displayed in Fig. 24.

To "bend a network" is a rather informal notion. We therefore now specify what we mean by this. If a quantum circuit is displayed as a quantum logic network, the vertical axis usually denotes some spatial dimension, i.e. the location of the qubit carriers, and the horizontal axis corresponds to the sequence of steps of a quantum computation, i.e. a logical time. As the basic blocks of quantum computation in the network model, the universal gates, are unitary transformations generated by suitably chosen Hamiltonians the logical time becomes associated with physical time. This is, however, a peculiarity of the network model. If on the $\mathrm{QC}_\mathcal{C}$ a quantum logic network is simulated, the temporal axis is converted into an additional spatial axis. The temporal axis in a $\mathrm{QC}_\mathcal{C}$-computation emerges anew. It has no counterpart in the network model. If we modify a quantum logic network in such a way that qubits travel from right to left, as done in Fig. 24, it does not mean that we propose to use particles that travel backwards in time because we do not need to respect the temporal axis implied by the network model. If one wants a semi-network picture that accounts for this, one may imagine the logical qubits as traveling through pipes on a two-dimensional surface.

The reason why we may let the auxiliary qubits travel "backwards" is the identity displayed in Fig. 22. This arrangement of gates makes the circuit more compact. To complete the description of components from which

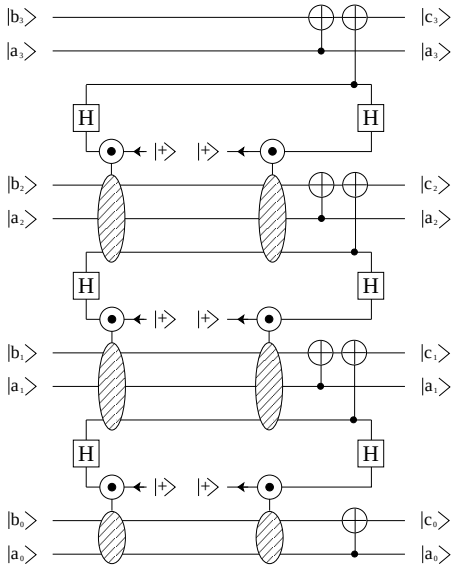


FIG. 24: Quantum logic network for 4-qubit adder, bent.

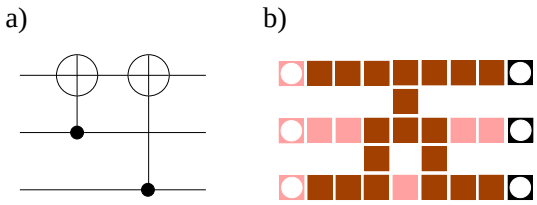


FIG. 25: Combination of two CNOT-gates (a) and its $\mathrm{QC}_\mathcal{C}$-realization (b).

the $\mathrm{QC}_\mathcal{C}$-version of the quantum adder is built, a compact measurement pattern for the two combined CNOT-gates is displayed in Fig. 25.

The realization of the quantum adder in the network layout of Fig. 24 directly leads to the $\mathrm{QC}_\mathcal{C}$-circuit for the quantum adder displayed in Fig. 26. Please note that the displayed $\mathrm{QC}_\mathcal{C}$-adder is for eight qubits while the networks in Figs. 23 and 24 are only for four qubits.

For the quantum adder circuit in Fig. 26 we have made two further minor simplifications. The first concerns the ancilla preparation. To prepare an ancilla qubit on the cluster in the state $|+\rangle$ means to measure the respective cluster qubit in the σ_x-eigenbasis (the randomness of the measurement outcome does not jeopardize the deterministic character of the circuit). As can be seen from the Toffoli gate and the three-qubit controlled gate displayed in Figs. 17 and 19, the ancilla qubits are located on cluster qubits which have only one next neighbor. As can be verified from the eigenvalue equations (11), to measure a qubit of a cluster state which only has one next neighbor in the eigenbasis of σ_x also has the effect of projecting this neighboring cluster qubit into an eigenstate of σ_z. Such cluster qubits may be removed from the cluster as

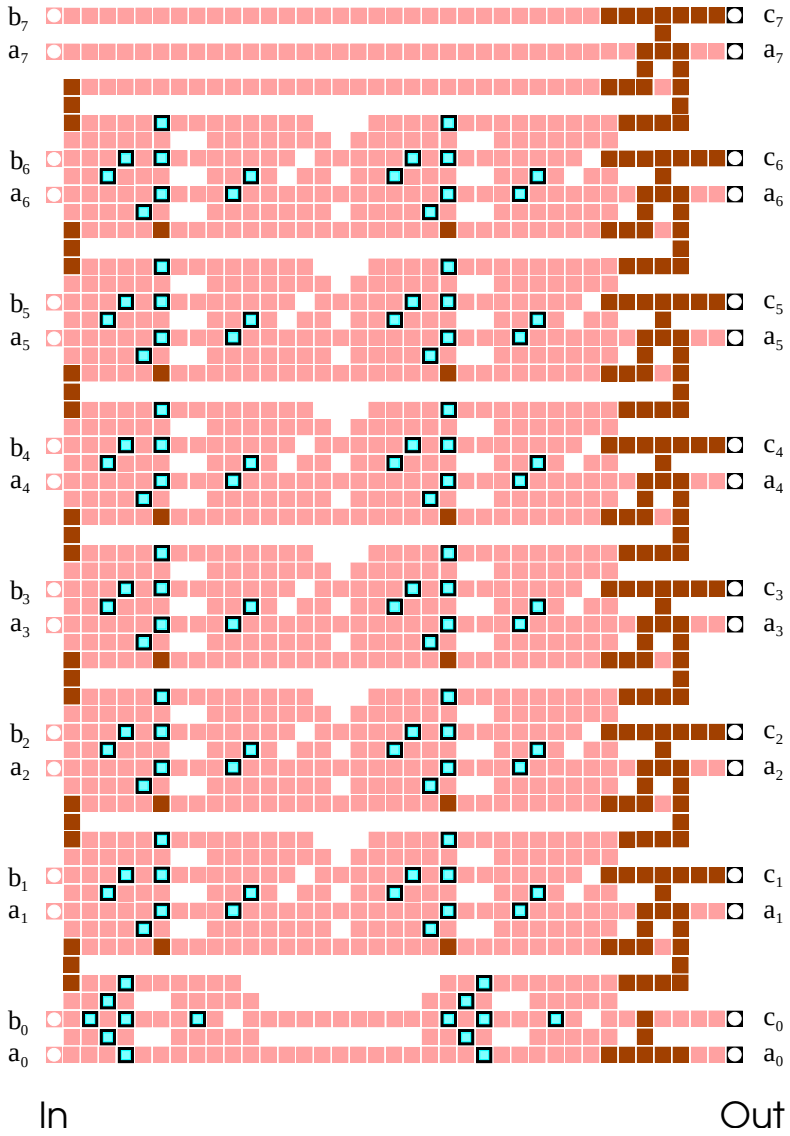


FIG. 26: Quantum adding circuit for two 8-qubit states. As in all figures displaying $\mathrm{QC}_{\mathcal{C}}$-circuits, squares in light and dark gray represent cluster qubits measured in the σ_x- and σ_y-eigenbasis, respectively. The measurement bases of qubits displayed as framed squares are adaptive.

explained in Section II C. With these neighboring qubits removed the cluster qubits on which the initial ancilla qubits were located become disconnected from the remaining cluster and may thus be removed as well. With the same argument, the cluster qubits carrying the ancillas in their output state, and their next neighbors may also be removed.

Second, between the $\mathrm{QC}_{\mathcal{C}}$-realization of the CARRY-gates on the left and the subsequent blocks of CNOT-gates we have removed pairs of adjacent cluster qubits that would be measured in the eigenbasis of σ_x. Why this can be done has been explained for adjacent qubits in wires in Section II G 2. Here the situation is a little more involved since, like in case of the circuit for Fourier transformation displayed in Section IV F, one of the removed qubits in each pair has more than two neighbors. But the method still works as can be easily verified.

Let us now briefly discuss the resources required for the $\mathrm{QC}_{\mathcal{C}}$-realization of an n-qubit adder. As can be seen directly from the circuit displayed in Fig. 26 and the underlying network shown in Fig. 24 with its repeating substructure, the adder requires a cluster of height $8n-5$ and of constant width 38. Thus the spatial and operational resources are, to leading order,

$$S = O = 304\, n. \tag{181}$$

Concerning the temporal resources note that each pair of three-qubit controlled phase gates using the same control qubits and the pair of Toffoli phase gates may be completed at one time instant but that one pair of gates

is completed after another. The reason why the measurements in the tilted bases that complete each pair of gates may be performed simultaneously is the same as the one given previously for the measurements in tilted bases of a single three-qubit controlled gate. The propagation of byproduct operators is most easily followed in the network of Fig. 23. The temporal complexity T of an n-qubit $\mathrm{QC}_{\mathcal{C}}$-adder is

$$T = n, \tag{182}$$

plus one step of σ_x-,σ_y- and σ_z-measurements for the entire circuit.

The corresponding network resources are to leading order $S_{\mathrm{qln}} = 3n$ and $O_{\mathrm{qln}} = T_{\mathrm{qln}} = 8n$. For the counting of the operational and temporal network resources we have assumed that the three-qubit controlled spin-flip gate used in the addition circuit is composed of two Toffoli gates and one CNOT-gate as described in [23], and that the CNOT- and the Toffoli-gate are regarded as elementary.

Thus we find for both the network and the $\mathrm{QC}_{\mathcal{C}}$-realization of the quantum adder that the spatial, temporal and operational resources scale linearly with n. Therefore, the resource overheads in one realization as compared to the other one are only constant. For the $\mathrm{QC}_{\mathcal{C}}$ this is much better than what is indicated by the bounds (138), (139) and (140), in particular for the spatial and operational resources. Equation (139) yields an upper bound on S which is $\sim n^3$ and (140) gives bounds on O and S which are $\sim n^2$. Thus, the quantum adder is an example for which these bounds are very loose. In general they should not be mistaken as estimates.

If the pre-factors are compared, one finds that for the realization of a quantum adder the $\mathrm{QC}_{\mathcal{C}}$ requires about 100 times more spatial and 38 times more operational resources, while it is 8 times faster. However, since we compare different objects these ratios do not mean much apart from the fact that they are constant. It may be argued that in case of the $\mathrm{QC}_{\mathcal{C}}$ spatial resources are not as precious as they usually are, for to create cluster states one needs a system with non-selective uniform interaction only while for quantum logic networks one generally requires a system with selective interactions among the qubits. Concerning the operational and temporal resources, the $\mathrm{QC}_{\mathcal{C}}$ only uses one-qubit measurements while the corresponding network uses two- and three-qubit gates as elementary operations.

H. Remarks

We would like to add two remarks, one with regard to the elementary constituents of the $\mathrm{QC}_{\mathcal{C}}$, and one with regard to their composition principle.

For the particular set of gate simulations used in the $\mathrm{QC}_{\mathcal{C}}$ universality proof in Section II, the CNOT-gate and arbitrary one-qubit rotations, there is only a single instance of where one of these gates has been used as part of a more complicated gate in all examples of this section. Namely, the next-neighbor CNOT-gate has been used as part of the long-distance CNOT described in Section IV C. Of universal gate simulations one might expect that any circuit is composed of them rather that they occur almost not at all. One could say, though, that the used set of gates is not a good choice for the universal set. In fact, in realizations of network quantum computers it is often the physics of the specific implementation that determines which gates are elementary. For the $\mathrm{QC}_{\mathcal{C}}$ this is not so. The $\mathrm{QC}_{\mathcal{C}}$ may simulate, for example, general one-qubit rotations and Toffoli gates alike. Any gate simulation may be called "elementary" with the same right as any other, but they cannot be all elementary. The elementary constituents of the $\mathrm{QC}_{\mathcal{C}}$ are not gate simulations.

As a consequence, the composition principle for these elements will be different from gate composition. At first sight, if we go through the examples of this section, we find that this is not yet reflected in the larger and more complicated constructions. For the quantum Fourier transform and the addition circuit we have, though playing with some tricks, ultimately imitated network composition.

However, in the smaller gates and sub-circuits such as the controlled phase gate, the Toffoli phase gate and the gate $CARRY$ we find something that might give rise to a new and more appropriate composition principle. First, for the $\mathrm{QC}_{\mathcal{C}}$ it is not the one-qubit and two-qubit operations that are particularly simple. In the Hamiltonian simulation circuit of Section IV B we found that it is easy to realize generalized rotations $\exp(i\varphi\,\sigma^{(J)})$ where $\sigma^{(J)}$ is a composite Pauli operator, $\sigma^{(J)} = \bigotimes_{a\in J}\sigma^{(a)}_{k_a}$, $k_a = x, y, z$. Furthermore, in the subsequent examples of the multi-qubit gates in Sections IV D and IV E we have decomposed the gates into such generalized rotations rather than into known standard gates on fewer qubits.

Any unitary transformation may be decomposed into a unitary transformation in the Clifford group followed by generalized rotations. So, is this a new composition principle? With our present state of knowledge, the answer must be "Not yet.". First, though any transformation may be rewritten in this form, it is presently not clear how to design quantum algorithms with these elements directly. Second, the construction uses the very concept of applying unitary transformations to the state of a quantum register. However, as we have explained in [7] and also briefly sketched in Section III A, the $\mathrm{QC}_{\mathcal{C}}$ has no quantum register. So, the generalized rotations and their concatenation at least have to be reformulated to fit the description of the $\mathrm{QC}_{\mathcal{C}}$. In particular, they have to be made compatible with the graph states identified in Section III B as characteristic quantum resource to represent algorithms. Nevertheless, it appears that the generalized rotations should be reflected in what may emerge as elementary constituents and composition principle for the $\mathrm{QC}_{\mathcal{C}}$.

V. COMPUTATION WITH LIMITED SPATIAL RESOURCES AND IN THE PRESENCE OF DECOHERENCE

In this section we describe how to perform $\mathrm{QC}_{\mathcal{C}}$-computation on finite and possibly small clusters. If the cluster that may be provided by a specific device is too small for a certain measurement pattern it does not mean that the respective $\mathrm{QC}_{\mathcal{C}}$-algorithm cannot be run on this device. Instead, the $\mathrm{QC}_{\mathcal{C}}$-computation may be split into several parts such that each of those parts fits on the cluster.

To see this consider Scheme 1 for the realization of gates. Scheme 1 is applicable to any gate or sub-circuit. It is thus possible to divide the circuit into sub-circuits each of which fits onto the cluster. The adapted scheme is a process of repetitive re-entangling steps alternating with rounds of measurements.

Specifically, one starts with the realization of the first sub-circuit acting on the fiducial input state located on $I_1 \subset \mathcal{C}$. The fiducial input is, while being processed, teleported to some subset O_1 of the cluster $\mathcal{C}$. The set O_1 of qubits forms the intermediate output of the first sub-circuit. These qubits remain unmeasured while all the other qubits are measured to realize the first sub-circuit. Now the realization of the second sub-circuit begins. Its input state has already been prepared, $I_2 = O_1$. The cluster qubits $a \in \mathcal{C}\backslash O_1$ which have been measured in the realization of the first sub-circuit are now prepared individually in the state $|+\rangle_a$. This completes step 1 of Scheme 1 to realize the second sub-circuit. Step 2 is to entangle the whole cluster via the Ising interaction. In the third step all cluster qubits except those of the intermediate output O_2 are measured whereby the realization of the second sub-circuit is completed. The intermediate output is now located on O_2. For the realization of the subsequent sub-circuits one proceeds accordingly.

An advantage of this modified procedure is that one gets by with smaller clusters. A disadvantage is that the Clifford part of the circuit may no longer be performed in a single time step.

Perhaps the most important advantage of the above construction is that in this way a basic requirement to make the $\mathrm{QC}_{\mathcal{C}}$ fault-tolerant can be fulfilled. Namely, decoherence can be controlled. If a single large cluster is used the computation might reach certain cluster qubits only after a long time such that the cluster would have already decohered significantly and it is not clear how error-correction could help in such a situation. This might, for any error rate, limit the duration of a computation. On the contrary, if the computation is split then the size of the sub-circuits may be adjusted such that each of them can be performed within a fixed time T and in this way, each cluster qubit is, before being measured, exposed to a bounded amount of decoherence specified by T. Thus, "fresh" qubits for computation are always provided.

VI. CONCLUSION

In this paper we have given a detailed account of the one-way quantum computer. We have shown that the $\mathrm{QC}_{\mathcal{C}}$ can be regarded as a simulator of quantum logic networks. This way, we clarified the relation of the $\mathrm{QC}_{\mathcal{C}}$ to the network model of quantum computation and gave the universality proof.

We have based our description on the correlations exhibited by cluster states, and states that can be created from them under one-qubit measurements. For this purpose, theorem 1 of Section II E is an important tool. It relates unitary transformations to quantum correlations exhibited by certain pure states.

In Section IV we have presented a number of example circuits such as the circuit for quantum Fourier transformation and for addition. In this way, hopefully, we also have acquainted the reader with a number of construction principles for $\mathrm{QC}_{\mathcal{C}}$-circuits. Note that the simulations of the universal gates required in the universality proof are hardly used. Instead, more compact measurement patterns have been found.

The main purpose of this paper has been to provide a comprehensive description of the $\mathrm{QC}_{\mathcal{C}}$ from the network perspective. Beyond that, we have pointed out the non-network aspects of the $\mathrm{QC}_{\mathcal{C}}$, such as the different nature of information processing [7, 8], and the connection to mathematical graphs.

Acknowledgements

This work has been supported by the Deutsche Forschungsgemeinschaft (DFG) and in part by IST-1999-13021. We would like to thank D. Schlingemann, M. Grassl, M. Hein, H. Aschauer, B. Neuburger and H. Wagner for valuable discussions.

APPENDIX A: CLUSTER DECOMPOSITION

In Section II A we have associated the cluster state $|\phi_{\{\kappa\}}\rangle_{\mathcal{C}_N}$ on a cluster $\mathcal{C}_N$ with a graph $G(\mathcal{C}_N, E_{\mathcal{C}_N})$ where the set $E_{\mathcal{C}_N}$ of edges is defined in the same way as in (22) for $E_{\mathcal{C}}$. To decompose the cluster means in more precise terms to decompose the associated graph $G(\mathcal{C}_N, E_{\mathcal{C}_N})$ into subgraphs, that is we decompose both the set of vertices, $\mathcal{C}_N$, and the set of edges, $E_{\mathcal{C}_N}$. As in (48), the set of vertices is decomposed into the subsets $\mathcal{C}(g_i)$, the sub-clusters corresponding to the gates g_i,

$$\mathcal{C}_N = \bigcup_{i=1}^{|\mathcal{N}|} \mathcal{C}(g_i).$$

Herein, the sets $\mathcal{C}(g_i)$ are overlapping. The output vertices of some sub-cluster $\mathcal{C}(g_k)$, corresponding to the output cluster qubits of the gate g_k, form –if they are not the

output vertices of the whole graph– (some of) the input vertices of other sub-clusters $\{\mathcal{C}(g_l)\}$. We define the sets I and O of input and output vertices of $\mathcal{C}_N$, and the set of overlapping vertices $V_{I/O}$ as follows:

$$\begin{aligned} I &= \{a \in \mathcal{C}_N : \exists i \,|\, a \in \mathcal{C}_I(g_i) \wedge \neg\exists j \,|\, a \in \mathcal{C}_O(g_j)\} \\ O &= \{a \in \mathcal{C}_N : \neg\exists i \,|\, a \in \mathcal{C}_I(g_i) \wedge \exists j \,|\, a \in \mathcal{C}_O(g_j)\} \\ V_{I/O} &= \{a \in \mathcal{C}_N : \exists i \,|\, a \in \mathcal{C}_I(g_i) \wedge \exists j \,|\, a \in \mathcal{C}_O(g_j)\}. \end{aligned} \tag{A1}$$

In the same way as we decompose the set of vertices, $\mathcal{C}_N$, into subsets $\mathcal{C}(g_i)$, according to (49), we decompose the set of edges, $E_{\mathcal{C}_N}$, into subsets $E(g_i)$,

$$E_{\mathcal{C}_N} = \bigcup_{i=1}^{|\mathcal{N}|} E(g_i).$$

Now, for the decomposition to be useful, the subsets $\mathcal{C}(g_i)$ and $E(g_i)$ must fulfill a number of constraints. The first of them is that each pair $(\mathcal{C}(g_i), E(g_i))$ is again a graph, $G(\mathcal{C}(g_i), E(g_i))$. As in (51), this requires in particular, that the endpoints of all the edges in $E(g_i)$ are in $\mathcal{C}(g_i)$,

$$\forall\, a \in \mathcal{C}_N \,|\, (\exists e \in E(g_i) \text{ s.th. } a \in e) :\ a \in \mathcal{C}(g_i).$$

This already excludes a cluster $\mathcal{C}_N$ as displayed in Fig. 27a. There, the cluster $\mathcal{C}_N$ is decomposed into sub-clusters $\mathcal{C}(g_1)$ and $\mathcal{C}(g_2)$. But there are edges, namely those which connect $\mathcal{C}(g_2)$ and $\mathcal{C}(g_1)$, which can neither be included in $G(\mathcal{C}(g_1), E(g_1))$ nor $G(\mathcal{C}(g_2), E(g_2))$. Therefore, condition (49) cannot be satisfied and consequently the decomposition of $\mathcal{C}_N$ into $\mathcal{C}(g_1)$ and $\mathcal{C}(g_2)$ is not allowed.

It is necessary to exclude a decomposition as in Fig 27a as the circuit displayed there cannot be understood from its components on the sub-clusters $\mathcal{C}(g_1)$ and $\mathcal{C}(g_2)$. The reason for this is that the cluster states on the sub-clusters $\mathcal{C}(g_1)$ and $\mathcal{C}(g_2)$ are mutually entangled. This is caused by precisely those interactions S^{ab} that correspond to the edges in $E_{\mathcal{C}_N}$ which could not be included in either of the subgraphs.

The central condition (50) is that, in contrast to the sets of vertices $\mathcal{C}(g_i)$, the sets of edges $E(g_i)$ do not overlap,

$$\forall i, j = 1\,..\,|\mathcal{N}|, i \neq j :\ E(g_i) \cap E(g_j) = \emptyset.$$

We need a way to assign the edges to the vertices in the sub-clusters. In this paper, for simplicity we adopt the convention that sets of edges $E(g_i)$ are chosen such that the subgraphs $G(\mathcal{C}(g_i), E(g_i))$ are *induced subgraphs* in $G(\mathcal{C}_N, E_{\mathcal{C}_N})$, i.e.

$$G(\mathcal{C}(g_i), E(g_i)) = G[\mathcal{C}(g_i)]. \tag{A2}$$

As we have overlapping vertices, this simple assignment may run into conflict with condition (50). To avoid this,

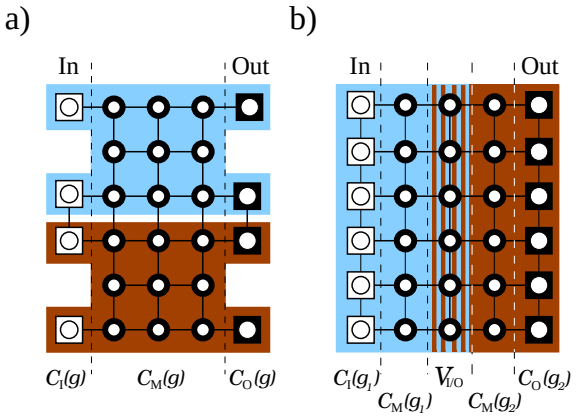


FIG. 27: Two forbidden divisions of a cluster into sub-clusters. The functioning of the 4-qubit gate in a) cannot be understood from the functioning of the two 2-qubit gates on the sub-clusters. The displayed subdivision is excluded by constraint (51). The situation in b) can be treated with a careful assignment of the edges to the subgraphs. In this paper, however, it is excluded for simplicity by the assignment (A2) together with the constraint (A3).

we require that

$$\begin{aligned} G[\mathcal{C}_I(g_i)] &= G(\mathcal{C}_I(g_i)), \emptyset), \text{ and} \\ G[\mathcal{C}_O(g_i)] &= G(\mathcal{C}_O(g_i)), \emptyset),\ \forall\ i = 1\,..\,|\mathcal{N}|. \end{aligned} \tag{A3}$$

That is, the vertices within the sets $\mathcal{C}_I(g_i)$, $\mathcal{C}_O(g_i)$ are not connected by edges.

The assignment convention (A2) together with the condition (A3) exclude decompositions of a cluster like the one displayed in Fig 27b. In principle, however, such a decomposition is possible. In such a case the assignment of the edges to the sub-clusters is not as simple as (A2). Instead, each edge had to be assigned to only one sub-cluster while respecting condition (51). In order to keep the notation as simple as possible, in this paper we do not consider decompositions of the sort displayed in Fig 27b.

The constraints displayed so far applied to the subgraphs. We have two further constraints on the graph $G(\mathcal{C}_N, E_{\mathcal{C}_N})$, with regard to its decomposition. Or, to put it in different terms, the remaining constraints are for the proper composition of the graph out of the subgraphs. They correspond to the usual gate composition rules. We require that each input and output vertex is the input or output vertex of exactly one gate,

$$\begin{aligned} &\forall a \in I \cup V_{I/O} :\ \neg\exists\, i, j \,|\, i \neq j,\ a \in \mathcal{C}_I(g_i) \wedge a \in \mathcal{C}_I(g_j) \\ &\forall a \in O \cup V_{I/O} :\ \neg\exists\, i, j \,|\, i \neq j,\ a \in \mathcal{C}_O(g_i) \wedge a \in \mathcal{C}_O(g_j). \end{aligned} \tag{A4}$$

Further, the graph $G(\mathcal{C}_N, E_{\mathcal{C}_N})$ with the vertices of $I \cup O \cup V_{I/O}$ and associated edges removed disintegrates into mutually disconnected induced subgraphs corresponding

to the gate bodies,

$$G(\mathcal{C}_N, E_{\mathcal{C}_N})\backslash(I \cup O \cup V_{I/O}) = \bigcup_{i=1}^{|\mathcal{N}|} G[\mathcal{C}_M(g_i)]. \qquad \text{(A5)}$$

To summarize, the two central conditions (49) and (50) for the decomposition of the edges $E_{\mathcal{C}_N}$ of the initial graph and the constraint (51) are fulfilled if the subgraphs $G(\mathcal{C}(g_i), E(g_i))$ are chosen in accordance with the assignment (A2) and the constraint (A3). All the examples for $\mathrm{QC}_{\mathcal{C}}$-gate simulations displayed in this paper are of this type.

[*] present address: QOLS, Blackett Laboratory, Imperial College, London, UK

[1] R. Raussendorf and H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[2] H.J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[3] M.A. Nielsen and I.L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[4] D. Gottesman and I.L. Chuang, Nature (London) **402**, 390 (1999).

[5] E. Knill, R. Laflamme and G.J. Milburn, Nature (London) **409**, 46 (2001).

[6] M.A. Nielsen, quant-ph/0108020 (2001), D.W. Leung, quant-ph/0111122 (2001).

[7] R. Raussendorf and H.J. Briegel, Quant. Inf. Comp. **6**, 443 (2002), quant-ph/0108063 (2001).

[8] R. Raussendorf and H.J. Briegel, quant-ph/0207183 (2002).

[9] D. Schlingemann and R.F. Werner, Phys. Rev. **A** 65, 012308 (2001).

[10] T. Rudolph, quant-ph/0206068 (2002).

[11] R. Diestel, *Graphentheorie*, Springer-Verlag (2000).

[12] D. Jaksch *et al.*, Phys. Rev. Lett. **82**, 1975 (1999).

[13] L.-M. Duan, E. Demler, and M.D. Lukin, cond-mat/0210564 (2002).

[14] S. Perdrix, IQUING workshop on Quantum Information, Imperial College London, Sept. 2002.

[15] P.W. Shor, SIAM J. Sci. Statist. Comput. **26**, 1484 (1997).

[16] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[17] C. Moore and M. Nilsson, quant-ph/9808027 (1998).

[18] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[19] Theorem 10.7 in [18].

[20] M. Grassl, A. Klappenecker, and M. Rötteler, *Graphs, Quadratic Forms, and Quantum Codes.* IEEE international symposium on information theory, Lausanne (2001).

[21] D. Schlingemann, private communication (2002).

[22] R.B. Griffiths and C.-S. Niu, Phys. Rev. Lett. **76**, 3228 (1996).

[23] V. Vedral, A. Barenco and A. Ekert, quant-ph/9511018 (1995).

Efficient classical simulation of slightly entangled quantum computations

Guifré Vidal[1]

[1]*Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125, USA*

(Dated: February 1, 2008)

We present a scheme to efficiently simulate, with a classical computer, the dynamics of multipartite quantum systems on which the amount of entanglement (or of correlations in the case of mixed-state dynamics) is conveniently restricted. The evolution of a pure state of n qubits can be simulated by using computational resources that grow linearly in n and exponentially in the entanglement. We show that a pure-state quantum computation can only yield an exponential speed-up with respect to classical computations if the entanglement increases with the size n of the computation, and gives a lower bound on the required growth.

PACS numbers: 03.67.-a, 03.65.Ud, 03.67.Hk

In quantum computation, the evolution of a multipartite quantum system is used to efficiently perform computational tasks that are believed to be intractable with a classical computer. For instance, provided a series of severe technological difficulties are overcome, Shor's quantum algorithm [1] can be used to decompose a large number into its prime factors efficiently —that is, exponentially faster than with any known classical algorithm.

While it is not yet clear what physical resources are responsible for such suspected quantum computational speed-ups, a central observation, as discussed by Feynman [2], is that simulating quantum systems by classical means appears to be hard. Suppose we want to simulate the joint evolution of n interacting spin systems, each one described by a two-dimensional Hilbert space $\mathcal{H}_2$. Expressing the most general pure state $|\Psi\rangle \in {\mathcal{H}_2}^{\otimes n}$ of the n spins already requires specifying about 2^n complex numbers $c_{i_1\cdots i_n}$,

$$|\Psi\rangle = \sum_{i_1=0}^{1}\cdots\sum_{i_n=0}^{1} c_{i_1\cdots i_n}\ |i_1\rangle\otimes\cdots\otimes|i_n\rangle, \qquad (1)$$

where $\{|0\rangle, |1\rangle \in \mathcal{H}_2\}$ denotes a single-spin orthonormal basis; and computing its evolution in time is not any simpler. This exponential overhead of classical computational resources –as compared to the quantum resources needed to directly implement the physical evolution by using n spin systems– strongly suggests that quantum systems are indeed computationally more powerful than classical ones.

On the other hand, some specific quantum evolutions can be efficiently simulated by a classical computer – and therefore cannot yield an exponential computational speed-up. Examples include a system of fermions with only quadratic interactions [3], or a set of two-level systems or qubits initially prepared in a computational-basis state and acted upon by gates from the Clifford group [4]. Recently, Jozsa and Linden [5] have also shown how to efficiently simulate any quantum evolution of an n-qubit system when its state factors, at all times, into a product of states each one involving, at most, a constant (i.e. independent of n) number of qubits.

Here we show how to efficiently simulate, with a classical computer, pure-state quantum dynamics of n entangled qubits, whenever only a restricted amount of entanglement is present in the system. It follows that entanglement is a necessary resource in (pure-state) quantum computational speed-ups. More generally, we establish an upper bound, in terms of the amount of entanglement, for the maximal speed-up a quantum computation can achieve. An analogous upper bound, but in terms of correlations (either classical or quantum), also applies to quantum computations with mixed states.

For simplicity sake the analysis is focused on a computation in the quantum circuit model. Thus we consider a discretized evolution of the n qubits, initially in state $|0\rangle^{\otimes n}$, according to a sequence of poly(n) (i.e., a number polynomial in n) single-qubit and two-qubit gates. We recall, however, that *any* evolution of n qubits according to single-qubit and two-qubit Hamiltonians can be efficiently approximated, with arbitrary accuracy, by the above circuit model, so that the present results also apply to this more general setting [6].

Consider, as in Eq. (1), a pure state $|\Psi\rangle \in {\mathcal{H}_2}^{\otimes n}$ of an n-qubit system. Let A denote a subset of the n qubits and B the rest of them. The Schmidt decomposition SD of $|\Psi\rangle$ with respect to the partition A:B reads

$$|\Psi\rangle = \sum_{\alpha=1}^{\chi_A} \lambda_\alpha |\Phi_\alpha^{[A]}\rangle \otimes |\Phi_\alpha^{[B]}\rangle, \qquad (2)$$

where the vector $|\Phi_\alpha^{[A]}\rangle$ ($|\Phi_\alpha^{[B]}\rangle$) is an eigenvector with eigenvalue $|\lambda_\alpha|^2 > 0$ of the reduced density matrix $\rho^{[A]}$ ($\rho^{[B]}$), whereas the coefficient λ_α follows from the relation $\langle\Phi_\alpha^{[A]}|\Psi\rangle = \lambda_\alpha|\Phi_\alpha^{[B]}\rangle$. The Schmidt rank χ_A is a natural measure of the entanglement between the qubits in A and those in B [7]. Accordingly, we quantify the entanglement of state $|\Psi\rangle$ by χ,

$$\chi \equiv \max_A \chi_A, \qquad (3)$$

that is, by the maximal Schmidt rank over all possible bipartite splittings A:B of the n qubits. We shall say that $|\Psi\rangle$ is only slightly entangled if χ is "small". In particular, here we are interested in sequences of states $\{|\Psi_n\rangle\}$ of

an increasing number n of qubits (corresponding, say, to quantum computations with increasingly large inputs). In such a context we consider χ to be "small" if it grows at most polynomially with n, $\chi_n = \text{poly}(n)$ [8].

Definition.– A pure-state quantum evolution is *slightly entangled* if, at all times t, the state $|\Psi(t)\rangle$ of the system is slightly entangled —that is, if $\chi(t)$ is small. A sequence of evolutions with an increasingly large number n of qubits is *slightly entangled* if $\chi_n(t)$ is upper bounded by $\text{poly}(n)$.

The key ingredient of our simulation protocol is a *local decomposition* of the state $|\Psi\rangle \in {H_2}^{\otimes n}$ in terms of n tensors $\{\Gamma^{[l]}\}_{l=1}^{n}$ and $n-1$ vectors $\{\lambda^{[l]}\}_{l=1}^{n-1}$, denoted

$$|\Psi\rangle \quad \longleftrightarrow \quad \Gamma^{[1]}\lambda^{[1]}\Gamma^{[2]}\lambda^{[2]}\cdots\Gamma^{[l]}\cdots\lambda^{[n-1]}\Gamma^{[n]}. \qquad (4)$$

Here, tensor $\Gamma^{[l]}$ is assigned to qubit l and has (at most) three indices, $\Gamma^{[l]i}_{\alpha\alpha'}$, where $\alpha,\alpha' = 1,\cdots,\chi$ and $i = 0,1$, whereas $\lambda^{[l]}$ is a vector whose components $\lambda^{[l]}_{\alpha'}$ store the Schmidt coefficients of the splitting $[1\cdots l]$:$[(l+1)\cdots n]$. More explicitly, we have [9]

$$c_{i_1 i_2\cdots i_n} = \sum_{\alpha_1,\cdots,\alpha_{n-1}} \Gamma^{[1]i_1}_{\alpha_1}\lambda^{[l]}_{\alpha_1}\Gamma^{[2]i_2}_{\alpha_1\alpha_2}\lambda^{[2]}_{\alpha_2}\cdots\Gamma^{[n]i_n}_{\alpha_{n-1}}. \qquad (5)$$

so that the 2^n coefficients $c_{i_1\cdots i_n}$ are expressed in terms of about $(2\chi^2+\chi)n$ parameters, a number that grows only linearly in n for a fixed value of χ. This decomposition is local in that, as we shall see, when a two-qubit gate is applied to qubits l and $l+1$, only $\Gamma^{[l]}$, $\lambda^{[l]}$ and $\Gamma^{[l+1]}$ need be updated.

Decomposition (4) (but not χ) depends on the particular way qubits have been ordered from 1 to n, and essentially consists of a concatenation of $n-1$ SDs. We first compute the SD of $|\Psi\rangle$ according to the bipartite splitting of the systems into qubit 1 and the $n-1$ remaining qubits [from now on we omit the tensor product symbol],

$$|\Psi\rangle = \sum_{\alpha_1}\lambda^{[1]}_{\alpha_1}|\Phi^{[1]}_{\alpha_1}\rangle|\Phi^{[2\cdots n]}_{\alpha_1}\rangle \qquad (6)$$

$$= \sum_{i_1,\alpha_1}\Gamma^{[1]i_1}_{\alpha_1}\lambda^{[1]}_{\alpha_1}|i_1\rangle|\Phi^{[2\cdots n]}_{\alpha_1}\rangle, \qquad (7)$$

where in the last line we have expanded each Schmidt vector $|\Phi^{[1]}_{\alpha_1}\rangle = \sum_{i_1}\Gamma^{[1]i_1}_{\alpha_1}|i_1\rangle$ in terms of the basis vectors $\{|0\rangle,|1\rangle\}$ for qubit 1. We then proceed according to the following three steps: (i) first we expand each Schmidt vector $|\Phi^{[2\cdots n]}_{\alpha}\rangle$ in a local basis for qubit 2,

$$|\Phi^{[2\cdots n]}_{\alpha_1}\rangle = \sum_{i_2}|i_2\rangle|\tau^{[3\cdots n]}_{\alpha_1 i_2}\rangle; \qquad (8)$$

(ii) then we write each (possibly unnormalized) vector $|\tau^{[3\cdots n]}_{\alpha_1 i_2}\rangle$ in terms of the *at most* χ Schmidt vectors $\{|\Phi^{[3\cdots n]}_{\alpha_2}\rangle\}_{\alpha_2=1}^{\chi}$ (i.e., the eigenvectors of $\rho^{[3\cdots n]}$) and the corresponding Schmidt coefficients $\lambda^{[2]}_{\alpha_2}$,

$$|\tau^{[3\cdots n]}_{\alpha_1 i_2}\rangle = \sum_{\alpha_2}\Gamma^{[2]i_2}_{\alpha_1\alpha_2}\lambda^{[2]}_{\alpha_2}|\Phi^{[3\cdots n]}_{\alpha_2}\rangle; \qquad (9)$$

(iii) finally we substitute Eq. (9) in Eq. (8) and the latter in Eq. (7) to obtain

$$|\Psi\rangle = \sum_{i_1,\alpha_1,i_2,\alpha_2}\Gamma^{[1]i_1}_{\alpha_1}\lambda^{[1]}_{\alpha_1}\Gamma^{[2]i_2}_{\alpha_1\alpha_2}\lambda^{[2]}_{\alpha_2}|i_1 i_2\rangle|\Phi^{[3\cdots n]}_{\alpha_1}\rangle. \qquad (10)$$

Iterating steps (i)-(iii) for the Schmidt vectors $|\Phi^{[3\cdots n]}_{\alpha_2}\rangle$, $|\Phi^{[4\cdots n]}_{\alpha_3}\rangle$, $\cdots$, $|\Phi^{[n]}_{\alpha_{n-1}}\rangle$, one can express state $|\Psi\rangle$ in terms of tensors $\Gamma^{[l]}$ and $\lambda^{[l]}$, as in Eq. (4).

A useful feature of description (4) is that it readily gives the SD of $|\Psi\rangle$ according to the bipartite splitting $[1\cdots l] : [(l+1)\cdots n]$,

$$|\Psi\rangle = \sum_{\alpha_l}\lambda^{[l]}_{\alpha_l}|\Phi^{[1\cdots l]}_{\alpha_l}\rangle|\Phi^{[(l+1)\cdots n]}_{\alpha_l}\rangle. \qquad (11)$$

Indeed, it can be checked by induction over l that

$$|\Phi^{[1\cdots l]}_{\alpha_l}\rangle \longleftrightarrow \Gamma^{[1]}\lambda^{[1]}\cdots\lambda^{[l-1]}\Gamma^{[l]}_{\alpha_l}, \qquad (12)$$

meaning that

$$|\Phi^{[1\cdots l]}_{\alpha_l}\rangle = \sum_{\alpha_1,\cdots,\alpha_{l-1}}\Gamma^{[1]i_1}_{\alpha_1}\lambda^{[1]}_{\alpha_1}\cdots\Gamma^{[l]i_l}_{\alpha_{l-1}\alpha_l}|i_1\cdots i_l\rangle; \qquad (13)$$

whereas by construction we already had that

$$|\Phi^{[(l+1)\cdots n]}_{\alpha_l}\rangle \longleftrightarrow \Gamma^{[l+1]}_{\alpha_l}\lambda^{[l+1]}\cdots\lambda^{[n-1]}\Gamma^{[n]}, \qquad (14)$$

which stands for

$$|\Phi^{[(l+1)\cdots n]}_{\alpha_l}\rangle = \sum_{\alpha_{l+1},\cdots,\alpha_n}\Gamma^{[l+1]i_{l+1}}_{\alpha_l\alpha_{l+1}}\cdots\lambda^{[n-1]}_{\alpha_{n-1}}\Gamma^{[n]i_n}_{\alpha_{n-1}}|i_{l+1}\cdots i_n\rangle. \qquad (15)$$

The following lemmas explain how to update the description of state $|\Psi\rangle$ when a single-qubit gate or a two-qubit gate (acting on consecutive qubits) is applied to the system. Remarkably, the computational cost of the updating is independent of the number n of qubits, and only grows in χ as a polynomial of low degree.

Lemma 1.– Updating the description (4) of state $|\Psi\rangle$ after a unitary operation U acts on qubit l does only involve transforming $\Gamma^{[l]}$. The incurred computational cost is of $\emptyset(\chi^2)$ basic operations.

Proof.– In the SD according to the splitting $[1\cdots(l-1)] : [l\cdots n]$, a unitary operation U on qubit l does not modify the Schmidt vectors for part $[1\cdots(l-1)]$ and therefore $\Gamma^{[j]}$ and $\lambda^{[j]}$ $(1 \le j \le l-1)$ remain the same. Similarly, by considering the SD for the splitting $[1\cdots l] : [(l+1)\cdots n]$, we conclude that also $\Gamma^{[j]}$ and $\lambda^{[j-1]}$ $(l+1 \le j \le n)$ remain unaffected. Instead, $\Gamma^{[l]}$ changes according to

$$\Gamma'^{[l]i}_{\alpha\beta} = \sum_{j=0,1}U^i_j\Gamma^{[l]j}_{\alpha\beta} \qquad \forall\alpha,\beta = 1,\cdots,\chi. \qquad (16)$$

Lemma 2.– Updating the description (4) of state $|\Psi\rangle$ after a unitary operation V acts on qubits l and $l+1$ does only involve transforming $\Gamma^{[l]}$, $\lambda^{[l]}$ and $\Gamma^{[l+1]}$. This can be achieved with $\emptyset(\chi^3)$ basic operations.

Proof.– In order to ease the notation we regard $|\Psi\rangle$ as belonging to only 4 subsystems,

$$\mathcal{H} = \mathcal{J} \otimes \mathcal{H}_C \otimes \mathcal{H}_D \otimes \mathcal{K}. \tag{17}$$

Here, $\mathcal{J}$ is spanned by the χ eigenvectors of the reduced density matrix

$$\rho^{[1\cdots(l-1)]} = \sum_\alpha |\alpha\rangle\langle\alpha|, \quad |\alpha\rangle \equiv \lambda_\alpha^{[l-1]} |\Phi_\alpha^{[1\cdots(l-1)]}\rangle; \tag{18}$$

and, similarly, $\mathcal{K}$ is spanned by the χ eigenvectors of the reduced density matrix

$$\rho^{[(l+2)\cdots n]} = \sum_\gamma |\gamma\rangle\langle\gamma|, \quad |\gamma\rangle \equiv \lambda_\gamma^{[l+1]} |\Phi_\gamma^{[(l+2)\cdots n]}\rangle; \tag{19}$$

whereas $\mathcal{H}_C$ and $\mathcal{H}_D$ correspond, respectively, to qubits l and $l+1$. In this notation we have

$$|\Psi\rangle = \sum_{\alpha,\beta,\gamma=1}^{\chi} \sum_{i,j=0}^{1} \Gamma_{\alpha\beta}^{[C]i} \lambda_\beta \Gamma_{\beta\gamma}^{[D]j} |\alpha i j \gamma\rangle, \tag{20}$$

and, reasoning as in the proof of lemma 1, when applying unitary V to qubits C and D we need only update $\Gamma^{[C]}, \lambda, \Gamma^{[D]}$. We can expand $|\Psi'\rangle \equiv V|\Psi\rangle$ as

$$|\Psi'\rangle = \sum_{\alpha,\gamma=1}^{\chi} \sum_{i,j=0}^{1} \Theta_{\alpha\gamma}^{ij} |\alpha i j \gamma\rangle, \tag{21}$$

where

$$\Theta_{\alpha\gamma}^{ij} = \sum_\beta \sum_{kl} V_{kl}^{ij} \Gamma_{\alpha\beta}^{[C]k} \lambda_\beta \Gamma_{\beta\gamma}^{[D]l}. \tag{22}$$

By diagonalizing $\rho'^{[D\mathcal{K}]}$,

$$\begin{aligned} \rho'^{[D\mathcal{K}]} &= \mathrm{tr}_{\mathcal{J}C} |\Psi'\rangle\langle\Psi'| \qquad (23)\\ &= \sum_{j,j',\gamma,\gamma'} \left(\sum_{\alpha,i} \langle\alpha|\alpha\rangle \Theta_{\alpha\gamma}^{ij} (\Theta_{\alpha\gamma'}^{ij'})^* \right) |j\gamma\rangle\langle j'\gamma'|, \end{aligned}$$

we obtain its eigenvectors $\{|\Phi_\beta'^{[D\mathcal{K}]}\rangle\}$, which we can expand in terms of $\{|j\gamma\rangle\}$ to obtain $\Gamma'^{[D]}$,

$$|\Phi_\beta'^{[D\mathcal{K}]}\rangle = \sum_{j,\gamma} \Gamma_{\beta\gamma}'^{[D]j} |j\gamma\rangle. \tag{24}$$

The eigenvectors of $\rho'^{[\mathcal{J}C]}$ and λ' follow then from

$$\begin{aligned} \lambda_\beta' |\Phi_\beta'^{[\mathcal{J}C]}\rangle &= \langle\Phi_\beta'^{[D\mathcal{K}]}|\Psi'\rangle \qquad (25)\\ &= \sum_{i,j,\alpha,\gamma} (\Gamma_{\beta\gamma}'^{[D]j})^* \Theta_{\alpha\gamma}^{ij} \langle\gamma|\gamma\rangle |\alpha i\rangle, \qquad (26) \end{aligned}$$

and by expanding each $|\Phi_\beta'^{[\mathcal{J}C]}\rangle$,

$$|\Phi_\beta'^{[\mathcal{J}C]}\rangle = \sum_{i\alpha} \Gamma'^{[C]i}_{\alpha\beta} |\alpha i\rangle, \tag{27}$$

we also obtain $\Gamma'^{[C]}$. All the above manipulations can be performed by storing $\emptyset(\chi^2)$ coefficients and require $\emptyset(\chi^3)$ basic operations.

We now state our main results. We consider a pure-state quantum computation using n qubits, and consisting of poly(n) one- and two-qubit gates and a final local measurement. The simulation protocol works as follows. We use tensors $\Gamma^{[l]}$ and $\lambda^{[l]}$ to store the initial state $|0\rangle^{\otimes n}$ and update its description as the gates are applied [10]. Recall that in description (4) each qubit has been associated a position from 1 to n. In order to update $|\Psi\rangle$ according to a two-qubit gate between non-consecutive qubits C and D, we will first simulate $\emptyset(n)$ swap gates between adjacent qubits to bring C and D together. Computing the expectation value for any product operator (e.g. a projection corresponding to a local measurement) from $\{\Gamma^{[l]}, \lambda^{[l]}\}$ is straightforward and can also be done with n poly(χ) operations.

Theorem 1.— If through a pure-state quantum computation χ_n is upper bounded by poly(n), then the computation can be classically simulated with poly(n) memory space and computational time.

Theorem 2.— If χ_n grows subexponentially in n, then the quantum computation can be classically simulated with subexp(n) memory space and computational time.

Thus, theorem 1 provides us with a *sufficient* condition for the efficient classical simulation of a quantum computation, which by extension also applies to generic pure-state, multi-particle unitary dynamics generated by local interactions [6]. In turn theorem 2 provides us with a more general condition under which a quantum computation cannot yield an exponential speed-up with respect to classical computations. Both theorems follow straightforwardly from the previous lemmas and considerations.

The above results establish a clear connection between the amount of entanglement in a multipartite system and the computational cost of simulating the system with a classical computer. This suggests a new approach to the study of multipartite entanglement, based on the complexity of describing and simulating quantum systems. We propose to quantify the entanglement of a pure state $|\Psi\rangle$ through measures that indicate how difficult it is to express $|\Psi\rangle$ in terms of local states or, relatedly, to account for a local change in the system. An example of such entanglement measures is the function

$$E_\chi \equiv \log_2 \chi, \tag{28}$$

which, apart from serving the purposes, has a series of other appealing properties: (i) E_χ only vanishes for product (i.e., unentangled) vectors; (ii) E_χ is additive under tensor products, $E_\chi(\Psi \otimes \Psi') = E_\chi(\Psi) + E_\chi(\Psi')$; (iii) E_χ monotonically decreases under (both deterministic and stochastic) LOCC manipulations of the system. We also note that $E_\chi(\Psi)$ is not a continuous function of $|\Psi\rangle$ with respect any reasonable distance [11].

We can rephrase the results of this paper in terms of E_χ. Notice that the maximum value of E_χ in a system of n particles is *linear* in n. Theorem 1 states that an efficient simulation of quantum dynamics is possible

whenever E_χ grows at most *logarithmically* in n. More generally, we have shown how a state $|\Psi\rangle$ can be given a description in terms of local states by using a number of parameters that grows linearly in the number of systems and exponentially in the amount of entanglement E_χ,

$$\begin{array}{c}\text{local description}\\ \text{of an } n\text{-qubit state}\end{array} \approx \begin{array}{c} n\exp(E_\chi)\\ \text{parameters.}\end{array} \qquad (29)$$

This expression implies an upper bound, in terms of the entanglement, for the computational speed-up a quantum evolution can achieve with respect to classical computations.

So far we have only considered pure-state dynamics. But if the n qubits are in a mixed state $\rho \in \mathcal{B}({\mathcal{H}_2}^{\otimes n})$, we can regard density matrices as vectors in the space of linear operators. By using product expansions and the Schmidt decomposition in this space, one can readily re-derive the above results, but with the former role of entanglement played now by both quantum and classical correlations. Thus, an efficient simulation is possible if the total amount of correlations (as measured by the analog of χ) is sufficiently restricted. In particular, this results do not rule out the possibility of obtaining a computational speed-up through a quantum computation with very noisy mixed states [12].

Finally, [a simple modification of] the simulation protocol discussed in this paper may find practical applications as a tool to study quantum systems [13]. The results of [14] suggest that, at zero temperature, non-critical spin-chains typically meet sufficient conditions for an efficient classical simulation. Perhaps, then, understanding the structure of multipartite entanglement is the key to achieve efficient simulation of certain multipartite quantum phenomena.

The author thanks Dave Bacon, Ignacio Cirac, Ann Harvey and Richard Jozsa and Debbie Leung for valuable advice. Support from the US National Science Foundation under Grant No. EIA-0086038 is acknowledged.

[1] P. Shor, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, 20 to 22 November 1994, S. Goldwasser, Ed. (IEEE Computer Society, Los Alamitos, CA, 1994) p. 124.

[2] R. P. Feynman, Opt. News **11**, 11 (1985): Found. Phys. **16** 507 (1986); Int. J. Theor. Phys. **21**, 467 (1982).

[3] L. Valiant, Proceedings of 33rd STOC, 114-123 (2001). B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A 65, 032325/1-10 (2002).

[4] D. Gottesman, Ph. D. Thesis, 1997 (Caltech, Pasadena).

[5] R. Jozsa and N. Linden, *On the role of entanglement in quantum computational speed-up*, quant-ph/0201143.

[6] A straightforward generalization of the present results is possible to the case of d-level subsystems with m-body interactions, provided d and m do not grow with the total number n of subsystems.

[7] The use of χ_A as a measure of entanglement can be justified by considering a trade-off of non-local resources that becomes possible when subsystems A and B are manipulated using local operations and classical communication LOCC. About $\log_2\chi$ EPR pairs shared between A and B (equivalently, $\log_2\chi$ CNOT gates involving A and B) are necessary and sufficient to prepare $|\Psi\rangle$ with the additional help of LOCC. Also, $\log_2\chi$ is the maximal number of EPR pairs that, with finite probability, can be extracted from $|\Psi\rangle$ by LOCC. The Schmidt rank χ can be shown not to increase (not even probabilistically) under LOCC, as required to any entanglement measure, and is related to the more popular measure *entropy of entanglement* $E(\Psi) \equiv -\mathrm{tr}(\rho_A \log_2 \rho_A)$ [15] through $E(\Psi) \leq \log_2\chi$. Notice that using $E(\Psi)$ to quantify the entanglement of $|\Psi\rangle$ in the present context may not be an appropriate choice, since $E(\Psi)$ refers to asymptotic properties of $|\Psi\rangle$, *i.e.* to properties of $|\Psi\rangle^{\otimes N}$ in the limit $N\to\infty$, whereas here we are concerned with the case $N=1$.

[8] For a general n-qubit state, χ_A is upper bounded by $2^{n/2}$ [value reached when A contains half of the n qubits and, e.g., $|\Psi\rangle$ is maximally entangled between A and B]. Thus, states for which $\chi = \mathrm{poly}(n)$ contain exceptionally little entanglement.

[9] Expansion (5) very much resembles that of a product vector $|\Psi_{prod}\rangle = |\Phi^{[1]}\rangle\otimes\cdots\otimes|\Phi^{[n]}\rangle$, in which case the coefficients $c_{i_1\cdots i_l\cdots i_n} = \Gamma^{[1]i_1}\cdots\Gamma^{[l]i_l}\cdots\Gamma^{[n]i_n}$ can be expressed in terms of tensors $\Gamma^{[l]}$, where $\Gamma^{[l]}$ completely characterizes the pure state $|\Phi^{[l]}\rangle$ of qubit l. The extra indices α's in (5) account for the correlations between qubits.

[10] A digital computer only allows for an approximate description of gates and states, since real coefficients are truncated. See Ref. [5] for a discussion on how to obtain efficient approximations by using rational numbers.

[11] Discontinuity of $E\chi$ implies that a good approximation $|\tilde\Psi\rangle$ to $|\Psi\rangle$ may exists with a significantly lower value of $E\chi$. Correspondingly, a more efficient simulation may be obtained, at the expenses of a tolerable inaccuracy, if we consider *truncated* Schmidt decompositions. That is, for a given $\delta>0$ and any partition $A{:}B$ of the n qubits, we may consider keeping only a number χ_λ of the Schmidt terms in the SD of $|\Psi\rangle$, where χ_δ is determined by requiring that $\sum_{\alpha=1}^{\chi_\delta}|\lambda_\alpha|^2 \geq 1-\delta$. Then, for a small λ, the truncated SD corresponds to a state $|\tilde\Psi\rangle$ very similar to $|\Psi\rangle$ ($|\langle\Psi|\tilde\Psi\rangle|^2 \geq 1-\delta$), but χ_λ may be much smaller than χ. The function $E\chi_\delta = \log_2\chi_\delta$ can then be used to measure the computational cost of simulating quantum dynamics with degree δ of accuracy.

[12] E. Knill, R. Laflamme, Phys. Rev. Lett. **81** (1998) 5672-5675.

[13] G. Vidal, in preparation.

[14] G. Vidal, J. I. Latorre, E. Rico, A. Kitaev, *Entanglement in quantum critical phenomena*, quant-ph/0211074.

[15] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046-2052 (1996).

Cavity quantum electrodynamics for superconducting electrical circuits: an architecture for quantum computation

Alexandre Blais,[1] Ren-Shou Huang,[1,2] Andreas Wallraff,[1] S. M. Girvin,[1] and R. J. Schoelkopf[1]

[1]*Departments of Physics and Applied Physics, Yale University, New Haven, CT 06520*
[2]*Department of Physics, Indiana University, Bloomington, IN 47405*

(Dated: February 2, 2008)

We propose a realizable architecture using one-dimensional transmission line resonators to reach the strong coupling limit of cavity quantum electrodynamics in superconducting electrical circuits. The vacuum Rabi frequency for the coupling of cavity photons to quantized excitations of an adjacent electrical circuit (qubit) can easily exceed the damping rates of both the cavity and the qubit. This architecture is attractive both as a macroscopic analog of atomic physics experiments and for quantum computing and control, since it provides strong inhibition of spontaneous emission, potentially leading to greatly enhanced qubit lifetimes, allows high-fidelity quantum non-demolition measurements of the state of multiple qubits, and has a natural mechanism for entanglement of qubits separated by centimeter distances. In addition it would allow production of microwave photon states of fundamental importance for quantum communication.

PACS numbers: 03.67.Lx, 73.23.Hk, 74.50.+r, 32.80.-t

I. INTRODUCTION

Cavity quantum electrodynamics (cQED) studies the properties of atoms coupled to discrete photon modes in high Q cavities. Such systems are of great interest in the study of the fundamental quantum mechanics of open systems, the engineering of quantum states and the study of measurement-induced decoherence [1, 2, 3], and have also been proposed as possible candidates for use in quantum information processing and transmission [1, 2, 3]. Ideas for novel cQED analogs using nanomechanical resonators have recently been suggested by Schwab and collaborators [4, 5]. We present here a realistic proposal for cQED via Cooper pair boxes coupled to a one-dimensional (1D) transmission line resonator, within a simple circuit that can be fabricated on a single microelectronic chip. As we discuss, 1D cavities offer a number of practical advantages in reaching the strong coupling limit of cQED over previous proposals using discrete LC circuits [6, 7], large Josephson junctions [8, 9, 10], or 3D cavities [11, 12, 13]. Besides the potential for entangling qubits to realize two-qubit gates addressed in those works, in the present work we show that the cQED approach also gives strong and controllable isolation of the qubits from the electromagnetic environment, permits high fidelity quantum non-demolition (QND) readout of multiple qubits, and can produce states of microwave photon fields suitable for quantum communication. The proposed circuits therefore provide a simple and efficient architecture for solid-state quantum computation, in addition to opening up a new avenue for the study of entanglement and quantum measurement physics with macroscopic objects. We will frame our discussion in a way that makes contact between the language of atomic physics and that of electrical engineering.

We begin in Sec. II with a brief general overview of cQED before turning to a discussion of our proposed solid-state realization of cavity QED in Sec. III. We then discuss in Sec. IV the case where the cavity and the qubit are tuned in resonance and in Sec. V the case of large detuning which leads to lifetime enhancement of the qubit. In Sec. VI, a quantum non-demolition read-out protocol is presented. Realization of one-qubit logical operations is discussed in Sec. VII and two-qubit entanglement in Sec. VIII. We show in Sec. IX how to take advantage of encoded universality and decoherence-free subspace in this system.

II. BRIEF REVIEW OF CAVITY QED

Cavity QED studies the interaction between atoms and the quantized electromagnetic modes inside a cavity. In the optical version of cQED [2], schematically shown in Fig. 1(a), one drives the cavity with a laser and monitors changes in the cavity transmission resulting from coupling to atoms falling through the cavity. One can also monitor the spontaneous emission of the atoms into transverse modes not confined by the cavity. It is not generally possible to directly determine the state of the atoms after they have passed through the cavity because the spontaneous emission lifetime is on the scale of nanoseconds. One can, however, infer information about the state of the atoms inside the cavity from real-time monitoring of the cavity optical transmission.

In the microwave version of cQED [3], one uses a very high Q superconducting 3D resonator to couple photons to transitions in Rydberg atoms. Here one does not directly monitor the state of the photons, but is able to determine with high efficiency the state of the atoms after they have passed through the cavity (since the excited state lifetime is of order 30 ms). From this state-selective detection one can infer information about the state of the photons in the cavity.

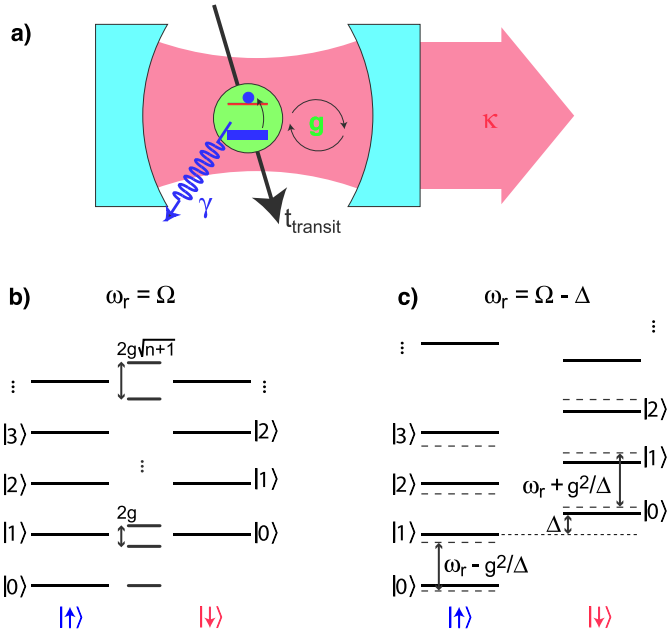


FIG. 1: (color online). a) Standard representation of cavity quantum electrodynamic system, comprising a single mode of the electromagnetic field in a cavity with decay rate κ coupled with a coupling strength $g = \mathcal{E}_{\rm rms}d/\hbar$ to a two-level system with spontaneous decay rate γ and cavity transit time $t_{\rm transit}$. b) Energy spectrum of the uncoupled (left and right) and dressed (center) atom-photon states in the case of zero detuning. The degeneracy of the two-dimensional manifolds of states with $n-1$ quanta is lifted by $2g\sqrt{n+1}$. c) Energy spectrum in the dispersive regime (long dash lines). To second order in g, the level separation is independent of n, but depends on the state of the atom.

The key parameters describing a cQED system (see Table I) are the cavity resonance frequency $\omega_{\rm r}$, the atomic transition frequency Ω, and the strength of the atom-photon coupling g appearing in the Jaynes-Cummings Hamiltonian [14]

$$H = \hbar\omega_{\rm r}\left(a^\dagger a + \frac{1}{2}\right) + \frac{\hbar\Omega}{2}\sigma^z + \hbar g(a^\dagger\sigma^- + a\sigma^+) + H_\kappa + H_\gamma. \tag{1}$$

Here H_κ describes the coupling of the cavity to the continuum which produces the cavity decay rate $\kappa = \omega_{\rm r}/Q$, while H_γ describes the coupling of the atom to modes other than the cavity mode which cause the excited state to decay at rate γ (and possibly also produce additional dephasing effects). An additional important parameter in the atomic case is the transit time $t_{\rm transit}$ of the atom through the cavity.

In the absence of damping, exact diagonalization of the Jaynes-Cumming Hamiltonian yields the excited eigenstates (dressed states) [15]

$$\left|\overline{+,n}\right\rangle = \cos\theta_n\left|\downarrow,n\right\rangle + \sin\theta_n\left|\uparrow,n+1\right\rangle \tag{2}$$
$$\left|\overline{-,n}\right\rangle = -\sin\theta_n\left|\downarrow,n\right\rangle + \cos\theta_n\left|\uparrow,n+1\right\rangle \tag{3}$$

and ground state $|\uparrow,0\rangle$ with corresponding eigenenergies

$$E_{\overline{\pm,n}} = (n+1)\hbar\omega_{\rm r} \pm \frac{\hbar}{2}\sqrt{4g^2(n+1)+\Delta^2} \tag{4}$$
$$E_{\uparrow,0} = -\frac{\hbar\Delta}{2}. \tag{5}$$

In these expressions,

$$\theta_n = \frac{1}{2}\tan^{-1}\left(\frac{2g\sqrt{n+1}}{\Delta}\right), \tag{6}$$

and $\Delta \equiv \Omega - \omega_{\rm r}$ the atom-cavity detuning.

Figure 1b) shows the spectrum of these dressed-states for the case of zero detuning, $\Delta = 0$, between the atom and the cavity. In this situation, degeneracy of the pair of states with n quanta is lifted by $2g\sqrt{n+1}$ due to the atom-photon interaction. In the manifold with a single excitation, Eqs. (2) and (3) reduce to the maximally entangled atom-field states $\left|\overline{\pm,0}\right\rangle = (|\uparrow,1\rangle \pm |\downarrow,0\rangle)/\sqrt{2}$. An initial zero-photon excited atom state $|\uparrow,0\rangle$ will therefore flop into a photon $|\downarrow,1\rangle$ and back again at the vacuum Rabi frequency g/π. Since the excitation is half atom and half photon, the decay rate of $\left|\overline{\pm,0}\right\rangle$ is $(\kappa+\gamma)/2$. The pair of states $\left|\overline{\pm,0}\right\rangle$ will be resolved in a transmission experiment if the splitting $2g$ is larger than this linewidth. The value of $g = \mathcal{E}_{\rm rms}d/\hbar$ is determined by the transition dipole moment d and the rms zero-point electric field of the cavity mode. Strong coupling is achieved when $g \gg \kappa, \gamma$ [15].

For large detuning, $g/\Delta \ll 1$, expansion of Eq. (4) yields the dispersive spectrum shown in Fig. 1c). In this situation, the eigenstates of the one excitation manifold take the form [15]

$$\left|\overline{-,0}\right\rangle \sim -(g/\Delta)\left|\downarrow,0\right\rangle + \left|\uparrow,1\right\rangle \tag{7}$$
$$\left|\overline{+,0}\right\rangle \sim \left|\downarrow,0\right\rangle + (g/\Delta)\left|\uparrow,1\right\rangle. \tag{8}$$

The corresponding decays rates are then simply given by

$$\Gamma_{\overline{-,0}} \simeq (g/\Delta)^2\gamma + \kappa \tag{9}$$
$$\Gamma_{\overline{+,0}} \simeq \gamma + (g/\Delta)^2\kappa. \tag{10}$$

More insight into the dispersive regime is gained by making the unitary transformation

$$U = \exp\left[\frac{g}{\Delta}(a\sigma^+ - a^\dagger\sigma^-)\right] \tag{11}$$

and expanding to second order in g (neglecting damping for the moment) to obtain

$$UHU^\dagger \approx \hbar\left[\omega_{\rm r} + \frac{g^2}{\Delta}\sigma^z\right]a^\dagger a + \frac{\hbar}{2}\left[\Omega + \frac{g^2}{\Delta}\right]\sigma^z. \tag{12}$$

As is clear from this expression, the atom transition is ac-Stark/Lamb shifted by $(g^2/\Delta)(n+1/2)$. Alternatively, one can interpret the ac-Stark shift as a dispersive shift of the cavity transition by $\sigma_z g^2/\Delta$. In other words, the atom pulls the cavity frequency by $\pm g^2/\kappa\Delta$.

parameter	symbol	3D optical	3D microwave	1D circuit
resonance/transition frequency	$\omega_r/2\pi$, $\Omega/2\pi$	350 THz	51 GHz	10 GHz
vacuum Rabi frequency	g/π, g/ω_r	220 MHz, 3×10^{-7}	47 kHz, 1×10^{-7}	100 MHz, 5×10^{-3}
transition dipole	d/ea_0	~ 1	1×10^{3}	2×10^{4}
cavity lifetime	$1/\kappa, Q$	10 ns, 3×10^{7}	1 ms, 3×10^{8}	160 ns, 10^{4}
atom lifetime	$1/\gamma$	61 ns	30 ms	2 μs
atom transit time	$t_{\rm transit}$	$\geq 50\,\mu$s	100 μs	∞
critical atom number	$N_0 = 2\gamma\kappa/g^2$	6×10^{-3}	3×10^{-6}	$\leq 6\times10^{-5}$
critical photon number	$m_0 = \gamma^2/2g^2$	3×10^{-4}	3×10^{-8}	$\leq 1\times10^{-6}$
# of vacuum Rabi flops	$n_{\rm Rabi} = 2g/(\kappa+\gamma)$	~ 10	~ 5	$\sim 10^{2}$

TABLE I: Key rates and cQED parameters for optical [2] and microwave [3] atomic systems using 3D cavities, compared against the proposed approach using superconducting circuits, showing the possibility for attaining the strong cavity QED limit ($n_{\rm Rabi} \gg 1$). For the 1D superconducting system, a full-wave ($L = \lambda$) resonator, $\omega_r/2\pi = 10$ GHz, a relatively low Q of 10^4 and coupling $\beta = C_g/C_\Sigma = 0.1$ are assumed. For the 3D microwave case, the number of Rabi flops is limited by the transit time. For the 1D circuit case, the intrinsic Cooper-pair box decay rate is unknown; a conservative value equal to the current experimental upper bound $\gamma \leq 1/(2\,\mu$s) is assumed.

III. CIRCUIT IMPLEMENTATION OF CAVITY QED

We now consider the proposed realization of cavity QED using superconducing circuits shown in Fig. 2. A 1D transmission line resonator consisting of a full-wave section of superconducting coplanar waveguide plays the role of the cavity and a superconducting qubit plays the role of the atom. A number of superconducting quantum circuits could function as artificial atom, but for definiteness we focus here on the Cooper pair box [6, 16, 17, 18].

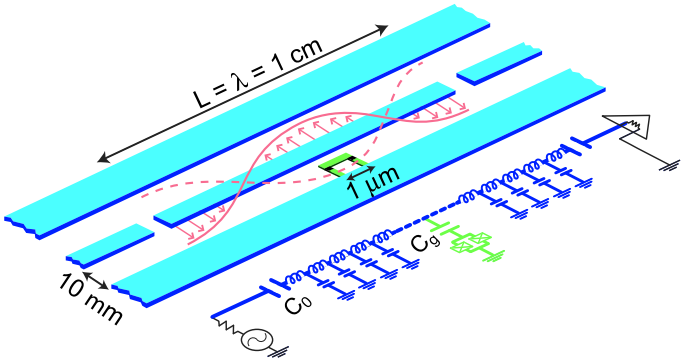


FIG. 2: (color online). Schematic layout and equivalent lumped circuit representation of proposed implementation of cavity QED using superconducting circuits. The 1D transmission line resonator consists of a full-wave section of superconducting coplanar waveguide, which may be lithographically fabricated using conventional optical lithography. A Cooper-pair box qubit is placed between the superconducting lines, and is capacitively coupled to the center trace at a maximum of the voltage standing wave, yielding a strong electric dipole interaction between the qubit and a single photon in the cavity. The box consists of two small ($\sim 100\,$nm$\times 100\,$nm) Josephson junctions, configured in a $\sim 1\,\mu$m loop to permit tuning of the effective Josephson energy by an external flux $\Phi_{\rm ext}$. Input and output signals are coupled to the resonator, via the capacitive gaps in the center line, from 50 Ω transmission lines which allow measurements of the amplitude and phase of the cavity transmission, and the introduction of dc and rf pulses to manipulate the qubit states. Multiple qubits (not shown) can be similarly placed at different antinodes of the standing wave to generate entanglement and two-bit quantum gates across distances of several millimeters.

A. Cavity: coplanar stripline resonator

An important advantage of this approach is that the zero-point energy is distributed over a very small effective volume ($\approx 10^{-5}$ cubic wavelengths) for our choice of a quasi-one-dimensional transmission line 'cavity.' As shown in appendix A, this leads to significant rms voltages $V^0_{\rm rms} \sim \sqrt{\hbar\omega_r/cL}$ between the center conductor and the adjacent ground plane at the antinodal positions, where L is the resonator length and c is the capacitance per unit length of the transmission line. At a resonant frequency of 10 GHz ($h\nu/k_B \sim 0.5\,$K) and for a 10 μm gap between the center conductor and the adjacent ground plane, $V_{\rm rms} \sim 2\,\mu$V corresponding to electric fields $\mathcal{E}_{\rm rms} \sim 0.2\,$V/m, some 100 times larger than achieved in the 3D cavity described in Ref. [3]. Thus, this geometry might also be useful for coupling to Rydberg atoms [19].

In addition to the small effective volume, and the fact that the on-chip realization of cQED shown in Fig. 2 can be fabricated with existing lithographic techniques, a transmission-line resonator geometry offers other practical advantages over lumped LC circuits or current-biased large Josephson junctions. The qubit can be placed within the cavity formed by the transmission line to strongly suppress the spontaneous emission, in contrast to a lumped LC circuit, where without additional special filtering, radiation and parasitic resonances may be induced in the wiring [20]. Since the resonant frequency of

the transmission line is determined primarily by a fixed geometry, its reproducibility and immunity to 1/f noise should be superior to Josephson junction plasma oscillators. Finally, transmission line resonances in coplanar waveguides with $Q \sim 10^6$ have already been demonstrated [21, 22], suggesting that the internal losses can be very low. The optimal choice of the resonator Q in this approach is strongly dependent on the intrinsic decay rates of superconducting qubits which as described below, are presently unknown, but can be determined with the setup proposed here. Here we assume the conservative case of an overcoupled resonator with a $Q \sim 10^4$, which is preferable for the first experiments.

B. Artificial atom: the Cooper pair box

Our choice of 'atom', the Cooper pair box [6, 16] is a mesoscopic superconducting island. As shown in Fig. 3, the island is connected to a large reservoir through a Josephson junction with Josephson energy E_J and capacitance C_J. It is voltage biased from a lead having capacitance C_g to the island. If the superconducting gap is larger than both the charging energy $E_c = e^2/2C_\Sigma$ (where $C_\Sigma = C_J + C_g$ is the total box capacitance) and temperature, the only relevant degree of freedom is the number of Cooper pairs N on the island. In this basis, the Hamiltonian describing the superconducting island takes the form

$$\begin{aligned} H_Q &= 4E_c \sum_N (N - N_g)^2 \left|N\right\rangle \left\langle N\right| \\ &\quad -\frac{E_J}{2} \sum_N \left(\left|N+1\right\rangle \left\langle N\right| + h.c.\right), \end{aligned} \tag{13}$$

where $N_g = C_g V_g / 2e$ is the dimensionless gate charge representing the total polarization charge injected into the island by the voltage source.

In the charge regime, $4E_c \gg E_J$, and restricting the gate charge to the range $N_g \in [0, 1]$, only a pair of adjacent charge states on the island are relevant and the

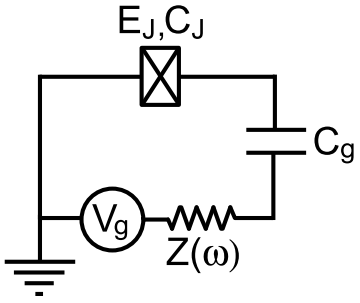


FIG. 3: Circuit diagram of the Cooper pair box. The gate voltage is connected to the island through an environmental impedance $Z(\omega)$.

Hamiltonian then reduces to a 2×2 matrix

$$H_Q = -\frac{E_{\rm el}}{2}\bar{\sigma}^z - \frac{E_J}{2}\bar{\sigma}^x, \tag{14}$$

with $E_{\rm el} = 4E_C(1 - 2N_g)$. The Cooper pair box can in this case be mapped to a pseudo spin-1/2 particle, with effective fields in the x and z directions.

Replacing the Josephson junction by a pair of junctions in parallel each with energy $E_J/2$, the effective field in the x direction becomes $E_J \cos(\pi\Phi_{\rm ext}/\Phi_0)/2$. By threading a flux $\Phi_{\rm ext}$ in the loop formed by the pair of junctions and changing the gate voltage V_g, it is possible to control the effective field acting on the qubit. In the setup of Fig. 2, application of dc gate voltage on the island can be conveniently achieved by applying a bias voltage to the center conductor of the transmission line. The resonator coupling capacitance C_0, the gate capacitance C_g (the capacitance between the center conductor of the resonator and the island) and the capacitance to ground of the resonator then act as a voltage divider.

C. Combined system: superconducting cavity QED

For a superconducting island fabricated inside a resonator, in addition to a dc part $V_{\rm g}^{\rm dc}$, the gate voltage has a quantum part v. As shown in appendix A, if the qubit is placed in the center of the resonator, this latter contribution is given by $v = V^0_{\rm rms}(a^\dagger + a)$. Taking into account both $V_{\rm g}^{\rm dc}$ and v in (14), we obtain

$$\begin{aligned} H_Q &= -2E_C(1 - 2n_g^{\rm dc})\bar{\sigma}^z - \frac{E_J}{2}\bar{\sigma}^x \\ &\quad -e\frac{C_g}{C_\Sigma}\sqrt{\frac{\hbar\omega_{\rm r}}{Lc}}(a^\dagger + a)(1 - 2N_g - \bar{\sigma}^z). \end{aligned} \tag{15}$$

Working in the eigenbasis $\{|\uparrow\rangle, |\downarrow\rangle\}$ of the first two terms of the above expression [23], and adding the Hamiltonian of the oscillator mode coupled to the qubit, the Hamiltonian of the interacting qubit and resonator system takes the form

$$\begin{aligned} H &= \hbar\omega_{\rm r}\left(a^\dagger a + \frac{1}{2}\right) + \frac{\Omega}{2}\sigma^z \\ &\quad -e\frac{C_g}{C_\Sigma}\sqrt{\frac{\hbar\omega_{\rm r}}{Lc}}(a^\dagger + a)(1 - 2N_g - \cos(\theta)\sigma^z + \sin(\theta)\sigma^x). \end{aligned} \tag{16}$$

Here, σ^x and σ^z are Pauli matrices in the eigenbasis $\{|\uparrow\rangle, |\downarrow\rangle\}$, $\theta = \arctan[E_J/4E_C(1 - 2N_g^{\rm dc})]$ is the mixing angle and the energy splitting of the qubit is $\Omega = \sqrt{E_J^2 + [4E_C(1 - 2N_g^{\rm dc})]^2}$ [23]. Note that contrary to the case of a qubit fabricated outside the cavity where the N_g^2 term in (13) has no effect, here this term slightly renormalize the cavity frequency $\omega_{\rm r}$ and displaces the oscillator coordinate. These effects are implicit in Eq. (16).

At the charge degeneracy point (where $N_{\rm g} = C_{\rm g}V_{\rm g}^{\rm dc}/2e = 1/2$ and $\theta = \pi/2$), neglecting rapidly oscillating terms and omitting damping for the moment,

Eq. (16) reduces to the Jaynes-Cummings Hamiltonian (1) with $\Omega = E_J$ and the vacuum Rabi frequency

$$g = \frac{\beta e}{\hbar}\sqrt{\frac{\hbar\omega_r}{cL}}, \qquad (17)$$

where $\beta \equiv C_g/C_\Sigma$. The quantum electrical circuit of Fig. 2 is therefore mapped to the problem of a two-level atom inside a cavity. Away from the degeneracy point, this mapping can still be performed, but with a coupling strength reduced by $\sin\theta$ and an additional term proportional to $(a^\dagger + a)$.

In this circuit, the 'atom' is highly polarizable at the charge degeneracy point, having transition dipole moment $d \equiv \hbar g/\mathcal{E}_{\rm rms} \sim 2\times 10^4$ atomic units (ea_0), or more than an order of magnitude larger than even a typical Rydberg atom [15]. An experimentally realistic [18] coupling $\beta \sim 0.1$ leads to a vacuum Rabi rate $g/\pi \sim 100$ MHz, which is three orders of magnitude larger than in corresponding atomic microwave cQED experiments [3], or approximately 1% of the transition frequency. Unlike the usual cQED case, these artificial 'atoms' remain at fixed positions indefinitely and so do not suffer from the problem that the coupling g varies with position in the cavity.

A comparison of the experimental parameters for implementations of cavity QED with optical and microwave atomic systems and for the proposed implementation with superconducting circuits is presented in Table I. We assume here a relatively low $Q = 10^4$ and a worst case estimate, consistent with the bound set by previous experiments with superconducting qubits (discussed further below), for the intrinsic qubit lifetime of $1/\gamma \geq 2\,\mu$s.

The standard figures of merit [24] for strong coupling are the critical photon number needed to saturate the atom on resonance $m_0 = \gamma^2/2g^2 \leq 1\times 10^{-6}$ and the minimum atom number detectable by measurement of the cavity output $N_0 = 2\gamma\kappa/g^2 \leq 6\times 10^{-5}$. These remarkably low values are clearly very favorable, and show that superconducting circuits could access the interesting regime of very strong coupling.

IV. ZERO DETUNING

In the case of a low Q cavity ($g < \kappa$) and zero detuning, the radiative decay rate of the qubit into the transmission line becomes strongly *enhanced* by a factor of Q relative to the rate in the absence of the cavity [15]. This is due to the resonant enhancement of the density of states at the atomic transition frequency. In electrical engineering language, the $\sim 50\,\Omega$ external transmission line impedance is transformed on resonance to a high value which is better matched to extract energy from the qubit.

For strong coupling $g > \kappa, \gamma$, the first excited state becomes a doublet with line width $(\kappa+\gamma)/2$, as explained in section III. As can be seen from Table I, the coupling

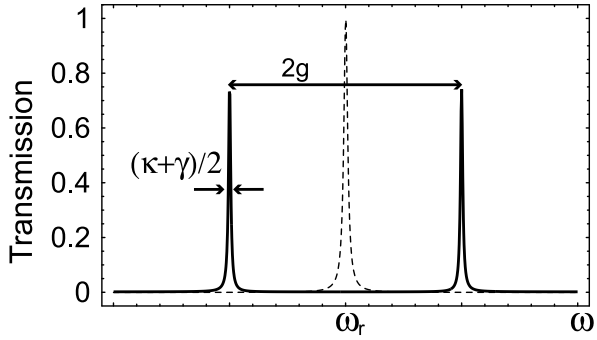


FIG. 4: Expected transmission spectrum of the resonator in the absence (broken line) and presence (full line) of a superconducting qubit biased at its degeneracy point. Parameters are those presented in Table I. The splitting exceeds the line width by two orders of magnitude.

in the proposed superconducting implementation is so strong that, even for the low $Q = 10^4$ we have assumed, $2g/(\kappa+\gamma) \sim 100$ vacuum Rabi oscillations are possible. Moreover, as shown in Fig. 4, the frequency splitting ($g/\pi \sim 100$ MHz) will be readily resolvable in the transmission spectrum of the resonator. This spectrum, calculated here following Ref. [25], can be observed in the same manner as employed in optical atomic experiments, with a continuous wave measurement at low drive, and will be of practical use to find the dc gate voltage needed to tune the box into resonance with the cavity.

Of more fundamental importance than this simple avoided level crossing however, is the fact that the Rabi splitting scales with the square root of the photon number, making the level spacing anharmonic. This should cause a number of novel non-linear effects [14] to appear in the spectrum at higher drive powers when the average photon number in the cavity is large ($\langle n\rangle > 1$).

A conservative estimate of the noise energy for a 10 GHz cryogenic high electron mobility (HEMT) amplifier is $n_{\rm amp} = k_B T_N/\hbar\omega \sim 100$ photons, where T_N is the noise temperature of the amplification circuit. As a result, these spectral features should be readily observable in a measurement time $t_{\rm meas} = 2n_{\rm amp}/\langle n\rangle\kappa$, or only $\sim 32\,\mu$s for $\langle n\rangle \sim 1$.

V. LARGE DETUNING: LIFETIME ENHANCEMENT

For qubits *not* inside a cavity, fluctuation of the gate voltage acting on the qubit is an important source of relaxation and dephasing. As shown in Fig. 3, in practice the qubit's gate is connected to the voltage source through external wiring having, at the typical microwave transition frequency of the qubit, a real impedance of value close to the impedance of free space ($\sim 50\,\Omega$). The relaxation rate expected from purely quantum fluctuations across this impedance (spontaneous emission)

is [18, 23]

$$\frac{1}{T_1} = \frac{E_J^2}{E_J^2 + E_{el}^2} \left(\frac{e}{\hbar}\right)^2 \beta^2 S_V(+\Omega), \tag{18}$$

where $S_V(+\Omega) = 2\hbar\Omega\,\mathrm{Re}[Z(\Omega)]$ is the spectral density of voltage fluctuations across the environmental impedance (in the quantum limit). It is difficult in most experiments to precisely determine the real part of the high frequency environmental impedance presented by the leads connected to the qubit, but reasonable estimates [18] yield values of T_1 in the range of $1\,\mu$s.

For qubits fabricated inside a cavity, the noise across the environmental impedance does not couple directly to the qubit, but only indirectly through the cavity. For the case of strong detuning, coupling of the qubit to the continuum is therefore substantially reduced. One can view the effect of the detuned resonator as filtering out the vacuum noise at the qubit transition frequency or, in electrical engineering terms, as providing an impedance transformation which strongly *reduces* the real part of the environmental impedance seen by the qubit.

Solving for the normal modes of the resonator and transmission lines, including an input impedance R at each end of the resonator, the spectrum of voltage fluctuations as seen by the qubit fabricated in the center of the resonator can be shown to be well approximated by

$$S_V(\Omega) = \frac{2\hbar\omega_r}{Lc} \frac{\kappa/2}{\Delta^2 + (\kappa/2)^2}. \tag{19}$$

Using this transformed spectral density in (18) and assuming a large detuning between the cavity and the qubit, the relaxation rate due to vacuum fluctuations takes a form that reduces to $1/T_1 \equiv \gamma_\kappa = (g/\Delta)^2\kappa \sim 1/(64\,\mu\mathrm{s})$, at the qubit's degeneracy point. This is the result already obtained in Eq. (10) using the dressed state picture for the coupled atom and cavity, except for the additional factor γ reflecting loss of energy to modes outside of the cavity. For large detuning, damping due to spontaneous emission can be much less than κ.

One of the important motivations for this cQED experiment is to determine the various contributions to the qubit decay rate so that we can understand their fundamental physical origins as well as engineer improvements. Besides γ_κ evaluated above, there are two additional contributions to the total damping rate $\gamma = \gamma_\kappa + \gamma_\perp + \gamma_{NR}$. Here $\gamma_\perp$ is the decay rate into photon modes other than the cavity mode, and γ_{NR} is the rate of other (possibly non-radiative) decays. Optical cavities are relatively open and $\gamma_\perp$ is significant, but for 1D microwave cavities, $\gamma_\perp$ is expected to be negligible (despite the very large transition dipole). For Rydberg atoms the two qubit states are both highly excited levels and γ_{NR} represents (radiative) decay out of the two-level subspace. For Cooper pair boxes, γ_{NR} is completely unknown at the present time, but could have contributions from phonons, two-level systems in insulating [20] barriers and substrates, or thermally excited quasiparticles.

For Cooper box qubits *not* inside a cavity, recent experiments [18] have determined a relaxation time $1/\gamma = T_1 \sim 1.3\,\mu$s despite the back action of continuous measurement by a SET electrometer. Vion et al. [17] found $T_1 \sim 1.84\,\mu$s (without measurement back action) for their charge-phase qubit. Thus in these experiments, if there are non-radiative decay channels, they are at most comparable to the vacuum radiative decay rate (and may well be much less) estimated using Eq. (18). Experiments with a cavity will present the qubit with a simple and well controlled electromagnetic environment, in which the radiative lifetime can be enhanced with detuning to $1/\gamma_\kappa > 64\,\mu$s, allowing γ_{NR} to dominate and yielding valuable information about any non-radiative processes.

VI. DISPERSIVE QND READOUT OF QUBIT

In addition to lifetime enhancement, the dispersive regime is advantageous for read-out of the qubit. This can be realized by microwave irradiation of the cavity and then probing the transmitted or reflected photons [26].

A. Measurement Protocol

A drive of frequency $\omega_{\mu w}$ on the resonator can be modeled by [15]

$$H_{\mu w}(t) = \hbar\varepsilon(t)(a^\dagger e^{-i\omega_{\mu w}} + a e^{+i\omega_{\mu w}}), \tag{20}$$

where $\varepsilon(t)$ is a measure of the drive the amplitude. In the dispersive limit, one expects from Fig. 1c) peaks in the transmission spectrum at $\omega_r - g^2/\Delta$ and $\Omega + 2g^2/\Delta$ if the qubit is initially in its ground state. In a frame rotating at the drive frequency, the matrix elements for these transitions are respectively

$$\begin{aligned} \langle\uparrow,0|\, H_{\mu w}\, |\overline{-,n}\rangle &\sim \varepsilon \\ \langle\uparrow,0|\, H_{\mu w}\, |\overline{+,n}\rangle &\sim \frac{\varepsilon g}{\Delta}. \end{aligned} \tag{21}$$

In the large detuning case, the peak at $\Omega + 2g^2/\Delta$, corresponding approximatively to a qubit flip, is highly suppressed.

The matrix element corresponding to a qubit flip from the excited state is also suppressed and, as shown in Fig. 5, depending on the qubit being in its ground or excited states, the transmission spectrum will present a peak of width κ at $\omega_r - g^2/\Delta$ or $\omega_r + g^2/\Delta$. With the parameters of Table II, this dispersive pull of the cavity frequency is $\pm g^2/\kappa\Delta = \pm 2.5$ line widths for a 10% detuning. Exact diagonalization (4) shows that the pull is power dependent and decreases in magnitude for cavity photon numbers on the scale $n = n_{crit} \equiv \Delta^2/4g^2$. In the regime of non-linear response, single-atom optical bistability [14] can be expected when the drive frequency is off resonance at low power but on resonance at high power [29].

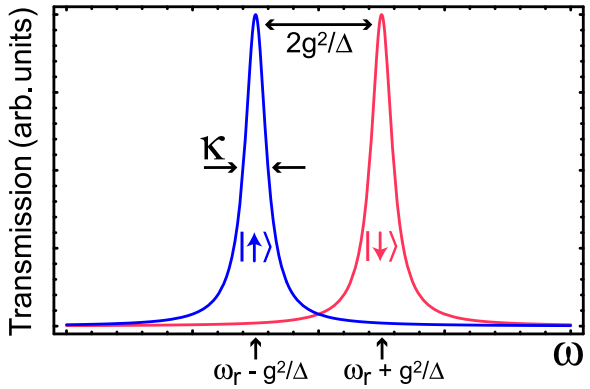


FIG. 5: (color online). Transmission spectrum of the cavity, which is "pulled" by an amount $\pm g^2/\Delta = 2.5 \times 10^{-4} \times \omega_r$, depending on the state of the qubit (red for the excited state, blue for the ground state). To perform a measurement of the qubit, a pulse of microwave photons, at a probe frequency $\omega_{\mu w} = \omega_r$ or $\omega_r \pm g^2/\Delta$ is sent through the cavity. Additional peaks near Ω corresponding to qubit flips are suppressed by g/Δ.

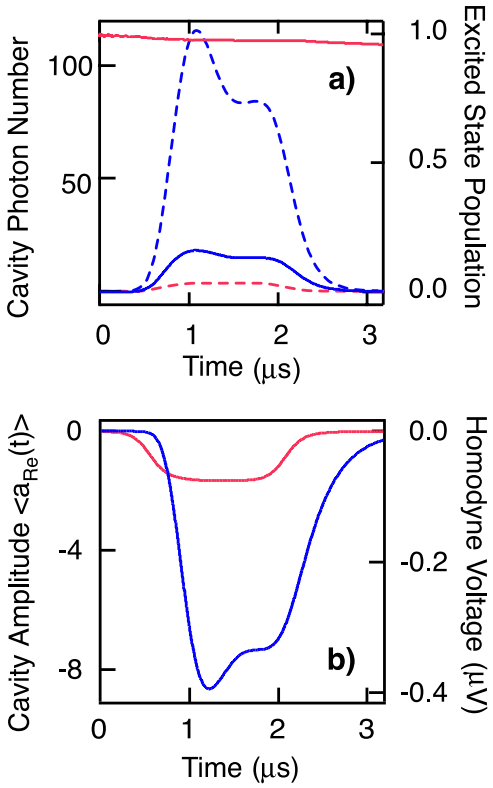


FIG. 6: (color online). Results of numerical simulations using the quantum state diffusion method. A microwave pulse of duration $\sim 15/\kappa$ and centered at the pulled frequency $\omega_r + g^2/\Delta$ drives the cavity. a) The occupation probability of the excited state (right axis), for the case in which the qubit is initially in the ground (blue) or excited (red) state and intracavity photon number (left axis), are shown as a function of time. Though the qubit states are temporarily coherently mixed during the pulse, the probability of real transitions is seen to be small. Depending on the qubit's state, the pulse is either on or away from the combined cavity-qubit resonance, and therefore is mostly transmitted or mostly reflected. b) The real component of the cavity electric field amplitude (left axis), and the transmitted voltage phasor (right axis) in the output transmission line, for the two possible initial qubit states. The parameters used for the simulation are presented in Table I.

The state-dependent pull of the cavity frequency by the qubit can be used to entangle the state of the qubit with that of the photons transmitted or reflected by the resonator. For $g^2/\kappa\Delta > 1$, as in Fig. 5, the pull is greater than the line width and irradiating the cavity at one of the pulled frequencies $\omega_r \pm g^2/\Delta$, the transmission of the cavity will be close to unity for one state of the qubit and close to zero for the other [30].

Choosing the drive to be instead at the bare cavity frequency ω_r, the state of the qubit is encoded in the phase of the reflected and transmitted microwaves. An initial qubit state $|\chi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$ evolves under microwave irradiation into the entangled state $|\psi\rangle = \alpha|\uparrow,\theta\rangle + \beta|\downarrow,-\theta\rangle$, where $\tan\theta = 2g^2/\kappa\Delta$, and $|\pm\theta\rangle$ are (interaction representation) coherent states with the appropriate mean photon number and opposite phases. In the situation where $g^2/\kappa\Delta \ll 1$, this is the most appropriate strategy.

It is interesting to note that such an entangled state can be used to couple qubits in distant resonators and allow quantum communication [31]. Moreover, if an independent measurement of the qubit state can be made, such states can be turned into photon Schrödinger cats [15].

To characterize these two measurement schemes corresponding to two different choices of the drive frequency, we compute the average photon number inside the resonator $\bar{n}$ and the homodyne voltage on the 50Ω impedance at the output of the resonator. Since the power coupled to the outside of the resonator is $P = \langle n\rangle\hbar\omega_r\kappa/2 = \langle V_{out}\rangle^2/R$, the homodyne voltage can be expressed as $\langle V_{out}\rangle = \sqrt{R\hbar\omega_r\kappa}\langle a + a^\dagger\rangle/2$ and is proportional to the real part of the field inside the cavity.

In the absence of dissipation, the time dependence of the field inside the cavity can be obtained in the Heisenberg picture from Eqs. (12) and (20). This leads to a closed set of differential equations for a, σ_z and $a\sigma_z$ which is easily solved. In the presence of dissipation however (i.e. performing the transformation (11) on H_κ and H_γ, and adding the resulting terms to Eqs. (12) and (20)), the set is no longer closed and we resort to numerical stochastic wave function calculations [32].

Figures 6 and 7 show the numerical results for the two choices of drive frequency and using the parameters of Table I. For these calculations, a pulse of duration $\sim 15/\kappa$ with a hyperbolic tangent rise and fall, is used to excite the cavity. Fig. 6 corresponds to a drive at the pulled frequency $\omega_r + g^2/\Delta$. In Fig. 6a) the probability

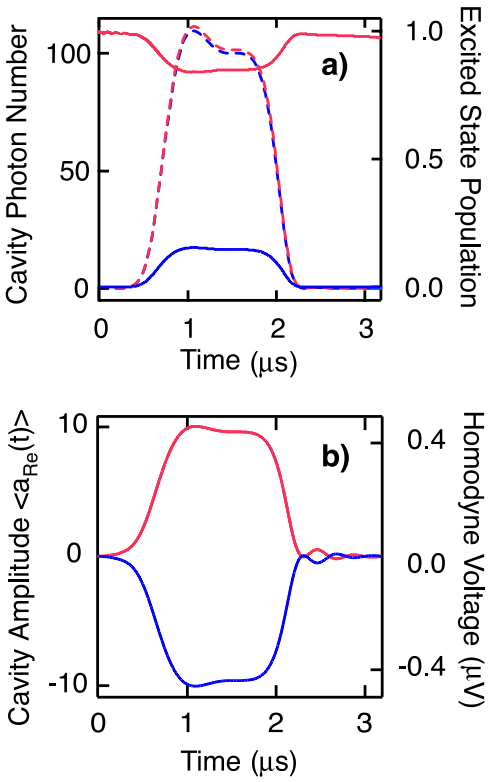


FIG. 7: (color online). Same as Fig. 6 for the drive at the bare cavity frequency ω_r. Depending on the qubit's state, the pulse is either above or below the combined cavity-qubit resonance, and so is partly transmitted and reflected but with a large relative phase shift that can be detected with homodyne detection. In b), the opposing phase shifts cause a change in sign of the output, which can be measured with high signal-to-noise to realize a single-shot, QND measurement of the qubit.

$P_\downarrow$ to find the qubit in its excited state (right axis) is plotted as a function of time for the qubit initially in the ground (blue) or excited state (red). The dashed lines represent the corresponding number of photons in the cavity (left axis). Fig. 6b) shows, in a frame rotating at the drive frequency, the real part of the cavity electric field amplitude (left axis) and transmitted voltage phase (right axis) in the output transmission line, again for the two possible initial qubit states. These quantities are shown in Fig. 7 for a drive at the bare frequency ω_r.

As expected, for the first choice of drive frequency, the information about the state of the qubit is mostly stored in the number of transmitted photons. When the drive is at the bare frequency however, there is very little information in the photon number, with most of the information being stored in the phase of the transmitted and reflected signal. This phase shift can be measured using standard heterodyne techniques. As also discussed in appendix B, both approaches can serve as a high efficiency quantum non-demolition dispersive readout of the state of the qubit.

B. Measurement Time and Backaction

As seen from Eq. (12), the back action of the dispersive cQED measurement is due to quantum fluctuations of the number of photons n within the cavity. These fluctuations cause variations in the ac Stark shift $(g^2/\Delta)n\sigma^z$ that in turn dephase the qubit. It is useful to compute the corresponding dephasing rate and compare it with the measurement rate, i.e. the rate at which information about the state of the qubit can be acquired.

To determine the dephasing rate, we assume that the cavity is driven at the bare cavity resonance frequency and that the pull of the resonance is small compared to the line width κ. The relative phase accumulated between the ground and excited states of the qubit is

$$\varphi(t) = 2\frac{g^2}{\Delta}\int_0^t dt' n(t') \tag{22}$$

which yield a mean phase advance $\langle\varphi\rangle = 2\theta_0 N$ with $\theta_0 = 2g^2/\kappa\Delta$ and $N = \kappa\bar{n}t/2$ the total number of transmitted photons [14]. For weak coupling, the dephasing time will greatly exceed $1/\kappa$ and, in the long time limit, the noise in φ induced by the ac Stark shift will be gaussian. Dephasing can then be evaluated by computing the long time decay of the correlator

$$\begin{aligned}\langle\sigma^+(t)\sigma^-(0)\rangle &= \langle e^{i\int_0^t dt'\varphi(t')}\rangle \\ &\simeq e^{-\frac{1}{2}\left(2\frac{g^2}{\Delta}\right)^2\int_0^t\int_0^t dt_1 dt_2\langle n(t_1)n(t_2)\rangle}.\end{aligned} \tag{23}$$

To evaluate this correlator in the presence of a continuous-wave (CW) drive on the cavity, we first perform a canonical transformation on the cavity operators $a^{(\dagger)}$ by writing them in terms of a classical $\alpha^{(*)}$ and a quantum part $d^{(\dagger)}$:

$$a(t) = \alpha(t) + d(t). \tag{24}$$

Under this transformation, the coherent state obeying $a|\alpha\rangle = \alpha|\alpha\rangle$, is simply the vacuum for the operator d. It is then easy to verify that

$$\langle(n(t)-\bar{n})(n(0)-\bar{n})\rangle = \alpha^2\langle d(t)d^\dagger(0)\rangle = \bar{n}e^{-\frac{\kappa}{2}|t|}. \tag{25}$$

It is interesting to note that the factor of 1/2 in the exponent is due to the presence of the coherent drive. If the resonator is not driven, the photon number correlator rather decays at a rate κ. Using this result in (23) yields the dephasing rate

$$\Gamma_\varphi = 4\theta_0^2\frac{\kappa}{2}\bar{n}. \tag{26}$$

Since the rate of transmission on resonance is $\kappa\bar{n}/2$, this means that the dephasing per transmitted photon is $4\theta_0^2$.

To compare this result to the measurement time $T_{\rm meas}$, we imagine a homodyne measurement to determine the transmitted phase. Standard analysis of such an interferometric set up [14] shows that the minimum phase change

which can be resolved using N photons is $\delta\theta = 1/\sqrt{N}$. Hence the measurement time to resolve the phase change $\delta\theta = 2\theta_0$ is

$$T_{\rm m} = \frac{1}{2\kappa\bar{n}\theta_0^2}, \tag{27}$$

which yields

$$T_{\rm m}\Gamma_\varphi = 1. \tag{28}$$

This exceeds the quantum limit [33] $T_{\rm m}\Gamma_\varphi = 1/2$ by a factor of 2. Equivalently, in the language of Ref. [34] (which uses a definition of the measurement time twice as large as that above) the efficiency ratio is $\chi \equiv 1/(T_{\rm m}\Gamma_\varphi) = 0.5$.

The failure to reach the quantum limit can be traced [35] to the fact that that the coupling of the photons to the qubit is not adiabatic. A small fraction $R \approx \theta_0^2$ of the photons incident on the resonator are reflected rather than transmitted. Because the phase shift of the reflected wave [14] differs by π between the two states of the qubit, it turns out that, despite its weak intensity, the reflected wave contains precisely the same amount of information about the state of the qubit as the transmitted wave which is more intense but has a smaller phase shift. In the language of Ref. [34], this 'wasted' information accounts for the excess dephasing relative to the measurement rate. By measuring also the phase shift of the reflected photons, it could be possible to reach the quantum limit.

Another form of possible back action is mixing transitions between the two qubit states induced by the microwaves. First, as seen from Fig. 6a) and 7a), increasing the average number of photons in the cavity induces mixing. This is simply caused by dressing of the qubit by the cavity photons. Using the dressed states (2) and (3), the level of this coherent mixing can be estimated as

$$P_{\downarrow,\uparrow} = \frac{1}{2}\langle\overline{\pm,n}|\,\mathbb{1} \pm \sigma^z\,|\overline{\pm,n}\rangle \tag{29}$$

$$= \frac{1}{2}\left(1 \pm \frac{\Delta}{\sqrt{4g^2(n+1)+\Delta^2}}\right) \tag{30}$$

Exciting the cavity to $n = n_{\rm crit}$, yields $P_\downarrow \sim 0.85$. As is clear from the numerical results, this process is completely reversible and does not lead to errors in the readout.

The drive can also lead to real transitions between the qubit states. However, since the coupling is so strong, large detuning $\Delta = 0.1\,\omega_{\rm r}$ can be chosen, making the mixing rate limited not by the frequency spread of the drive pulse, but rather by the width of the qubit excited state itself. The rate of driving the qubit from ground to excited state when n photons are in the cavity is $R \approx n(g/\Delta)^2\gamma$. If the measurement pulse excites the cavity to $n = n_{\rm crit}$, we see that the excitation rate is still only 1/4 of the relaxation rate. As a result, the main limitation on the fidelity of this QND readout is the decay of the excited state of the qubit during the course of the readout. This occurs (for small γ) with probability $P_{\rm relax} \sim \gamma t_{\rm meas} \sim 15 \times \gamma/\kappa \sim 3.75\,\%$ and leads to a small error $P_{\rm err} \sim 5\gamma/\kappa \sim 1.5\,\%$ in the measurement, where we have taken $\gamma = \gamma_\kappa$. As confirmed by the numerical calculations of Fig. 6 and 7, this dispersive measurement is therefore highly non-demolition.

C. Signal-to-Noise

For homodyne detection in the case where the cavity pull $g^2/\Delta\kappa$ is larger than one, the signal-to-noise ratio (SNR) is given by the ratio of the number of photons $n_{\rm sig} = n\kappa\Delta t/2$ accumulated over an integration period Δt, divided by the detector noise $n_{\rm amp} = k_B T_N/\hbar\omega_{\rm r}$. Assuming the integration time to be limited by the qubit's decay time $1/\gamma$ and exciting the cavity to a maximal amplitude $n_{\rm crit} = 100 \sim n_{\rm amp}$, we obtain SNR $= (n_{\rm crit}/n_{\rm amp})(\kappa/2\gamma)$. If the qubit lifetime is longer than a few cavity decay times ($1/\kappa = 160\,$ns), this SNR can be very large. In the most optimistic situation where $\gamma = \gamma_\kappa$, the signal-to-noise ratio is SNR=200.

When taking into account the fact that the qubit has a finite probability to decay during the measurement, a better strategy than integrating the signal for a long time is to take advantage of the large SNR to measure quickly. Simulations have shown that in the situation where $\gamma = \gamma_\kappa$, the optimum integration time is roughly 15 cavity lifetimes. This is the pulse length used for the stochastic numerical simulations shown above. The readout fidelity, including the effects of this stochastic decay, and related figures of merit of the single-shot high efficiency QND readout are summarized in Table II.

This scheme has other interesting features that are worth mentioning here. First, since nearly all the energy used in this dispersive measurement scheme is dissipated in the remote terminations of the input and output transmission lines, it has the practical advantage of avoiding quasiparticle generation in the qubit.

Another key feature of the cavity QED readout is that it lends itself naturally to operation of the box at the charge degeneracy point ($N_g = 1/2$), where it has been shown that T_2 can be enormously enhanced [17] because the energy splitting has an extremum with respect to gate voltage and isolation of the qubit from 1/f dephasing is optimal. The derivative of the energy splitting with respect to gate voltage is the charge difference in the two qubit states. At the degeneracy point this derivative vanishes and the environment cannot distinguish the two states and thus cannot dephase the qubit. This also implies that a charge measurement cannot be used to determine the state of the system [4, 5]. While the first derivative of the energy splitting with respect to gate voltage vanishes at the degeneracy point, the second derivative, corresponding to the difference in charge *polarizability* of the two quantum states, is *maximal*. One can think of the qubit as a non-linear quantum system having a state-dependent capacitance (or in general, an admit-

parameter	symbol	1D circuit
dimensionless cavity pull	$g^2/\kappa\Delta$	2.5
cavity-enhanced lifetime	$\gamma_\kappa^{-1} = (\Delta/g)^2\kappa^{-1}$	64 μs
readout SNR	SNR $= (n_{\rm crit}/n_{\rm amp})\kappa/2\gamma$	200 (6)
readout error	$P_{\rm err} \sim 5\times\gamma/\kappa$	1.5 % (14%)
1 bit operation time	$T_\pi > 1/\Delta$	> 0.16 ns
entanglement time	$t_{\sqrt{i\rm SWAP}} = \pi\Delta/4g^2$	~ 0.05 μs
2 bit operations	$N_{\rm op} = 1/[\gamma\, t_{\sqrt{i\rm SWAP}}]$	> 1200 (40)

TABLE II: Figures of merit for readout and multi-qubit entanglement of superconducting qubits using dispersive (off-resonant) coupling to a 1D transmission line resonator. The same parameters as Table 1, and a detuning of the Cooper pair box from the resonator of 10% ($\Delta = 0.1\,\omega_{\rm r}$), are assumed. Quantities involving the qubit decay γ are computed both for the theoretical lower bound $\gamma = \gamma_\kappa$ for spontaneous emission via the cavity, and (in parentheses) for the current experimental upper bound $1/\gamma \geq 2\,\mu$s. Though the signal-to-noise of the readout is very high in either case, the estimate of the readout error rate is dominated by the probability of qubit relaxation during the measurement, which has a duration of a few cavity lifetimes ($\sim 1-10\ \kappa^{-1}$). If the qubit non-radiative decay is low, both high efficiency readout and more than 10^3 two-bit operations could be attained.

tance) which changes sign between the ground and excited states [36]. It is this change in polarizability which is measured in the dispersive QND measurement.

In contrast, standard charge measurement schemes [18, 37] require moving away from the optimal point. Simmonds et al. [20] have recently raised the possibility that there are numerous parasitic environmental resonances which can relax the qubit when its frequency Ω is changed during the course of moving the operating point. The dispersive cQED measurement is therefore highly advantageous since it operates best at the charge degeneracy point. In general, such a measurement of an ac property of the qubit is strongly desirable in the usual case where dephasing is dominated by low frequency (1/f) noise. Notice also that the proposed quantum non-demolition measurement would be the inverse of the atomic microwave cQED measurement in which the state of the photon field is inferred non-destructively from the phase shift in the state of atoms sent through the cavity [3].

VII. COHERENT CONTROL

While microwave irradiation of the cavity at its resonance frequency constitutes a measurement, irradiation close to the qubit's frequency can be used to coherently control the state of the qubit. In the former case, the phase shift of the transmitted wave is strongly dependent on the state of the qubit and hence the photons become entangled with the qubit, as shown in Fig. 8. In the latter case however, driving is *not* a measurement because, for large detuning, the photons are largely reflected with a phase shift which is independent of the state of the qubit. There is therefore little entanglement between the field and the qubit in this situation and the rotation fidelity is high.

To model the effect of the drive on the qubit, we add the microwave drive of Eq. (20) to the Jaynes-Cumming Hamiltonian (11) and apply the transformation (11) (again neglecting damping) to obtain the following effective one-qubit Hamiltonian

$$H_{1q} = \frac{\hbar}{2}\left[\Omega + 2\frac{g^2}{\Delta}\left(a^\dagger a + \frac{1}{2}\right) - \omega_{\mu w}\right]\sigma^z + \hbar\frac{g\varepsilon(t)}{\Delta}\sigma^x + \hbar(\omega_{\rm r} - \omega_{\mu w})a^\dagger a + \hbar\varepsilon(t)(a^\dagger + a), \quad (31)$$

in a frame rotating at the drive frequency $\omega_{\mu w}$. Choosing $\omega_{\mu w} = \Omega + (2n+1)g^2/\Delta$, H_{1q} generates rotations of the qubit about the x axis with Rabi frequency $g\varepsilon/\Delta$.

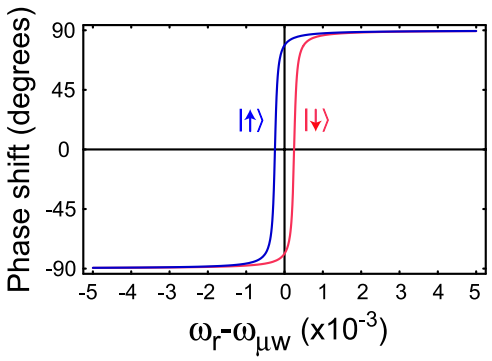


FIG. 8: (color online). Phase shift of the cavity field for the two states of the qubit as a function of detuning between the driving and resonator frequencies. Obtained from the steady-state solution of the equation of motion for $a(t)$ while only taking into account damping on the cavity and using the parameters of Table II. Read-out of the qubit is realized at, or close to, zero detuning between the drive and resonator frequencies where the dependence of the phase shift on the qubit state is largest. Coherent manipulations of the qubit are realized close to the qubit frequency which is 10% detuned from the cavity (not shown on this scale). At such large detunings, these is little dependence of the phase shift on the qubit's state.

Different drive frequencies can be chosen to realize rotations around arbitrary axes in the x–z plane. In particular, choosing $\omega_{\mu w} = \Omega + (2n+1)g^2/\Delta - 2g\varepsilon/\Delta$ and $t = \pi\Delta/2\sqrt{2}g\varepsilon$ generates the Hadamard transformation $\mathcal{H}$. Since $\mathcal{H}\sigma_x\mathcal{H} = \sigma_z$, these two choices of frequency are sufficient to realize any 1-qubit logical operation.

Assuming that we can take full advantage of lifetime enhancement inside the cavity (i.e. that $\gamma = \gamma_\kappa$), the number of π rotations about the x axis which can be carried out is $N_\pi = 2\varepsilon\Delta/\pi g\kappa \sim 10^5\varepsilon$ for the experimental parameters assumed in Table I. For large ε, the choice of drive frequency must take into account the power dependence of the cavity frequency pulling.

Numerical simulation shown in Fig. 9 confirms this simple picture and that single-bit rotations can be performed with very high fidelity. It is interesting to note that since detuning between the resonator and the drive is large, the cavity is only virtually populated, with an average photon number $\bar{n} \approx \varepsilon^2/\Delta^2 \sim 0.1$. Virtual population and depopulation of the cavity can be realized much faster than the cavity lifetime $1/\kappa$ and, as a result, the qubit feels the effect of the drive rapidly after the drive has been turned on. The limit on the speed of turn on and off of the drive is set by the detuning Δ. If the drive is turned on faster than $1/\Delta$, the frequency spread of the drive is such that part of the drive's photons will pick up phase information (see Fig. 8) and dephase the qubit. As a result, for large detuning, this approach leads to a fast and accurate way to coherently control the state of the qubit.

To model the effect of the drive on the resonator an alternative model is to use the cavity-modified Maxwell-Bloch equations [25]. As expected, numerical integration of the Maxwell-Bloch equations reproduce very well the stochastic numerical results when the drive is at the qubit's frequency but do *not* reproduce these numerical results when the drive is close to the bare resonator frequency (Fig. 6 and 7), i.e. when entanglement between the qubit and the photons cannot be neglected.

VIII. RESONATOR AS QUANTUM BUS: ENTANGLEMENT OF MULTIPLE QUBITS

The transmission-line resonator has the advantage that it should be possible to place multiple qubits along its length ($\sim 1\,\mathrm{cm}$) and entangle them together, which is an essential requirement for quantum computation. For the case of two qubits, they can be placed closer to the ends of the resonator but still well isolated from the environment and can be separately dc biased by capacitive coupling to the left and right center conductors of the transmission line. Additional qubits would have to have separate gate bias lines installed.

For the pair of qubits labeled i and j, both coupled with strength g to the cavity and detuned from the resonator but in resonance with each other, the transformation (11) yields the effective two-qubit Hamiltonian

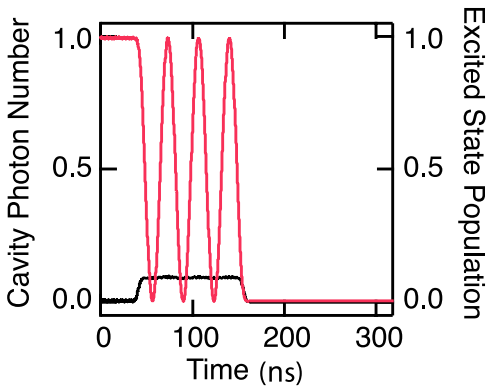


FIG. 9: (color online). Numerical stochastic wave function simulation showing coherent control of a qubit by microwave irradiation of the cavity at the ac-Stark and Lamb shifted qubit frequency. The qubit is first left to evolve freely for about 40ns. The drive is turned on for $t = 7\pi\Delta/2g\varepsilon \sim$115ns, corresponding to 7π pulses, and then turned off. Since the drive is tuned far away from the cavity, the cavity photon number is small even for the moderately large drive amplitude $\varepsilon = 0.03\omega_{\mathrm{r}}$ used here.

[3, 38, 39]

$$H_{2q} \approx \hbar\left[\omega_{\mathrm{r}} + \frac{g^2}{\Delta}(\sigma_i^z + \sigma_j^z)\right] a^\dagger a + \frac{1}{2}\hbar\left[\Omega + \frac{g^2}{\Delta}\right](\sigma_i^z + \sigma_j^z) + \hbar\frac{g^2}{\Delta}(\sigma_i^+\sigma_j^- + \sigma_i^-\sigma_j^+). \quad (32)$$

In addition to ac-Stark and Lamb shifts, the last term couples the qubits thought virtual excitations of the resonator.

In a frame rotating at the qubit's frequency Ω, H_{2q} generates the evolution

$$U_{2q}(t) = \exp\left[-i\frac{g^2}{\Delta}t\left(a^\dagger a + \frac{1}{2}\right)(\sigma_i^z + \sigma_j^z)\right] \cdot \begin{pmatrix} 1 & & & \\ & \cos\frac{g^2}{\Delta}t & i\sin\frac{g^2}{\Delta}t & \\ & i\sin\frac{g^2}{\Delta}t & \cos\frac{g^2}{\Delta}t & \\ & & & 1 \end{pmatrix} \otimes \mathbb{1}_r, \quad (33)$$

where $\mathbb{1}_r$, is the identity operator in the resonator space. Up to phase factors, this corresponds at $t = \pi\Delta/4g^2 \sim 50\,\mathrm{ns}$ to a $\sqrt{i\mathrm{SWAP}}$ logical operation. Up to one-qubit gates, this operation is equivalent to the controlled-NOT. Together with one-qubit gates, the interaction H_{2q} is therefore sufficient for universal quantum computation [40]. Assuming again that we can take full advantage of the lifetime enhancement inside the cavity, the number of $\sqrt{i\mathrm{SWAP}}$ operations which can be carried out is $N_{2\mathrm{q}} = 4\Delta/\pi\kappa \sim 1200$ for the parameters assumed above. This can be further improved if the qubit's non-radiative decay is sufficiently small, and higher Q cavities are employed.

When the qubits are detuned from each other, the off-diagonal coupling provided by H_{2q} is only weakly effective and the coupling is for all practical purposes turned off. Two-qubit logical gates in this setup can therefore be controlled by individually tuning the qubits. Moreover, single-qubit and two-qubit logical operations on different qubits and pairs of qubits can both be realized simultaneously, a requirement to reach presently known thresholds for fault-tolerant quantum computation [41].

It is interesting to point out that the dispersive QND readout presented in section VI may be able to determine the state of multiple qubits in a single shot without the need for additional signal ports. For example, for the case of two qubits with different detunings, the cavity pull will take four different values $\pm g_1^2/\Delta_1 \pm g_2^2/\Delta_2$ allowing single-shot readout of the coupled system. This can in principle be extended to N qubits provided that the range of individual cavity pulls can be made large enough to distinguish all the combinations. Alternatively, one could read them out in small groups at the expense of having to electrically vary the detuning of each group to bring them into strong coupling with the resonator.

IX. ENCODED UNIVERSALITY AND DECOHERENCE-FREE SUBSPACE

Universal quantum computation can also be realized in this architecture under the encoding $\mathcal{L} = \{|\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle\}$ by controlling only the qubit's detuning and, therefore, by turning on and off the interaction term in H_{2q} [42].

An alternative encoded two-qubit logical operation to the one suggested in Ref. [42] can be realized here by tuning the four qubits forming the pair of encoded qubits in resonance for a time $t = \pi\Delta/3g^2$. The resulting effective evolution operator can be written as $\hat{U}_{2q} = \exp\left[-i(\pi\Delta/3g^2)\hat{\sigma}_{x1}\hat{\sigma}_{x2}\right]$, where $\hat{\sigma}_{xi}$ is a Pauli operator acting on the i^{th} encoded qubit. Together with encoded one-qubit operations, $\hat{U}_{2q}$ is sufficient for universal quantum computation using the encoding $\mathcal{L}$.

We point out that the subspace $\mathcal{L}$ is a decoherence-free subspace with respect to global dephasing [43] and use of this encoding will provide some protection against noise. The application of $\hat{U}_{2q}$ on the encoded subspace $\mathcal{L}$ however causes temporary leakage out of this protected subspace. This is also the case with the approach of Ref. [42]. In the present situation however, since the Hamiltonian generating $\hat{U}_{2q}$ commutes with the generator of global dephasing, this temporary excursion out of the protected subspace does not induce noise on the encoded qubit.

X. SUMMARY AND CONCLUSIONS

In summary, we propose that the combination of one-dimensional superconducting transmission line resonators, which confine their zero point energy to extremely small volumes, and superconducting charge qubits, which are electrically controllable qubits with large electric dipole moments, constitutes an interesting system to access the strong-coupling regime of cavity quantum electrodynamics. This combined system is an advantageous architecture for the coherent control, entanglement, and readout of quantum bits for quantum computation and communication. Among the practical benefits of this approach are the ability to suppress radiative decay of the qubit while still allowing one-bit operations, a simple and minimally disruptive method for readout of single and multiple qubits, and the ability to generate tunable two-qubit entanglement over centimeter-scale distances. We also note that in the structures described here, the emission or absorption of a single photon by the qubit is tagged by a sudden large change in the resonator transmission properties [29] making them potentially useful as single photon sources and detectors.

Acknowledgments

We are grateful to David DeMille, Michel Devoret, Clifford Cheung and Florian Marquardt for useful conversations. We also thank André-Marie Tremblay and the Canadian Foundation for Innovation for access to computing facilities. This work was supported in part by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) contract number DAAD19-02-1-0045, NSF DMR-0196503, NSF DMR-0342157, the David and Lucile Packard Foundation, the W.M. Keck Foundation and NSERC.

APPENDIX A: QUANTIZATION OF THE 1D TRANSMISSION LINE RESONATOR

A transmission line of length L, whose cross section dimension is much less then the wavelength of the transmitted signal can be approximated by a 1-D model. For relatively low frequencies it is well described by an infinite series of inductors with each node capacitively connected to ground, as shown in Fig. 2. Denoting the inductance per unit length l and the capacitance per unit length c, the Lagrangian of the circuit is

$$\mathcal{L} = \int_{-L/2}^{L/2} dx \left(\frac{l}{2}j^2 - \frac{1}{2c}q^2\right), \tag{A1}$$

where $j(x,t)$ and $q(x,t)$ are the local current and charge density, respectively. We have ignored for the moment the two semi-infinite transmission lines capacitively coupled to the resonator. Defining the variable $\theta(x,t)$

$$\theta(x,t) \equiv \int_{-L/2}^{x} dx'\, q(x',t), \tag{A2}$$

the Lagrangian can be rewritten as

$$\mathcal{L} = \int_{-L/2}^{L/2} dx \left(\frac{l}{2}\dot{\theta}^2 - \frac{1}{2c}(\nabla\theta)^2 \right). \tag{A3}$$

The corresponding Euler-Lagrange equation is a wave equation with the speed $v = \sqrt{1/lc}$. Using the boundary conditions due to charge neutrality

$$\theta(-L/2,t) = \theta(L/2,t) = 0, \tag{A4}$$

we obtain

$$\begin{aligned}\theta(x,t) &= \sqrt{\frac{2}{L}} \sum_{k_o=1}^{k_{o,\mathrm{cutoff}}} \phi_{k_o}(t) \cos\frac{k_o \pi x}{L} \\ &+ \sqrt{\frac{2}{L}} \sum_{k_e=2}^{k_{e,\mathrm{cutoff}}} \phi_{k_e}(t) \sin\frac{k_e \pi x}{L},\end{aligned} \tag{A5}$$

for odd and even modes, respectively. For finite length L, the transmission line acts as a resonator with resonant frequencies $\omega_k = k\pi v/L$. The cutoff is determined by the fact that the resonator is not strictly one dimensional.

Using the normal mode expansion (A5) in (A3), one obtains, after spatial integration, the Lagrangian in the form of a set of harmonic oscillators

$$\mathcal{L} = \sum_k \frac{l}{2}\dot{\phi_k}^2 - \frac{1}{2c}\left(\frac{k\pi}{L}\right)^2 \phi_k^2. \tag{A6}$$

Promoting the variable ϕ_k and its canonically conjugated momentum $\pi_k = l\dot{\phi}_k$ to conjugate operators and introducing the boson creation and annihilation operators $a_k^\dagger$ and a_k satisfying $[a_k, a_{k'}^\dagger] = \delta_{kk'}$, we obtain the usual relations diagonalizing the Hamiltonian obtained from the Lagrangian (A6)

$$\hat{\phi}_k(t) = \sqrt{\frac{\hbar\omega_k c}{2}}\frac{L}{k\pi}(a_k(t) + a_k^\dagger(t)) \tag{A7}$$

$$\hat{\pi}_k(t) = -i\sqrt{\frac{\hbar\omega_k l}{2}}(a_k(t) - a_k^\dagger(t)). \tag{A8}$$

From these relations, the voltage on the resonator can be expressed as

$$\begin{aligned}V(x,t) &= \frac{1}{c}\frac{\partial\theta(x,t)}{\partial x} \\ &= -\sum_{k_o=1}^{\infty}\sqrt{\frac{\hbar\omega_{k_o}}{Lc}}\sin\left(\frac{k_o\pi x}{L}\right)[a_{k_o}(t) + a_{k_o}^\dagger(t)] \\ &+ \sum_{k_e=1}^{\infty}\sqrt{\frac{\hbar\omega_{k_e}}{Lc}}\cos\left(\frac{k_e\pi x}{L}\right)[a_{k_e}(t) + a_{k_e}^\dagger(t)].\end{aligned} \tag{A9}$$

In the presence of the two semi-infinite transmission lines coupled to the resonator, the Lagrangian (A3) and the boundary conditions (A4) are modified to take into account the voltage drop on the coupling capacitors C_0. Assuming no spatial extent for the capacitors C_0, the problem is still solvable analytically. Due to this coupling, the wavefunction can now extend outside of the central segment which causes a slight red-shift, of order C_0/Lc, of the cavity resonant frequency.

As shown in Fig. 2, we assume the qubit to be fabricated at the center of the resonator. As a result, at low temperatures, the qubit is coupled to the mode $k = 2$ of the resonator, which as an anti-node of the voltage in its center. The rms voltage between the center conductor and the ground plane is then $V_{\mathrm{rms}}^0 = \sqrt{\hbar\omega_r/cL}$ with $\omega_r = \omega_2$ and the voltage felt by the qubit is $V(0,t) = V_{\mathrm{rms}}^0(a_2(t) + a_2^\dagger(t))$. In the main body of this paper, we work only with this second harmonic and drop the mode index on the resonator operators.

APPENDIX B: QUANTUM NON-DEMOLITION MEASUREMENTS

Read-out of a qubit can lead to both mixing and dephasing [23, 33]. While dephasing is unavoidable, mixing of the measured observable can be eliminated in a QND measurement by choosing the qubit-measurement apparatus interaction such that the measured observable is a constant of motion. In that situation, the measurement-induced mixing is rather introduced in the operator conjugate to the operator being measured.

In the situation of interest in this paper, the operator being probed is σ_z and, from Eq. (12), the qubit-measurement apparatus interaction Hamiltonian is $H_{\mathrm{int}} = (g^2/\Delta)\sigma_z a^\dagger a$, such that $[\sigma_z, H_{\mathrm{int}}] = 0$. For σ_z to be a constant of motion also requires that it commutes with the qubit Hamiltonian. This condition is also satisfied in Eq. (12).

That the measured observable is a constant of motion implies that repeated observations will yield the same result. This allows for the measurement result to reach arbitrary large accuracy by accumulating signal. In practice however, there are always environmental dissipation mechanisms acting on the qubit independently of the read-out. Even in a QND situation, these will lead to a finite mixing rate $1/T_1$ of the qubit in the course of the measurement. Hence, high fidelity can only be achieved by a strong measurement completed in a time $T_m \ll T_1$. This simple point is not as widely appreciated as it should be.

[1] H. Mabuchi and A. Doherty, Science **298**, 1372 (2002).
[2] C. J. Hood, T. W. Lynn, A. C. Doherty, A. S. Parkins, and H. J. Kimble, Science **287**, 1447 (2000).
[3] J. Raimond, M. Brune, and S. Haroche, Rev. Mod. Phys.

73, 565 (2001).
[4] A. Armour, M. Blencowe, and K. C. Schwab, Phys. Rev. Lett. **88**, 148301 (2002).
[5] E. K. Irish and K. Schwab (2003), cond-mat/0301252.
[6] Y. Makhlin, G. Schön, and A. Shnirman, Rev. Mod. Phys. **73**, 357 (2001).
[7] O. Buisson and F. Hekking, in *Macroscopic Quantum Coherence and Quantum Computing*, edited by D. V. Averin, B. Ruggiero, and P. Silvestrini (Kluwer, New York, 2001).
[8] F. Marquardt and C. Bruder, Phys. Rev. B **63**, 054514 (2001).
[9] F. Plastina and G. Falci, Phys. Rev. B **67**, 224514 (2003).
[10] A. Blais, A. Maassen van den Brink, and A. Zagoskin, Phys. Rev. Lett. **90**, 127901 (2003).
[11] W. Al-Saidi and D. Stroud, Phys. Rev. B **65**, 014512 (2001).
[12] C.-P. Yang, S.-I. Chu, and S. Han, Phys. Rev. A **67**, 042311 (2003).
[13] J. Q. You and F. Nori, Phys. Rev. B **68**, 064509 (2003).
[14] D. Walls and G. Milburn, *Quantum optics* (Spinger-Verlag, Berlin, 1994).
[15] S. Haroche, in *Fundamental Systems in Quantum Optics*, edited by J. Dalibard, J. Raimond, and J. Zinn-Justin (Elsevier, 1992), p. 767.
[16] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, and M. Devoret, Physica Scripta **T76**, 165 (1998).
[17] D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, and M. Devoret, Science **296**, 886 (2002).
[18] K. Lehnert, K. Bladh, L. Spietz, D. Gunnarsson, D. Schuster, P. Delsing, and R. Schoelkopf, Phys. Rev. Lett. **90**, 027002 (2003).
[19] A. S. Sorensen, C. H. van der Wal, L. Childress, and M. D. Lukin (2003), (quant-ph/0308145).
[20] R. W. Simmonds, K. M. Lang, D. A. Hite, D. P. Pappas, and J. Martinis (2003), submitted to Phys. Rev. Lett.
[21] P. K. Day, H. G. LeDuc, B. A. Mazin, A. Vayonakis, and J. Zmuidzinas, Nature (London) **425**, 817 (2003).
[22] A. Wallraff and R. Schoelkopf, unpublished.
[23] R. Schoelkopf, A. Clerk, S. Girvin, K. Lehnert, and M. Devoret, *Quantum noise in mesoscopic physics* (Kluwer Ac. Publ., 2003), chap. Qubits as Spectrometers of Quantum Noise, pp. 175–203.
[24] H. Kimble, *Structure and dynamics in cavity quantum electrodynamics* (Academic Press, 1994).
[25] C. Wang and R. Vyas, Phys. Rev. A **55**, 823 (1997).
[26] A lumped LC circuit was used in Ref. [27, 28] to probe flux qubits in a different way.
[27] E. Il'ichev, N. Oukhanski, A. Izmalkov, T. Wagner, M. Grajcar, H.-G. Meyer, A. Y. Smirnov, A. Maassen van den Brink, M. Amin, and A. Zagoskin, Phys. Rev. Lett. **91**, 097906 (2003).
[28] A. Izmalkov, M. Grajcar, E. Il'ichev, T. Wagner, H.-G. Meyer, A. Smirnov, M. Amin, A. Maassen van den Brink, and A. Zagoskin (2004), cond-mat/0312332.
[29] S. Girvin, A. Blais, and R. Huang, unpublished.
[30] We note that for the case of $Q = 10^6$, the cavity pull is a remarkable ± 250 line widths, but, depending on the non-radiative decay rate of the qubit, this may be in the regime $\kappa < \gamma$, making the state measurement too slow.
[31] S. van Enk, J. Cirac, and P. Zoller, Science **279**, 2059 (1998).
[32] R. Schack and T. A. Brun, Comp. Phys. Comm. **102**, 210 (1997).
[33] M. Devoret and R. Schoelkopf, Nature **406**, 1039 (2000).
[34] A. Clerk, S. Girvin, and A. Stone, Phys. Rev. B **67**, 165324 (2003).
[35] F. Marquardt, unpublished.
[36] D. Averin and C. Bruder, Phys. Rev. Lett. **91**, 057003 (2003).
[37] Y. Nakamura, Y. Pashkin, and J. Tsai, Nature (London) **398**, 786 (1999).
[38] A. Sørensen and K. Mølmer, Phys. Rev. Lett. **82**, 1971 (1999).
[39] S.-B. Zheng and G.-C. Guo, Phys. Rev. Lett. **85**, 2392 (2000).
[40] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, S. P, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[41] D.Aharonov and M. Ben-Or, in *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1996), p. 46.
[42] D. Lidar and L.-A. Wu, Phys. Rev. Lett. **88**, 017905 (2002).
[43] J. Kempe, D. Bacon, D. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).

Experimental One-Way Quantum Computing

P.Walther[1], K.J.Resch[1], T.Rudolph[2], E.Schenck[1,*], H.Weinfurter[3,4], V.Vedral[1,5,6], M.Aspelmeyer[1] & A.Zeilinger[1,7]

[1] *Institute of Experimental Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*

[2] *QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, United Kingdom*

[3] *Department of Physics, Ludwig-Maximilians-University, D-80799 Munich, Germany*

[4] *Max-Planck-Institute for Quantum Optics, D-85741 Garching, Germany*

[5] *The Erwin Schrödinger Institute for Mathematical Physics, Boltzmanngasse 9, 1090 Vienna, Austria*

[6] *The School of Physics and Astronomy, University of Leeds, Leeds, LS2 9JT, United Kingdom*

[7] *IQOQI, Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*

[*] *permanent address:* Ecole normale supérieure, 45, rue d´Ulm, 75005 Paris, France

Standard quantum computation is based on sequences of unitary quantum logic gates which process qubits. The one-way quantum computer proposed by Raussendorf and Briegel is entirely different. It has changed our understanding of the requirements for quantum computation and more generally how we think about quantum physics. This new model requires qubits to be initialized in a

highly-entangled cluster state. From this point, the quantum computation proceeds by a sequence of single-qubit measurements with classical feedforward of their outcomes. Because of the essential role of measurement a one-way quantum computer is irreversible. In the one-way quantum computer the order and choices of measurements determine the algorithm computed. We have experimentally realized four-qubit cluster states encoded into the polarization state of four photons. We fully characterize the quantum state by implementing the first experimental four-qubit quantum state tomography. Using this cluster state we demonstrate the feasibility of one-way quantum computing through a universal set of one- and two-qubit operations. Finally, our implementation of Grover's search algorithm demonstrates that one-way quantum computation is ideally suited for such tasks.

The quantum computer[1,2] is a powerful application of the laws of quantum physics. Such a device will be far more efficient at factoring[3] or database searches[4] compared to its classical counterparts[5]. Considerable effort has been directed toward understanding the role of measurement and entanglement in quantum computation[6-12]. A significant step forward in our understanding was the introduction of the "one-way" quantum computer[13-17] which highlights the importance of both measurement and entanglement in a striking way. In this model, all of the entanglement is provided in advance through a highly-entangled multi-particle cluster state[13]. The quantum computation on the cluster state proceeds via local, single-qubit projective measurements with the outcomes potentially affecting those measurement settings that follow. It is a strength of the cluster state model that the intrinsic randomness of quantum measurement results creates specific types of errors which can be corrected through this classical feedforward. Most importantly, feedforward makes cluster state quantum computation deterministic. In the present, proof-of-principle experiment we perform measurements using fixed single-port polarizers making our computations probabilistic. Different

algorithms require only a different pattern of adapted single-qubit operations on a sufficiently large cluster state. Since it is entirely based on single-particle measurements instead of unitary evolution, the computation is inherently not time-reversible - it is one-way. Most importantly cluster state quantum computation is universal[14,17] in that any quantum circuit can be implemented on a suitable cluster state. Open theoretical questions remain about the scalability under realistic noise conditions required for fault-tolerant one-way quantum computation. Although a threshold has been proven to exist[18], it is unknown whether cluster state quantum computation will be more or less sensitive to noise than the standard model.

The one-way quantum computer does not perform quantum logic on the individual qubits of the cluster state. In order to describe the computational circuit, we need to distinguish between the *physical qubits*, in our case the polarization state of photons, which make up the cluster state and on which actual measurements are carried out, and *encoded qubits*, on which the computation is actually taking place. Due to the specific entanglement of the cluster state, no individual physical qubit carries any information about an input state. Therefore, each encoded qubit is written on the cluster state non-locally, i.e. the information is carried by the correlations between the physical qubits. As the quantum computation proceeds, the encoded input qubits are processed in the imprinted circuit, whose output is finally transferred onto physical readout qubits. Interestingly, while the entanglement between the physical qubits in general decreases as a result of the measurement sequence, the entanglement between encoded qubits may increase.

A cluster state can be thought of as emerging from an array of equally prepared independent qubits, which then interact via controlled-phase (CPhase) gates with their nearest (connected) neighbours. Specifically, a cluster state can be built up as follows: A large number of physical qubits are each prepared in the superposition state

$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are the computational basis of the physical qubits. A CPhase operation $|j\rangle|k\rangle \rightarrow (-1)^{jk}|j\rangle|k\rangle$, with $(j,k \in 0,1)$ is then applied between pairs of neighbouring, connected qubits and effectively generates entanglement between them. The choice which physical qubit neighbours are entangled by the CPhase operations, drawn as connecting "bonds" (Figure 1), determines the structure of the cluster state which defines the basic type quantum circuit it can implement. This construction provides an intuitive understanding for the graphical representation of cluster states as connected arrays of physical qubits, in which each line corresponds to a previous nearest-neighbour interaction. We will later demonstrate how the highly entangled cluster states can be generated in a different way, directly from nonlinear optical processes.

Given a cluster state, two basic types of single-particle measurements suffice to operate the one-way quantum computer. Measurements in the computational basis $\{|0\rangle_j, |1\rangle_j\}$ have the effect of disentangling, i.e., removing, the physical qubit j from the cluster leaving a smaller cluster state. Such operations can be used to modify the structure of the cluster and thus the imprinted circuit. The measurements which perform the actual quantum information processing are made in the basis $B_j(\alpha) = \{|+\alpha\rangle_j, |-\alpha\rangle_j\}$ where $|\pm\alpha\rangle_j = (|0\rangle_j \pm e^{i\alpha}|1\rangle_j)/\sqrt{2}$ (α is a real number). The choice of measurement basis determines the single-qubit rotation, $R_z(\alpha) = \exp(-i\alpha\sigma_z/2)$, followed by a Hadamard operation, $H = (\sigma_x + \sigma_z)/\sqrt{2}$, on encoded qubits in the cluster ($\sigma_x, \sigma_y, \sigma_z$ being the usual Pauli matrices). Combinations of rotations about the z-axis and Hadamard operations can implement $R_x(\alpha) = \exp(-i\alpha\sigma_x/2)$ rotations through the matrix identity $R_x(\alpha) = HR_z(\alpha)H$. Any quantum logic operation can be carried out by the correct choice of $B_j(\alpha)$ on a sufficiently large cluster state. We define the outcome s_j of a measurement on the physical qubit j 0 if the measurement outcome is $|+\alpha\rangle_j$ and 1 if the outcome is $|-\alpha\rangle_j$. In those cases where the 0 outcome is found, the computation proceeds as desired.

However, in those cases where the 1 outcome is found, a well-defined Pauli error is introduced. Feedforward, such that the output controls future measurement, compensates for these known errors.

For the implementations of single- and two-qubit quantum logic, we post-select only those cases where the 0 outcome is found and the computation proceeds error free. In the final section, where we report the implementation of Grover's search algorithm, the feedforward determines the final, classical, measurement. There we measured all possible combinations of the measurement results individually and applied the feedforward relation in such a way that the earlier measurements define the physical meaning of the final ones.

Even a small cluster state suffices to demonstrate all the essential features of one-way quantum computing. Each of the three- and four-particle cluster states shown in Figure 1 can implement the quantum circuit shown to its right that consist of a series of single- and two-qubit quantum gates. The computation proceeds via single-particle measurements carried out from the left side of the cluster to the right side, where the final readout takes place. The important feature of the quantum circuits is that the output of one circuit can be fed into the input of a subsequent one if their cluster states are bonded together by CPhase operations. Thus these small circuits, which form a universal set of logic gates, can be used as subunits for a fully-functional quantum computer.

As an example, consider the four-particle box cluster state $\left|\Phi_{\square 4}\right\rangle$ on a 2-dimensional lattice (Figure 1e). The encoded input to the two-qubit quantum circuit is the product state $\left|\Psi_{in}\right\rangle = \left|+\right\rangle_{1E}\left|+\right\rangle_{2E}$, where the numerical subscript labels the qubit and the subscript E is used to distinguish encoded qubits from physical qubits. The circuit processes this pair of encoded qubits through a sequence beginning with a CPhase gate,

followed by single-qubit rotations $R_z(-\alpha)$ and $R_z(-\beta)$ on encoded qubits 1 and 2, then a Hadamard operation, H , on both qubits, ending with a second CPhase operation. The values for α and β of the rotation gates are set by the choice of measurement bases $B_1(\alpha)$ and $B_4(\beta)$ on the physical qubits 1 and 4 respectively. The output of the quantum computation is transferred onto physical qubits 2 and 3. This kind of two-qubit quantum gate is essential for universal quantum computation since it can generate entanglement between the encoded qubits.

On the other hand, by changing the geometry of the cluster state to the one-dimensional cluster $|\Phi_{lin4}\rangle$ (Figure 1b), it now results in a different quantum circuit corresponding to a set of single-qubit rotations on one encoded qubit. Consecutive measurements $B_1(\alpha)$, $B_2(\beta)$, and $B_3(\gamma)$ on the physical qubits 1, 2, and 3 transform the input state, in our case $|\Psi_{in}\rangle = |+\rangle_{1E}$, to $|\Psi_{out}\rangle = HR_z(-\gamma)R_x(-\beta)R_z(-\alpha)|\Psi_{in}\rangle$ and store the output on qubit 4.

In order to demonstrate all the circuits shown in Figure 1a-1e, it is sufficient to first produce a linear cluster state of four qubits. The particular circuit implemented is then determined by the order of the measurements performed. Specifically, the one-dimensional linear structure (Figure 1a and 1b) is implemented by sequentially measuring qubits 1, 2 and 3, with the final result then being available at qubit 4. The two-dimensional horseshoe structures (Figure 1c and 1d) are implemented by measuring either qubits 2 and 3 or 1 and 4 with the final result then being available at qubits 1 and 4 or 2 and 3, respectively. The four qubit box cluster (Figure 1e) can be obtained from the four-qubit linear cluster by Hadamard rotations and by swapping (i.e., relabeling) the physical qubits 2 and 3. All this will be described in more detail in the next section and in the section “two-qubit gates”.

The difficulty of one-way quantum computer lies with the cluster-state preparation. Cluster states naturally arise in spin chains or spin lattices via nearest-neighbour Ising interaction[13], a well-known interaction model in solid-state physics. Therefore, the first proposals to achieve cluster states were based on analogues in dipole-dipole coupling between atoms in optical lattices[15,19]. Although photon-photon interactions are negligible, recent proposals have nevertheless shown that optical systems may be well-suited for implementing the cluster state model. These schemes utilize sequences of probabilistic quantum-logic gates[8,20-23] based on linear optical elements to construct large photonic cluster states[24,25]. These optical one-way quantum computation proposals are less demanding on resources than the comparable optical implementation in the standard model[8].

In the present work, we have employed nonlinear optics to directly produce four-photon cluster states. This method exploits a mode- and polarization-entangled four-photon state[26] produced in pulsed-pump spontaneous parametric down conversion (SPDC) (see Methods). We reconstructed the density matrix of the four-qubit cluster state using quantum state tomography and studied the state's entanglement properties relevant for quantum computation. We then implement all of the quantum circuits shown in Figure 1a-1e and demonstrate a two-qubit quantum search algorithm. In doing so, we have demonstrated the first universal set of gates and an important algorithm in a one-way quantum computer.

Creation and Characterization of the Cluster State

Our cluster state is produced experimentally using the mode- and polarization-entangled output of nonlinear spontaneous parametric down-conversion and linear optical elements as described in detail in the Methods section. When four photons are emitted

into the output modes of the polarizing beam-splitters 1, 2, 3, and 4, they are in the highly-entangled cluster state,

$$|\Phi_{cluster}\rangle = \frac{1}{2}\left(|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 + |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4\right), \quad (1)$$

where $|H\rangle$ and $|V\rangle$ represent horizontally- and vertically-polarized photon states and the subscript labels the spatial mode. This state, $|\Phi_{cluster}\rangle$, is equivalent to the four-qubit linear cluster, $|\Phi_{lin4}\rangle$, and the horse-shoe cluster states, $|\Phi_{\subset 4}\rangle$ & $|\Phi_{\supset 4}\rangle$ (Figure 1) under the local unitary operation $H_1 \otimes I_2 \otimes I_3 \otimes H_4$ on the physical qubits, where H_i (I_i) is a Hadamard (Identity) operation on qubit i. The four-qubit linear cluster can easily be reduced to a three-qubit linear cluster by measuring qubit 1 in the computational basis of the cluster and thus disentangling it from the rest. The state, $|\Phi_{cluster}\rangle$, can be converted to the box cluster state (Figure 1e) by the local unitary operation $H_1 \otimes H_2 \otimes H_3 \otimes H_4$ and a swap (or relabeling) of qubits 2 and 3. Note that the four-qubit cluster state thus realized is also the smallest cluster state that represents a new kind of entanglement[28], while the two-qubit and three-qubit cluster states are locally-equivalent to a maximally-entangled Bell state and the three-qubit GHZ state, respectively.

State Tomography

We have completely characterized our state via quantum-state tomography, which is a method for extracting the density matrix of a quantum state, from a discrete set of experimental measurements. While quantum process and state tomography has been performed with up to three qubits[28,29] this is the first time that a four-qubit density matrix has been determined from a complete, experimentally-obtained density matrix. For a four-photon polarization state, like our cluster state, the full density matrix, ρ, is a 16×16 dimensional object that can be reconstructed by linear combinations of 256 linearly-independent four-photon polarization projections. We performed each of these

256 measurements for 600 seconds using all combinations of $\{|H\rangle,|V\rangle,|+\rangle,|R\rangle\}$, where $|+\rangle=(|H\rangle+|V\rangle)/\sqrt{2}$ and $|R\rangle=(|H\rangle-i|V\rangle)/\sqrt{2}$. A maximum of 127 four-fold coincidence counts in 600 seconds were measured in the case of the setting $|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$. Instead of a direct linear combination of measurement results which can lead to unphysical density matrices due to experimental noise, we employ a maximum-likelihood reconstruction technique[30-32]. The resulting density matrix is shown in Figure 2. The dominant diagonal elements represent the four components $|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4$, $|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$, $|V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4$ and $|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ as expected from Eq. (1), while off-diagonal elements indicate strong coherences between them. The negative coherences are due to the required π phase shift in the amplitude for the $|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ term. Our reconstructed state is in good qualitative agreement with the target state, $|\Phi_{cluster}\rangle$. This can be quantified by the state fidelity $F=\langle\Phi_{cluster}|\rho|\Phi_{cluster}\rangle=(0.63\pm0.02)$, which is the state vector overlap with the ideal state $|\Phi_{cluster}\rangle$. At present no theoretical results exist concerning the fidelity requirements in cluster state quantum computation, therefore the full implication of the value we found for the fidelity are unclear. Nevertheless, it has been proven that bi-separable four-qubit states cannot have a fidelity greater than 0.5 with our target cluster state. Our measured fidelity is clearly above this threshold and therefore the observed fidelity is proof the fact that the state contains the required four-particle entanglement[34] to a significant degree. Our cluster state is a coherent superposition of four different terms, each from a different physical origin (see methods). The fidelity of our state is not perfect because of partial distinguishability of these terms and because of imperfect phase stability in our setup. We expect that, achieving high fidelity with the target state will become rapidly more difficult as the size of the Hilbert space is increased. However, the acceptable amount of noise per qubit is independent of the size of the cluster, whereas it becomes exponentially small for GHZ states[34]. Thus the problem of noise does not increase for larger clusters[34].

Entanglement Properties

One-way cluster state quantum computation is based entirely on the entanglement properties of the physical qubits of the initial cluster state. For three-qubit states, there are only two classes of entanglement typified by the GHZ state[35], $|GHZ\rangle = \left(|H\rangle_1|H\rangle_2|H\rangle_3 + |V\rangle_1|V\rangle_2|V\rangle_3\right)/\sqrt{2}$, and by the W state[36,37], $|W\rangle = \left(|V\rangle_1|H\rangle_2|H\rangle_3 + |H\rangle_1|V\rangle_2|H\rangle_3 + |H\rangle_1|H\rangle_2|V\rangle_3\right)/\sqrt{3}$. As such, the three-qubit cluster state cannot represent a fundamentally different type of state and is, in fact, a GHZ state. On the other hand, our four-qubit cluster state cannot be converted via local unitary operations to either the four-qubit generalizations of the GHZ or the W state but combines important characteristics of both.

As in a four-qubit GHZ state, one can make local measurements on one or two of the qubits and, with only classical communication, leave the remaining qubits in a three-qubit GHZ or in a two-qubit Bell state both of which can serve as an entanglement resource for quantum communication. For an explicit example, we reconstructed the density matrix of qubits 2, 3, and 4 by considering only the subset of our full tomographic measurements where qubit 1 was successfully measured in the state $|+\rangle_1$. Its fidelity compared to an ideal three-photon GHZ state was (0.60 ± 0.02), which is above the local realism threshold[38] of 0.56.

While the loss of one qubit in a GHZ state is already sufficient to completely disentangle the state, $N/2$ particles have to be removed from an N-particle cluster state in order to leave a separable state. The cluster states share this *persistency of entanglement*[14] with the W states, which show an even stronger robustness against such decoherence. We demonstrate this property by considering the reduced density matrix of qubits 2, 3, and 4, $\rho_{2,3,4}^{red}$ after ignoring qubit 1, i.e., after tracing out the first qubit. This trace has been implemented by summing the two subsets of our tomographic measurements in which the first qubit was measured in the state $|H\rangle_1$ or $|V\rangle_1$. To test

for entanglement in the remaining three-qubit state, we employed the entanglement-witness operator $W = \frac{1}{4} I^{\otimes 3} - \frac{1}{2}\left(\left|H\right\rangle_2 \left\langle H\right|_2 \otimes \left|\Phi^+\right\rangle_{3,4} \left\langle \Phi^+\right|_{3,4} + \left|V\right\rangle_2 \left\langle V\right|_2 \otimes \left|\Phi^-\right\rangle_{3,4} \left\langle \Phi^-\right|_{3,4} \right)$, where $Tr(W\rho) \geq 0$ for all separable states, but is negative for some entangled states. Our state gives a value of $\left(-0.115 \pm 0.007\right)$, which is negative by 16σ and thus proves that entanglement in qubits 2, 3, and 4 persists even after "loss" of qubit 1. This remaining entanglement is between qubits 3 and 4. The loss of another particle destroys all entanglement and leaves a separable two-qubit state. We test this by calculating the eigenvalues of the partial transpose reduced density matrix of qubits 3 and 4 which are $\lambda_1 = 0.49$, $\lambda_2 = 0.45$, $\lambda_3 = 0.05$ and $\lambda_4 = 0.008$. These values are all positive and thus fulfil the necessary and sufficient conditions for separability in two-particle systems[39,40].

A One-Way Quantum Computer

Given a cluster state, quantum gates are implemented on the encoded qubits using only a series of single-qubit measurements and classical feed-forward. In this section, we demonstrate the essentials of cluster-state quantum computation. In the present experiment, we created a cluster state and performed fixed polarization measurements, i.e., projections onto the $\left|+\alpha\right\rangle_j$ in the bases, $B_j(\alpha)$, which require no feed-forward or subsequent corrections. This reduces the success rate of the computation by a factor of two for every measurement as compared to ideal, deterministic gate operations but it certainly suffices as a proof-of principle. An important challenge for future work is to implement the fast active switching and logic requirements for one-way quantum computation with feed-forward. We have realized a universal set of quantum logic operations in the form of single-qubit rotations and nontrivial two-qubit gates. In the following sections we characterize the quality of each quantum computation by comparing the measured output state to the ideal using the state fidelity. Interesting

avenues for study include full quantum gate characterization using quantum process tomography[41,42] or related measures[43].

Single-Qubit Rotations

We start with the one-dimensional four-qubit linear cluster state, $|\Phi_{lin4}\rangle$, which implements an arbitrary single-qubit rotation gate as shown in Figure 1b. In particular, we perform $B_1(\alpha)$, $B_2(\beta)$ and $B_3(\gamma)$ on the physical qubits in the linear cluster basis. The parameters α, β, γ are sufficient to rotate the input qubit to anywhere on the Bloch sphere, or more generally to implement an arbitrary $SU(2)$ single-qubit rotation. This computation rotates the encoded input qubit $|\Psi_{in}\rangle = |+\rangle_{1E}$ to the output state $|\Psi_{out}\rangle = HR_z(-\gamma)R_x(-\beta)R_z(-\alpha)|\Psi_{in}\rangle$, while the output of this computation is left in the quantum state of qubit 4. We finally characterize physical qubit 4 to verify the performance of the computation using single-qubit quantum state tomography (Table 1a).

The three-qubit linear cluster state $|\Phi_{lin3}\rangle$ is generated from $|\Phi_{lin4}\rangle$ by disentangling physical qubit 1 from the cluster. This is achieved by measuring physical qubit 1 in the computational basis for the linear cluster, i.e. $\{|+\rangle_1, |-\rangle_2\}$ in the lab basis. We consider only those cases where we find the "+" outcome. This resulting cluster state implements the quantum circuit in Figure 1a, which is a simpler single-qubit rotation gate with rotations determined by the measurements $B_2(\alpha)$ and $B_3(\beta)$ of the second and the third qubit. This rotates the encoded input qubit $|\Psi_{in}\rangle = |+\rangle_{1E}$ to the final state, $|\Psi_{out}\rangle = R_x(-\beta)R_z(-\alpha)|\Psi_{in}\rangle$, which is again left on physical qubit 4. The computation is directly implemented by performing single-particle measurements on qubits 1, 2 and 3. The single-qubit output stored on qubit 4 is completely characterized by single-qubit tomography. We compare this single output qubit with both the theoretically expected output and the predicted output from our reconstructed four-particle cluster state density matrix. Figure 3 shows the state of qubit 4 on the Bloch

sphere in the lab basis in the ideal (left-hand side) and measured (right-hand side) case for three different measurement settings. These measurement settings were chosen to clearly show the effect of changing a single measurement basis. For the three state vectors shown as 1, 2, and 3, α was set to $\pi/2$, $\pi/4$ and 0, respectively, while β was fixed to $-\pi/2$. The state fidelities of these and other measurement settings compared to the ideal gate action are shown in Table 1b.

Two-Qubit Gates

In order to perform universal quantum computation nontrivial two-qubit quantum-logic gates[4] are required in addition to single-qubit rotations. Well-known examples of such gates are the controlled-NOT (CNOT) or controlled Phase (CPhase) operations. The crucial trait of these gates is that they can change the entanglement between qubits. Gates of this type can be implemented with a two-dimensional cluster. In Figure 1, we show two-dimensional cluster states, the horseshoe cluster states (Figure 1c and 1d) and the box cluster state (Figure 1e), that satisfy this condition for two-qubit quantum logic. Both of their quantum circuits are comprised of single-qubit rotations and CPhase operations that can generate entanglement between two initially separable encoded qubits. Whether or not entanglement is generated depends on the specific circuit and the initial states. We will give a specific example of a two-qubit quantum computation that does not generate entanglement (in the box cluster) and a second computation that does generate entanglement (in the horseshoe cluster).

The box cluster transforms the two-qubit encoded input state according to

$$\left|\Psi_{out}\right\rangle = CPhase\left(H_1 \otimes H_2\right)\left[R_z(-\alpha) \otimes R_z(-\beta)\right] CPhase \left|\Psi_{in}\right\rangle, \qquad (2)$$

where α and β are determined by measurements $B_1(\alpha)$ and $B_4(\beta)$ on qubits 1 and 4 respectively. For the isolated box (or horseshoe) cluster state, the encoded qubit input state is the product state $\left|\Psi_{in}\right\rangle = \left|+\right\rangle_{1E}\left|+\right\rangle_{2E}$. Consider the case where photons 1 and 4

are measured to be $|V\rangle_1$ and $|H\rangle_4$ in the lab basis. For the box cluster, this corresponds to measuring the "0" outcome of $B_1(\pi)$ and $B_4(0)$ respectively on physical qubits 1 and 4. According to the box quantum circuit, this should perform the computation $|+\rangle_{1E}|+\rangle_{2E} \rightarrow |+\rangle_{1E}|-\rangle_{2E}$ with the resulting product state outcome left on qubits 2 and 3. The experimentally-measured final state of qubits 2 and 3, in the lab basis, are shown as a two-qubit density matrix in Figure 4a. The state has a single dominant diagonal element corresponding to the state $|V\rangle_2|H\rangle_3$ and no off-diagonal elements. Recall the conversion from the box basis to the lab basis requires a swap of qubits 2 and 3 and application of a Hadamard on each qubit. This converts $|+\rangle_{1E}|-\rangle_{2E}$ to $|V\rangle_{1E}|H\rangle_{2E}$ in agreement with our measured density matrix. The fidelity of this measured density matrix of qubits 2 and 3 with the ideal output is (0.93 ± 0.01). We can quantify the entanglement in the output state using the tangle[44] defined as $\tau = \left[Max\left(0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\right)\right]^2$, where λ_i are the eigenvalues of the matrix $\rho\Sigma\rho^T\Sigma$ and $\Sigma = \sigma_y \otimes \sigma_y$, and are decreasingly ordered with λ_1 being the largest. The tangle can range from 0 for separable states to 1 for maximally-entangled states. The tangle of our measured density matrix is (0.01 ± 0.01) in agreement with the expected value of 0 - no entanglement has been generated in this case. The fidelities of other quantum computations in the box cluster are shown in Table 2a including an example where entanglement is generated.

Two-qubit operations are crucial for quantum computation since they can dependent on the measurement settings generate entanglement. The horseshoe cluster state of Figure 1c performs the following quantum circuit

$$|\Psi_{out}\rangle = (H_1 \otimes H_2)\left[R_z(-\alpha) \otimes R_z(-\beta)\right] CPhase\, |\Psi_{in}\rangle \qquad (3)$$

For our input state $|\Psi_{in}\rangle = |+\rangle_{1E}|+\rangle_{2E}$, this circuit always generates maximal entanglement. Consider the case where photons 2 and 3 are both measured in the state $|+\rangle$. This measurement corresponds to the "0" outcome of $B_2(0)$ and $B_3(0)$ on

physical qubits 2 and 3 and should perform the transformation $|+\rangle_{1E}|+\rangle_{2E} \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle_{1E}|+\rangle_{2E} + |1\rangle_{1E}|-\rangle_{2E}\right)$, where the output is maximally entangled. The experimentally-measured output density matrix of photons 2 and 3 is shown in Figure 4b (right-hand side). For comparison, the ideal output density matrix is also shown in Figure 4b (left-hand side). The two density matrices are qualitatively very similar and, indeed, the state fidelity of our measured state with the ideal state is (0.84 ± 0.03). The tangle of this output state is $\tau = (0.65 \pm 0.11)$ confirming the generation of entanglement between the logical qubits as a result of the quantum computation. Furthermore, this experimentally measured density matrix implies a maximum CHSH Bell parameter[45] of $S = (2.47 \pm 0.08)$, this is well above the $S = 2$ upper limit for local realistic theories. The fidelities of other quantum computations in the horseshoe cluster are shown in Table 2b.

Grover's search algorithm

The excitement over quantum computation is based on just a few algorithms, the most well-known being Shor's[3] factorization algorithm and Grover's search algorithm[6]. The latter is extremely important from a fundamental standpoint since it is provably more efficient than the best classical algorithm and from a practical standpoint since fast searching is central to solving difficult problems. Grover's algorithm has been implemented under the standard model[46,47] both in NMR[48,49] and in optical experiments. Here, we demonstrate a two-qubit implementation of Grover's fast quantum search using the cluster state model.

The goal of a search is to identify one out of *N* elements of a database. Formally one could consider the database as a black box which labels one of *N* possible inputs leaving all others unchanged. The challenge, then, is to find that labelled state. The best classical strategy chooses the inputs randomly one by one and checks for the label; it

takes, on average, about $N/2$ calculations to find the special input. Quantum parallelism in Grover's algorithm allows for all inputs to be processed simultaneously in superposition while interference enhances the probability of finding the desired outcome in only $O\left(\sqrt{N}\right)$ calculations of the function. In the case of a two-bit function ($N = 4$), the difference is even more dramatic since Grover's algorithm needs only one calculation of the function, whereas classically three evaluations are needed in the worst case, and 2.25 evaluations are needed on average.

The quantum circuit for the two-qubit Grover algorithm is shown in Figure 5a. Two input qubits, 1 and 2, are prepared in the state $|+\rangle_1|+\rangle_2$. This is a superposition of all four computational basis states $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$. As one of four possibilities, the black box could label the state $|0\rangle|1\rangle \rightarrow -|0\rangle|1\rangle$ by changing its sign and leaving all other states unchanged. Note that the change of sign is equivalent to a bit flip on an ancillary qubit. Any of the four possibilities can be set by proper choices of the rotation angles α and β. The output from the black box is processed by an operation which inverts the amplitudes for each computational state about the mean value. This process amplifies the labelled amplitude and reduces the rest. In the two-qubit case, theory predicts that after a single application of this inversion, the computer outputs the labelled state with probability 1.

We can compare this circuit for the two-qubit Grover algorithm to that implemented by the box cluster state in Figure 1e. The Grover algorithm circuit contains extra fixed single-qubit operations, a σ_Z followed by a Hadamard transformation, H, on each qubit before the readout in the computational basis. Measurement of a final physical qubit in the computational basis after a σ_Z followed by H is equivalent to direct measurement of those qubits in the basis $B(\pi)$, i.e., we can absorb these additional fixed single-qubit operations into the readout stage. The quantum circuit implemented by the box cluster can be seen as precisely that one required for Grover's

algorithm provided the final readout measurements are made in $B_{2,3}(\pi)$ on physical qubits 2 and 3.

The cluster state computation proceeds as follows. The encoded qubits begin in the state $|+\rangle_1|+\rangle_2$. Setting the measurement angles, $\alpha\beta$, to $\pi\pi$, $\pi 0$, 0π, and 00 determine the black box settings 00, 01, 10, and 11, respectively. In principle these settings remain hidden. The result of a measurement of physical qubit i is s_i which is 0 (1) for a measurement of $|+\alpha\rangle$ $\left(|-\alpha\rangle\right)$. For the computation to proceed deterministically, the black box must provide the measurement outcomes for feed-forward. The encoded qubits are transferred nonlocally to the remaining physical qubits in the cluster. Remarkably, the inversion-about–the-mean process is already hard-wired into the structure of the cluster state and is automatically implemented. The output of the computation, including feed-forward (FF), are two bits $\{s_2 \oplus s_4, s_3 \oplus s_1\}$ identifying the black box.

In Figure 5b, we show the experimental outcomes of the quantum computation. As in the previous computations, measurements were made using quarter-wave plates and polarizers. The "no FF" data are those computational outputs given that the black box outcomes, s_1 and s_4, were 0 which requires no feed-forward but reduces the success rate to $1/4$. In addition, we have measured individually all possible correlations between the measurement results from the black box and the readout. This enables us to implement the simplest feed-forward possible, where the earlier measurement determines the meaning of the final readout. Thus, when the black box measurement outcomes are other than $s_1 = 0$ and $s_4 = 0$, it is necessary to reinterpret the readout via the bit-wise addition shown above; the "FF" row of data shows the sum of the readouts interpreted in this way. In either case, the probability of the quantum computer determining the correct outcome is about 90%. These high-fidelity results shown in

Figure 5b constitute the first demonstration of a quantum algorithm in a cluster state quantum computer.

Conclusion

We have generated a four-qubit cluster state and characterized that state and its entanglement features. With that cluster, and taking advantage of a curious equivalence of a number of cluster states, we have demonstrated a universal set of single- and nontrivial two-qubit quantum logic gates in a one-way quantum computer. Our final realization of the Grover algorithm strongly underlines the basic simplicity of the cluster state approach. Given the various alternatives for their creation, such as linear optics, ion traps, and optical lattices, and the recent advances in the preparation of multi-particle entangled states, cluster states are promising for inclusion in future implementations of quantum computation. The most important challenges for the optical approach presented here are (a) realization of cluster states on demand, (b) generating cluster states with more qubits and (c) implementation of fast feedforward where the earlier measurement actually changes the setting of a future measurement in real time.

Methods

Experimental Preparation of Cluster States

In our experiment, entangled photons are created by using type-II parametric down-conversion[50]. A frequency-doubled laser pulse at 395nm makes two passes through a β-barium borate (BBO) crystal, which emits highly-entangled photons into the forward pair of modes a & b and backward pair of modes c & d (see Figure 6). To counter the

effect of birefringence in the BBO crystal, the polarization in each mode is rotated by 90° and the photons pass through compensation crystals which erase transverse and longitudinal walk-off. Final half wave plates (HWPs), one for each photon pair, and the tilt of the compensation crystals allow for the production of any of the four Bell states. The modes of the forward emitted pairs a & b and the modes of the backward emitted pairs c & d are coherently combined at polarizing beam-splitters (PBSs) by adjusting the position of the delay mirror for the UV-pump. The preparation of the cluster state is based on the simultaneous emission of four photons. The construction of the setup allows for four photon events to come from either two entangled pairs, one forward and one backward, or form double-pair emission into the modes a & b and c & d[26].

Proposed methods for producing cluster states are based on series of two-qubit gates such as the CPhase or CNOT. In our case the four-photon cluster state is generated directly from parametric down-conversion. Because of its intrinsic probabilistic nature the down-conversion process becomes exponentially inefficient for generating larger cluster states. Our way of generating the cluster states furthermore exploits the properties of polarizing beam-splitters (PBSs) and uses post-selection. A PBS is an optical device which transmits horizontally-polarized light and reflects vertically-polarized light. Considering the two-photon case, where after the PBS in each mode one photon has to be detected in each mode after the PBS, both incoming photons must have the same polarization, when they come from different input modes, or they must have orthogonal polarizations when entering along the same input mode. If the source produces simultaneously into the forward pair of modes a $\left|\Phi^{-}\right\rangle_{a,b}$ state, and backwards a $\left|\Phi^{+}\right\rangle_{c,d}$ state, only the state $\left|H\right\rangle_1\left|H\right\rangle_2\left|H\right\rangle_3\left|H\right\rangle_4-\left|V\right\rangle_1\left|V\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4$ results in a four-photon coincidence. However, there exists also the case where a four-photon emission into the two modes on either side results in a four-fold coincidence. The state must be in this case $-\left|H\right\rangle_1\left|H\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4$ coming from the $\left|\Phi^{-}\right\rangle_{a,b}$ setting and $+\left|V\right\rangle_1\left|V\right\rangle_2\left|H\right\rangle_3\left|H\right\rangle_4$

coming from the $\left|\Phi^{+}\right\rangle_{c,d}$ setting. The final emerging state is a superposition of all four terms.

In order to end up in a cluster state the phase of the $-\left|H\right\rangle_1\left|H\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4$ term has to be shifted by π. This can be done using a HWP in one mode, where according to a rotation by an angle ϕ the state after the PBSs evolves to $-\cos(2\phi)\left|H\right\rangle_1\left|H\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4$. Thus any HWP rotation larger than 22.5° results in a sign flip. At the same time, the Bell state is rotated to $\cos(\phi)\left|\Phi^{-}\right\rangle_{a,b}+\sin(\phi)\left|\Psi^{+}\right\rangle_{a,b}$, where the amount of the wanted $\left|\Phi^{-}\right\rangle_{a,b}$ state is decreased by a factor of $\cos(\phi)$. Due to the intrinsic property of the PBS only the amplitudes for the $\left|H\right\rangle_1\left|H\right\rangle_2\left|H\right\rangle_3\left|H\right\rangle_4-\left|V\right\rangle_1\left|V\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4$ terms are affected, while the $\left|\Psi^{+}\right\rangle_{1,2}$ Bell state does not contribute to any four-fold coincidence.

Note that after each PBS a quarter-wave plate (QWP) was placed to compensate birefringence effects. For each measurement, the phase of the back-reflected pair or four-photon was kept fixed and verified for each measurement setting. Taking into account the emission rates of the source for the entangled pairs, 28000 s^{-1} two-photon coincidences for the forward-emitted pair and 18000 s^{-1} coincidences for the backward-emitted pair, theoretical calculations show that a HWP rotation by 27.5° results in the maximally entangled cluster state of the form $\left|\Phi_{cluster}\right\rangle=\frac{1}{2}\left(\left|H\right\rangle_1\left|H\right\rangle_2\left|H\right\rangle_3\left|H\right\rangle_4+\left|H\right\rangle_1\left|H\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4+\left|V\right\rangle_1\left|V\right\rangle_2\left|H\right\rangle_3\left|H\right\rangle_4-\left|V\right\rangle_1\left|V\right\rangle_2\left|V\right\rangle_3\left|V\right\rangle_4\right)$. Thus, a HWP in mode a has been rotated to prepare this state. Fine-tuning has been done by short measurements to obtain approximately equal count-rates for each component.

1. Deutsch, D. & Ekert, E. Quantum computation. *Phys. World* **11**, 47-52 (1998).

2. Experimental proposals for quantum computation). *Fort. Phys.* **48** (special focus issue 9-11) (eds. Braunstein, S.L. and Lo, H.-K.), 767-1138 (2000).

3. Shor, P. W. in Proc. 35th Annu. Symp. Foundations of Computer Science (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, Los Alamitos, 1994)

4. Grover, L. K. Quantum mechanics helps in search for a needle in a haystack. Phys. Rev. Lett. 79, 325-328 (1997).

5. Bennett, C. & DiVicenzo, D. Quantum information and computation. *Nature* **404**, 247-255 (2000).

6. Ekert, A. & Josza, R. Quantum algorithms: entanglement enhanced information processing. *Philos. Trans. Roy. Soc. Lond. A* **356**, 1769-1782 (1998).

7. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402**, 390-393 (1999).

8. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46-52 (2001).

9. Linden, N. & Popescu, S. Good dynamics versus bad kinematics: Is entanglement needed for quantum computation?" *Phys. Rev. Lett.* **87**, 047901 (2001).

10. Josza, R. & Linden, N. On the role of the entanglement in quantum computational speed-up. *Proc. Roy. Soc. Lond. A* **459**, 2011-2032 (2003).

11. Nielsen, M. A. Quantum computation by measurement and quantum memory. *Phys. Lett. A* **308**, 96-100 (2003) **.**

12. Biham, E., Brassard, G., Kenigsberg, D. & Mor, T. Quantum computing without entanglement. *Theor. Comp. Sci.* **320**, 15-33 (2004).

13. Briegel, H. J. & Raussendorf, R. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.* **86**, 910-913 (2001).

14. Raussendorf R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188-5191 (2001).

15. Raussendorf R. & Briegel, H. J. Computational model underlying the one-way quantum computer. *Quant. Inform. Comput.* **2**, 344-386 (2001).

16. Raussendorf, R., Brown, D. E. & Briegel, H. J. The one-way quantum computer – a non-network model of quantum computation. *J. Mod. Opt.* **49**, 1299-1306 (2002).

17. Raussendorf, R., Brown, D. E. & Briegel, H. J. Measurement-based quantum computation on cluster states. *Phys. Rev. A* **68**, 022312 (2003).

18. Nielsen, M. & Dawson, C. M. Fault-tolerant quantum computation with cluster states. *quant-ph/0405134* (2004).

19. Mandel, O. et al. Controlled collisions for multiparticle entanglement of optically trapped ions. *Nature* **425**, 937-940 (2003).

20. O'Brien J. L., Pryde, G. J., White, A. G., Ralph, T. C. & Branning, D. Demonstration of an all-optical quantum controlled-not gate. *Nature* **426**, 264-267 (2003).

21. Pittman, T. B., Fitch, M. J., Jacobs, B. C. & Franson, J. D. Experimental controlled-not logic gate of single photons in the coincidence basis. *Phys. Rev. A* **68**, 032316 (2003).

22. Gasparoni, S., Pan, J.-W., Walther, P. Rudolph, T. & Zeilinger, A. Realization of a photonic controlled-NOT gate sufficient for quantum computation. *Phys. Rev. Lett.* **92**, 020504 (2004).

23. Sanaka, K., Jennewein, T., Pan, J.-W., Resch, K. & Zeilinger, A. Experimental nonlinear sign-shift for linear optics quantum computation. *Phys. Rev. Lett.* **92**, 017902 (2004).

24. Nielsen, M. A. Optical quantum computation using cluster states. *Phys. Rev. Lett.* **93**, 040503 (2004).

25. Browne, D. E. & Rudolph, T. Efficient linear optical quantum computation. *quant-ph/0405157* (2004).

26. Walther, P. et al. De Broglie wavelength of a non-local four-photon state. *Nature* **429**, 158-161 (2004).

27. Hein, M., Eisert, J. & Briegel, H.-J. Multi-party entanglement in graph states. *Phys. Rev. A* **69**, 062311 (2004)

28. Roos, C. F. et al. Control and measurement of three-qubit entangled states. *Science* **304**, 1478-1480 (2004)

29. Weinstein, Y. et al. Quantum process tomography of the quantum Fourier transform. *J. Chem. Phys.* **121**(13), 6117-6133 (2004).

30. Hradil, Z. Quantum-state estimation. *Phys. Rev. A* **55**, R1561-R1564 (1997).

31. Banaszek, K., Ariano, A., Paris, M. & Sacchi, M. Maximum-likelihood estimation of the density matrix. *Phys. Rev. A* **61**, 010304 (1999).

32. James, D., Kwiat, P., Munro, W. & White, A. Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001).

33. Toth, G. & Guehne, O. Detecting Genuine Multipartite Entanglement with Two Local Measurements. *quant-ph/0405165* (2004).

34. Dür, W. & Briegel, H.-J. Stability of macroscopic entanglement under decoherence. *Phys. Rev. Lett.* **92**, 180403 (2004).

35. Greenberger, D. M., Horne, M. A. & Zeilinger, A. Going beyond Bell´s theorem. *Bell´s Theorem, Quantum Theory and Concepts of the Universe.* M. Kafatos, Ed. Dordrecht: Kluwer, 49 (1989).

36. Zeilinger, A., Horne, M. & Greenberger, D. Higher-Order Quantum Entanglement *Squeezed States and Quantum Uncertainty.* College Park, D. Han, Y.S. Kim, W.W. Zachary (Eds.), NASA Conference Publication 3135, National Aeronautics and Space Administration (1992).

37. Dür, W, Vidal, G. & Cirac, J. I. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A* **62**, 62314-62325 (2000).

38. SenDe, A., Sen, U., Wiesniak, M., Kaszlikowski, D. and Zukowski, M. Multi-qubit W states lead to stronger nonclassicality than Greenberger-Horne-Zeilinger states. *Phys. Rev. A* **68**, 623306 (2003).

39. Horodecki, M., Horodecki, P. & Horodecki, R. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett.* A **223**, 1-8 (1996).

40. Peres, A. Separability criterion for density matrices. *Phys Rev. Lett.* **77**, 1413-1415 (1996).

41. Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455-2467 (1997).

42. Poyatos, J. F., Cirac, J. I., Zoller, P. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.* **78**, 390-393 (1997).

43. Schumacher, B. Quantum coding. *Phys. Rev. A* **51**, 2738-2747 (1995).

44. Coffman, V., Kundu, J. & Wootters, W. K., Distributed entanglement. *Phys. Rev. A* **61**, 052306 (2000).

45. Horodecki, R., Horodecki, P. & Horodecki, M. Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition. *Phys. Lett. A* **200**, 340-344 (1995).

46. Ahn, J., Weinacht, T. C. & Bucksbaum, P. H. Information storage and retrieval through quantum phase. *Science* **287**, 463-465 (2000).

47. Bhattacharya, N., van Linden van den Heuvell, H. B. & Spreeuw, R. J. C. Implementation of quantum search algorithm using classical Fourier optics. *Phys. Rev. Lett.* **88**, 137901 (2002).

48. Chuang, I. L., Gershenfeld, N. & Kubinec, M. Experimental implementation of a fast quantum searching. *Phys. Rev. Lett.* **80**, 3408-3411 (1997).

49. Jones, J. A., Mosca, M. & Hansen, R. H. Implementation of a quantum search algorithm on a quantum computer. *Nature* **393**, 344-346 (1998).

50. Kwiat, P. G. et al. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337-4342 (1995).

Acknowledgements: The authors thank H. J. Briegel, D. Browne and M. Zukowski for theoretical discussions and C. Först for assistance with graphics. This work was supported by the Austrian Science Foundation (FWF), NSERC, EPSRC, the European Commission under project RAMBOQ, and by the Alexander von Humboldt-Foundation.

Correspondences and requests for materials should be addressed to Ph.W. (pwalther@quantum.at) or A.Z. (zeilinger-office@quantum.at)

Figure 1 Few-qubit cluster states and the quantum circuits they implement. For each three- and four-qubit cluster the quantum state and the operations by its circuit are shown. In our experiment the computational basis $|0\rangle$ and $|1\rangle$ is represented by the horizontal and vertical polarization state, $|H\rangle$ and $|V\rangle$, respectively.The quantum state of those four physical qubits in the box is also explicitly written out as a polarization state where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization states and also represent our computational-basis states $|0\rangle$ and $|1\rangle$ respectively. For the case of the linear clusters **a)** $|\Phi_{lin3}\rangle$ and **b)** $|\Phi_{lin4}\rangle$, consecutive measurements on the qubits (1), 2, and 3 will perform a computation as a series of one-qubit rotation gates. The encoded input state undergoes single-qubit rotations with controllable angles and the output is left on physical qubit 4. In contrast, the horse-shoe clusters **c)** $|\Phi_{\subset 4}\rangle$ and **d)** $|\Phi_{\supset 4}\rangle$ and the box cluster **e)** $|\Phi_{\square 4}\rangle$ form more complex circuits containing both single-qubit *and* two-qubit gates, both of which are necessary to form a universal set of logic gates for quantum computation. In particular, measurements on two of the physical qubits (2 & 3 in the case of $|\Phi_{\subset 4}\rangle$**,** and 1 & 4 in the case of $|\Phi_{\supset 4}\rangle$ or $|\Phi_{\square 4}\rangle$) will perform the circuit defined by the particular cluster and transfer the logical output onto the remaining two physical qubits (1 & 4 in the case of $|\Phi_{\subset 4}\rangle$**,** and 2 & 3 in the case of $|\Phi_{\supset 4}\rangle$ or $|\Phi_{\square 4}\rangle$). When these cluster states are not a part of a larger cluster, the encoded input states are always $|\Psi_{in}\rangle = |+\rangle_{1E}$ for the one-qubit gates and $|\Psi_{in}\rangle = |+\rangle_{1E}|+\rangle_{2E}$ for the two-qubit gates. **f)** General input states can be prepared and processed through these operations when these clusters are subunits of larger clusters.

Figure 2 Density matrix of the four-qubit cluster state in the laboratory basis. Shown are the real (top) and imaginary (bottom) part of the density matrix for the ideal case **a)** and the reconstruction from the experimental four-photon tomography data **b)**. In both cases, there are four large diagonal components

corresponding to HHHH, HHVV, VVHH, and VVVV. The coherences between each of these diagonal elements show up as off-diagonal contributions and are necessary for quantum entanglement. The real density matrix was reconstructed via a maximum likelihood method using four-photon coincidence rates obtained in 256 polarization projections.

Figure 3 Output Bloch vectors from single qubit rotations using a three-qubit linear cluster $|\Phi_{lin3}\rangle$. The result of the ideal rotations **a)** are compared with the results of the measured rotations **b)** on the encoded input state $|+\rangle_{1E}$ for three different choices of measurement bases $B_2(\alpha)$. The output state is written in the laboratory basis. The measurement basis $B_3(\beta)$ for qubit 3 was fixed at $\beta = -\frac{\pi}{2}$. The angle α is set to $\frac{\pi}{2}$, $\frac{\pi}{4}$, and 0 for the Bloch vectors labelled 1, 2, and 3 respectively. These different choices of α result in different rotations about the $|L\rangle$-axis. The sense of the rotation is shown for decreasing α. Our final states, extracted from measured single-qubit tomography, had fidelities of $(0.86 \pm 0.03), (0.85 \pm 0.04)$, and (0.83 ± 0.03) with respect to the ideal output states. Outcomes for other choices of angles and hence other rotations are shown in Table 1b.

Figure 4 The output density matrices from two different two-qubit computations. Each density matrix is shown as two bar charts with the upper bar chart depicting the real part of the matrix and the lower chart depicting the imaginary part. In the case **a)**, single-qubit measurements were made on qubit 1 and 4 in the box cluster state $|\Phi_{\square 4}\rangle$. The measurement settings were $B_1(\pi)$ and $B_4(0)$ which results in the expected output state $|V\rangle_2|H\rangle_3$ in the lab basis. The

measured density matrix has (0.93 ± 0.01) fidelity with this state and no entanglement. In case **b)** single-qubit measurements in $B_2(0)$ and $B_3(0)$ were made on the horseshoe cluster state $|\Phi_{\subset 4}\rangle$**.** In this case, the expected output density matrix (left-hand side) and the experimentally-measured density matrix (right-hand side) are shown both in the lab basis. The measured and expected density matrices are in good agreement and this is reflected in the fidelity (0.84 ± 0.03). We extracted the tangle, a measure of entanglement, from the experimentally-measured density matrix to be $\tau = (0.65 \pm 0.11)$. This conclusively demonstrates that our cluster state quantum computer can generate quantum entanglement necessary for universal quantum computation.

Figure 5 Grover's algorithm in a cluster state quantum computer. **a)** The quantum circuit implementing Grover's search algorithm for two qubits. The box cluster state implements the quantum circuit shown in Figure 1e. These two circuits perform the equivalent computation when the readout measurements on physical qubits 2 and 3 in the box cluster are carried out in the bases $B_{2,3}(\pi)$. The rotations, and hence black box function, are fixed by the measurement settings $B_1(\alpha)$ and $B_4(\beta)$ on physical qubits 1 and 4. The circuit implements one of the four black-boxes in the search algorithm and processes the output through an inversion-about-the-mean operation. The output, which is the final states of physical qubits 2 and 3, reveals which black box was applied. **b)** The experimentally measured outputs of this quantum computation. The data labelled "no FF" show the computational outputs $\{s_2, s_3\}$ in those cases where the measurements in the black box found the "0" outcome. The data labelled "FF" show the outputs for all individually-measured outcomes from the black

box to which the feed-forward relation $\{s_2 \oplus s_4, s_3 \oplus s_1\}$ has been applied to the output results. The probability for successful identification of the function is approximately 90% in all cases.

Figure 6 The experimental setup to produce and measure cluster states. An ultra-violet laser pulse makes two passes through a nonlinear crystal which is aligned to produce entangled photon pairs $\left|\Phi^-\right\rangle_{a,b}$ in the forward direction in modes a & b and $\left|\Phi^+\right\rangle_{c,d}$ in the backward direction in modes c & d. Including the possibility of double-pair emission and the action of the polarizing beam-splitters, the four components of the cluster state can be prepared. The incorrect phase on the HHVV amplitude can easily be changed by using a half-wave plate in mode a. The amplitudes can be equalized by adjusting the relative coupling efficiency of those photon pairs produced in the backward pass as compared to the forward pass. Polarization measurements were carried out in modes 1 through 4 using quarter-wave plates and linear polarizers followed by single-mode fibre-coupled single-photon counting detectors behind 3nm interference filters.

Table 1 Fidelities of single-qubit rotations for the linear clusters states. The measured fidelities of the rotated output states are compared to the ideal rotation gate for the **a)** four-qubit linear cluster $|\Phi_{lin4}\rangle$ and **b)** three-qubit linear cluster $|\Phi_{lin3}\rangle$ from single-qubit tomography (1QT). For additional comparison we also extract the expected performance from full four-qubit tomography (4QT) based on ideal projective measurements on our reconstructed density matrix. The angles **a)** $\{\alpha,\beta,\gamma\}$ and **b)** $\{\alpha,\beta\}$ determine the set of single-qubit rotations implemented on the encoded qubits and are explained in the text. All output states are given in the lab basis.

a)

α	β	γ	*Output State (lab basis)*	*Fidelity (1QT)*	*Fidelity (4QT)*
0	0	0	$\|H\rangle$	0.97±0.03	0.81±0.03
π	0	$-\frac{\pi}{2}$	$\|V\rangle$	0.93±0.01	0.91±0.02
0	$-\frac{\pi}{2}$	$-\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)=\|+\rangle$	0.58±0.08	0.63±0.03
$\frac{\pi}{2}$	0	$-\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)=\|-\rangle$	0.87±0.04	0.84±0.03
0	$-\frac{\pi}{2}$	-0	$\frac{1}{\sqrt{2}}(\|H\rangle-i\|V\rangle)=\|R\rangle$	$0.99^{+0.01}_{-0.06}$	0.78±0.03
$\frac{\pi}{2}$	0	0	$\frac{1}{\sqrt{2}}(\|H\rangle+i\|V\rangle)=\|L\rangle$	$0.99^{+0.01}_{-0.02}$	0.94±0.03

b)

α	β	*Output State (lab basis)*	*Fidelity (1QT)*	*Fidelity (4QT)*
$\frac{\pi}{2}$	0	$\frac{1}{\sqrt{2}}\left(\lvert H\rangle + i\lvert V\rangle\right) = \lvert L\rangle$	0.60±0.05	0.73±0.04
$\frac{\pi}{2}$	$-\frac{\pi}{4}$	$\frac{1}{\sqrt{2}}\left(\lvert H\rangle - e^{-i\pi/4}\lvert V\rangle\right)$	0.74±0.06	0.78±0.03
$\frac{\pi}{2}$	$-\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}\left(\lvert H\rangle - \lvert V\rangle\right) = \lvert -\rangle$	0.86±0.03	0.83±0.03
$\frac{\pi}{4}$	$-\frac{\pi}{2}$	$\cos\left(\frac{\pi}{8}\right)\lvert H\rangle - \sin\left(\frac{\pi}{8}\right)\lvert V\rangle$	0.85±0.04	0.87±0.03
0	$-\frac{\pi}{2}$	$\lvert H\rangle$	0.83±0.03	0.80±0.02
$\frac{\pi}{4}$	$-\frac{\pi}{12}$	$\cos\left(\frac{\pi}{8}\right)\lvert H\rangle - \sin\left(\frac{\pi}{8}\right)e^{i7\pi/12}\lvert V\rangle$	0.67±0.05	0.75±0.03
$\frac{\pi}{2}$	$-\frac{\pi}{6}$	$\frac{1}{\sqrt{2}}\left(\lvert H\rangle - e^{i2\pi/3}\lvert V\rangle\right)$	0.65±0.5	0.76±0.03

Table 2 Fidelities of the output from two-qubit quantum computations in the **a)** box cluster, $|\Phi_{\square 4}\rangle$, and **b)** horseshoe cluster, $|\Phi_{\subset 4}\rangle$. In both cases, the encoded input state $|\Psi_{in}\rangle = |+\rangle_{1E}|+\rangle_{2E}$ evolves to a different output state depending on the settings for α and β. The fidelities of the two-qubit output state were extracted from two-qubit tomography (2QT) and predicted from the four-qubit tomography (4QT). All output states are written in the laboratory basis.

a)

α	β	*Output State (lab basis)*	*Fidelity (2QT)*	*Fidelity (4QT)*
0	0	$\|H\rangle_2\|H\rangle_3$	0.86±0.02	0.80±0.02
π	0	$\|V\rangle_2\|H\rangle_3$	0.93±0.01	0.93±0.01
π	π	$\|V\rangle_2\|V\rangle_3$	0.93±0.01	0.90±0.01
π	$\frac{\pi}{2}$	$\|V\rangle_2\|L\rangle_3$	0.94±0.01	0.84±0.02
$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}\left(\|V\rangle_2\|R\rangle_3 - i\|H\rangle_2\|L\rangle_3\right)$	0.64±0.05	0.64±0.02

b)

α	β	*Output State (lab basis)*	*Fidelity (2QT)*	*Fidelity (4QT)*
0	0	$\frac{1}{\sqrt{2}}\left(\|H\rangle_1\|+\rangle_4 + \|V\rangle_1\|-\rangle_4\right)$	0.84±0.03	0.77±0.02
0	$-\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}\left(\|H\rangle_1\|L\rangle_4 + \|V\rangle_1\|R\rangle_4\right)$	0.54±0.03	0.64±0.02
$-\frac{\pi}{2}$	0	$\frac{1}{\sqrt{2}}\left(\|H\rangle_1\|+\rangle_4 + i\|V\rangle_1\|-\rangle_4\right)$	0.76±0.03	0.73±0.02
$-\frac{\pi}{2}$	$-\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}\left(\|H\rangle_1\|L\rangle_4 + i\|V\rangle_1\|R\rangle_4\right)$	0.66±0.04	0.62±0.02

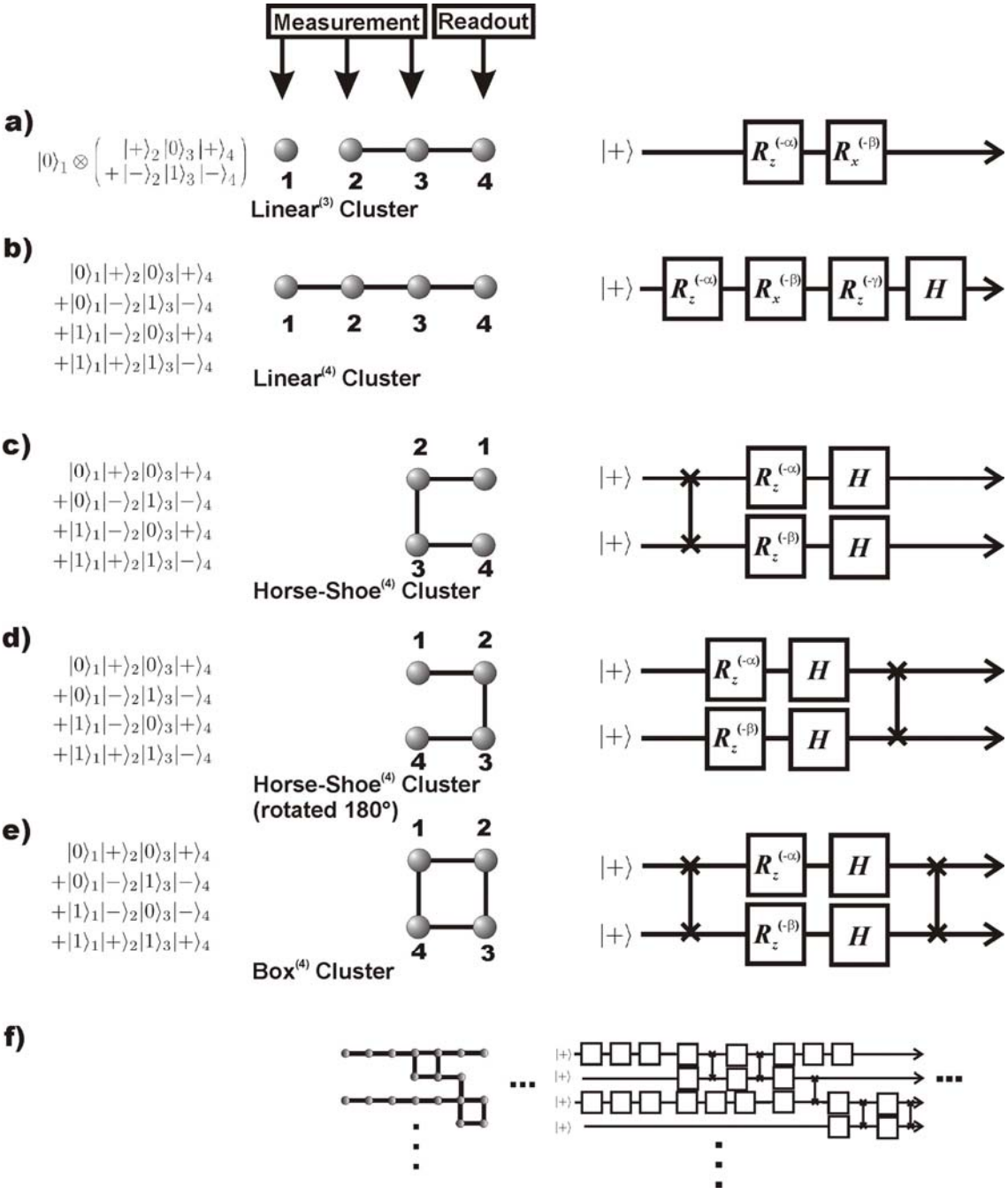

Measurement
Readout
a)
$|0\rangle_1 \otimes \begin{pmatrix} |+\rangle_2|0\rangle_3|+\rangle_4 \\ +|-\rangle_2|1\rangle_3|-\rangle_4 \end{pmatrix}$
1 2 3 4
Linear(3) Cluster
$|+\rangle$ $R_z^{(-\alpha)}$ $R_x^{(-\beta)}$
b)
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|-\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|+\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|-\rangle_4$
1 2 3 4
Linear(4) Cluster
$|+\rangle$ $R_z^{(-\alpha)}$ $R_x^{(-\beta)}$ $R_z^{(-\gamma)}$ H
c)
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|-\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|+\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|-\rangle_4$
2 1 3 4
Horse-Shoe(4) Cluster
$|+\rangle$ $R_z^{(-\alpha)}$ H
$|+\rangle$ $R_z^{(-\beta)}$ H
d)
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|-\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|+\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|-\rangle_4$
1 2 4 3
Horse-Shoe(4) Cluster
(rotated 180°)
$|+\rangle$ $R_z^{(-\alpha)}$ H
$|+\rangle$ $R_z^{(-\beta)}$ H
e)
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|-\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|-\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|+\rangle_4$
1 2 4 3
Box(4) Cluster
$|+\rangle$ $R_z^{(-\alpha)}$ H
$|+\rangle$ $R_z^{(-\beta)}$ H
f)

Figure 1

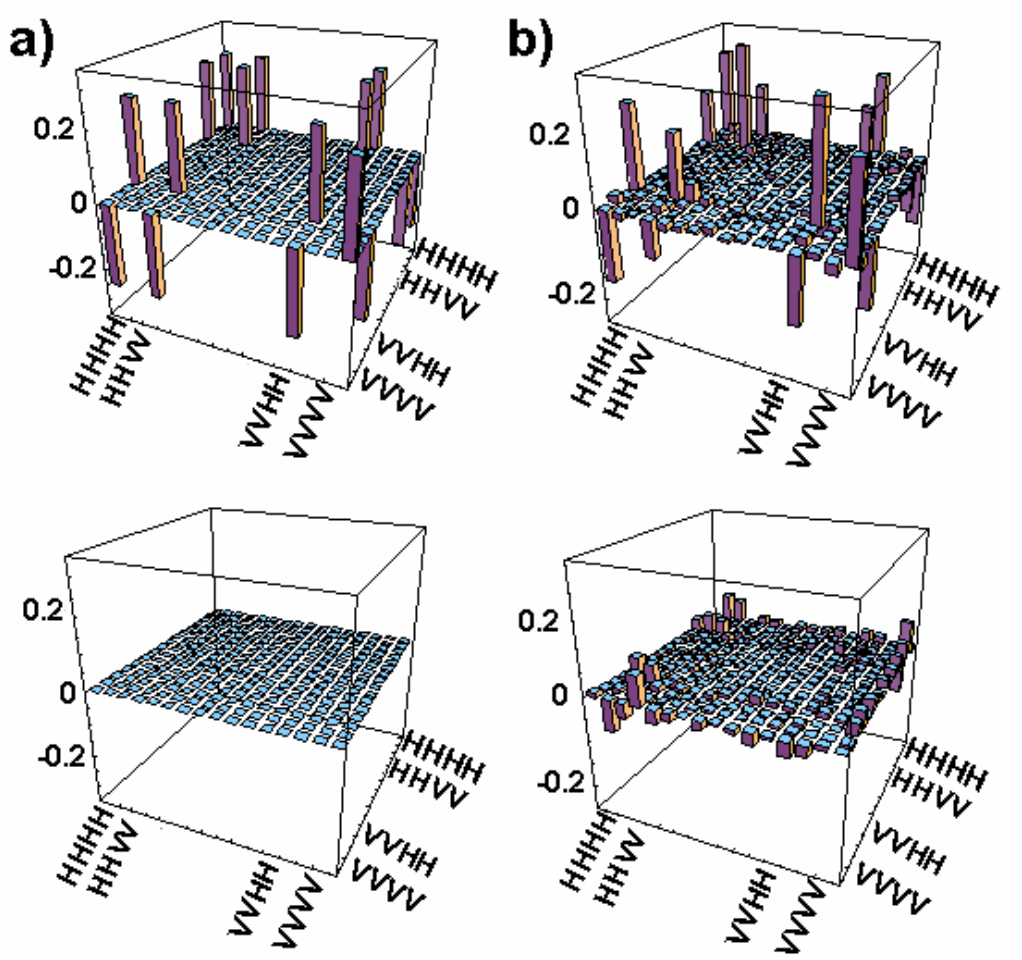


Figure 2

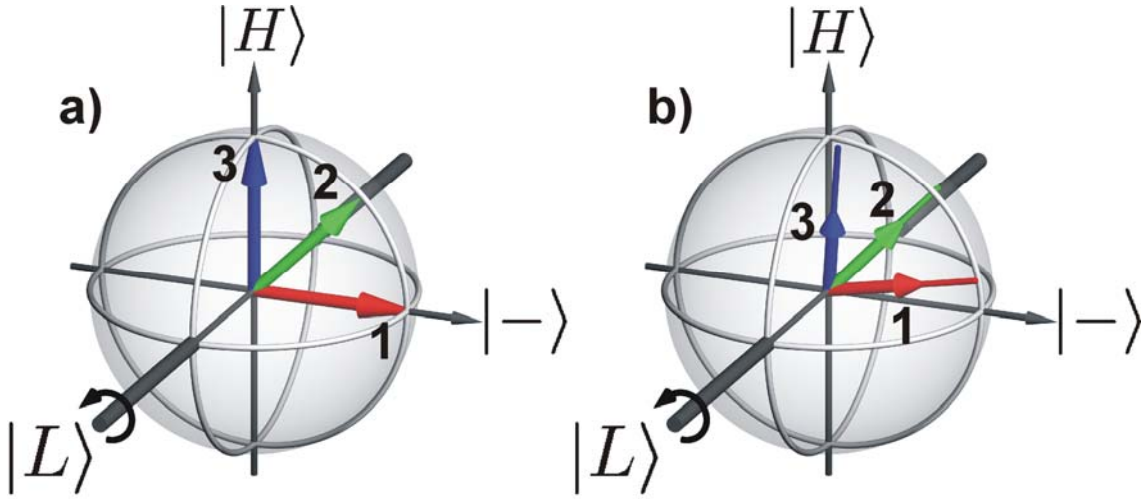


Figure 3

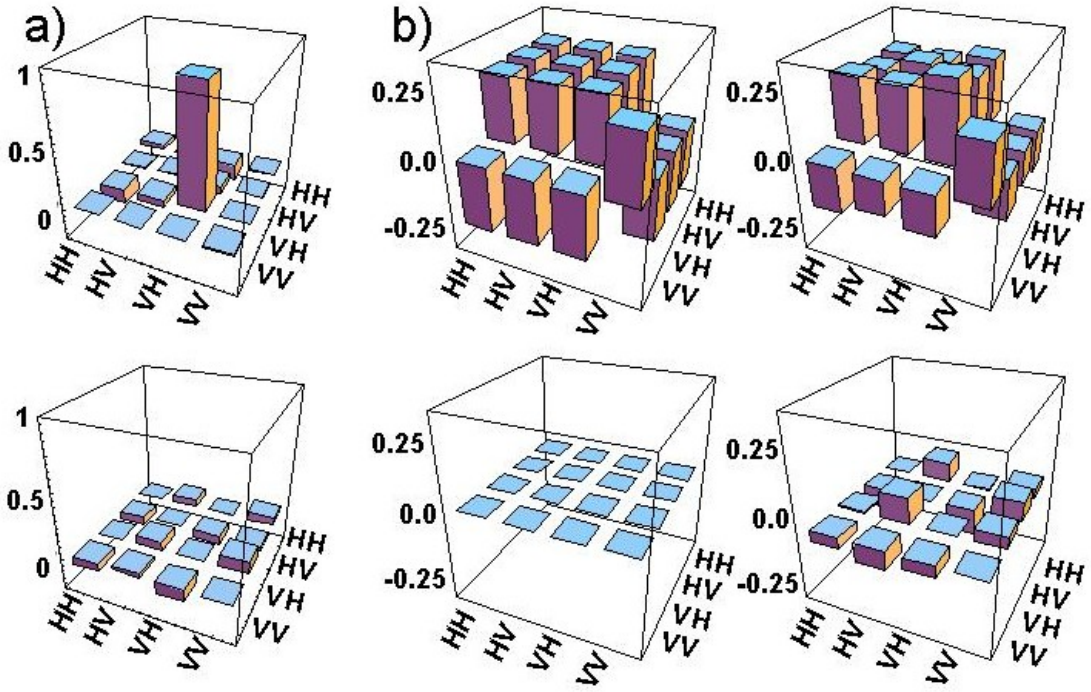


Figure 4

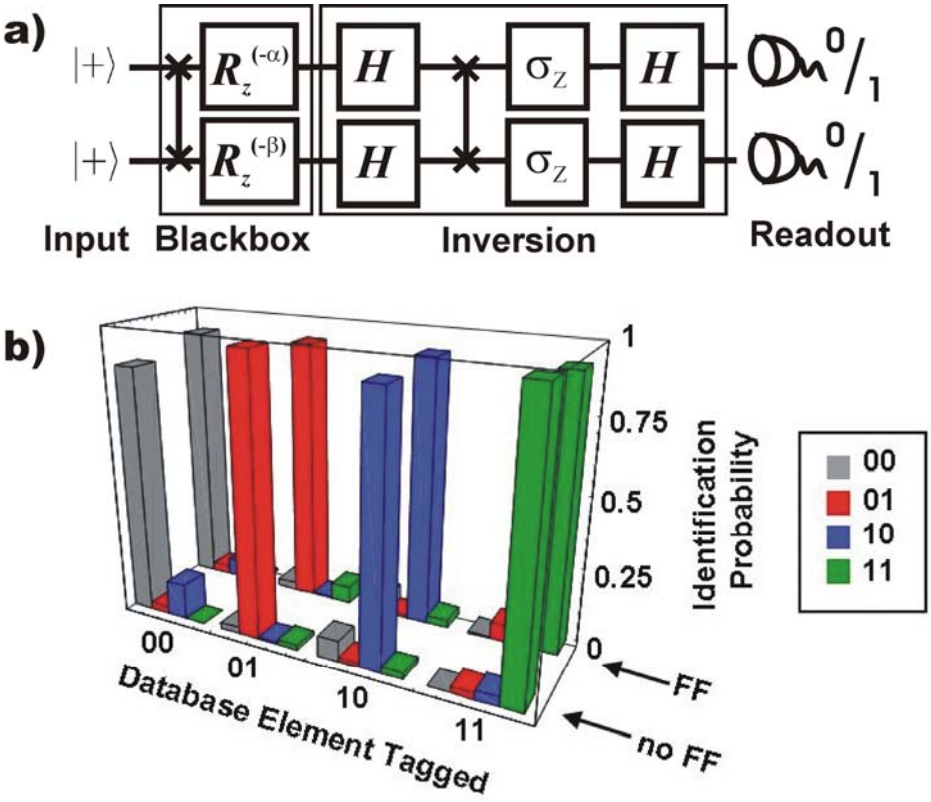


Figure 5

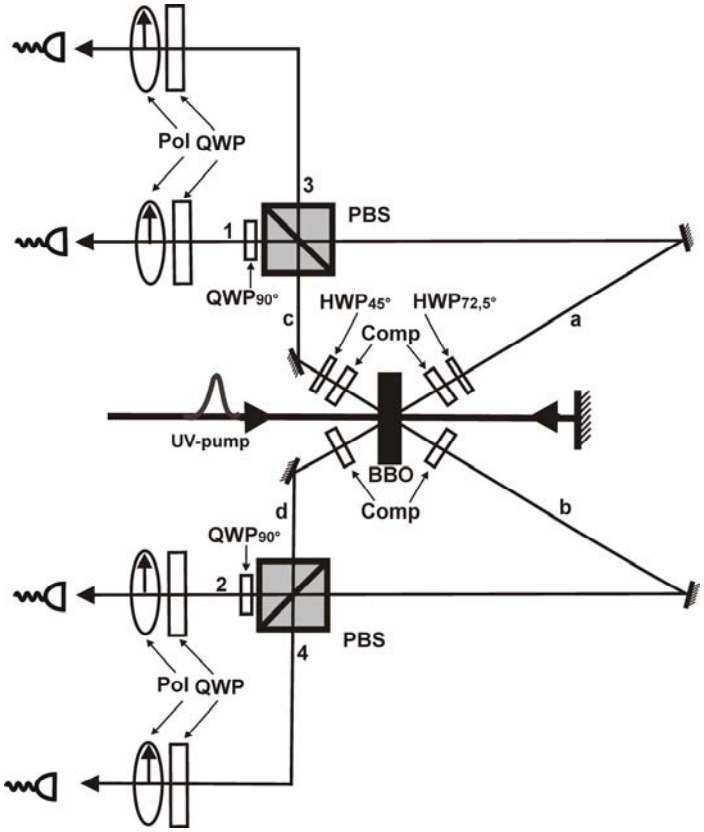

Pol QWP
3
PBS
1
QWP90°
c
HWP45°
HWP72,5°
Comp
a
UV-pump
BBO
Comp
d
b
QWP90°
2
PBS
4
Pol QWP

Figure 6

Quantum computation with ions in thermal motion

Anders Sørensen and Klaus Mølmer
Institute of Physics and Astronomy, University of Aarhus
DK-8000 Århus C

We propose an implementation of quantum logic gates via virtual vibrational excitations in an ion trap quantum computer. Transition paths involving unpopulated, vibrational states interfere destructively to eliminate the dependence of rates and revolution frequencies on vibrational quantum numbers. As a consequence quantum computation becomes feasible with ions whos vibrations are strongly coupled to a thermal reservoir.

Pacs. 03.67.Lx, 03.65 Bz, 89.70+c

Recently, methods to entangle states of two or several quantum systems in controlled ways have become subject of intense studies. Such methods may find applications in fundamental tests of quantum physics [1] and in precision spectroscopy [2]; and they offer fundamentally new possibilities in quantum communication and computing [3]. A major obstacle to these efforts is decoherence of the relevant quantum states. In many proposed implementations of quantum computation the quantum bits (qubits) are stored in physical degrees of freedom with long coherence times, like nuclear spins, and decoherence is primarily due to the environment interacting with the channel used to perform logic gates between qubits [4]. In this Letter we present a scheme which is insensitive to the interaction between the quantum channel and the environment. Specifically, we consider an implementation of quantum computation in an ion trap, but we hope to stimulate similar ideas to reduce decoherence in other physical implementations.

The ion trap was originally proposed by Cirac and Zoller [5] as a system with good experimental (optical) access and control of the quantum degrees of freedom, and they suggested an implementation of the necessary ingredients in terms of one-bit and two-bit operations to carry out quantum computation. In the ion trap computer, qubits are represented by internal states of the ions. The number of qubits equals the number of ions, and this system is scalable to the problem size in contrast to NMR quantum computation which is only applicable with a limited number of qubits [6].

The ion trap method [5] uses collective spatial vibrations for communication between ions, and it requires that the system is restricted to the joint motional ground state of the ions. For two ions this has recently been accomplished [7]. We present an alternative implementation of quantum gates that is both insensitive to the vibrational state and robust against changes in the vibrational motion occurring during operation, as long as the ions are in the Lamb-Dicke regime, *i.e.*, their spatial excursions are restricted to a small fraction of the wavelength of the exciting radiation. Our mechanism relies on features of quantum mechanics that are often responsible for "paradoxical effects": i) The vibrational degrees of freedom used for communication in our scheme only enter virtually *i.e.*, although they are crucial as intermediate states in our processes, we never transfer population to states with different vibrational excitation. ii) Transition paths involving different unpopulated, vibrational states interfere destructively to eliminate the dependence of rates and revolution frequencies on vibrational quantum numbers.

Like in the original ion trap scheme [5], we address each ion with a single laser, but quantum logic gates involving two ions are performed through off-resonant laser pulses. For the laser addressing the first ion, we choose a detuning close to the upper sideband, *i.e.*, close to resonance with a joint vibrational and internal excitation of the ion. We choose the detuning of the laser addressing the second ion to be the negative of the detuning of the first laser, see Fig. 1 (a). This laser setting couples the states $|ggn\rangle \leftrightarrow \{|egn+1\rangle, |gen-1\rangle\} \leftrightarrow |een\rangle$, where the first (second) letter denotes the internal state e or g of the first (second) ion and n is the quantum number for the relevant vibrational mode of the trap. We choose the detuning from the sideband so large that the intermediate states $|egn+1\rangle$ and $|gen-1\rangle$ are not populated in the process. As we shall show below, the internal state transition is insensitive to the vibrational quantum number n, and it may be applied even with ions which exchange vibrational energy with a surrounding reservoir.

If we tune the lasers sufficiently close to the sidebands we can neglect all other vibrational modes and concentrate on one collective degree of vibrational excitation of the ions [8]. In this case our system can be described by the following Hamiltonian

$$\begin{aligned} H &= H_0 + H_{\rm int} \\ H_0 &= \hbar\nu(a^\dagger a + 1/2) + \hbar\omega_{eg}\sum_i \sigma_{zi}/2 \\ H_{\rm int} &= \sum_i \frac{\hbar\Omega_i}{2}(\sigma_{+i}e^{i(\eta_i(a+a^\dagger)-\omega_i t)} + h.c.), \end{aligned} \qquad (1)$$

where ν is the frequency and $a^\dagger$ and a are the ladder operators of the vibrational mode and $\hbar w_{eg}$ is the energy difference between the internal states e and g. Pauli matrices σ_i represent the internal degrees of freedom for the

i'th ion, and ω_i and Ω_i are the frequency and Rabi frequency of the laser addressing the i'th ion. [In a practical realization, one might use Raman transitions between low lying states of the ions due to their long coherence time. By appropriate redefinition of the symbols our formalism also describes this implementation [9].] We consider an ion trap operating in the Lamb-Dicke limit, *i.e.* the ions are cooled to a regime with vibrational quantum numbers n ensuring that $\eta_i\sqrt{n+1}$ is well below unity (Note that this may still allow n-values well above unity.) In our analytical calculations we use an expansion of $H_{\rm int}$ to second order in η_i, but in our numerical treatment we apply the exact Hamiltonian (1).

We wish to perform an operation on the mutual state of two ions 1 and 2 selected freely within the string of ions, and we assume that $\eta_1 = \eta_2 = \eta$ and $\Omega_1 = \Omega_2 = \Omega$. With the choice of detunings described above, the only energy conserving transitions are between $|ggn\rangle$ and $|een\rangle$. The Rabi frequency $\tilde{\Omega}$ for the transition between these states, via intermediate states m, can be determined in second order perturbation theory,

$$(\frac{\tilde{\Omega}}{2})^2 = \frac{1}{\hbar^2}\mid \sum_m \frac{\langle een|H_{\rm int}|m\rangle\langle m|H_{\rm int}|ggn\rangle}{E_{ggn}+\hbar\omega_i - E_m}\mid^2, \qquad (2)$$

where the laser energy $\hbar\omega_i$ is the energy of the laser addressing the ion which is excited in the intermediate state $|m\rangle$. If we restrict the sum to $|egn+1\rangle$ and $|gen-1\rangle$, we get

$$\tilde{\Omega} = -\frac{(\Omega\eta)^2}{2(\nu-\delta)}, \qquad (3)$$

where $\delta = \omega_1 - \omega_{eg}$ is the detuning of the laser addressing the first ion [10].

The remarkable feature in Eq. (3) is that it contains no dependence on the vibrational quantum number n. This is due to interference between the two paths indicated in Fig. 1(b). If we take the path where ion No. 1 is excited first, we have a factor of $n+1$ appearing in the enumerator ($\sqrt{n+1}$ from raising and $\sqrt{n+1}$ from lowering the vibrational quantum number). In the other path we obtain a factor of n. Due to the opposite detunings, the denominators in Eq. (2) have opposite signs and the n dependence disappears when the two terms are subtracted. The coherent evolution of the internal atomic state is thus insensitive to the vibrational quantum numbers, and it may be observed with ions in any superposition or mixture of vibrational states.

From the above arguments we expect to see perfect sinusoidal oscillations between the population of the internal states $|gg\rangle$ and $|ee\rangle$. To confirm the validity of our pertubative analysis we have performed a direct numerical integration of the Scrödinger equation with the Hamiltonian (1) to all orders in η. We have considered a situation, where both ions are initially in the internal ground state. For the vibrational state, we have investigated a number of different states, including Fock, coherent and thermal states, all yielding qualitatively similar results. The outcome of the computation for a coherent state of vibrational motion can be seen in Fig. 2, where we show the evolution of relevant terms of the atomic internal state density matrix $\rho_{ij,kl} = Tr_n(\rho|kl\rangle\langle ij|)$, where $i,j,k,l = e$ or g, and where Tr_n denotes the partial trace over the unobserved vibrational degrees of freedom. The figure clearly shows that we have Rabi oscillations between the atomic states $|gg\rangle$ and $|ee\rangle$, and the values of the off diagonal element $\rho_{gg,ee}$ confirm that we have a coherent evolution of the internal atomic state which is not entangled with the vibrational motion. Superimposed on the sinusoidal curves are small oscillations with a high frequency due to off resonant couplings of the type $|ggn\rangle \rightarrow |egn+1\rangle$,$|ggn\rangle \rightarrow |gen-1\rangle$ and $|ggn\rangle \rightarrow |egn\rangle$. The magnitude of these oscillation and the deviation from ideal transfer between $|gg\rangle$ and $|ee\rangle$ can be suppressed by decreasing Ω.

The analysis given so far is sufficient for creation of internal state entanglement, completely decoupled from the external motion of the ions. By optical pumping we can prepare a state $\rho = |gg\rangle\langle gg| \otimes \rho_{vib}$, and if we apply radiation fields corresponding to a pulse of duration $T = \frac{\pi}{2|\tilde{\Omega}|}$, our system is described by the density operator $\rho = |\psi\rangle\langle\psi| \otimes \rho_{vib}$, where $|\psi\rangle$ is a maximally entangled EPR-state $\frac{1}{\sqrt{2}}(|gg\rangle - i|ee\rangle)$.

Since the states $|eg\rangle$ and $|ge\rangle$ do not fulfill any resonance condition one might expect that they are unaffected by the laser pulses. Due to n-dependent perturbations of the energy levels by the lasers this is, however, not the case. Keeping only the most important terms, we get the energy shifts

$$\begin{aligned}
\Delta E_{ggn} &= \Delta E_{een} = -\hbar\frac{(\eta\Omega)^2}{4}\frac{1}{\nu-\delta}\\
\Delta E_{egn} &= \hbar\left(\frac{(\eta\Omega)^2}{2}\frac{n}{\nu-\delta} - \frac{\Omega^2}{2\delta}\right)\\
\Delta E_{gen} &= \hbar\left(-\frac{(\eta\Omega)^2}{2}\frac{n+1}{\nu-\delta} + \frac{\Omega^2}{2\delta}\right).
\end{aligned} \qquad (4)$$

The energy shifts of the $|een\rangle$ and $|ggn\rangle$ are identical and independent of n, but since the energy shifts of $|egn\rangle$ and $|gen\rangle$, depend on the vibrational quantum number, the time evolution introduces phase factors $e^{-i\Delta E_{egn}t/\hbar}$, which depend on n, and *e.g.*, at the time $t = T_{inv} = \frac{2\pi(\nu-\delta)}{\eta^2\Omega^2}$ where $|gg\rangle$ end $|ee\rangle$ are inverted, factors of $(-1)^n$ will tend to extinguish the coherence between internal states $|ee\rangle$ and $|eg\rangle$. This coherence can be restored by a trick resembling photon echoes [11]. Notice that the n dependent part of ΔE_{egn} is minus the n dependent part of ΔE_{gen}. If at any time $T/2$ we change the sign of the laser detuning δ, phase components proportional to n will begin to rotate in the opposite direction and at

time T we will have a revival of the coherence. This is confirmed by our numerical solution of the Schrödinger equation presented in Fig. 3, where we change the laser detunings at the time $T_{inv}/2$ and at the time T_{inv} we have completed the transfer $\frac{1}{\sqrt{2}}(|gg\rangle + |eg\rangle) \rightarrow \frac{1}{\sqrt{2}}(-i|ee\rangle + |eg\rangle)$.

No particularly demanding assumptions have been made for the experimental parameters. With a vibrational frequency $\nu/2\pi = 200$ kHz, the transition shown in Fig. 2, require Rabi frequencies $\Omega/2\pi$ of modest 20 kHz, and the evolution from $|gg\rangle$ to $|ee\rangle$ is accomplished in 5 ms. To be relevant for real computational tasks it is necessary that our evolution is robust against decoherence effects on this long time scale. An important source of decoherence is heating of the vibrational motion, and it is a major asset of our proposal that it can be made insensitive to the interaction with the environment: The arguments leading to Eq. (3) do not require that the ions remain in the same vibrational state, and the coherent oscillation from $|gg\rangle$ to $|ee\rangle$ may still be observed when the vibrational motion exchange energy with a thermal reservoir. The photon echo trick, however, is sensitive to heating: If the vibrational quantum number n change its value at the time $T/2$ where the detunings are inverted, the second half of the gate, will no longer revert the phase evolution due to the new value of n and coherence is lost. If instead the detunings are inverted N times during a gate, the erroneous phase will only be on the order of the phase evolution in time T/N, and the effect of the heating is reduced.

Rather than inverting the detunings a large number of times, we suggest to continuously apply lasers with both detunings $\pm\delta$ on both ions. With two fields of opposite detunings and identical Rabi frequency Ω there are two contributing paths in addition to the two paths in Fig. 1. The contribution from the two additional paths are identical to the two original paths and the only modifications to the $|gg\rangle \leftrightarrow |ee\rangle$ Rabi frequency in Eq. (3) is multiplication by a factor of two. With bichromatic fields there also exists a resonant transition from $|eg\rangle$ to $|ge\rangle$. The Rabi frequency of this transition is the negative of the Rabi frequency from $|gg\rangle$ to $|ee\rangle$ and the evolution will be described by

$$\begin{aligned}
|gg\rangle &\rightarrow \cos(\frac{\tilde{\Omega}T}{2})|gg\rangle + i\ \sin(\frac{\tilde{\Omega}T}{2})|ee\rangle \\
|ee\rangle &\rightarrow \cos(\frac{\tilde{\Omega}T}{2})|ee\rangle + i\ \sin(\frac{\tilde{\Omega}T}{2})|gg\rangle \\
|ge\rangle &\rightarrow \cos(\frac{\tilde{\Omega}T}{2})|ge\rangle - i\ \sin(\frac{\tilde{\Omega}T}{2})|eg\rangle \\
|eg\rangle &\rightarrow \cos(\frac{\tilde{\Omega}T}{2})|eg\rangle - i\ \sin(\frac{\tilde{\Omega}T}{2})|ge\rangle. \qquad (5)
\end{aligned}$$

To validate that the evolution in Eq. (5) is in fact stable against heating we introduce a thermal reservoir described by relaxation operators $c_1 = \sqrt{\Gamma(1+n_{\rm therm})}a$ and $c_2 = \sqrt{\Gamma n_{\rm therm}}a^\dagger$, where Γ characterizes the strength of the interaction and $n_{\rm therm}$ is the mean vibrational number in thermal equilibrium. We analyse the dynamics of the system using Monte Carlo wavefunctions [12], which evolve with a non Hermitian Hamiltonian interrupted by jumps at random times. The result of the computation can be seen in Fig. 4, where we show (left) the result of a single Monte Carlo realization with quantum jumps indicated by arrows and (right) the average over 10 realizations. In the figure we have chosen $n_{\rm therm} = 2$. This rather low value could represent a heating mechanism counteracted by laser cooling on a particular ion reserved for this purpose. In the simulations 34 vibrational quanta are exchanged with the reservoir on average, and we wish to emphasize that with the proposed scheme the gate is almost unaffected even though the duration of the gate is much longer than the coherence time of the channel used to communicate between the qubits.

It has been proven that any unitary evolution involving a number of qubits can be constructed using only single qubit operations and a simple universal quantum gate like for instance the two-qubit control-not operation [13]. With the evolution described by Eq. (5) a control-not operation is created by the following sequence of operations: P_1, ${P_2}^{-1}$, H_2, R, P_1, H_1, P_1, R and P_2, where R is the evolution in Eq. (5) with $T = \frac{\pi}{2|\tilde{\Omega}|}$, P_i is a $\pi/2$ phase change of $|e\rangle$ in ion i, and H_i is a Hadamard transformation on ion i. With ready access to one-qubit operations in the ion trap we thus have available the ingredients for successful quantum computation.

We note that with only two ions in the trap, the use of bichromatic light leads to the evolution (5) even without individual optical access, and if many ions are illuminated by the same field, multi particle entanglement is created [14]. As a further remarkable feature of our implementation, we note how easy it is to simultaneously operate on different pairs of ions: If we wish to apply our gate on the pairs (i,j) and (k,l), we simply illuminate ions i and j with fields of detunings $\pm\delta_{ij}$ and ions k and l with another pair of detunings $\pm\delta_{kl}$. The only resonant transitions are the ones of the two desired gates and, however mind boggling this may be, the virtually excited but never populated vibrational mode has been used for two processes at the same time.

Note added: Since submission of this work, two proposals for computing with vibrationally excited ions have appeared. [15] uses widely separated vibrational states, and can hardly be generalized beyond 2 or 3 qubits; [16] involves dynamics which is conditioned on the vibrational state and is not applicable during heating.

[1] D. M. Greenberger, M. A. Horne and A. Zeilinger, Physics Today **46**, 22-29, August 1993.

[2] J. J. Bollinger, W. M. Itano, D. J. Wineland and D. J. Heinzen, Phys. Rev. A **54**, 4649 (1996).

[3] Physics World **11**, 33-57, March 1998. Special issue on Quantum Information.

[4] B. E. Kane, Nature **393**, 133 (1998), T. Pellizari, S. A. Gardiner, J. I. Cirac and P. Zoller, Phys. Rev. Lett. **75**, 3788 (1995).

[5] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[6] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung and S. Lloyd, Nature vol. **393**, 143 (1998); I. L. Chuang, N. Gershenfeld and M. Kubinec, Phys. Rev. lett. **80**, 3408 (1998); J. Jones, M. Mosca and R. H. Hansen, Nature vol **393**, 344 (1998).

[7] B. E. King, C. S. Wood, C. J. Myatt, Q. A. Turchette, D. Leibfried, W. M. Itano, C. Monroe, D. J. Wineland, Phys. Rev. Lett. **81**, 1525 (1998); Q. A. Turchette, C. S. Wood, B. E. King, C. J. Myatt, D. Liebfried, W. M. Itano, C. Monroe and D. J. Wineland, Phys. Rev. Lett. **81**, 3631 (1998).

[8] Numerical calculations retaining two collective vibrations for a two ion system have confirmed the validity of the omission of the far off-resonant vibration modes.

[9] D. M. Meekhof, C. Monroe, B. E. King, W. M. Itano and D. J. Wineland, Phys. Rev. Lett. **76**, 1796 (1996).

[10] If the additional coupling to the lower (higher) sideband of ion 1 (2) is included $2(\nu-\delta)$ in Eq. (3) is replaced by $(\nu^2-\delta^2)/\nu$.

[11] L. Allan and J. M. Eberly, 'Optical resonance and two-level atoms' Ch. 9, Dover, New York, 1987.

[12] K. Mølmer, Y. Castin and J. Dalibard, J. Opt. Soc. Am. B **10 524** (1993).

[13] A. Barenco, C. H. Bennet, R. Cleve, D. P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin and H. Weinfurter, Phys. Rev. A **55**, 3457 (1995).

[14] K. Mølmer and A. Sørensen, Schrödinger's cat in a hot trap, quant-ph 9810040.

[15] J. F. Poyatos, J. I. Cirac and P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998).

[16] S. Schneider, D. F. V. James and G. J. Milburn, quant-ph 9808012.

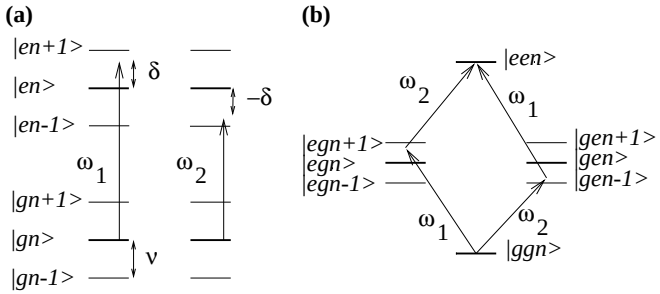


FIG. 1. Energy levels and laser detunings. **(a)** Two ions with quantised vibrational motion are illuminated with lasers detuned close to the upper and lower sidebands. **(b)** The ions oscillate in collective vibrational modes, and two interfering transition paths are identified.

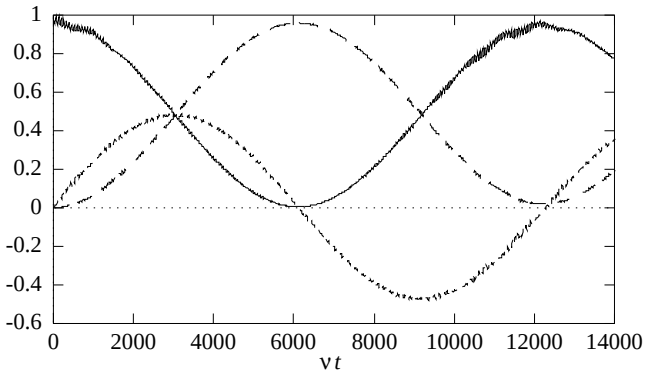


FIG. 2. Rabi oscillations between $|gg\rangle$ and $|ee\rangle$. The figure shows the time evolution of the internal atomic density matrix elements $\rho_{gg,gg}$ (full line), $\rho_{ee,ee}$ (long dashed line) and $Im(\rho_{gg,ee})$ (short dashed line). The magnitude of $Re(\rho_{gg,ee})$ is below 0.03 and is not shown. In the initial state, the ions are in the internal ground state and a coherent vibrational state with mean excitation $\bar{n}=2$. Parameters are $\delta=0.90\ \nu$, $\Omega=0.10\ \nu$ and $\eta=0.10$

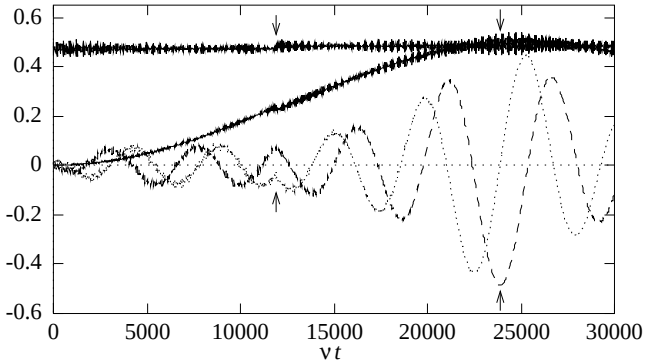


FIG. 3. Revival of coherence at T_{inv}. Initially ion 1 is in a superposition $\frac{1}{\sqrt{2}}(|g\rangle+|e\rangle)$ and ion 2 is in $|g\rangle$. The sign of δ is changed at $T_{inv}/2$ (left arrows), to ensure the perfect transition at T_{inv} (right arrows). The full lines represent populations of $|ee\rangle$ and $|eg\rangle$. The dotted and the dashed curves represent the real and imaginary part of the coherence $\rho_{ee,eg}$. Parameters are $\delta=0.90\ \nu$, $\Omega=0.05\ \nu$ and $\eta=0.1$

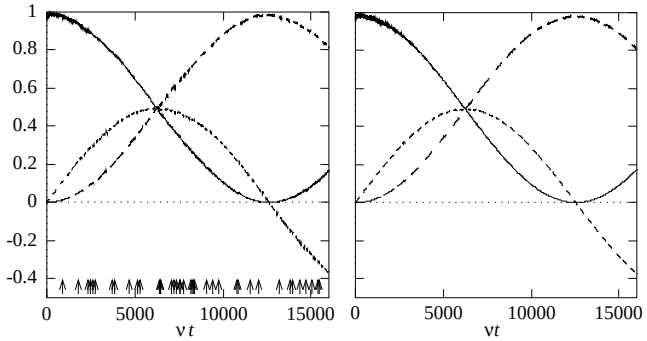


FIG. 4. Rabi oscillations in a heating trap. The left panel shows the result of a single Monte Carlo realization with a total of 39 jumps occuring at times indicated by the arrows. The right panel is an average over 10 realizations. The curves represent $\rho_{gg,gg}$ (full line), $\rho_{ee,ee}$ (long dashed) and $Im(\rho_{gg,ee})$ (short dashed). Parameters are $\delta = 0.90\ \nu$, $\Omega = 0.10\ \nu$, $\eta = 0.1$, $\Gamma = 2 * 10^{-4}\ \nu$ and $n_{\rm term} = 2$.

Separability of very noisy mixed states and implications for NMR quantum computing

S. L. Braunstein,[1] C. M. Caves,[2] R. Jozsa,[3] N. Linden,[4] S. Popescu,[4,5] and R. Schack[2,6]
[1] *SEECS, University of Wales, Bangor LL57 1UT, UK*
[2] *Center for Advanced Studies, Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156, USA*
[3] *School of Mathematics and Statistics, University of Plymouth, Devon PL4 8AA, UK*
[4] *Isaac Newton Institute for Mathematical Sciences, Cambridge, CB3 0EH, UK*
[5] *BRIMS, Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, UK*
[6] *Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK*
(1998 December 2)

We give a constructive proof that all mixed states of N qubits in a sufficiently small neighborhood of the maximally mixed state are separable. The construction provides an explicit representation of any such state as a mixture of product states. We give upper and lower bounds on the size of the neighborhood, which show that its extent decreases exponentially with the number of qubits. We also discuss the implications of the bounds for NMR quantum computing.

PACS numbers: 03.67.-a, 03.67.Lx, 76.60.-k, 89.80.+h

In this Letter we investigate the structure of the space of density matrices of N spin-1/2 particles (qubits). In particular, we consider density matrices that are close to the maximally mixed density matrix and ask whether or not they are separable, i.e., whether they can be written as mixtures of direct products. One might imagine that the issue is straightforward, in that the maximally mixed state seems to be very far from the boundary between separable and nonseparable states. It might be the case, however, that the maximally mixed density matrix is surrounded by separable matrices, but that these separable density matrices lie in a low-dimensional subspace within the space of all density matrices. By leaving this subspace, even infinitesimally, one could reach entangled density matrices.

In [1] this problem is addressed by an existence proof; namely, it is shown that there exists a sufficiently small neighborhood of the maximally mixed density matrix inside which all density matrices are separable. In [2], a lower bound on the size of the neighborhood is given. Here we go further by giving a constructive proof that provides an explicit representation of any state sufficiently close to the maximally mixed one as a mixture of product states. We give an upper and a much improved lower bound on the size of the neighborhood, which show that it decreases exponentially with the number of qubits.

Our results have immediate implications for present research that makes use of high-temperature nuclear magnetic resonance (NMR) for quantum information processing and quantum computation [3–14]. Since the first proposals to use NMR for quantum computation, there has been surprise about the apparent ability to perform quantum computations in room-temperature thermal ensembles. It has been a puzzle how these thermal states, which are very close to the maximally mixed state, could correspond to truly entangled states [15]. The bounds we calculate show that *all states so far used in NMR to simulate quantum computations or other quantum-information protocols are separable.* This is not to say that NMR techniques are incapable of producing entangled states, in principle. Increasing the number of correlated spins might eventually lead to nonseparable states, but this question is left open by the bounds derived in this paper.

We consider arbitrary density matrices for N qubits, written as

$$\rho_\epsilon = (1-\epsilon)M_d + \epsilon\rho_1 \ , \tag{1}$$

where $d = 2^N$ is the Hilbert-space dimension for N qubits, $M_d = 1_d/d$ is the maximally mixed density matrix (1_d is the identity matrix in d dimensions), and ρ_1 is an arbitrary density matrix. Any density matrix can be written in the form (1). We show that for ϵ sufficiently small, all density matrices of the form (1) are separable. We define two kinds of representations of ρ_ϵ in terms of product states, which provide candidates for ensemble decompositions of ρ_ϵ as a mixture of product states. By considering these candidate decompositions, we derive an explicit lower bound on the size of the neighborhood of separable states. We conclude by establishing an explicit upper bound on the size of the neighborhood.

Our approach is to represent an arbitrary density matrix in an overcomplete matrix basis, each basis element of which is a pure direct-product density matrix. If all the coefficients of a density matrix in this representation are nonnegative, the coefficients can be considered to represent probabilities, and the density matrix is separable, as it is then a mixture of direct products.

All of our representations arise ultimately from expanding a density matrix for N qubits in terms of direct products of Pauli matrices:

$$\rho = \frac{1}{2^N} c_{\alpha_1\ldots\alpha_N}\sigma_{\alpha_1}\otimes\cdots\otimes\sigma_{\alpha_N} \ . \tag{2}$$

Here and throughout we sum over repeated indices: Greek indices run over the values 0,1,2,3, and Latin in-

dices take on the values 1,2,3. The matrix $\sigma_0 = 1_2$ is the two-dimensional identity matrix, and the matrices σ_i, $i = 1, 2, 3$, are the Pauli matrices. The (real) expansion coefficients in Eq. (2) are given by

$$c_{\alpha_1 \ldots \alpha_N} = \mathrm{tr}\big(\rho\, \sigma_{\alpha_1} \otimes \cdots \otimes \sigma_{\alpha_N}\big) \ . \tag{3}$$

Normalization requires that $c_{0\ldots0} = 1$. Since the eigenvalues of the Pauli matrices are ± 1, the expansion coefficients satisfy

$$-1 \le c_{\alpha_1 \ldots \alpha_N} \le 1 \ . \tag{4}$$

To be concrete, we consider first the case of two qubits. For each qubit we introduce six pure density matrices, $P_i \equiv \frac{1}{2}(1_2 + \sigma_i)$ and $\overline{P}_i \equiv \frac{1}{2}(1_2 - \sigma_i)$. A convenient discrete overcomplete basis for discussing separability consists of the 36 direct-product projectors, each of which is a pure direct-product density matrix: $P_i \otimes P_j$, $P_i \otimes \overline{P}_j$, $\overline{P}_i \otimes P_j$, $\overline{P}_i \otimes \overline{P}_j$. Any density matrix of two qubits can be expanded in this basis, but since the basis is overcomplete, the representation is not unique. We make a specific choice, as follows. Noting that $\sigma_i = P_i - \overline{P}_i$ and $1_2 = P_i + \overline{P}_i$, we can write $1_2 = \omega_i(P_i + \overline{P}_i)$, where $\omega_i = 1/3$, $i = 1, 2, 3$. With these results we can convert the Pauli representation (2) into the form

$$\begin{aligned}\rho = \frac{1}{4}\big[&\big(\omega_i\omega_j + c_{i0}\omega_j + \omega_i c_{0j} + c_{ij}\big) P_i \otimes P_j \\ &+ \big(\omega_i\omega_j - c_{i0}\omega_j + \omega_i c_{0j} - c_{ij}\big) \overline{P}_i \otimes P_j \\ &+ \big(\omega_i\omega_j + c_{i0}\omega_j - \omega_i c_{0j} - c_{ij}\big) P_i \otimes \overline{P}_j \\ &+ \big(\omega_i\omega_j - c_{i0}\omega_j - \omega_i c_{0j} + c_{ij}\big) \overline{P}_i \otimes \overline{P}_j\big] \ . \end{aligned} \tag{5}$$

If the coefficient of each of the 36 basis elements is nonnegative, the density matrix is separable. We note that when the maximally mixed density matrix for two qubits, $M_4 = \frac{1}{4} 1_2 \otimes 1_2$, is represented as in Eq. (5), the coefficient of each of the basis matrices is 1/36.

Consider now an arbitrary entangled (nonseparable) density matrix ρ_1. Since ρ_1 is entangled, at least one of the coefficients in the representation of ρ_1 in the form (5) is negative. Suppose now that ρ_1 is mixed with the maximally mixed density matrix M_4 as in Eq. (1), i.e., $\rho_\epsilon = (1-\epsilon) M_4 + \epsilon \rho_1$. Although some of the coefficients of ρ_1 are negative, all of the coefficients of M_4 are strictly positive. Hence, for ϵ small enough, all the coefficients of ρ_ϵ are nonnegative, making ρ_ϵ separable. Thus *all* density matrices in a sufficiently small neighborhood of the maximally mixed density matrix are separable.

Furthermore, we can find an explicit bound on ϵ such that ρ_ϵ is separable for any ρ_1. To find a bound, we use Eq. (4) to bound the coefficients of the basis matrices in a representation of ρ_1 of the form (5). The minimum value of any of the coefficients is $(1/4)(1/9 - 1/3 - 1/3 - 1) = -14/36$. Thus all the coefficients of the density matrix ρ_ϵ in the discrete overcomplete basis are nonnegative if $(1-\epsilon)/36 - 14\epsilon/36 \ge 0$, i.e., if $\epsilon \le 1/15$. For $\epsilon \le 1/15$, the representation (5) is an explicit decomposition of ρ_ϵ as a mixture of direct products.

A similar analysis can be carried out for any number of qubits. Starting from the Pauli representation (2), we introduce a discrete product basis, like that for two qubits, and define a representation analogous to that in Eq. (5). Using Eq. (4) to limit the size of the coefficients in this representation, we find an asymptotic lower bound on the size of the neighborhood of separable density matrices that is of order $\epsilon \sim 1/4^N$ for N qubits.

One particularly interesting example is the GHZ state [12,16], a state for three qubits whose density matrix is

$$\begin{aligned}\rho_{\mathrm{GHZ}} &= \frac{1}{2}\big(|111\rangle + |222\rangle\big)\big(\langle 111| + \langle 222|\big) \\ &= \frac{1}{8}\Big(1_2 \otimes 1_2 \otimes 1_2 + 1_2 \otimes \sigma_3 \otimes \sigma_3 + \sigma_3 \otimes 1_2 \otimes \sigma_3 \\ &\quad + \sigma_3 \otimes \sigma_3 \otimes 1_2 + \sigma_1 \otimes \sigma_1 \otimes \sigma_1 - \sigma_1 \otimes \sigma_2 \otimes \sigma_2 \\ &\quad - \sigma_2 \otimes \sigma_1 \otimes \sigma_2 - \sigma_2 \otimes \sigma_2 \otimes \sigma_1\Big) \ . \end{aligned} \tag{6}$$

We now express the maximally mixed density matrix, M_8, and the GHZ density matrix in terms of an overcomplete set of $6^3 = 216$ basis matrices analogous to the 2-qubit matrices introduced above. We find that M_8 has coefficient 1/216 for all the basis elements and that the smallest coefficient for ρ_{GHZ} in this basis is $-(1/8)(26/27) = -26/216$. Thus for $\epsilon \le 1/27$, the state

$$\rho_\epsilon = (1-\epsilon) M_8 + \epsilon \rho_{\mathrm{GHZ}} \tag{7}$$

is separable. We return to the GHZ example below.

We have also considered another overcomplete basis for the space of density matrices, a basis labeled by continuous parameters. An arbitrary density matrix for N qubits can be represented as

$$\rho = \int d\Omega_1 \cdots d\Omega_N \, w(\vec{n}_1, \ldots, \vec{n}_N) P_{\vec{n}_1} \otimes \cdots \otimes P_{\vec{n}_N} \ , \tag{8}$$

where the integral runs over N Bloch spheres and where $P_{\vec{n}} \equiv \frac{1}{2}(1_2 + \vec{n} \cdot \vec{\sigma})$ is the projector onto the pure state located at unit vector $\vec{n}$ on the Bloch sphere. The representation (8) is by no means unique. In a spherical-harmonic expansion of $w(\vec{n}_1, \ldots, \vec{n}_N)$, the density matrix determines only the $l = 0$ and $l = 1$ parts; the higher-order spherical-harmonic content corresponds to the freedom in representing ρ as a sum of one-dimensional product projectors. A separable density matrix is one for which there is an expansion such that $w(\vec{n}_1, \ldots, \vec{n}_N)$ is everywhere nonnegative.

We can generate a candidate for a separable ensemble decomposition of ρ by considering the unique representation of the form (8) such that $w(\vec{n}_1, \ldots, \vec{n}_N)$ has only $l = 0$ and $l = 1$ components. We can obtain this unique representation by noting that

$$\frac{1}{2}\sigma_\alpha = \frac{3}{4\pi}\int d\Omega\, n_\alpha P_{\vec{n}}\ , \tag{9}$$

where $n_0 \equiv 1/3$. Inserting this result into the Pauli-matrix expansion (2) and using Eq. (3) gives

$$\begin{aligned} &w(\vec{n}_1,\ldots,\vec{n}_N) \\ &= \left(\frac{3}{4\pi}\right)^N c_{\alpha_1\ldots\alpha_N}(n_1)_{\alpha_1}\cdots(n_N)_{\alpha_N} \\ &= \frac{1}{(4\pi)^N}\mathrm{tr}\Big(\rho(1_2+3\vec{n}_1\cdot\vec{\sigma})\otimes\cdots\otimes(1_2+3\vec{n}_N\cdot\vec{\sigma})\Big)\ . \end{aligned} \tag{10}$$

The maximally mixed density matrix, M_{2^N}, has $w = (1/4\pi)^N$.

Let us concentrate on the operator product in the last form of Eq. (10). Each operator in the product has eigenvalues 4 and -2. Thus the most negative eigenvalue of the operator product is $4^{N-1}(-2) = -2^{2N-1}$, which implies that

$$w(\vec{n}_1,\ldots,\vec{n}_N) \geq -\frac{2^{2N-1}}{(4\pi)^N}\ . \tag{11}$$

Consider now the density matrix (1). Its candidate ensemble probability satisfies

$$\begin{aligned} w_\epsilon(\vec{n}_1,\ldots,\vec{n}_N) &= \frac{1-\epsilon}{(4\pi)^N} + \epsilon w_1(\vec{n}_1,\ldots,\vec{n}_N) \\ &\geq \frac{1-\epsilon(1+2^{2N-1})}{(4\pi)^N}\ . \end{aligned} \tag{12}$$

Therefore ρ_ϵ is separable if

$$\epsilon \leq \frac{1}{1+2^{2N-1}} \underset{N\to\infty}{\sim} \frac{2}{4^N}\ . \tag{13}$$

We see again that all density matrices in the neighborhood of the maximally mixed density matrix are separable, and we obtain a lower bound on the size of the separable neighborhood, which for large N is much better than the bound, $\epsilon \leq (1+2^{N-1})^{-(N-1)}$, given in [2].

It is instructive to return to the GHZ state (6) and to note that Eq. (10) gives

$$\begin{aligned} w_{\mathrm{GHZ}}(\vec{n}_1,\vec{n}_2,\vec{n}_3) &= \frac{1}{(4\pi)^3}\big[1+9(c_1c_2+c_2c_3+c_1c_3) \\ &\qquad +27 s_1s_2s_3\cos(\varphi_1+\varphi_2+\varphi_3)\big] \\ &\geq -\frac{26}{(4\pi)^3}\ . \end{aligned} \tag{14}$$

Here $c_j \equiv \cos\theta_j$ and $s_j \equiv \sin\theta_j$, and the minimum value occurs at $\theta_1 = \theta_2 = \theta_3 = \pi/2$ and $\varphi_1+\varphi_2+\varphi_3 = \pi$. Equation (14) shows that the mixed state (7) is separable if $\epsilon \leq 1/27$, the same bound obtained above.

This bound is not optimal. To find a bound for a particular state, such as the GHZ state, one should expand the state in terms of a tailor-made set of direct products, instead of a general-purpose set. The continuous set in Eq. (8) provides a starting point for developing a more efficient representation (treated in an upcoming publication) that uses a linearly independent set of 4^N direct products of the form $P_{\vec{n}_1}\otimes\cdots\otimes P_{\vec{n}_N}$. The explicit form of this representation is

$$\rho = \sum_{\vec{n}_1,\ldots,\vec{n}_N} w(\vec{n}_1,\ldots,\vec{n}_N) P_{\vec{n}_1}\otimes\cdots\otimes P_{\vec{n}_N}\ , \tag{15}$$

where $w(\vec{n}_1,\ldots,\vec{n}_N)$ is given by Eq. (10), and the sum runs over Bloch vectors that lie at the vertices of tetrahedra. Using a representation of this sort matched to the GHZ state, one can improve the bound for separability of the state (7) to $\epsilon \leq 1/(3+6\sqrt{2}) \simeq 1/11.5$.

In this Letter we have been using ϵ to characterize how close a density matrix of the form (1) is to the maximally mixed density matrix, M_d. An alternative distance measure, defined by $\delta \equiv \sqrt{\mathrm{tr}\big((\rho-M_d)^2\big)}$, leads to similar overall conclusions, for using the representation of ρ in Eq. (10), one can show that all states with $\delta \leq 1/(2\sqrt{5})^N$ are separable.

Up to this point we have been thinking of the number of qubits as being fixed, and we have investigated the boundary between separability and nonseparability as the amount of noise, specified by ϵ, changes. We now shift gears, thinking of the qubits as particles with spin and asking what happens as the number of particles or their dimension changes, while ϵ is held fixed. In general, as we go to more particles or higher spins, we find that we can tolerate more mixing with the maximally mixed state and still have states that are not separable. In other words, for a given ϵ, we can always find states of sufficiently large numbers of particles or sufficiently high spin for which ρ_ϵ is nonseparable. We translate this result into an upper bound on the size of the separable neighborhood around the maximally mixed state.

Consider now two spin-$(d-1)/2$ particles, each living in a d-dimensional Hilbert space. What we have in mind is that each of these particles is an aggregate of $N/2$ spin-1/2 particles (qubits), in which case $d = 2^{N/2}$. We consider a specific joint density matrix of the two particles,

$$\rho_\epsilon = (1-\epsilon)M_{d^2} + \epsilon|\psi\rangle\langle\psi|\ . \tag{16}$$

where $|\psi\rangle$ is a maximally entangled state of the two particles,

$$|\psi\rangle = \frac{1}{\sqrt{d}}\big(|1\rangle|1\rangle + |2\rangle|2\rangle + \ldots + |d\rangle|d\rangle\big)\ . \tag{17}$$

Now project each particle onto the subspace spanned by $|1\rangle$ and $|2\rangle$. The state after projection is

$$\begin{aligned} \tilde{\rho} &= \frac{1}{A}\left(\frac{1-\epsilon}{d^2}1_4 + \frac{\epsilon}{d}\big(|1\rangle|1\rangle + |2\rangle|2\rangle\big)\Big(\langle 1|\langle 1| + \langle 2|\langle 2|\big)\right) \\ &= (1-\epsilon')M_4 + \epsilon'|\phi\rangle\langle\phi|\ , \end{aligned} \tag{18}$$

where $A = (4/d^2)[1 + \epsilon(d/2 - 1)]$ is the normalization factor,

$$|\phi\rangle = \frac{1}{\sqrt{2}}\big(|1\rangle|1\rangle + |2\rangle|2\rangle\big) \tag{19}$$

is a maximally entangled state of two qubits, and

$$\epsilon' = \frac{2\epsilon/d}{A} = \frac{\epsilon d/2}{1 + \epsilon(d/2 - 1)} \; . \tag{20}$$

The projected state $\tilde{\rho}$ is a Werner state [17], a mixture of the maximally mixed state for two qubits, M_4, and the maximally entangled state $|\phi\rangle$. The proportion ϵ' of maximally entangled state increases linearly with d. Thus, as d increases for fixed ϵ, there is a critical dimension beyond which $\tilde{\rho}$ becomes entangled. Indeed, the Werner state is nonseparable for $\epsilon' > 1/3$ [17,18], which is equivalent to $d > \epsilon^{-1} - 1$. Moreover, since the local projections on the two particles cannot create entanglement from a separable state, we can conclude that the state (16) of N qubits is nonseparable under the same conditions, i.e., if

$$\epsilon > \frac{1}{1 + d} = \frac{1}{1 + 2^{N/2}} \; . \tag{21}$$

This result establishes an *upper* bound, scaling like $2^{-N/2}$, on the size of the separable neighborhood around the maximally mixed state.

Our results have implications for attempts to use high-temperature NMR techniques to perform quantum computations or other quantum-information-processing tasks. They imply that NMR experiments performed to date have not produced genuinely entangled density matrices. This is because in current experiments, the parameter ϵ, which measures the deviation from the maximally mixed state, has a value $\sim 10^{-5}$, much smaller than the lower bounds we have found for the radius of the separable neighborhood of the maximally mixed state, for the cases of two or three spins used in these experiments.

Present high-temperature NMR techniques, based on synthesizing a pseudopure state in the deviation density matrix, imply that ϵ scales like $N/2^N$ as the number of qubits increases at constant temperature [3,5]. With this scaling, the state ρ_ϵ leaves the region where our lower bound implies that all states are separable at about 14 qubits, but it never enters the region where our upper bound guarantees that there are entangled states. Thus, it is unclear whether present NMR techniques can produce entangled states. Different techniques might lead to a more favorable scaling behavior for ϵ [19].

The results in this Letter suggest that current NMR experiments should be considered as simulations of quantum computations rather than true quantum computations, since no entanglement appears in the physical states at any stage of the process [20]. We stress, however, that we have not given a proof of this conclusion, since we would need to analyze further the power of general unitary operations in their action on separable states. Much more needs to be understood about what it means for a computation to be a "quantum" computation.

SLB, RJ, and RS are supported by the UK Engineering and Physical Sciences Research Council. RJ is supported in part by the European TMR Research Network ERB-FMRX-CT96-0087. CMC is supported in part by the US Office of Naval Research N00014-93-1-0116. SLB, RJ, and RS acknowledge the support and hospitality of the Workshop on Quantum Information, Decoherence and Chaos held on Heron Island, Queensland, in September 1998, where the issues in this work were raised, and are grateful to T. F. Havel and R. Laflamme for discussions about NMR computing at that workshop.

[1] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, quant-ph/9804024.
[2] G. Vidal and R. Tarrach, quant-ph/9806094.
[3] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Nat. Acad. Sci. USA **94**, 1634 (1997).
[4] D. G. Cory, M. D. Price, and T. F. Havel, Physica D **120**, 82 (1998).
[5] N. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
[6] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung, Proc. R. Soc. Lond. A **454**, 447 (1998).
[7] I. L. Chuang *et al.*, Nature **393**, 143 (1998).
[8] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).
[9] J. A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).
[10] J. A. Jones, M. Mosca, and R. H. Hansen, Nature **393**, 344 (1998).
[11] D. G. Cory *et al.*, Phys. Rev. Lett. **81**, 2152 (1998).
[12] R. Laflamme *et al.*, Phil. Trans. Roy. Soc. London A **356**, 1743 (1998).
[13] N. Linden, H. Barjat, and R. Freeman, Chem. Phys. Lett. **296**, 61 (1998).
[14] M. A. Nielsen, E. Knill, and R. Laflamme, Nature **396**, 52 (1998).
[15] See, for example, D. DiVincenzo's review of [1] at http://qso.lanl.gov/~gottesma/qcreviews/main.html
[16] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), p. 173.
[17] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[18] S. Popescu, Phys. Rev. Lett. **72**, 797 (1994); C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
[19] L. J. Schulman and U. Vazirani, e-print quant-ph/9804060.
[20] A. Ekert and R. Jozsa, Phil. Trans. Roy. Soc. London A **356**, 1769 (1998).

Holonomic Quantum Computation

Paolo Zanardi [1,2] and Mario Rasetti [1,3]
[1] *Istituto Nazionale Fisica della Materia (INFM)*
[2] *Institute for Scientific Interchange Foundation, Villa Gualino, Viale Settimio Severo 65, I-10133 Torino, Italy*
[3] *Dipartimento di Fisica, Politecnico di Torino, Corso Duca degli Abruzzi 24, I-10129 Torino, Italy*

We show that the notion of generalized Berry phase i.e., non-abelian holonomy, can be used for enabling quantum computation. The computational space is realized by a n-fold degenerate eigenspace of a family of Hamiltonians parametrized by a manifold $\mathcal{M}$. The point of $\mathcal{M}$ represents classical configuration of control fields and, for multi-partite systems, couplings between subsystem. Adiabatic loops in the control $\mathcal{M}$ induce non trivial unitary transformations on the computational space. For a generic system it is shown that this mechanism allows for universal quantum computation by composing a generic pair of loops in $\mathcal{M}$.

PACS numbers: 03.67.Lx, 03.65.Bz

In this paper we shall speculate about a novel potential application of non-abelian geometric phases (*holonomies*) to Quantum Computation [1]. Ever since their discovery geometric phases in quantum theory have been considered a deep and fascinating subject [2]. This is due on the one hand to their unexpected and ubiquitous role in many physical systems, on the other hand to the elegant formulation they admit in terms of concepts borrowed from differential-geometry and topology [3]. Furthermore the existence of analog geometric terms associated with *non-abelian* groups e.g., $U(N)$ [4] showed how many of the notions developed in (non-abelian) gauge theory have a scope that extends far beyond the study of fundamental interactions.

We shall show how by encoding quantum information in one of the eigenspaces of a degenerate Hamiltonian H one can in principle achieve the full quantum computational power by using holonomies only. These holonomic computations are realized by moving along loops in a suitable space $\mathcal{M}$ of control parameters labelling the family of Hamiltonians to which H belongs. Attached to each point $\lambda \in \mathcal{M}$ there is a quantum code, and this bundle of codes is endowed with a non-trivial global topology described by a non-abelian gauge field potential A. For generic A the associated holonomies will allow for universal quantum computing. In a sense the ideas presented here suggest that gauge fields might play a role also in the arena of information processing.

In the very same way of classical information processing, general quantum computations are realized by networks of elementary bulding blocks. More specifically the dynamics is obtained by switching on and off *gate* Hamiltonians $\{H_l\}_{l=1}^{g}$. If in this way any unitary over the state-space can be approximated arbitrarily well, the set of gates $U_l := e^{i H_l}$ is termed *universal* [5]. A (universal) quantum computer is defined by the state-space $\mathcal{H} \cong \mathbf{C}^N$ for data encoding and by a (universal) set of quantum gates. A quantum algorithm consists of the given computation $U(T)$ that acts on the quantum state $|\psi\rangle_{in}$ encoding initial data, its realization as a network of basic gates, along with a (measurement) prescription for extracting the relevant information from $|\psi\rangle_{out}$. For the aims of this paper it is worthwile to reformulate this setup in a geometrical fashion.

Any quantum evolution $U(T) = \mathbf{T}\exp[-i\int_0^T dt H(t)]$ can be associated with a path in a space whose points describe the configurations of suitable "control fields" λ, on which the Hamiltonian depends. Indeed any Hamiltonian in $\mathbf{C}^N$ can be written as $H_\lambda = i\sum_{l=1}^{N^2}\Phi_l(\lambda)\,\Gamma_l\,(\Phi_l \in \mathbf{R})$ where the Γ_l's are a basis of the space of anti-hermitean matrices i.e., they are the generators of the Lie algebra $u(N)$. The control parameter space $\mathcal{M}$ is a manifold over which is defined a smooth map Φ to $u(N)$. If one is able to drive the control field configuration $\lambda \in \mathcal{M}$ through a (smooth) path $\gamma\colon [0,T] \to \mathcal{M}$ then a family $H(t) := H_{\gamma(t)}$ is defined along with the associated unitary U_γ. Conversely any smooth family $H(t)$ defines a path in $\mathcal{M} = \mathbf{R}^{N^2}$. Resorting to this language Quantum Computation can be described as the experimenter's capability of generating a small set of $\{\gamma_i\}_{i=1}^{g}$ of basic paths such that sequences of the corresponding U_{γ_i}'s approximate with arbitrary good accuracy any unitary transformation on the quantum state-space. It is important to stress the, obvious, fact that the path generation is achieved through a classical control process.

Non-Abelian Holonomies– In the situation which we are interested in, one deals with γ's that are *loops* in $\mathcal{M}$ i.e., $\gamma(T) = \gamma(0)$, and with a family of Hamiltonians $\{H_\lambda\}_{\lambda\in\mathcal{M}}$ with same degeneracy structure i.e., no-level crossing. In the general case $H_\lambda = H_{\gamma(t)}$ has R different eigenvalues $\{\varepsilon_i\}_{i=1}^{R}$ with degeneracies $\{n_i\}$. If $\Pi_i(\lambda)$ denotes the projector over the eigenspace $\mathcal{H}_i(\lambda) := \mathrm{span}\,\{|\psi_i^\alpha(\lambda)\rangle\}_{\alpha=1}^{n_i}$, of H_λ, one has the spectral λ-dependent resolution $H_\lambda = \sum_{i=1}^{R}\varepsilon_i(\lambda)\,\Pi_i(\lambda)$.

The state vector evolves according the time-dependent Schroedinger equation $i\,\partial_t|\psi(t)\rangle = H_{\gamma(t)}\,|\psi(t)\rangle$. We shall restrict ourselves to the case in which the loop γ's are *adiabatic* i.e., $\hbar\dot\gamma/\gamma \ll \min_{i\neq j}|\varepsilon_j - \varepsilon_i|$. Then it is well known

that any initial preparation $|\psi_0\rangle \in \mathcal{H}$ will be mapped, after the period T, onto: $|\psi(T)\rangle = U(T)\,|\psi_0\rangle$, $U(T) = \oplus_{l=1}^{R} e^{i\,\phi_l(T)}\,\Gamma_{A_l}(\gamma)$, where, $\phi_l(T) := \int_0^T d\tau\,\varepsilon_l(\lambda_\tau)$, is the dynamical phase and

$$\Gamma_{A_l}(\gamma) := \mathbf{P}\exp\int_\gamma A_l \in U(n_l), \quad (l = 1, \ldots, R) \qquad (1)$$

is called the *holonomy* associated with the loop γ, (here $\mathbf{P}$ denotes path ordering). In particular when $|\psi_0\rangle \in \mathcal{H}_l$ the final state belongs to the *same* eigenspace. In the following we will drop dynamical phases and focus on the geometrical contribution (1). For $n = 1$ this term is nothing but the celebrated Berry phase, and A is the so-called Bott-Chern connection [6]. For $n_l > 1$ the holonomy $\Gamma_{A_l}(\gamma)$ is sometimes referred to as *non-abelian* geometric phase [4]. The matrix-valued form A_l appearing in Eq. (1) is known as the *adiabatic connection* and it is given by $A_l = \Pi_l(\lambda)\,d\,\Pi_l(\lambda) = \sum_\mu A_{l,\mu}\,d\lambda_\mu$, where [2]

$$(A_{l,\mu})^{\alpha\beta} := \langle\psi_l^\alpha(\lambda)|\,\partial/\partial\lambda^\mu\,|\psi^\beta(\lambda)\rangle \qquad (2)$$

$(\lambda_\mu)_{\mu=1}^d$ local coordinates on $\mathcal{M}$. The A_l's are a non-abelian gauge potentials that allow for parallel transport of vectors over $\mathcal{M}$. Indeed the linear mapping (1) of the fiber $\mathcal{H}_l$ onto itself is nothing but the parallel transport of the vector $|\psi_0\rangle$ associated with the connection form A_l.

In view of the crucial role played by degeneracy, before moving to the main part of the paper, we briefly discuss this issue in a geometric fashion by considering the space of Hamiltonians H of a quantum state-space $\mathcal{H} \cong \mathbf{C}^N$.

The control manifold is mapped by Φ onto a set of Hamiltonians iso-degenerate with $H = H_{\gamma(0)}$. Locally one has $\Phi(\mathcal{M}) \cong \mathcal{O}(H) \times (\mathbf{R}^R - \Delta_R)$, where $\Delta_R := \{x \in \mathbf{R}^R : i \neq j \Rightarrow x_i \neq x_j\}$, and $\mathcal{O}(H) := \{X\,H\,X^\dagger\,/\,X \in U(N)\}$ is the orbit of H under the (adjont) action of $U(N)$. Indeed any pair of isospectral Hamiltonians belongs to $\mathcal{O}(H)$, moreover once the orbit is given one has still R degrees of freedom (the different eigenvalues) for getting the whole manifold of Hamiltonian with fixed degeneracy structure. By factoring out the the symmetry group of H, one finds

$$\mathcal{O}(H) := \frac{U(N)}{U(n_1) \times \cdots \times U(n_R)}, \qquad (3)$$

From eq. (3) it stems that dimension of this manifold reach its maximum (minimun) for the non (maximally) degenerate case $R = N$ ($R = 1$): $d_{max} = N\,(N-1)+N = N^2$ ($d_{min} = 0 + 1 = 1$). This means that the set of non-degenerate Hamiltonians is an *open* submanifold of $\mathbf{R}^{N^2}$, expressing the well-known fact that degeneracy – due to the symmetry constraints that it involves – is a singular case, while non-degeneracy is the generic one. Indeed if one slightly perturbs a non-degenerate Hamiltonian H the resulting operator is, generically, still non-degenerate.

Universal Computation –The above considerations make clear that the degeneracy requirement for the existence of non-abelian holonomies is rather stringent from a purely geometrical point of view. On the other hand quite often the physics of the systems under concern provides the required symmetries for having (large) degenerate eigenspaces. Notice that discrete symmetries, like charge conjugation and rotational invariance are rather generic in many-body systems. For example non-abelian holonomies have been recently shown to play a role in the $SO(5)$ theory of superconductivity [7].

In the following we will take degeneracy for granted and we will fix our attention to a given n-dimensional eigenspace $\mathcal{C}$ of H. The state-vectors in $\mathcal{C}$ will be our quantum codewords, and $\mathcal{C}$ will be referred to as the *code*. Clearly the optimal choice is to take the code to be the largest eigenspace of H. Our aim is to perform as many as possible unitary transformations i.e., *computations,* over the code resorting only on the non-abelian holonomies (1) generated by adiabatic loops in $\mathcal{M}$. A first crucial question is:

How many transformations can be obtained, by eq. (1), as γ varies over the space of loops in $\mathcal{M}$?

To address this point let us begin by considering the properties of the holonomy map Γ_A. On the loop space (we set $T = 1$)

$$L_{\lambda_0} := \{\gamma : [0,\,1] \mapsto \mathcal{M}\,/\,\gamma(0) = \gamma(1) = \lambda_0\} \qquad (4)$$

over a point $\lambda_0 \in \mathcal{M}$, there exists a composition law for loop [i.e., $(\gamma_2 \cdot \gamma_1)(t) = \theta(\frac{1}{2} - t)\,\gamma_1(2\,t) + \theta(t - \frac{1}{2})\,\gamma_1(2t-1)$] and a unity element $\gamma_0(t) = \lambda_0$, $t \in [0,\,1]$. The basic property of map $\Gamma_A : L_{\lambda_0} \mapsto U(n)$ are easily derived from eq. (1): i) $\Gamma_A(\gamma_2 \cdot \gamma_1) = \Gamma_A(\gamma_2)\,\Gamma_A(\gamma_1)$; ii) $\Gamma_A(\gamma_0) = \mathbb{1}$; moreover, by denoting with γ^{-1} the loop $t \mapsto \gamma(1-t)$, one has iii) $\Gamma_A(\gamma^{-1}) = \Gamma_A^{-1}$. This means that by composing loops in $\mathcal{M}$ one obtains a unitary evolution that is the product of the evolutions associated with the individual loops and that staying at rest in the parameter space correspond to no evolution at all. Finally iii) tells us that for getting the time-reversed evolution one has simply to travel along γ with the opposite orientation. Another noteworthy property of Γ_A – on which its geometric nature is based – is its invariance under reparametrizations: $\Gamma_A(\gamma \circ \varphi) = \Gamma_A(\gamma)$, where φ is any diffeomorphism of $[0,\,1]$. Physically this means that the evolution map – as long as adiabaticity holds – does not depend on the rate at which γ is travelled but just on its geometry. This property is quite non-trivial and, obviously, does not hold for general time-dependent quantum evolutions.

From i)–iii) it follows immediately that the set $\mathrm{Hol}(A) := \Gamma_A(L_{\lambda_0})$ is a *subgroup* of $U(n)$ known as the *holonomy group* of the connection A. Notice that the distinguished point λ_0 is not crucial, in that $\Gamma_A(L_{\lambda_0}) \cong \Gamma_A(L_{\lambda_0'})$ provided λ_0 and λ_0' can be conncetd by a

smooth path. When $\mathrm{Hol}(A) = U(n)$, the connection A is called *irreducible*. To our aims the key observation is that irreducibility is the *generic* situation. This result can be stated geometrically by saying that in the space of connections over $\mathcal{M}$, the irreducible ones are an open dense set. The condition of irreducibility can be stated in terms of the *curvature* 2-form of the connection $F = \sum_{\mu\nu} F_{\mu\nu}\, dx^\mu \wedge dx^\nu$ where

$$F_{\mu\nu} = \partial_\nu A_\mu - \partial_\mu A_\nu - [A_\mu,\, A_\nu]. \tag{5}$$

If the $F_{\mu\nu}$'s linearly span the whole Lie algebra $u(n)$, then A is irreducible [3]. It follows that in the generic case adiabatic connections will provide a mean for realizing universal quantum computation over $\mathcal{C}$. For any chosen unitary transformation U over the code there exists a path γ in $\mathcal{M}$ such that $\|\Gamma_A(\gamma) - U\| \leq \epsilon$, with ϵ arbitrarily small. Therefore any computation on the code $\mathcal{C}$ can be realized by driving the control fields configuration λ along closed paths γ in the control manifold $\mathcal{M}$.

Now we show that the connections associated with non abelian geometric phases are *actually* irreducible. For simplicity in eq. (3) we set $R = 2$, $n_1 = 1$, $n_2 = N-1$ obtaining the $N-1$-dimensional complex projective space

$$\mathcal{O}(H_0) \cong \frac{U(N)}{U(N-1)\times U(1)} \cong \frac{SU(N)}{U(N-1)} \cong \mathbf{CP}^{N-1}. \tag{6}$$

The orbit $\mathcal{O}(H_0)$ of $H_0 \equiv H_{\lambda_0}$ coincides with the manifold of pure states over $\mathbf{C}^N$. When $N = 2$ one recovers the original Berry-Simon case, $H_{BS} = \mathbf{B}\cdot\mathbf{S}, (\mathbf{S} := (\sigma_x,\, \sigma_y,\, \sigma_z),\, \mathbf{B} \in S^2 \cong \mathbf{CP}^1)$, for a spin $\frac{1}{2}$ particle in an external magnetic field $\mathbf{B}$. Here $\mathrm{Hol}\,(A_{BS}) = \{e^{i\,S_\gamma}\}_\gamma \cong U(1)$, where S_γ is the area enclosed by the loop γ in the sphere S^2. Of course this case, being abelian, has no computational meaning, nevertheless it shows how controllable loops in an external field manifold (the $\mathbf{B}$-space) can be used for generating quantum phases.

For the characterization of the holonomy group we observe first of all that one can identify the control manifold with orbit $\mathcal{O}$. Technically this is due to the fact that the bundle of $N-1$-dimensional "codes" over $\mathcal{M}$ is vector bundle with structure group $U(N-1)$. The associated $U(N-1)$-principal bundle is the pull back, through Φ, of $\pi{:}\, U(N)/U(1) \mapsto \mathbf{CP}^{N-1}$. The result follows being the latter an universal classifying bundle [8].

For general N the points of $\mathbf{CP}^{N-1}$ are parametrized by the transformations $\mathcal{U}(\mathbf{z}) := \mathbf{P}\prod_{\alpha=1}^{N-1} U_\alpha(z_\alpha)$, where $U_\alpha(z_\alpha) := \exp(z_\alpha\, |\alpha\rangle\langle N| - \mathrm{h.c.})$. The relevant projectors are given by $\Pi_{\mathbf{z}} = \mathcal{U}(\mathbf{z})\Pi\mathcal{U}(\mathbf{z})^\dagger$, where Π is the projector over the first $N-1$ degenerate eigenstates. By using def. (3) and setting $z_\alpha = z_\alpha^0 + i\, z_\alpha^1$, one checks that at $\mathbf{z} = 0$ the components of the curvature are given by

$$F_{z_\alpha^n, z_\beta^m}(0) = \Pi\,[\frac{\partial U_\alpha}{\partial z_\alpha^n},\, \frac{\partial U_\beta}{\partial z_\beta^m}]\,\Pi|_{\mathbf{z}=0}, \tag{7}$$

with $\alpha, \beta = 1, \ldots, N-1,\, ;\, m, n = 0, 1$.

Since $\partial U_\alpha/\partial z_\alpha^n = i^n\,(|\alpha\rangle\langle N| - (-1)^n\,|N\rangle\langle\alpha|)$, one finds

$$F_{z_\alpha^n, z_\beta^m}(0) = i^{m+n}\,[(-1)^n|\beta\rangle\langle\alpha| - (-1)^m\,|\alpha\rangle\langle\beta|]. \tag{8}$$

From this expression it follows that components of F span the whole $u(N-1)$. As remarked earlier, this result does not depend on the specific point chosen, therefore this example is irreducible i.e., $\mathrm{Hol}(A) \cong U(N-1)$. The general case (3) can be worked out along similar lines it turns out to be irreducible as well. Notice how, for generating control loops for N qubits, one needs to control 2^{N+1} real parameters instead of the $2^{2\,N}$ ones necessary for labelling a generic Hamiltonian.

For practical purposes is relevant the question:

How many loops should an experimenter be able to generate for getting the whole holonomy group?

An existential answer is given below by using arguments close to the ones of ref. [9]. As the non-trivial topology associated with the irreducible gauge-field A allows to map the loop "alphabet" densely into the group of unitaries over the code, we have the

Proposition Two generic loops $\gamma_i\,(i = 1, 2)$ generate a universal set of gates over $\mathcal{C}$.

Proof. It is known that two generic unitaries U_1 and U_2 belonging to a subgroup $\mathcal{G}$ of $U(N)$ generate, by composition, a subgroup G dense in $\mathcal{G}$ [9]. In particular if $\mathcal{G} = U(N)$ the U_i's are a universal set of gates. Formally: let $U_{\pm\alpha} := U_\alpha^{\pm 1}\,(\alpha = 0, \pm 1, \pm 2)\,; U_0 := \mathbb{1}$, then the set G of transformations obtainable by composing the U_i's (along with their inverses) is given by $U_f := \mathbf{P}\prod_{p\in\mathbf{N}} U_{f(p)}$, where f is a map from the natural numbers $\mathbf{N}$ to the set $\{0, \pm 1, \pm 2\}$ nonvanishing only for finitely many p's.

From the basic relation i) it follows that the transformations U_f are generated by composing loops in L_{λ_0} :

$$U_f = \Gamma_A(\gamma_f), \quad \gamma_f := \mathbf{P}\prod_{p\in\mathbf{N}} \gamma_{f(p)}. \tag{9}$$

We set $\{U_i := \Gamma_A(\gamma_i)\}_{i=1}^2$, then $\overline{G} = \mathrm{Hol}(A) = U(N)$, the latter relation follows from irreducibility of A. □

Of course this result does not provide an explicit recipe for obtaining the desired transformations, nevertheless it is conceptually quite remarkable. It shows that, even though adiabatic holonomies are a very special class of quantum evolutions, they still provide the full computational power for processing quantum information.

On the other hand our result is not completely surprising. Indeed it is important to stress that the parameters λ, for a multi-partite system, will contain in general external fields as well as couplings between sub-systems. For example if $\mathcal{H} = \mathbf{C}^2 \otimes \mathbf{C}^2$ is two-qubits space a possible basis for $u(4)$ is given by $i\,\sigma_\mu \otimes \sigma_\nu$, where $\sigma_0 := \mathbb{1}$ and $\{\sigma_i\}_{i=1}^3$ are the Pauli matrices. Then for $ij \neq 0$ the Γ_{ij}'s describe non-trivial interactions between the two qubits,

while for $ij = 0$ the corresponding generators are single qubit operators. Only the control fields associated with these latter Γ_{ij}'s can be properly interpreted as external fields while the others generate true entanglement among subsystems. Moreover, quite often, the parameters λ are indeed quantum degrees of freedom, which are considered frozen in view of the adiabatic decoupling [2]. In this case the generation of loops γ is on *its own* a problem of quantum control.

So far we have been concerned just with existential issues of unitary evolutions. In the following we shall briefly address the associated problem of computational complexity. A detailed discussion of this point is given elsewhere [10]. It is widely recognized that a crucial ingredient that provides quantum computing with its additional power is *entaglement*. This means that the computational state-space has to be multi-partite e.g., $\mathcal{H} = (\mathbf{C}^2)^{\otimes N}$, and the computations are, efficiently, obtained by composing local gates that act non trivially over a couple of subsystems at most [3]. In general the degenerate eigenspaces in which we perform our holonomic computations do not have any preferred tensor product structure. Once one of these structures has been chosen over a N-qubit code $\mathcal{C}$ i.e., an isomorphism $\varphi{:}\mathcal{C} \mapsto (\mathbf{C}^2)^{\otimes N}$ has been selected, any unitary transformation over $\mathcal{U}$ can written as a suitable sequence of CNOT's and single qubit transformations. In the $\mathbf{CP}^N$ model discussed above it can be proven, by explicit computations, that one can contructively get any single-qubit and two-qubit gate as well by composing elementary holonomic loops restricted with suitable 2-dimensional manifolds. The point, bearing on the complexity issue, is that the number of such elementary loops scales exponentially as a function of the qubit number.

A possible way out is given by considering a system that is multipartite from the outset and a special form of the Hamiltonian family $H(\lambda)$. The latter is given by a sum, over all the possible pairs (i, j) of subsystems, of Hamiltonian families $\{H(\mu_{ij})\}$. Suppose that the dependence on the local control parameters μ_{ij} is such that one can holonomically generate any transformation on a two-qubit subspace $\mathcal{C}_{ij} \subset \mathcal{H}_i \otimes \mathcal{H}_j$ e.g., a $U(8)/U(4) \times U(4)$-model, then one can *efficiently* generate any unitary over the computational subspace $\otimes_{(i,\,j)}\mathcal{C}_{ij}$ by using holonomies only [10].

An example– Let $\mathcal{H} := \mathrm{span}\,\{|n\rangle\}_{n\in\mathbf{N}}$ be the Fock space of a single bosonic mode, $H_0 = \hbar\omega\, n(n-1)$ ($n := a^\dagger a$, $[a,\, a^\dagger] = 1$). Hamiltonians of this kind can arise in quantum optics when one condider higher order nonlinearities. By construction the space $\mathcal{C} = \mathrm{span}\,\{|0\rangle,\, |1\rangle\}$ is a two-fold degenerate eigenspace of H_0 i.e., $H_0\,\mathcal{C} = 0$. Consider the two-parameter isospectral family of Hamiltonians $H_{\lambda\mu} := U_{\lambda\mu}\, H_0\, U^\dagger_{\lambda\mu}$, $(\lambda, \mu \in \mathbf{C})$ where

$$U_{\lambda,\mu} := \exp(\lambda\, a^\dagger - \bar\lambda\, a)\, \exp(\mu\, a^{2\dagger} - \bar\mu\, a^2). \qquad (10)$$

The first (second) factor in this equation is nothing but the unitary transformation from the Fock vacuum $|0\rangle$ to the familiar coherent (squezeed) state basis. If Π denotes the projector over the degenerate eigenspace of H_0, one gets $A = \Pi\, U^{-1}_{\lambda\mu}\, dU_{\lambda\mu}\, \Pi = A_\lambda d\lambda + A_\mu d\mu$ − h.c., where (at $\lambda = \mu = 0$) $A_\lambda := -\Pi\, a^\dagger\, \Pi$, $\quad A_\mu := -\Pi\, a^{2\dagger}\, \Pi$. From this relations the explicit matrix form of A can be immediately computed and irreducibility for the single-qubit space $\mathcal{C}$ verified.

This example, at the formal level, can be easily generalized. i) Choose an Hamiltonian H belonging to a representation ρ of some dynamical (Lie) algebra $\mathcal{A}$, ii) Build a k-fold degenerate $H_f := f(H)$, iii) Consider the orbit of $\mathcal{O}(H_f) = f(\mathcal{O}(H))$ under the inner automorphisms of $\mathcal{A}$. In point ii) f is a smooth real-valued map such that $f(\varepsilon_i) = E$, $(i = 1, \ldots, k)$, with the ε_i's belong to some subset of the spectrum of H. In the present case one has $\mathcal{A} := \{a,\, a^\dagger,\, a^2,\, a^{\dagger\,2},\, n := a^\dagger\, a,\, \mathbb{1}\}$, $f(z) = z\,(z-1)$, and ρ is the bosonic Fock representation.

Conclusions– In this paper we have shown how the notion of non-abelian holonomy (generalized Berry phase) might in principle provide a a novel way for implementing universal quantum computation. The quantum space (the code) for encoding information is realized by a degenerate eigenspace of an Hamiltonian belonging of a smooth iso-degenerate family parametrized by points of a control manifold $\mathcal{M}$. The computational bundle of eigenspaces over $\mathcal{M}$ is endowed by a non-trivial holonomy associated with a generalized Berry connection A. Loops in $\mathcal{M}$ induce unitary transformations over the code attacched to a distinguished point $\lambda_0 \in \mathcal{M}$. We have shown that, in the generic i.e., irreducible, case universal quantum computation can then be realized by composing in all possible ways a pair of adiabatic loops.

The required capability of generating loops by changing coupling constants, along with the necessity of large degenerate eigenspace, makes evident that from the experimental point of view the scheme we are analysing is exceptionally demanding like any other proposal for quantum computing. However we think that the connection between a differential-geometric concept like that of non-abelian holonomy and the general problematic of quantum information processing is non-trivial and quite intriguing. The individuation of promising physical systems for implementing the "gauge-theoretic" quantum computer we have been discussing in this paper is still an open problem that will require a deal of further investigations.

The authors thank H. Barnum, G. Segre and L. Faoro for discussions, A. Uhlmann for useful correspondence. P.Z. is supported by Elsag, a Finmeccanica Company.

[1] For reviews, see D.P. DiVincenzo, *Science* **270**, 255 (1995); A. Steane, Rep. Prog. Phys. **61**, 117 (1998)
[2] For a review see, *Geometric Phases in Physics*, A. Shapere and F. Wilczek, Eds. World Scientific, 1989
[3] M. Nakahara, *Geometry, Topology and Physics*, IOP Publishing Ltd., 1990
[4] F. Wilczek and A. Zee., Phys. Rev. Lett. **52**, 2111 (1984)
[5] D. Deutsch, A. Barenco and A. Ekert, Proc. R. Soc. London A, **449**, 669 (19 95); D.P. Di Vincenzo, Phys. Rev. A, **50**, 1015 (1995)
[6] R. Bott, and S.S. Chern, *Acta Math.* **114**, 71 (1985)
[7] E. Demler and S.C. Zhang, LANL e-print archive cond-mat/9805404
[8] A. Mostafazadeh, J. Math. Phys. **37**, 1218 (1996)
[9] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995)
[10] J. Pachos et al. Phys. Rev. A (To be published)

Electron Spin Resonance Transistors for Quantum Computing in Silicon-Germanium Hetero-structures

Rutger Vrijen[1], Eli Yablonovitch[1], Kang Wang[1], Hong Wen Jiang[2], Alex Balandin[1], Vwani Roychowdhury[1], Tal Mor[1] and David DiVincenzo[3]

[1] *University of California, Los Angeles, Electrical Engineering Dept., Los Angeles, California*
[2] *University of California, Los Angeles, Physics Dept., Los Angeles, California*
[3] *IBM T. J. Watson Research Center, Yorktown Heights, New York*

We apply the full power of modern electronic band structure engineering and epitaxial hetero-structures to design a transistor that can sense and control a single donor electron spin. Spin resonance transistors may form the technological basis for quantum information processing. One and two qubit operations are performed by applying a gate bias. The bias electric field pulls the electron wave function away from the dopant ion into layers of different alloy composition. Owing to the variation of the g-factor (Si:g=1.998, Ge:g=1.563), this displacement changes the spin Zeeman energy, allowing single- qubit operations. By displacing the electron even further, the overlap with neighboring qubits is affected, which allows two-qubit operations. Certain Silicon-Germanium alloys allow a qubit spacing as large as 200 nm, which is well within the capabilities of current lithographic techniques. We discuss manufacturing limitations and issues regarding scaling up to a large size computer.

I. INTRODUCTION

The development of efficient quantum algorithms for classically hard problems has generated interest in the construction of a quantum computer. A quantum computer uses superpositions of all possible input states. By exploiting this quantum parallelism, certain algorithms allow one to factorize [1] large integers with astounding speed, and rapidly search through large databases [2], and efficiently simulate quantum systems [3]. In the nearer term such devices could facilitate secure communication and distributed computing.

In any physical system, bit errors will occur during the computation. In quantum computing this is particularly catastrophic, because the errors cause decoherence [4] and can destroy the delicate superposition that needs to be preserved throughout the computation. With the discovery of quantum error correction [5] and fault-tolerant computing, in which these errors are continuously corrected without destroying the quantum information, the construction of a real computer has become a distinct possibility.

Even with the use of fault-tolerant computing a quantum computer engineer would still prefer a system that exhibits the smallest possible error rate on the qubits, the two level systems that hold the quantum information. In fact, Preskill [6] (in a review of the subject) presented a requirement for fault-tolerance; the ratio of the error rate to the computer clock rate has to be below a certain threshold.

Several systems have recently been proposed to obtain a physical implementation of a quantum computer. These systems include cold ion traps [7], nuclear magnetic resonance (NMR) systems [8,9], all-optical logic gates [10,11], Josephson junctions [12], and semiconductor nanostructures [13]. Successful experimental demonstrations of one and two qubit computers were reported for trapped ion systems [14] and NMR systems [15].

Last year, Bruce Kane [16] proposed a very interesting and elegant design for a spin resonance transistor (SRT). He proposed to use the nuclear spins of ^{31}P dopant atoms, embedded in a Silicon host, as the qubits. At low temperatures the dopant atoms do not ionize, and the donor electron remains bound to the ^{31}P nucleus. The control over the qubits is established by placing a gate-electrode, the so-called A-gate, over each qubit. By biasing the A-gate, one can control the overlap of the bound electron with the nucleus and thus the hyperfine interaction between nuclear spin and electron spin, which allows controlled one-qubit rotations. A second attractive gate, a J-gate, decreases the potential barrier between neighboring qubits, and allows two nuclear spins to interact by electron spin-exchange, which provides the required controlled qubit-qubit interaction.

The rate of loss of phase coherence between qubits in a quantum system is typically characterized by the dephasing time T_2. The T_2 dephasing time of the nuclear spins in silicon is extremely long. The silicon host efficiently isolates the nuclear spins from disturbances [17]. A quantum computer based on semiconductors offers an attractive alternative to other physical implementations due to compactness, robustness, the potentially large number of qubits [18], and semiconductor compatibility with industrial scale processing. However, the required transistors are very small, since their size is related to the size of the Bohr radius of the dopant electron. Furthermore, after the calculation is completed Kane's SRT requires a sophisticated spin transfer between nuclei and electrons to measure the final quantum state.

We suggest using the full power of modern electronic band structure engineering and epitaxial growth techniques, to introduce a new, more practical, field effect SRT transistor design that might lend itself to a near term demonstration of qubits on a Silicon wafer. We alter Kane's approach by the implementation of these spin-resonance transistors in engineered Germanium/Silicon hetero-structures that have a controlled band structure. Si-Ge strained hetero-structures, developed by IBM and other companies, are in the mainstream of Silicon technology, and are currently used for high frequency wireless communication transistors, and high-speed applications.

In Si-Ge hetero-structure layers we can control the effective mass of the donor electron to reduce the required lithographic precision, and to permit the SRT transistors to be as large as

$\approx$ 2000 Å. The Bohr radius of a bound electron in Si-Ge can be much larger than in Silicon due to the very small effective mass in strained Si-Ge alloys, and their higher dielectric constant. This places the lithographic burden well within the practical range of electron beam lithography and almost within range of contemporary optical lithography.

Among the other simplifications, we will employ an electron spin, rather than a nuclear spin as the qubit. Owing to the difference in the electronic g-factor, $g = 1.998$ for Si, and $g = 1.563$ for Ge, the electron spin resonance transition can be readily tuned by an electrostatic gate on a compositionally modulated Si-Ge epilayer structure. By working with electron spins rather than nuclear spins, we avoid the requirement of a sophisticated spin transfer between electrons and nuclei, for read-in/read-out of quantum data and for the operation of two-qubit gates. In addition, due to their higher Zeeman energy, electron spins will eventually permit a clock speed up to 1 GHz compared to a speed$\approx$ 75 kHz projected for the nuclear spins. Likewise, isotopic purity is not critical for electron spins.

In order to read-out the final result of a quantum calculation we will need to be able to detect single electron charges. Individual electro-static charges are readily detected by conventional field effect transistors (FET's) at low temperatures, which obviates the need for the sophisticated single electron transistors (SET's). In this paper, we illustrate our design for an electron spin resonance transistor.

II. ELECTRON SPIN DEPHASING TIME IN SILICON AND GERMANIUM

Electron spins benefit from the same protective environment provided by the silicon host as nuclear spins. Indeed, the ESR line in doped Silicon at low temperatures turns out to be exceptionally clean and narrow compared to other ESR lines.

Feher [19–21] found that the Si:^{31}P ESR line is inhomogeneously broadened by hyperfine interactions with neighboring nuclear spins. But the nuclear spin flip T_1 relaxation times were measured [20] to be in the 1-10 hour range. Thus the nuclei can be regarded as effectively static on the time scales needed for quantum computing. Likewise the direct electron spin-flip T_1 is also around [20] an hour.

On the question of the critical transverse T_2 ESR dephasing linewidth there was only a little information. Feher and Gere studied some heavily doped n-Si:P samples, and found that the ESR linewidth actually narrowed [22] at high doping, down to a 1 MHz linewidth at the 9 GHz ESR frequency, for the heavy doping level, $n = 3 \times 10^{18}/\mathrm{cm}^3$. This unusual behavior was clearly the result of exchange narrowing of the hyperfine inhomogeneity. For quantum computing, the issue is the linewidth of a single electron spin transition, rather than a heavily doped inhomogeneous ensemble.

Thus the outlook was optimistic. If the linewidth is only 1 MHz at such a high doping level, and is due to exchange with neighboring electrons, then the linewidth would surely be much narrower at lower doping levels, and especially for one isolated electron. Indeed that was confirmed by Chiba and Hirai [23] who measured a $1/2\pi T_2$ linewidth of only $\approx$1 kHz at a doping of 10^{16} Phosphorus ions per cm^3, by the very reliable spin-echo technique. The residual linewidth was interpreted as being due to spin diffusion via the nuclear spins. Indeed the linewidth was shown [24] to narrow further in isotopically purified, 0 spin, Si^{28}, making the T_2 dephasing even slower. The observed 1 kHz linewidth at n=$10^{16}/\mathrm{cm}^3$ is already narrow enough, in relation to the 9 GHz ESR frequency to allow enough operations for fault tolerant computing [6].

In germanium the dominant mechanism for spin dephasing is quite different from the one in silicon. Theory [25,26] and experiment [27] have confirmed that the dominant relaxation in germanium is through acoustic disturbances of the spin-orbit coupling. The g-factor in germanium is much different from 2, the free electron value, because of the relatively strong spin-orbit coupling. Germanium has four ellipsoidal conduction band minima, which are aligned with the $\langle 111 \rangle$ directions. In each minimum, the effective mass depends on the direction of electron motion, with a low effective mass (m_{xy}) in the transverse direction and a high effective mass in the longitudinal direction (m_z)(see Table I). The anisotropic effective mass results in an anisotropic g-factor, with $g = g_\parallel$ for magnetic field components in the $\langle 111 \rangle$ direction, and $g = g_\perp$ for magnetic field components perpendicular to this direction. For arbitrary angles ϕ between the magnetic field and the $\langle 111 \rangle$ direction the g-factor is given by

$$g^2 = g_\parallel^2 \cos^2 \phi + g_\perp^2 \sin^2 \phi \qquad (1)$$

The electronic ground state of the donor atom is an equal superposition (singlet) state of the four equivalent conduction band minima, and therefore has an isotropic g-factor, $g = g_\parallel/3 + 2g_\perp/3 = 1.563$. However, in the presence of lattice strain, the energies of the conduction band minima shift with respect to each other. In the new donor ground state, probability is shifted among the four valleys, with some valleys more populated than others. This produces a shift Δg in the g-factor, since each valley forms a different angle ϕ with the static magnetic field B. The corresponding relative energy shift of the spin states is proportional to $(\Delta g)\mu B$ with μ the Bohr magneton. At finite temperatures, acoustic phonons cause time-varying strains with a finite power density at the spin transition energy, which induce spin-lattice relaxation.

At these temperatures it follows from this theory that the phase relaxation time is of the same magnitude as the population relaxation time $T_2 \approx T_1$. Experiments have shown that T_1 is around 10^{-3} seconds for germanium at 1.2 K. We are not aware of direct measurements of T_2 by electron spin resonance experiments similar to those that were done in silicon. Unless there are other, as of yet unknown T_2 mechanisms in germanium, the T_2 will be determined by acoustic vibrations and be of the order of 10^{-3} seconds, which is equal to the best measured T_2 in silicon, and is again sufficiently long to allow fault tolerant computing.

Several mechanisms could lead to a further improvement in the T_1 and T_2 caused by acoustic vibrations. Firstly, working at lower temperatures will reduce the phonon energy density, which is proportional to T^4. Secondly, for the two orientations of germanium that we propose to use, $\langle 111 \rangle$ and $\langle 001 \rangle$, some special considerations can make the expected lifetimes longer. For germanium grown with strain in the $\langle 111 \rangle$ direction, the conduction band minimum along the growth direction has a

significantly lower energy than the other three minima. In the electronic ground state, virtually all population resides in this minimum, and there is little coupling to the three split-off valleys. In the theory by Roth and Hasegawa [25,26], this effect is accounted for by a square dependence of T_1 on the energy splitting between the electronic ground state and excited states (singlet-triplet splitting). The grown-in strain increases this splitting from 2 meV to 200 meV, with a corresponding increase in lifetime of 10^4. For germanium grown with strain in the $\langle 001 \rangle$ direction and with the magnetic field aligned with that direction, a symmetry argument forbids a strain induced g-shift: the $\langle 001 \rangle$ direction makes equal angles with all conduction band minima, and therefore a probability redistribution among these minima does not affect the g-factor, as can be seen from Equation 1. Thus, further improvements in the already acceptable lifetimes appear possible.

The electron spin resonance (ESR) of a bound donor in a semiconductor host provides many advantages: Firstly, in a magnetic field of 2 Tesla, the ESR resonance frequency is≈56 GHz, easily allowing qubit operations at up to ≈1 GHz. This is comparable to the clock speed of ordinary computers, and is consistent with the precision of electronic control signals that are likely to be available. Secondly, at temperatures well below 1 K, the electron spins are fully polarized allowing a reproducible starting point for the computation. And finally, for electron spins isotopic purity is not compulsory since the nuclear spin inhomogeneity remains frozen at low temperatures.

III. SRT TRANSISTOR SIZE AND LITHOGRAPHIC CRITICAL DIMENSION

The Bohr radius of the bound carrier wave function regulates the size scale of Spin Resonance Transistors. In semiconductors the Bohr radius is much larger than in vacuum, since the Coulomb force is screened by the dielectric constant, and the effective mass is much smaller. Thus the bound carrier roams farther. The Bohr radius is: $a_B = \epsilon \frac{m_0}{m^*}(\frac{\hbar^2}{m_0 q^2})$ in the semiconductor, where $\frac{m^*}{m_0}$ is the effective mass relative to the free electron mass, ϵ is the dielectric constant, $\epsilon = 16$ for Ge, and $\epsilon = 12$ for Si and the quantity in parenthesis is the Bohr radius in vacuum.

It is common in Si-Ge alloys to have strain available as an engineering parameter. Strain engineering of valence band masses has been very successful, and is used [28] in virtually all modern semiconductor lasers. As discussed above, in the conduction band, strain splits the multiple conduction band valley energies, allowing one valley to become the dominant lowest energy conduction band. If that valley also happens to be correctly aligned, the donor wave functions can have a low mass moving in the plane of the silicon wafer, and a high mass perpendicular to the wafer surface. That is exactly what we are looking for in spin resonance transistors. We want large wave functions in the directions parallel to the wafer surface, in order to relax the lithographic precision that would have been demanded if the Bohr radius were small.

In Si-rich alloys there are 6 conduction band minima, in the 6 cubic directions, that are frequently labeled as the X-directions. In Ge-rich alloys, there are 4 conduction minima located at the $\langle 111 \rangle$ faces of the Brillouin Zone, labeled L. The Ge-rich case is particularly interesting, since it has a conduction band mass of only $0.082 m_0$ in the transverse direction.

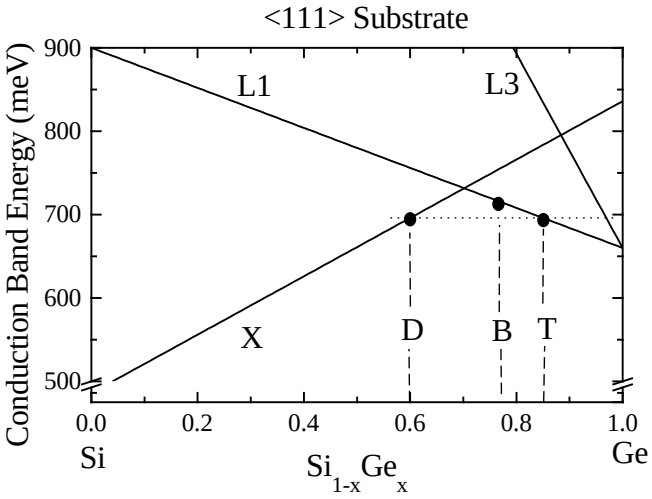


FIG. 1. The conduction band energy in Si-Ge alloys, compositionally strained in the $\langle 111 \rangle$ direction, from neutral strain at 100% Ge. The X-valley has 6 minima that remain degenerate. The L-valley has 4 minima that are split between L1 and L3. The conduction band changes from the X- to L1-character at a composition of $Si_{0.3}Ge_{0.7}$. At this band transformation, the xy-effective mass becomes relatively light, the Bohr radius increases, and the g-factor drops from $g \approx 1.998$ to $g = g_\parallel \approx 0.823$. The fractional compositions D, T, and B, will be used in our band structure engineered, spin resonance transistor.

Under $\langle 111 \rangle$ strain the 4 conduction band valleys split so that one of them is lowest in energy and is labeled L1. The other 3 valleys remain degenerate and are labeled L3. Figure 1 shows the conduction band structure in the Si-Ge alloys, grown compositionally strained in the $\langle 111 \rangle$ direction, with neutral strain at 100% Ge, as adapted from a more complete set of band structures from Wang *et al* [29].

The hydrogenic Schrödinger equation for anisotropic effective mass, m_{xy} in the plane of the wafer, and m_z perpendicular to the plane of the wafer, has been solved for arbitrary values of m_{xy}/m_z by Schindlmayr [30]. The Bohr radius in the xy-plane is influenced by both effective masses:

$$a_{B,xy} = \frac{2\epsilon}{3\pi} \frac{2 + (m_{xy}/m_z)^{1/3}}{m_{xy}} a_B^0 \qquad (2)$$

TABLE I. Conduction band effective masses relative to m_0, and the corresponding Bohr radii and g-factors in Si and Ge.

material	ϵ	m_{xy}	m_z	$a_{B,xy}$	$a_{B,z}$	$g_\parallel$	$g_\perp$
Germanium	16	0.082	1.59	64 Å	24 Å	0.823	1.933
Silicon	12	0.191	0.916	25 Å	15 Å	1.999	1.998

with a_B^0 the Bohr radius of a free hydrogen atom and $m_{xy} << m_z$ is assumed, as is appropriate for the z-oriented Si and Ge conduction band ellipsoids. The Bohr radius in the heavy mass direction, $a_{B,z}$ is given by $a_{B,z} = (\frac{m_{xy}}{m_z})^{1/3} a_{B,xy}$. Using the actual masses and the exact formula [30], we give the Bohr radii in Si and Ge for z-oriented conduction band ellipsoids in Table I.

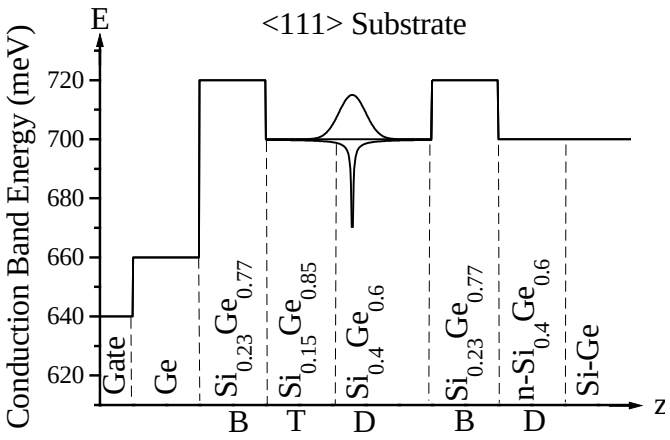


FIG. 2. The band structure diagram for the proposed spin-resonance transistor, showing the Coulombic potential well of the donor ion in the $Si_{0.4}Ge_{0.6}$ D-layer where the conduction band minimum is X-like. The hydrogenic wave function partly overlaps the $Si_{0.15}Ge_{0.85}$ T-layer where the conduction band minimum is L-like. The donor electron is confined by the two $Si_{0.23}Ge_{0.77}$ B-barrier layers. The epilayer thicknesses are not to scale.

In Table I, special note should be taken of the Bohr radius of 64 Å for $\langle 111 \rangle$ strained Ge-rich alloys in which the L1 band minimum forms the conduction band. At that orientation, the X-band minima in Si-rich alloys would have a Bohr radius of only $\approx$ 20 Å. Thus we achieve over a factor 3 increase in the transistor spacing by using a Ge-rich layer.

Given that the exchange interaction is a dominant influence among the donor spins, we make the point that Preskill's de-coherence criterion can be redefined [31] as the on/off ratio of the spin-spin interaction, as induced by the transistor gates. The actual required transistor spacing is set by the need for the weakest possible exchange interaction when the 2-qubit interaction is off, and a strong exchange interaction when 2-qubit interactions are turned on. The exchange energy $4J$ between hydrogenic wave functions determines both time scales:

$$\frac{4J(r)}{h} \approx 1.6 \frac{q^2}{\epsilon a_B} (\frac{r}{a_B})^{5/2} \exp \frac{-2r}{a_B} \qquad (3)$$

If we require the exchange energy in the off-state to be less than the measured [23] T_2 dephasing linewidth $\approx$1 kHz, then the donor ions would have to be about 29 Bohr radii apart, allowing a spacing of about 2000 Å. Such critical dimensions are well within the range that can be produced by electron beam lithography.

Later we will show that by gate-controlled Stark distortion of the hydrogenic wave functions, the Bohr radius can be further increased, switching on the 2- qubit interactions. Thus, band structure engineering allows us to use only one electrostatic gate to control both one- and two-qubit operations, rather than two separate A- and J-gates as required by Kane. This reduction of the number of gates by a factor of two, though not essential for the operation of the our ESR, means that all lithographic dimensions are doubled, which significantly increases the manufacturability of the device.

IV. GATE CONTROLLED SINGLE QUBIT ROTATIONS IN THE SPIN-RESONANCE TRANSISTOR

The essence of a spin-resonance transistor (SRT) qubit is that a gate electrode should control the spin-resonance frequency. By tuning this frequency with respect to the frequency of a constant radiation field, that is always present while the computer is being operated, single qubit rotations can be readily implemented on the electron spin. A band structure diagram for the SRT is shown in Figure 2.

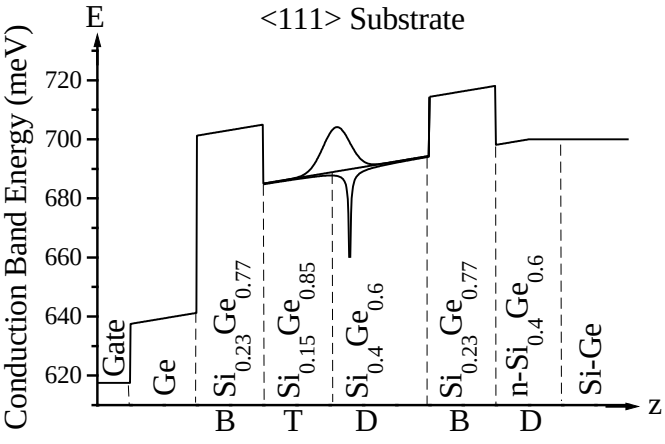


FIG. 3. The donor electron wave function is electrostatically attracted toward the $Si_{0.15}Ge_{0.85}$ T-layer where the conduction band minimum is L1-like. There it will experience a smaller g-factor, that is gate tunable. The actual g-factor will be a weighted average between the D- and T-layers.

We rely on the difference in electronic g-factor, $g = 1.998$ for Si-rich alloys, and $g = g_{\|} = 0.823$ for Ge-rich alloys, strained in the $\langle 111 \rangle$ direction. Thus, the electron spin resonance transition can be readily tuned by an electrostatic gate on a compositionally modulated Si-Ge epilayer structure, such as shown in Figure 3. In a study of the composition dependence of the g-factor in Si-Ge alloys, Vollmer and Geist [32] showed that the g-factor is most influenced by the band structure crossover from X to L1 at a composition of $Si_{0.3}Ge_{0.7}$, and hardly at all by compositional changes away from that crossover. The ^{31}P dopant atoms are positioned in the $Si_{0.4}Ge_{0.6}$ D-layer, a composition which is to the left of

the crossover in Figure 1. By electrostatically attracting the electron wave function into the $Si_{0.15}Ge_{0.85}$ T-layer, the spin resonance can be tuned very substantially.

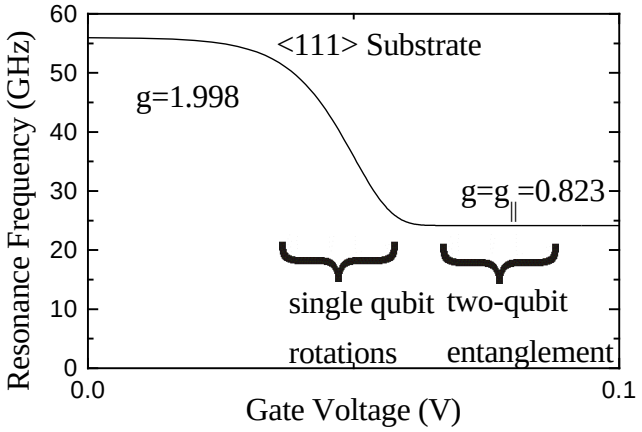


FIG. 4. A schematic of the dependence of the spin resonance frequency on the transistor gate voltage. As the electrons are pulled toward the positive gate electrode and into the more Ge-rich alloy compositions, the hetero-barrier B-layer prevents the donors from becoming completely ionized. At intermediate gate voltages, the g-factor can be tuned from g=1.998 to g=0.823. The frequencies on the vertical axis correspond to a magnetic field of 2 Tesla. The two-qubit tuning range will be explained in the next section.

The two barrier layers of composition $Si_{0.23}Ge_{0.77}$, labeled B in Figure 2, have a conduction band structure as indicated in Figure 1. They have an L1-like conduction band minimum, to the right of X-L1 band structure cross-over, and thus have the same g-factor as the $Si_{0.15}Ge_{0.85}$ T layer. The purpose of the B layers is to confine the donor electrons and prevent them from tunneling away and becoming lost. The energy height of the barrier need only be comparable to the donor binding energy, $\approx$ 20meV to fulfil this task. On the other hand the $Si_{0.4}Ge_{0.6}$ D-layer and the $Si_{0.15}Ge_{0.85}$ T-layer should have no energy barrier between them so that the g-factor can be freely tuned. Thus the D layer and the T layer are selected at compositions straddling the X-L1 crossover in Figure 1, so that their respective conduction band energies E_D and E_T are the same. A schematic tuning curve for our proposed spin resonance transistor is shown in Figure 4. As the spin resonance transistors are tuned in and out of resonance with the radiofrequency field the electron spin can be flipped, or subjected to a phase change.

The wave function distortion during tuning is shown for the left side transistor in Figure 3. The confinement barriers of composition B $Si_{0.23}Ge_{0.77}$, play an important role. They must confine the qubit donor electrons for long periods of time, or the carriers and their quantum information will be lost. For that purpose the B-barrier layers each need to be about 200 Å thick, for a carrier lifetime comparable to the $\approx$1hour T_1 spin-lattice relaxation for electron spin flips. The two layers combined would total about 400 Å, well within the practical strain limit [33] of $\approx$ 1000 Å for growth of a 23% compositionally strained alloy. The D and T layers have thicknesses similar to the $a_{B,z}$ vertical Bohr radius and contribute only slightly to the strain burden.

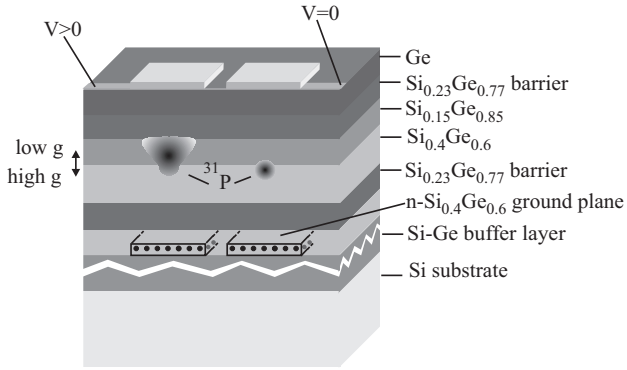


FIG. 5. The left transistor gate is biased $V > 0$ producing single qubit unitary transformations in the left SRT. The right gate is unbiased, $V = 0$. The n-$Si_{0.4}Ge_{0.6}$ ground plane is counter-electrode to the gate, and it also acts as an FET channel for sensing the spin.

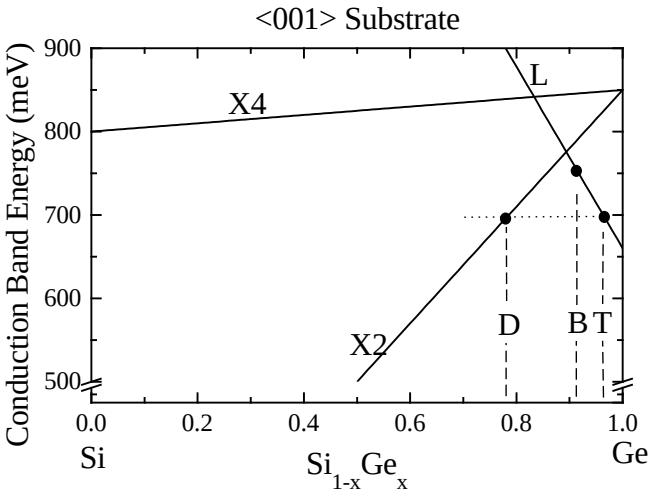


FIG. 6. The conduction band energy in Si-Ge alloys, compositionally strained in the $\langle 001 \rangle$ direction, from neutral strain at 100% Ge. The L-valley has 4 minima that remain degenerate. The X-valley has 6 minima along the cubic directions, that are split between X4 and X2. The compositions D, T, and B are much less strained than in the $\langle 111 \rangle$ case, and allow for higher barrier heights to confine the dopant electron. For this crystal orientation, the g-factor in the Ge-rich T- and B-layers is $g = 1.563$

If one uses alloys grown in the $\langle 001 \rangle$ direction instead, the numbers become even more favorable. Figure 6 shows the conduction band structure in the Si-Ge alloys, grown in the $\langle 001 \rangle$ direction [33], compositionally strained from neutral strain at 100% Ge. In this growth direction, the L band remains unsplit, and the X band splits up into a doubly degenerate X2

and a quadruply degenerate X4 band. As can be seen, the conduction band energy changes much more rapidly as a function of alloy composition for the ⟨001⟩ growth direction. Moreover, the X2 and the L bands cross over at approximately 90% Ge instead of 70% as in the Ge ⟨111⟩ case. This allows us to select alloys with much lower strain, while obtaining a barrier height of 50 meV, more than twice the barrier height obtained in the ⟨111⟩ direction. Consequently the layers can be made thinner while still preventing tunneling of the dopant electron and the strain tolerance is significantly improved. The corresponding band structure diagram for the ⟨001⟩ oriented SRT is shown in Figure 7.

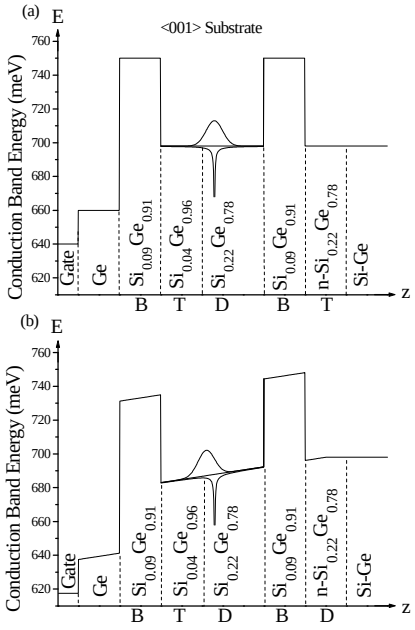


FIG. 7. The band structure diagram for the spin-resonance transistor, with epilayers grown in the ⟨001⟩ direction. Both the unbiased (a) and the biased case (b) are shown. The conduction band energies allow the selection of layers with composition D, T, and B such that the confining barrier height is increased to 50 meV, while the strain in the layers is reduced, compared to the ⟨111⟩ orientation. The epi-layer thicknesses are not to scale.

However, in the ⟨100⟩ direction, the g-factor is equal to the average value: $g = 1.563$, so that the tuning range for the spin resonance frequency is less than in the ⟨111⟩ case, as is demonstrated in Figure 8.

The use of the ⟨001⟩ growth direction comes at the expense of an increased effective mass in the xy-plane and a lighter mass in the z-direction. The conduction band ellipsoid pointing in the ⟨111⟩ direction is 55°away from the ⟨001⟩ direction and thus the z-direction no longer coincides with the heavy mass direction (⟨111⟩). Some of the heavy mass is transferred into the xy-plane, resulting in shorter Bohr radii. However, the lightest mass in Ge is equal to the heaviest mass in Si(see Table I). Therefore, the Ge-rich layer will always remain the layer with Bohr radii in the xy-direction which are at least as large as those in the Si-rich layer. Therefore Ge-rich layers will again perform the function of the tuning T-layer, and the barrier B-layer for structures grown in the ⟨001⟩ as they did for the ⟨111⟩ direction.

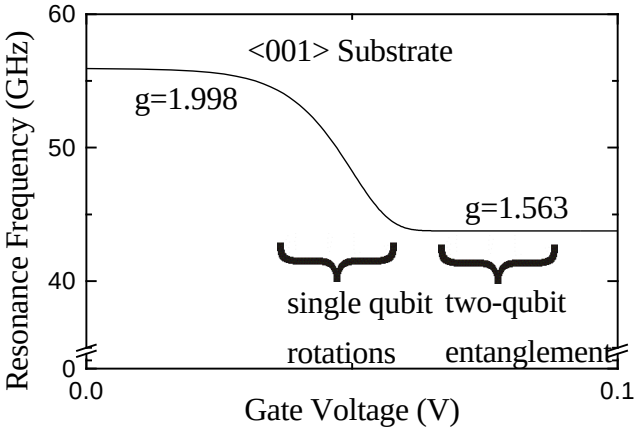


FIG. 8. A schematic of the dependence of the spin resonance frequency on the transistor gate voltage for the case of a ⟨001⟩ substrate. The static magnetic field is in the ⟨001⟩ direction and has a strength of 2 Tesla. The tuning range is reduced in this growth direction with respect to the ⟨111⟩ case, because the g-factor in the Ge-rich layer is different: $g = 1.563$.

V. TWO-QUBIT INTERACTIONS

The spin resonance transistors must be spaced far enough apart, that they will not produce phase errors in one another. At the same time it is necessary to allow wave function overlap for the exchange interaction to activate the 2-qubit interactions. These are needed to produce for example a Controlled NOT (CNOT) gate, which is required to build a universal set of quantum logic gates. To achieve this we rely on our ability to tune the Bohr radius of the donors in the xy-direction parallel to the semiconductor surface.

The Bohr radius a_B of a hydrogen-like donor increases with decreasing binding energy. A famous example is excitons confined in a 2-d flat quantum well: The excitonic binding energy is four times greater [34] than it would be in 3 dimensions. The reason is that spatial confinement forces the electron to spend more time near the positive charge, and it experiences tighter binding. Accordingly the Bohr radius is diminished. For the same reason, confinement by heavy mass in the z-direction reduces the Bohr radius in the xy-plane as can be seen from Equation 4. Without this reduction the effective mass in the xy-direction in strained ⟨111⟩ Ge would even be higher.

Our technique for 2-qubit interactions does not require any J-gates. By increasing the gate voltage, we pull the electron wave function away from the positive ion, to reduce the binding energy, and increase the wave function overlap between electrons bound to neighboring dopant ions. As shown in Fig-

ure 3, the electrons can be electrostatically attracted to one of the barriers formed by the $Si_{0.23}Ge_{0.77}$ B-composition layer, forming a type of modulation doped channel in the xy plane. The binding energy to the positive ions is greatly weakened, since the electrons are spending most of their time near the $Si_{0.23}Ge_{0.77}$ B-barrier.

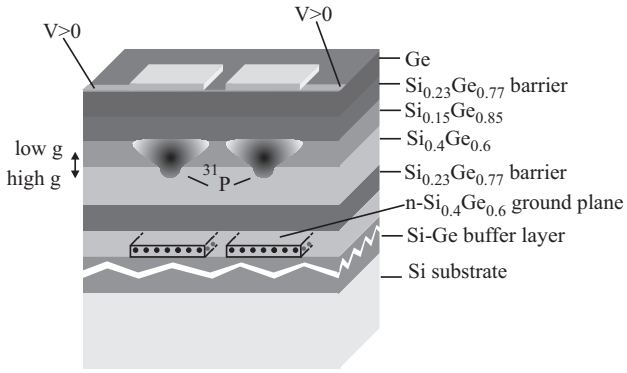


FIG. 9. Attracting the electrons to the $Si_{0.23}Ge_{0.77}$ B-barrier reduces their Coulomb binding energy and increases their wave function overlap, allowing 2-qubit interaction.

Consequently the Coulomb potential becomes weakened to the following form:

$$V = -\frac{1}{4\pi\epsilon_0\epsilon}\frac{q}{\sqrt{r^2+d^2}} \tag{4}$$

where $r^2 = x^2 + y^2$ is the horizontal distance from the donor ion, squared, and d is the vertical spacing from the barrier to the donor ion, and q is the electronic charge. Thus by adjusting the vertical depth of the ion, d, the Coulomb potential can be made as weak as desired. The weak Coulomb binding energy implies a large Bohr radius. The large radius permits a substantial wave function overlap in the xy-plane along the B-barrier layer, and a substantial 2-qubit exchange interaction. It should be possible to tune from negligible exchange interaction, all the way to a conducting metallic 2-d electron gas, by adjusting the vertical spacing d. As the electrons overlap, they will interact through the exchange interaction. It was already shown by DiVincenzo [35], that the exchange interaction can produce CNOT quantum gates.

The gate bias voltage range for 2-qubit entanglement, is indicated by the second curly bracket in Figure 4. That voltage range attracts the electrons away from the positive ions and toward the $Si_{0.23}Ge_{0.77}$ B barrier, thus increasing their wave function overlap. In the mid-voltage range, the first curly bracket in Figure 4, 1-qubit rotations take place. Thus both one- and two-qubit interactions can be controlled by a single gate. Gate tuning of a 2-qubit exchange interaction is illustrated in Figure 9.

VI. DETECTION OF SPIN RESONANCE BY A FET TRANSISTOR

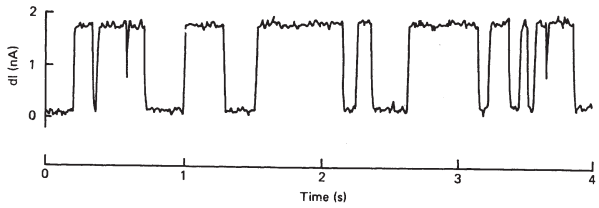


FIG. 10. The current noise in a small FET at 83 K from Kurten *et al* [37]. At this temperature the channel current fluctuates between two states, caused by a single trap being filled and emptied by a single charge. The change in channel current is ≈2nAmps, which represents a few percent of total channel current, and is easily measured.

It is a truism of semiconductor electronics that we need crystals of high perfection and extraordinary purity. Semiconductor devices are very sensitive to the presence of chemical and crystallographic faults down to the level of 10^{11} defects/cm3 in the volume, and 10^8 defects/cm2 on the surface. Such defect concentrations are far below the level of sensitivity of even the most advanced chemical analytical instruments. These imperfections influence the electrical characteristics of semiconductor devices, as they vary their charge states. Thus conventional electronic devices are sensitive to very low concentrations of defects.

The detection sensitivity becomes particularly striking when the electronic devices are very tiny, as they are today. If electronic devices are small enough, then there is a good probability that not even one single defect might be present in, or on, the device. That helps define the potential yield of essentially perfect devices. But if a defect were to be present, it would have an immediate effect on the current-voltage (I-V) characteristics of that device. Therefore, the new world of small transistors is making it relatively easy to detect single defects, as their charge states directly influence the I-V curves.

As Kane pointed out, the essential point for us is to detect spin, not by its miniscule magnetic moment, but by virtue [16] of the Pauli Exclusion Principle. A donor defect can bind [36] a second electron by 1meV, provided that second electron has opposite spin to the first electron. Thus spin detection becomes electric charge detection, the essential idea [35] behind Spin Resonance Transistors. In a small transistor, even a single charge can be relatively easily monitored.

A fairly conventional, small, Field Effect transistor, (FET) is very capable of measuring single charges, and therefore single spins as well. A single electronic charge, in the gate insulator, can have a profound effect on a low temperature FET. At more elevated temperatures for example, the motion of such individual charges produces telegraph noise in the FET channel current. An illustration of such single charge detection [37] is in Figure 10. A single electrostatic charge can add 1 additional carrier to the few hundred electrons in a FET channel. However the 2 nAmp change in channel cur-

rent seen in Figure 10 represents a few percent change, and is caused by long range Coulomb scattering influencing the resistance seen by all the electrons. At low FET operating temperatures, ≈1 K, the random flip-flops disappear, but the sensitivity to single charges remains [38].

In our spin-resonance transistor design, shown in Figures 5 and 9, the FET channel is labeled as the n-$Si_{0.4}Ge_{0.6}$ ground plane counter-electrode. It is located under the ^{31}P qubit donor, and in turn, the donor is under the top surface gate electrode. Thus the spin qubit is sandwiched between two electrodes. As in a normal FET the gate electrode modulates the n-$Si_{0.4}Ge_{0.6}$ channel current. The qubit electron donor is positioned in the gate insulator region where its charge state can have a strong influence on the channel current. Thus the successive charge states: ionized donor, neutral donor, and doubly occupied donor (D^- state) are readily sensed by measuring the channel current.

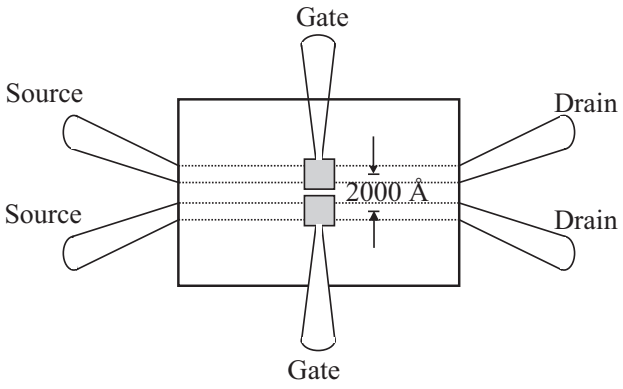


FIG. 11. Top view of the proposed device to demonstrate a CNOT gate. A perspective view (, not including the source and drain,) is shown in Figure 1. Fluctuations in the current that flows from source to drain signal the charge state of the dopant ion under each electrode.

In Figures 5 and 9, the two transistors have separate sensing channels under each transistor, so that they can be separately monitored, or indeed monitored differentially. By adjusting the gate electrodes, both qubit donor electrons can be attracted to the same donor. If they are in the singlet state they can join together forming the D- state on one of the two dopant ions, but in the triplet state they could never occupy the same site.

Since the D^- state forms on one transistor, and an ionized donor D^+, on the other transistor, there would be a substantial change in differential channel current to identify the singlet state. For the triplet state, both donors remain neutral and differential channel current would be constant. As indicated by the caption to Figure 10, we can anticipate a few percent change in FET current associated with the singlet spin state, making spin readily detectable.

VII. SMALL SCALE DEMONSTRATION

A possible 2-qubit demonstration device is shown in Figure 11. The differential current between the two FET's channels in Figure 9 would monitor the electron spin resonance. In practice a large number of transistor pairs would be arrayed along the two FET channels in Figure 11, to allow for a finite yield in getting successful pairs. A good pair can be sensed using the same technique used in the previous section for the detection (measurement) process.

There are two levels of doping in our proposed device: The first level of doping is the conducting FET channel doping, that needs to be at a heavy concentration to overcome freeze-out at low temperatures. This is a standard design technique in low temperature electronics. The second level of doping is in the qubit layer, that allows only one donor ion per transistor. Both doped regions need to be spatially patterned. The doped layers can be implemented by conventional ion- implantation through a patterned mask, possibly with an intermediate epitaxial growth step to minimize ion straggle. Conventional annealing can be used to remove ion damage.

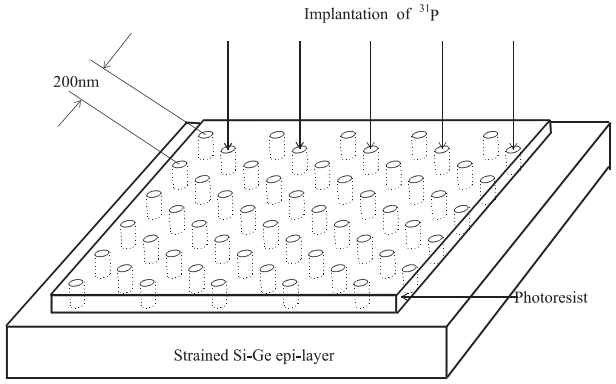


FIG. 12. The ion implantation step for inserting an array of qubit donor ions. The buried FET channels, that act as counter-electrodes to the gates and sense the spin/charge state, would be produced the same way. In a small-scale demonstration, the array would consist of only 2 rows, aligned with the FET channels of Figure 11. This should provide an adequate yield of good qubit pairs.

The ion-implantation dose for the qubit layer would be adjusted so that on average, only 1 Phosphorus ion would fall into each opening in the photoresist layer of Figure 12. By Poissonian statistics, the probability of getting exactly 1 Phosphorus ion is 36.7%. Thus the probability of getting two adjacent gates to work would be 13.5%. That is adequate yield for a small-scale two-qubit demonstration device. To improve the yield for scale-up, there are many options. For example, the dopant could be sensed by its electric charge, and re-implanted if it were absent. Sensing an individual dopant is not difficult. It can be done, for instance, by monitoring the I-V curve at each site. By changing the voltage on a particular A gate the electrons can be stripped off the donor. As result one can see no-change, a single-change, or a double-change of the current depending on whether there is

no donor, one donor or two donors (etc.) in that site.

VIII. SCALING UP

There are a number of potential problems in scaling to a large computer. The future usefulness of electron spins will depend heavily on the favorable homogeneous T_2 spin echo linewidth [23] in Silicon, only 10^3Hz. The T_2 lifetime in Si-Ge alloys has not been measured, and it will have to be demonstrated that it is as favorable as in pure Silicon. On the other hand there also appear to be methods such as isotopic purification, whereby this linewidth can be improved, particularly for well-isolated electrons.

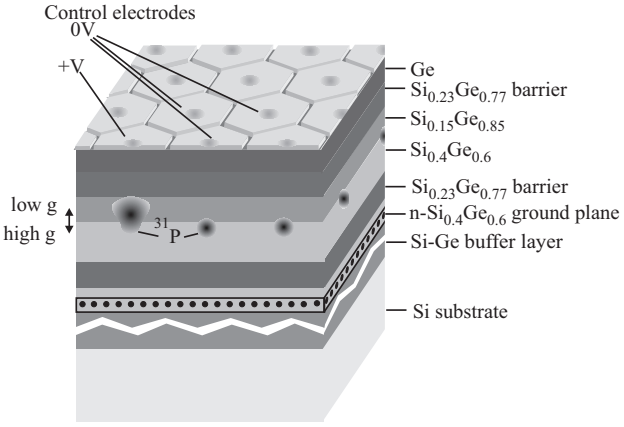


FIG. 13. In the future, we can expect arrays of Si-Ge SRT transistors. The center-to-center spacing would be ≈ 2000 Å. The gate electrodes on top will perform both single and 2-qubit operations, and can be used for data and instruction read-in.

In very large arrays, there are problems associated with the implantation yield of qubit donors. Poissonian statistics gives a yield of 36.7%, while a yield of 50% will required for percolation, or quantum connectivity, through the two- dimensional triangular array. There have been numerous non-Poissonian doping schemes proposed including sense/re-implant, self-assembly of molecular dopants, and scanning probe writing. Innovative doping methods have a long history, and we should anticipate that a suitable method will be optimized in time for scale-up to large quantum computers.

For instance, the sense/re-implant method (in which empty sites are sensed, and re-implanted with doping probability p_n in the n'th implant) yields $pe^{-p}(1-e^{-np})/(1-e^{-p})$ good sites when $p_i = p$ is chosen. With this formula, already $n = 2$ (only one additional implant) passes the percolation limit to yield 52.16%, while more implants, n=3,5,9, and 24, yield more than 60%, 70%, 80%, and 90% good sites respectively. With $n = 2$ an optimization of the doping probability in each implant (to be $p_1 = 0.632$ and $p_2 = 1$) provides the optimal yield of 53.15%.

The other scale up issue revolves around the fact that each transistor will not be identical. As Kane noted, the transistors will have to be checked and calibrated repeatedly for use in a full-fledged quantum computer. The reason is that the nuclear spins, although almost static, will be different for each transistor. In addition the local alloy structure is different near every donor. We should not be discouraged by this checking and calibration requirement. In manufacturing classical integrated circuits, testing and repair are the biggest expense. It is common to have only a finite yield of good devices, and to reroute wiring around bad transistors. This is probably inherent in the manufacture of any large-scale system.

The size of spin resonance transistors, the required defect density, the increasing use of Si-Ge alloys, are all near to the present state of technology. If the spin resonance transistor (SRT) is successfully developed, we can anticipate arrays of qubits appearing much as in Figure 13.

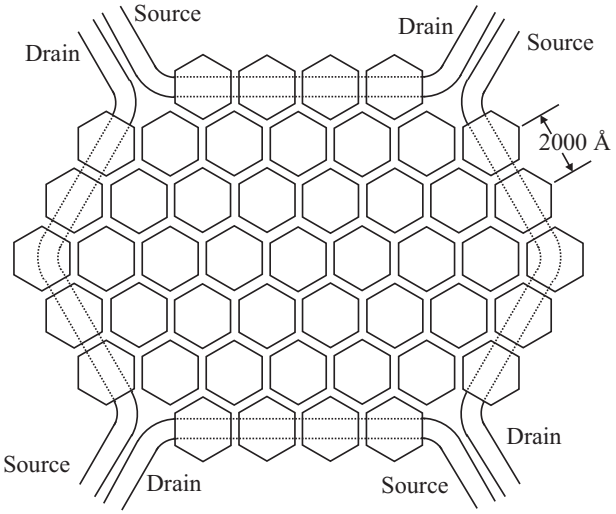


FIG. 14. In a large array, the read-out qubits would be located around the periphery. Buried FET channels would sense the spin/charge state of a selected qubit. The channel current can change by a few percent in response to a single electronic charge.

The read-out of data requires that the buried counter electrode, opposite the gate, should also function as an FET channel. In a quantum computer, the result of the quantum computation is usually displayed on a small sub-array of all the qubits. Hence the read-out qubits can be located at the edge of the array. Figure 14 shows a qubit array, with read-out FET channels (counter- electrodes) buried under the peripheral qubits of the array. A single buried FET read-out channel can serve many qubits, since a chosen qubit can be selected for readout by its gate electrode.

The read-out operation can be expedited if there is a thermal reservoir of donors surrounding the peripheral qubits as shown in Figure 15. These can be attracted by a field electrode to the $Si_0.23Ge_{0.77}$ B-barrier under the electrode, forming in effect a modulation doped layer. Since the operating temperature of the computer is such that $kT \ll E_z$ with E_z the Zeeman energy of the electron spins, these qubits would be oriented by the magnetic field, and would act as a spin heat bath of known orientation. By attracting those bath spins to a peripheral read-out qubit gate electrode, a singlet

state could be formed, sensing that the readout qubit had been flipped. The current in the FET channel would then change, completing the read-out operation.

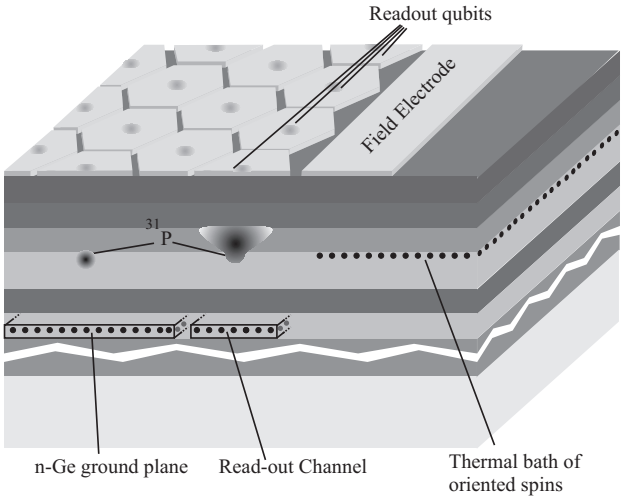


FIG. 15. A perspective view of Figure 14, gives more details of the readout architecture for the peripheral qubits. The field electrode allows the Readout Qubits to interact with the heat bath of oriented electron spins

After readout, the gate voltage could be made even more positive, and the read- out qubit could thermalize with the surrounding heat bath. In effect, this resets the initial state of that peripheral qubit, which could then be swapped into the interior qubits for re-use as fault correcting ancilla qubits.

Without a doubt there will be many other issues regarding scale-up. Semiconductors, particularly silicon, provide a track record of being tractable, engineerable materials in which many difficult accomplishments have become routine.

---

[1] P. W. Shor, Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, ed. by S. Goldwasser, (IEEE Comput. Soc. Press, Los Alamitos) 124 (1994).
[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[3] R. Feynman, Int. J. of Theoretical Physics **21**, 467 (1982).
[4] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).
[5] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[6] J. Preskill, Proc. R. Soc. London A **454**, 385 (1998).
[7] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[8] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
[9] D. G. Cory, M. D. Price, and T. F. Havel, Physica D **120**, 82 (1998).
[10] Q. A. Turchette *et al.*, Phys. Rev. Lett. **75**, 4710 (1995).
[11] G. J. Milburn, Phys. Rev. Lett. **62**, 2124 (1989).
[12] A. Shnirman, G. Schoen, and Z. Hermon, Phys. Rev. Lett. **79**, 2371 (1997).
[13] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).
[14] C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995).
[15] J. A. Jones and M. Mosca, LANL preprint quant-ph/980127 (1998).
[16] B. Kane, Nature **393**, 133 (1998).
[17] D. P. DiVincenzo, Mesoscopic Electron Transport, eds. L. Sohn, L. Kouwenhoven, and G. Schoen (NATO Advanced Study Institute, Curacao **345**, 657 (1996).
[18] S. Bandyopadhyay, A. Balandin, V. P. Roychowdhury, and F. Vatan, Superlatt. and Microstruct. **23**, 445 (1998).
[19] G. Feher, Phys. Rev. **114**, 1219 (1959).
[20] G. Feher and E. A. Gere, Phys. Rev. **114**, 1245 (1959).
[21] D. K. Wilson and G. Feher, Phys. Rev. **124**, 1068 (1961).
[22] G. Feher, Paramagnetic Resonance, Vol. II, ed. by W. Low ,Academic Press, N.Y. see esp. p.725 (1963).
[23] M. Chiba and A. Hirai, J. Phys. Soc. Japan **33**, 730 (1972).
[24] J. P. Gordon and K. D. Bowers, Phys. Rev. Lett. **1**, 368 (1958).
[25] L. M. Roth, Phys. Rev. **118**, 1534 (1960).
[26] H. Hasegawa, Phys. Rev. **118**, 1523 (1960).
[27] D. K. Wilson, Phys. Rev. **134**, A265 (1964).
[28] E. Yablonovitch and E. O. Kane, J. Lightwave Technol. **6**, 1292 (1988).
[29] K. L. Wang and R. P. G. Karunasiri, Semiconductor Quantum Wells for Long Wavelength Infrared Detectors, ed. by M.O. Manasreh, (Artech House, Norwood MA) (1993).
[30] A. Schindlmayr, Eur. J. Phys. **18**, 374 (1997).
[31] J. Gea-Banacloche, Phys. Rev. A **57**, R1 (1998).
[32] H. Vollmer and D. Geist, Phys. Stat. Sol. B **62**, 367 (1974).
[33] K. L. Wang, S. G. Thomas, and M. O. Tanner, J. Mat. Sci. **6**, 311 (1995).
[34] G. Bastard, Phys. Rev. B **24**, 4714 (1981).
[35] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).
[36] M. Taniguchi and S. Narita, J. Phys. Soc. Japan **43**, 1262 (1977).
[37] M. J. Kurten and M. J. Uren, Adv. Phys. **38**, 367 (1989).
[38] It should not be surprising that single electron charges are so easy to detect. That task was already accomplished many years ago in the Millikan oil-drop experiment of 1910 .

Environmentally decoupled *sds*-wave Josephson junctions for quantum computing

Lev B. Ioffe*‡, Vadim B. Geshkenbein†‡, Mikhail V. Feigel'man‡, Alban L. Fauchère† & Gianni Blatter†

** Department of Physics and Astronomy, Rutgers University, Piscataway, New Jersey 08854, USA*

† Theoretische Physik, ETH-Hönggerberg, CH-8093 Zürich, Switzerland

‡ Landau Institute for Theoretical Physics, 117940 Moscow, Russia

Quantum computers have the potential to outperform their classical counterparts in a qualitative manner, as demonstrated by algorithms[1] which exploit the parallelism inherent in the time evolution of a quantum state. In quantum computers, the information is stored in arrays of quantum two-level systems (qubits), proposals for which include utilizing trapped atoms and photons[2–4], magnetic moments in molecules[5] and various solid-state implementations[6–10]. But the physical realization of qubits is challenging because useful quantum computers must overcome two conflicting difficulties: the computer must be scalable and controllable, yet remain almost completely detached from the environment during operation, in order to maximize the phase coherence time[11]. Here we report a concept for a solid-state 'quiet' qubit that can be efficiently decoupled from the environment. It is based on macroscopic quantum coherent states in a superconducting quantum interference loop. Our two-level system is naturally bistable, requiring no external bias: the two basis states are characterized by different macroscopic phase drops across a Josephson junction, which may be switched with minimal external contact.

Our Josephson junction utilizes unconventional superconductors with order-parameter symmetry lower than the symmetry of the underlying crystal lattice. Recent phase-sensitive experiments on $YBa_2Cu_3O_7$ single crystals have established the *d*-wave nature of the copper oxide materials, thus identifying unambiguously the first unconventional superconductor[12,13]. The sign change in the order parameter of these materials can be exploited to construct a new type of *s*-wave–*d*-wave–*s*-wave Josephson junctions exhibiting a degenerate ground state and a double-periodic current–phase characteristic. The basic idea is sketched in Fig. 1: connecting the positive (100) and negative (010) lobes of a *d*-wave superconductor with a *s*-wave material produces a π-loop with a current-carrying ground state characteristic of *d*-wave symmetry[12]. Here we use an alternative geometry and match the *s*-wave superconductors (*S* in Fig. 1) to the (110) boundaries of the *d*-wave (D) material. The usual Josephson coupling (proportional to $(1-\cos\phi)$) vanishes for symmetry reasons and we arrive at a bistable device, where the leading term in the coupling takes the form $E_d\cos 2\phi$ with minima at $\phi = \pm\pi/2$ (here ϕ denotes the gauge-invariant phase drop across the junction and E_d is the coupling energy). In our design we need the minima at the positions $\phi = 0, \pi$—the necessary shift is achieved by going over to an asymmetric SDS′ junction with a large DS′ coupling (Fig. 1). The static DS′ junction shifts the minima of the active SD junction by the desired amount, $\pi/2$. A similar double-periodic junction was recently realized by combining two *d*-wave superconductors oriented at a 45° angle[14].

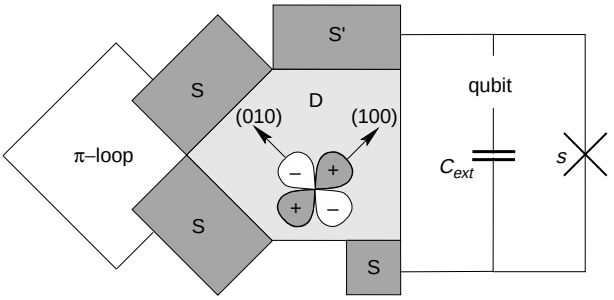


Figure 1 Schematic of the junction. Geometrical arrangements between *s*- and *d*-wave superconductors producing a π-loop (as in the phase-sensitive experiment by Wollman *et al.*[12]) and a qubit, basic building block of a quantum computer, are shown.

The ground states of our SDS′ junction are degenerate and carry no current, while still being distinguishable from one another: for example, after connecting the junction to a large inductance loop, the π state is easily identified through the induced current. It is this double-periodicity and the associated degeneracy in the ground state of the SDS′ which we want to exploit here for quantum computation: combining the SDS′ junction, a capacitor, and a conventional *s*-wave junction into a SDS′ SQUID loop, we construct a bistable element that satisfies all the requirements for a qubit, the basic building block of a quantum computer. (SQUID indicates a superconducting quantum interference device.) Below we give a detailed account of the operational features of our device.

Consider a small-inductance (L) SQUID loop with $I_JL \ll \Phi_0$, where I_J denotes the (Josephson) critical current of the loop and $\Phi_0 = hc/2e$ is the flux unit. Such a loop cannot trap magnetic flux ($\Phi = 0$) and the gauge-invariant phase differences ϕ_1 and ϕ_2 across the two junctions follow each other, as the uniqueness of the

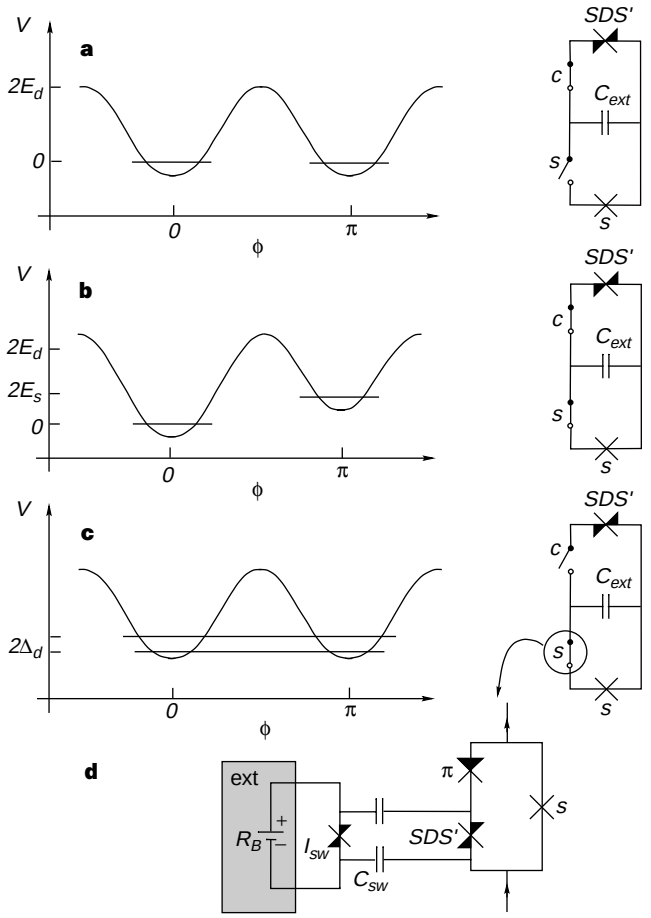


Figure 2 Energy–phase diagrams for the SDS′ SQUID loop. **a**, Idle-state: the switches are set to '*c* on' and '*s* off'–the relative dynamics are quenched, leaving the state unchanged. **b**, Phase-shifter: with the switch settings '*c* on' and '*s* on' the relative phase between $|0\rangle$ and $|\pi\rangle$ increases linearly with time. **c**, Amplitude-shifter: the switch setting '*c* off' isolates the *d*-wave junction. An initial state $|0\rangle$ oscillates back and forth between $|0\rangle$ and $|\pi\rangle$, allowing for a shift of amplitude. **d**, the SDS′ junction, a π junction, and a *s*-wave junction combined into a SQUID loop and serving as a switch.

wavefunction requires that $\phi_1 - \phi_2 = 2\pi\Phi/\Phi_0$ (ref. 15). Combining an SDS′ junction with a coupling energy E_d and a conventional *s*-wave junction (coupling E_s) into an SDS′ SQUID loop, we obtain a potential energy

$$V(\phi) = E_d(1 - \cos 2\phi) + E_s(1 - \cos\phi) \quad (1)$$

exhibiting two minima at $\phi = 0, \pi$ (Fig. 2). The switch *s* allows us to manipulate their energy separation, choosing between minima which are either degenerate or separated by $2E_s$.

In the quantum case, the phase fluctuates as a consequence of the particle–phase duality[15]. The phase fluctuations are driven by the electrostatic energy required to move a Cooper pair across the junction, and are described by the kinetic energy $T(\dot{\phi}) = (\hbar/2e)^2 C\dot{\phi}^2/2$, where C denotes the loop capacitance. The dynamics of ϕ are manipulated by inserting a large switchable (by switch *c*) capacitance C_{ext} into the loop acting in parallel with the capacitances C_d and C_s of the *d*- and *s*-wave junctions. We note that the lagrangean $L = T - V$ of our loop is formally equivalent to that of a particle with 'mass' $m \propto C$ moving in the potential $V(\phi)$.

With the switch settings '*c* on' '*s* off' (Fig. 2a), the loop capacitance is large and the junction exhibits a double degenerate ground state which we characterize via the phase coordinated ϕ, $|0\rangle$ and $|\pi\rangle$. Closing the switch *s* (Fig. 2b), the degeneracy is lifted and while $|0\rangle$ becomes the new ground state, the $|\pi\rangle$-state is shifted upwards by the energy $2E_s$ of the *s*-wave junction, the latter being frustrated (that is, pushed to maximal energy) when $\phi = \pi$. On the other hand, opening the switch *c* (Fig. 2c), completely isolates the *d*-wave junction and leads to the new ground and excited states $|\pm\rangle = [|0\rangle \pm |\pi\rangle]/\sqrt{2}$ separated by the tunnelling gap $2\Delta_d$. The latter relates to the barrier $2E_d$ and the capacitance C_d of the *d*-wave junction via[15] $\Delta_d \propto E_d \exp(-2\sqrt{C_d E_d/e^2})$. Closing the switch *c*, the capacitance is increased by C_{ext} and the tunnelling gap is exponentially suppressed. Using the above three settings, we can perform all the necessary single qubit operations, as follows.

Idle-state. The switch settings '*c*-on' and '*s*-off' define the qubit's idle-state. While the large capacitance C_{ext} inhibits tunnelling, the degeneracy of $|0\rangle$ and $|\pi\rangle$ guarantees a parallel time evolution of the two states. This idle-state is superior to other designs, where the two states of the qubit have different energies and it is necessary to keep track of the relative phase accumulated between the basis states.

Phase shifter. Closing the switch *s* separates the energies of the basis states $|0\rangle$ and $|\pi\rangle$ by an amount $2E_s$. Using a spinor notation for the two-level system, the relative time evolution of the two states is described by the hamiltonian $H_s = -E_s\sigma_z$, with σ_z a Pauli matrix. Keeping the switch *s* on during the time *t*, the time evolution of the two states is given by the unitary rotation $u_z(\varphi) = \exp(-i\sigma_z\varphi/2)$ with $\varphi = -2E_s t/\hbar$.

Amplitude shifter. Assume we have prepared the loop in the ground state $|0\rangle$ and wish to produce a superposition by shifting some weight to the $|\pi\rangle$ state. Opening the switch *c* in the loop (Fig. 2c), the time evolution generated by the hamiltonian $H_d = \Delta_d\sigma_x$ of the open loop induces the rotation $u_x(\vartheta) = \exp(-i\sigma_x\vartheta/2)$ with $\vartheta = 2\Delta_d t/\hbar$. The system then oscillates back and forth between $|0\rangle$ and $|\pi\rangle$ with frequency $\omega = \Delta_d/\hbar$ and keeping the switch *c* open for an appropriate time interval *t*, we obtain the desired shift in amplitude (note that the qubit remains isolated from the environment during these Rabi oscillations).

Imposing the conditions $E_d \gg E_s, \Delta_d$ on the coupling energies, we make sure that the two states $|0\rangle$ and $|\pi\rangle$ are well defined while simultaneously involving only the low-energy states $|0\rangle$ and $|\pi\rangle$ of the system. Furthermore, all times involved should be smaller than the decoherence time τ_{dec}, requiring $E_s, \Delta_d \gg \hbar/\tau_{\text{dec}}$.

The present set-up differs significantly from the conventional (large-inductance) SQUID loop design, where the low-lying states are distinguished via the different amount of trapped flux and their manipulation involves external magnetic fields or biasing currents. SQUID loops of this type are being used in the design of classical Josephson-junction computers[16] and have also been proposed[9] for the realization of quantum computers. However, this set-up suffers from the generic problem that the flux moving between the loops leads to a magnetic-field-mediated long-ranged interaction between the individual loops and also produces an unwanted coupling to the environment. By contrast, our device remains decoupled from the environment, the operating states do not involve currents, and switching between states can be triggered with a minimal contact to the external world—we therefore call our qubit implementation 'quiet'.

We now consider how to perform two-qubit operations within an array of SDS′ SQUID loops. A two-qubit state is a coherent superposition of single qubit states and can be expressed in the basis $\{|xy\rangle\}$, where $x, y \in \{0, \pi\}$ denote the phases on the *d*-wave junctions of the first (x) and second (y) qubit, respectively. Unitary operations acting on these states are represented as 4×4 unitary matrices. Single-qubit operations u acting on the second qubit take the block-matrix form

$$U_2 = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \quad (2)$$

and a similar block form selecting odd and even rows and columns defines the single-qubit operations on the first qubit. As all logic operations on two qubits can be constructed from combinations of single-qubit operations and the 'controlled-NOT' gate[1] it is sufficient to define the operational realization of the latter. The controlled-NOT gate performs the following action on the two qubits: with the first (controller) qubit in state $|x\rangle$ and the second (target qubit) in state $|y\rangle$ the operation shall leave the target qubit unchanged if $x = 0$, while flipping it between 0 and π when $x = \pi$, in matrix notation:

$$U_{\text{CNOT}} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & \sigma_x \end{pmatrix} \quad (3)$$

The above controlled-NOT operation can be constructed from the 2-qubit phase shifter. Connecting two individual qubits in their idle-state over a *s*-wave junction into a SQUID loop, the states $|00\rangle$ and $|\pi\pi\rangle$ become separated from the states $|0\pi\rangle$ and $|\pi 0\rangle$ by the energy $2E_{s_b}$ of the *s*-wave junction. Keeping the two qubits connected during the time *t* introduces a phase shift $\chi = -2E_{s_b}t/\hbar$ between the two pairs of states:

$$U_{\text{ps}}(\chi) = \begin{pmatrix} u_z(\chi) & 0 \\ 0 & u_z(-\chi) \end{pmatrix} \quad (4)$$

The controlled-NOT gate (equation (3)) then can be constructed from the phase-shifter (equation (4)) via the following sequence of single- and two-qubit operations (see ref. 6 for a similar realization of the controlled-NOT gate)

$$\begin{aligned} U_{\text{CNOT}} = {} & \exp(-i\pi/4)U_{2y}(\pi/2)U_{1z}(-\pi/2)U_{2z}(-\pi/2) \\ & \cdot U_{\text{ps}}(\pi/2)U_{2y}(-\pi/2) \end{aligned} \quad (5)$$

where the single qubit operations $U_{i\mu}(\theta)$ rotate the qubit i by an angle θ around the axis μ ($u_\mu(\theta) = \exp(-i\sigma_\mu\theta/2)$ acting on i) while leaving the other qubit unchanged.

The switches are important elements in our design, and a valid suggestion for their implementation is the single electron transistor[17]. Here we propose a quiet switch design optimally adapted to our SDS′ qubits. The basic idea derives from frustrating the junctions in a SQUID loop, resulting in a 'phase blockade': combining an SDS′ junction with energy E_d, a π-junction with $E_\pi \ll E_d$, and an *s*-wave junction with $E_s = E_\pi$ into a (small-inductance) SQUID loop (Fig. 2d), we obtain the following switching behaviour. The phase $\phi = 0$ on the SDS′ junction frustrates the remaining junctions, the loop's energy–phase relation is a constant, $E_{\text{sw}}(\phi_\pi = \phi_s - \pi) \equiv 0$, and the switch is open. A voltage pulse coming down the signal lines and switching the SDS′ junction into the $|\pi\rangle$ state changes the phase relation between

the π- and the s-wave junctions and closes the switch: the energy $E_{sw}(\phi_\pi = \phi_s) = 2E_\pi(1 - \cos\phi_\pi)$ produces the current–phase relation $I = (2e/\hbar)\partial_{\phi_\pi}E_{sw}$, thus suppressing the fluctuations of the phase across the switch. The appropriate voltage pulses could be generated by driving an external SDS′ junction unstable.

The quiet-device concept proposed above relies heavily on the double periodicity of the SD junction. As the second harmonic is strongly suppressed in a SID (s-wave–insulator–d-wave) tunnel junction, a more feasible suggestion for the realization of a $\cos 2\phi$ junction is the SND 'sandwich', where the superconductors are separated by a thin metallic layer N. For a clean metallic layer, the coupling energies for the nth harmonic are large and of the order of $E_J \approx k_F^2 A\hbar v_F/d$, producing the well known saw-tooth shape in the current–phase relation[18] (here, v_F (k_F) denotes the Fermi velocity (wavenumber) in the N layer while d and A are its width and area). In reality, it seems difficult to deposit a clean metallic film on top of a d-wave superconductor, and we have to account for the reduction in the coupling E_J due to the finite scattering length l in the metal layer. Using quasi-classical techniques to describe a dirty SN_dD junction (s-wave–dirty normal metal–d-wave), we obtain a second-harmonic coupling energy $E_d \approx k_F^2 A(\hbar v_F/d)(l/d)^3 \approx (R_Q/R)(l/d)E_T$, where l denotes the scattering length in the normal metal, $R_Q = \hbar/e^2$ is the quantum resistance, R is the junction resistance, and $E_T \approx (\hbar v_F/d)(l/d)$ is the Thouless energy.

The second important device parameter is the tunnelling gap Δ_d, which depends quite sensitively on the coupling to the environment. The usual reduction in the tunnelling probability by the environment[19] is modified if the system is effectively gapped at low energies[20]. This is the case for our $SN_dDN'_dS'$ junction where the low-energy quasiparticle excitations in the metal are gapped over the Thouless energy E_T (ref. 21). The dynamics of the junction are only affected by the presence of virtual processes involving energies larger than E_T, leading to a renormalized capacitance $C_{ren} \approx \hbar/RE_T$ (compare ref. 20) and resulting in the reduced tunnelling gap $\Delta_d \propto E_d \exp[-\nu(R_Q/R)\sqrt{l/d}]$, with ν of the order of unity. Consistency requires that the tunnelling process is 'massive' and hence slow, $\hbar/\tau < E_T$. With a tunnelling time $\tau \approx S/E_d$ ($S \approx \hbar(R_Q/R)\sqrt{l/d}$ gives tunnelling action) we find that the constraint $\hbar/\tau E_T \approx \sqrt{l/d} < 1$ is satisfied. The condition $\Delta_d \ll E_d$ requires the tunnelling gap Δ_d to be small, but large enough in order to allow for reasonable switching times, requiring $(R_Q/R)\sqrt{l/d}$ to be of the order of 10. With typical device dimensions $d \approx 1{,}000$ Å, $l \approx 10$ Å, and $R/R_Q \approx (d/l)(1/Ak_F^2) \approx 1/100$, this condition can be realized. The operating temperature T is limited by the constraint $S/\hbar > E_d/T$, guaranteeing that our device operates in the quantum regime, and the requirement $T < E_T$, that thermal quasi-particle excitations be absent. The first condition takes the form $T \ll \hbar/\tau \approx \sqrt{l/d}E_T$ and is the more stringent. Using the above parameters and a typical value $v_F \approx 10^8\ \mathrm{cm\,s^{-1}}$, we obtain a Thouless energy $E_T \approx 1$ K and hence $T \ll 0.1$ K.

An important topic in quantum computation is decoherence. Within our set-up it is the Thouless gap E_T which inhibits the excitation of quasiparticles. The longest trajectories in the $SN_dDN'_dS'$ junction limiting the size of E_T are those connecting the two s-wave superconductors over a path of length $L_{max} \approx 2d^2/l + d_d$, where the first term stems from the diffusive propagation through the two dirty metal layers, and the second term is due to the ballistic trajectory along the node of the d-wave superconductor (of width d_d). The conditions $\xi_d \ll d_d \ll d^2/l$, with ξ_d the coherence length in the d-wave superconductor, then guarantee that the d-wave layer is thick enough to avoid the quenching through the proximity to the s-wave superconductors, while still being thin enough to leave the Thouless gap unchanged. A further source of decoherence are the switches. Within the set-up sketched in Fig. 2d, the voltage pulse triggering the SDS′ junction in the switch is generated through an external junction driven by a current source. We then have to make sure that while the switching signal reaches the SDS′ junction of the switch loop, the external noise is kept away from the qubit's SDS′ junction. Most dangerous is the low-frequency part of the noise spectrum, as it would induce brownian motion of the relative phase in the wavefunction of the qubit. An appropriate filtering can be achieved through a capacitive decoupling (C_{sw}) of the external driven junction generating the pulses and the SDS′ switch, transparent at the high frequencies of the triggering pulse, but suppressing the low-frequency noise of the current source through a factor $(\omega C_{sw}R_B)^2$, where R_B denotes the resistivity of the external current source. Furthermore, the driven junction loop acts as a shunt, producing an additional suppression factor $(e\omega/I_{sw})^2R_Q/R_B$. □

Received 14 December 1998; accepted 8 March 1999.

1. Ekert, A. & Jozsa, R. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.* **68,** 733–753 (1996).
2. Cirac, J. I. & Zoller, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74,** 4091–4094 (1995).
3. Monroe, C., Meekhof, D., King, B., Itano, W. & Wineland, D. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.* **75,** 4714–4717 (1995).
4. Turchette, Q., Hood, C., Lange, W., Mabushi, H. & Kimble, H. J. Measurement of conditional phase shifts for quantum logics. *Phys. Rev. Lett.* **75,** 4710–4713 (1995).
5. Gershenfeld, N. A. & Chuang, I. L. Bulk spin-resonance quantum computation. *Science* **275,** 350–356 (1997).
6. Loss, D. & DiVincenzo, D. P. Quantum computation with quantum dots. *Phys. Rev. A* **57,** 120–126 (1998).
7. Shnirman, A., Schön, G. & Hermon, Z. Quantum manipulations of small Josephson junctions. *Phys. Rev. Lett.* **79,** 2371–2374 (1997).
8. Averin, D. V. Adiabatic quantum computation with Cooper pairs. *Solid State Commun.* **105,** 659–664 (1998).
9. Bocko, M. F., Herr, A. M. & Feldman, M. J. Prospects for quantum coherent computation using superconducting electronics. *IEEE Trans. Appl. Supercond.* **7,** 3638–3641 (1997).
10. Kane, B. E. A silicon-based nuclear spin quantum computer. *Nature* **393,** 133–137 (1998).
11. Haroche, S. & Raimond, J.-M. Quantum computing: dream or nightmare? *Phys. Today* **49,** 51–52 (1996).
12. Wollman, D. A., Van Harlingen, D. J., Lee, W. C., Ginsberg, D. M. & Leggett, A. J. Experimental determination of the superconducting pairing state in YBCO from the phase coherence of YBCO-Pb DC SQUID's. *Phys. Rev. Lett.* **71,** 2134–2137 (1993).
13. Kirtley, J. R. *et al.* Symmetry of the order parameter in the high-T_c superconductor $YBa_2Cu_3O_{7-\delta}$. *Nature* **373,** 225–228 (1995).
14. Il'ichev, E. *et al.* Anomalous periodicity of the current-phase relationship of grain-boundary Josephson junctions in high-T_c superconductors. Preprint cond-mat/9811017 at ⟨http://xxx.lanl.gov⟩ (1998).
15. Tinkham, M. in *Introduction to Superconductivity* Ch. 6.4 and 7.3, (McGraw-Hill, Singapore, 1996).
16. Likharev, K. K. & Semenov, V. K. RSFQ logic/memory family: A new Josephson-junction technology for sub-terahertz-clock-frequency digital systems. *IEEE Trans. Appl. Supercond.* **1,** 3–28 (1991).
17. Joyez, P., Lafarge, P., Filipe, A., Esteve, D. & Devoret, M. H. Observation of parity-induced suppression of Josephson tunneling in the superconducting single electron transistor. *Phys. Rev. Lett.* **72,** 2458–2461 (1994).
18. Ishii, C. Josephson currents through junctions with normal metal barriers. *Prog. Theor. Phys.* **44,** 1525–1547 (1970).
19. Caldeira, A. O. & Leggett, A. J. Quantum tunneling in a dissipative system. *Ann. Phys.* **149,** 374–456 (1983).
20. Ambegaokar, V., Eckern, U. & Schön, G. Quantum dynamics of tunneling between superconductors. *Phys. Rev. Lett.* **48,** 1745–1748 (1982).
21. Golubov, A. A. & Kuprianov, M. Yu. Theoretical investigation of Josephson tunnel junctions with spatially inhomogeneous superconducting electrodes. *J. Low Temp. Phys.* **70,** 83–130 (1988).

Acknowledgements. We thank A. Kitaev, D. Loss, A. Millis and B. Spivak for discussions. This work was supported by the Fonds National Suisse.

Correspondence and requests for materials should be addressed to G.B. (e-mail: blatterj@itp.phys.ethz.ch).

Metastable ice VII at low temperature and ambient pressure

S. Klotz*, J. M. Besson*, G. Hamel†, R. J. Nelmes‡, J. S. Loveday‡ & W. G. Marshall§

** Physique des Milieux Condensés UMR 7602 and † Départment des Hautes Pressions, Université P&M Curie, B77, 75252 Paris, France*

‡ Department of Physics and Astronomy, The University of Edinburgh, Edinburgh EH9 3JZ, UK

§ ISIS Facility, Rutherford Appleton Laboratory, Chilton, Didcot OX11 0QX, UK

Ice exhibits many solid-state transformations under pressure, and also displays a variety of metastable phases[1]. Most of the high-pressure phases of ice can be recovered at ambient pressure provided that they are first cooled below about 100 K. These ice polymorphs might exist on the surfaces of several satellites of the

Architecture for a large-scale ion-trap quantum computer

Article *in* Nature · July 2002

DOI: 10.1038/nature00784 · Source: PubMed

3 authors, including:

David Kielpinski
Griffith University
139 PUBLICATIONS **6,747** CITATIONS

Architecture for a large-scale ion-trap quantum computer

D. Kielpinski*, C. Monroe† & D. J. Wineland‡

** Research Laboratory of Electronics and Center for Ultracold Atoms, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
† FOCUS Center and Department of Physics, University of Michigan, Ann Arbor, Michigan 48109-1120, USA
‡ Time and Frequency Division, National Institute of Standards and Technology, Boulder, Colorado 80305, USA

Among the numerous types of architecture being explored for quantum computers are systems utilizing ion traps, in which quantum bits (qubits) are formed from the electronic states of trapped ions and coupled through the Coulomb interaction. Although the elementary requirements for quantum computation have been demonstrated in this system, there exist theoretical and technical obstacles to scaling up the approach to large numbers of qubits. Therefore, recent efforts have been concentrated on using quantum communication to link a number of small ion-trap quantum systems. Developing the array-based approach, we show how to achieve massively parallel gate operation in a large-scale quantum computer, based on techniques already demonstrated for manipulating small quantum registers. The use of decoherence-free subspaces significantly reduces decoherence during ion transport, and removes the requirement of clock synchronization between the interaction regions.

A quantum computer is a device that prepares and manipulates quantum states in a controlled way, offering significant advantages over classical computers in tasks such as factoring large numbers[1] and searching large databases[2]. The power of quantum computing derives from its scaling properties: as the size of these problems grows, the resources required to solve them grow in a manageable way. Hence a useful quantum computing technology must allow control of large quantum systems, composed of thousands or millions of qubits.

The first proposal for ion-trap quantum computation involved confining a string of ions in a single trap, using their electronic states as qubit logic levels, and transferring quantum information between ions through their mutual Coulomb interaction[3]. All the elementary requirements for quantum computation[4]—including efficient quantum state preparation[5–7], manipulation[7–10] and read-out[7,11,12]—have been demonstrated in this system. But manipulating a large number of ions in a single trap presents immense technical difficulties, and scaling arguments suggest that this scheme is limited to computations on tens of ions[13–15]. One way to escape this limitation involves quantum communication between a number of small ion-trap quantum registers. Recent proposals along these lines that use photon coupling[16–18] and spin-dependent Coulomb interactions[19] have not yet been tested in the laboratory. The scheme presented here, however, uses only quantum manipulation techniques that have already been individually experimentally demonstrated.

The quantum CCD

To build up a large-scale quantum computer, we have proposed a 'quantum charge-coupled device' (QCCD) architecture consisting of a large number of interconnected ion traps. By changing the operating voltages of these traps, we can confine a few ions in each trap or shuttle ions from trap to trap. In any particular trap, we can manipulate a few ions using the methods already demonstrated, while the connections between traps allow communication between sets of ions[13]. Because both the speed of quantum logic gates[20] and the shuttling speed are limited by the trap strength, shuttling ions between memory and interaction regions should consume an acceptably small fraction of a clock cycle.

Figure 1 shows a diagram of the proposed device. Trapped ions storing quantum information are held in the memory region. To perform a logic gate, we move the relevant ions into an interaction region by applying appropriate voltages to the electrode segments. In the interaction region, the ions are held close together, enabling the Coulomb coupling necessary for entangling gates[3,21]. Lasers are focused through the interaction region to drive gates. We then move the ions again to prepare for the next operation.

We can realize the trapping and transport potentials needed for the QCCD using a combination of radio-frequency (r.f.) and quasistatic electric fields. Figure 1 shows only the electrodes that support the quasistatic fields. By varying the voltages on these electrodes, we confine the ions in a particular region or transport them along the local trap axis, which lies along the thin arrows in Fig. 1. Two more layers of electrodes lie above and below the static electrodes, as shown in Fig. 2. Applying r.f. voltage to the outer layers creates a quadrupole field that confines the ions transverse to the local trap axis by means of the ponderomotive force[22]. This geometry allows stable transport of the ions around 'T' and 'X' junctions, so we can build complex, multiply connected trap structures.

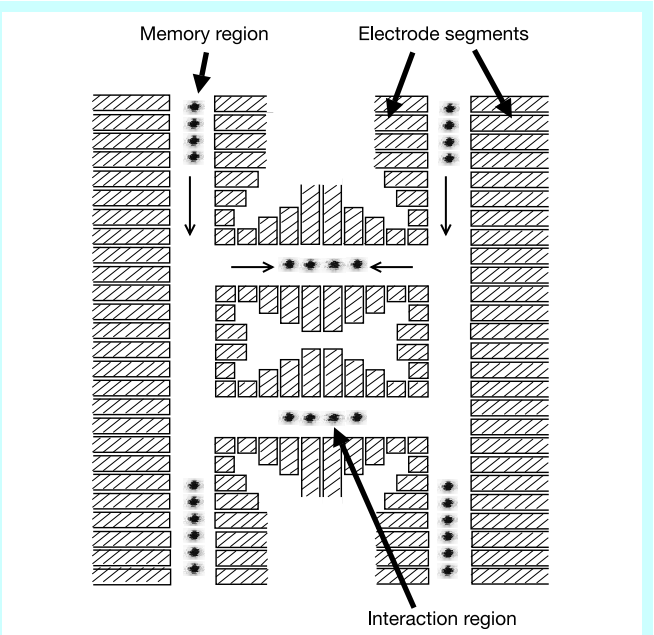


Figure 1 Diagram of the quantum charge-coupled device (QCCD). Ions are stored in the memory region and moved to the interaction region for logic operations. Thin arrows show transport and confinement along the local trap axis.

Electrode structures for the QCCD are relatively easy to fabricate. A number of ion traps have been built by laser-machining slits in alumina wafers and evaporating gold electrodes onto the alumina[23]. These traps have geometries similar to that needed for the QCCD, and have spacings between the static and r.f. electrodes of fractions of a millimetre, allowing confinement frequencies up to 20 MHz for r.f. field frequencies of ~250 MHz. Similar electrode structures are currently being constructed from heavily doped silicon using standard microfabrication techniques[24]. Here the silicon acts as the conductive electrode material, while glass spacers anodically bonded to the silicon insulate the r.f. electrodes from the static electrodes.

A first step towards a QCCD has been taken at the National Institute of Standards and Technology (NIST) by constructing a pair of interconnected ion traps; the individual traps are similar to those used in previous work[23] and are separated by 1.2 mm. Efficient coherent transport of a qubit between the two traps was demonstrated by performing a Ramsey-type experiment involving the two traps, where no loss of contrast within the experimental error (~0.6%) was observed[25]. Transport times were as short as ~50 μs, with corresponding ion velocities greater than 10 m s^{-1} (see also ref. 26). The transport did not cause any heating of the ion motion or shortening of ion lifetime in the trap.

To maximize the clock speed of the QCCD, we need to transport ions quickly. However, the entangling gate demonstrated in previous work at NIST[9,21] has low error only for ions cooled near the quantum ground state. To recool the ions after transport and to counteract the effects of heating[23], we propose to use sympathetic cooling of the ions used for quantum logic by another ion species[13,27,28]. Confining both species in the interaction region lets us use the cooling species as a heat sink, with the Coulomb interaction transferring energy between the two species, as experimentally demonstrated in refs 29–31.

Decoherence

Whereas the decoherence and gate errors in single-trap quantum registers have already been characterized, additional decoherence can occur during ion transport. For instance, the energy splitting of the qubit states of an ion depends on the magnetic field at the ion through the Zeeman effect. During ion transport, the spatial variations of the magnetic field strength along the transport path cause the qubit states to acquire a path-dependent relative phase α, so that, for example, $|\downarrow\rangle + |\uparrow\rangle \rightarrow |\downarrow\rangle + e^{i\alpha}|\uparrow\rangle$ over transport. If we do not know α, we have lost the phase information, effectively dephasing the quantum state. But knowing α for all relevant paths is tantamount to characterizing the magnetic field on micrometre length scales across the entire device, a very difficult task.

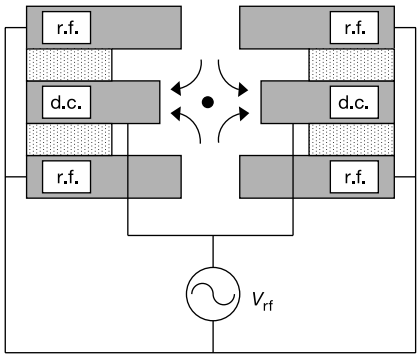


Figure 2 Configuration of radio-frequency (r.f.) and static (d.c.) electrodes for the QCCD. Dotted regions indicate insulating spacers. Applying high r.f. voltage to the two outer electrode layers while keeping the inner layer at r.f. ground creates the r.f. quadrupole field shown by the arrows. This field provides trapping potentials for confinement transverse to the local trap axis, which points perpendicular to the page and is located at the central black dot. View in Fig. 1 is from the top of this figure.

Retaining phase information during a computation also requires accurate positioning of the ions in the interaction regions. As the logic gate parameters depend on the phase of the driving laser fields at the ion positions, the ion positions and laser path lengths must be controllable with accuracies much better than an optical wavelength. Although this does not place unreasonable constraints on the accuracy of the voltage sources driving the QCCD electrodes, stray electric fields emanating from the electrodes or mechanical vibration of the QCCD can readily move the ions a fraction of a wavelength from their nominal positions, effectively adding a relative phase α of the type considered above.

Decoherence-free encoding

We can reduce these sources of decoherence by several orders of magnitude by encoding each qubit into a decoherence-free subspace (DFS) of two ions[32–34]. This DFS is spanned by the states $|0\rangle = |\downarrow\uparrow\rangle$, $|1\rangle = |\uparrow\downarrow\rangle$ of the ions. We refer to the ions as 'physical qubits' and call the effective two-level system formed by $|0\rangle$, $|1\rangle$ a 'logical qubit'. If the state $|\uparrow\rangle$ of ion j acquires a phase α_j over and above the predicted phase α_0 for the transport path, we see

$$|0\rangle + |1\rangle \rightarrow e^{i\alpha_1}|\downarrow\uparrow\rangle + e^{i\alpha_2}|\uparrow\downarrow\rangle = |0\rangle + e^{i\Delta\alpha}|1\rangle \quad (1)$$

where we write $\Delta\alpha \equiv \alpha_2 - \alpha_1$. If $\Delta\alpha = 0$, we see that the DFS logical qubit is unaffected by the acquired phase. Here the phases α_i are themselves unknown, but the ions acquire the same unknown phase, a process called collective dephasing. The logical qubit decoheres only insofar as the dephasing fails to be collective.

As an example, assume that the physical qubit energies have a linear dependence on magnetic field and that the field varies linearly over an extended QCCD device of size 10 cm. If each pair of physical qubits comprising a logical qubit is separated on average by 10 μm, a logical qubit dephases more slowly than a physical qubit by a factor of 10^4. Again, Stark shifts of the qubit levels can be induced by the electric fields that push the ions from place to place, but their dephasing effects on the logical qubits are also suppressed. In general, the effect of any external field varying over a length scale L_{ext} and inducing energy shifts of pth power in the field is suppressed by a factor $(L_{ext}/d)^p$ for DFS encoding. A DFS-encoded qubit is therefore robust against decoherence incurred during transport.

We can also perform universal quantum logic in the DFS, as we now show. If we hold two ions in an interaction region, we can use the entangling gate of refs 9 and 21 to apply the operator

$$U_2(\theta,\phi_1,\phi_2) = \cos\theta[I_1\otimes I_2] + i\sin\theta[X_{\phi_1}\otimes X_{\phi_2}]$$

$$= \cos\theta\, I^{DFS} + i\sin\theta\, X^{DFS}_{\Delta\phi_{12}} \quad (2)$$

$$X_\phi \equiv X\cos\phi + Y\sin\phi \quad (3)$$

where X, Y are the Pauli operators and the superscript 'DFS' indicates that the operator acts in the DFS logical basis. Though the individual phases ϕ_1, ϕ_2 depend sensitively on the path-length differences of the driving lasers over the macroscopic distance from the lasers to the ions[13], the DFS gate phase $\Delta\phi_{12} = \phi_1 - \phi_2$ depends only on the microscopic path length of the driving laser between the two ions, which can be readily controlled by small adjustments of the trap voltages[9,12,24]. The DFS encoding makes the computation insensitive to spatial phase fluctuations; as we will see, it protects against temporal phase fluctuations as well. We can set θ over a wide range of values[21,24], so the two-ion entangling gate lets us perform arbitrary rotations of a single logical qubit. Using the same entangling gate on four ions, we can obtain the operator

$$U_4 = \frac{1}{\sqrt{2}}[I_1\otimes I_2\otimes I_3\otimes I_4 - iX_{\phi_1}\otimes X_{\phi_2}\otimes X_{\phi_3}\otimes X_{\phi_4}] \quad (4)$$

$$= \frac{1}{\sqrt{2}}[I^{DFS}\otimes I^{DFS} - iX^{DFS}_{\Delta\phi_{12}}\otimes X^{DFS}_{\Delta\phi_{34}}] \quad (5)$$

where ions 1 and 2 encode one logical qubit and ions 3 and 4 encode another, and we write $\Delta\phi_{34} = \phi_3 - \phi_4$. This operator is equivalent to an XOR in the logical basis up to rotations of single logical qubits[35], so the operators of equations (2) and (5) suffice for universal quantum logic.

To use the DFS encoding in a large-scale quantum computation, we initialize the ions in pairs to the state $|\downarrow\uparrow\rangle$. Each pair of ions remains in the DFS through the quantum computation, so the logical qubits resist transport decoherence and all other types of collective dephasing. Read-out of the DFS qubit is straightforward, as we need only discriminate between $|\downarrow\uparrow\rangle$ and $|\uparrow\downarrow\rangle$. All the operators needed for universal quantum logic in the DFS have already been experimentally implemented[9,24], so we should be able to use the DFS encoding in a large-scale quantum computer. Notably, all logic gate operations can be accomplished by uniformly illuminating the ions in the interaction region, removing the need for tightly focused laser beams.

Logic gate synchronization

The DFS encoding also removes the requirement of clock synchronization between logic gates, a major but little-recognized obstacle to large-scale parallel quantum computation. As the energy levels of our physical qubits are non-degenerate, we must keep track of the resulting phase accumulation to preserve the quantum information in the physical qubit basis[34]. Parallel operations taking place in many interaction regions thus require clocks that remain synchronized over the whole computation time[36]. Synchronization can become very difficult for many qubits: for a transition frequency ω_0 between $|\downarrow\rangle$ and $|\uparrow\rangle$, the two components of the state $|\downarrow\rangle^N + |\uparrow\rangle^N$ acquire a significant relative phase in a time $\sim 1/(N\omega_0)$. To maintain phase stability of the computation, we therefore require a frequency reference with fractional frequency stability much better than $\lesssim 1/(N\omega_0\tau)$ at an averaging time τ equal to the duration of the quantum computation.

To be concrete, we consider trapped $^{40}Ca^+$ ions as qubits, with the ground $S_{1/2}$ state and metastable $D_{5/2}$ states as logic levels. This system is being investigated for quantum computation by a number of groups[7,15,37]. Here the transition frequency is 412 THz, comparable to the 533 THz operating frequency of the currently most stable laser oscillator[38], which has a fractional frequency instability of 3×10^{-16} as 1 s averaging time. If the computation takes about 1 s, equal to the lifetime of the metastable $D_{5/2}$ state, we see that current technology barely provides the appropriate phase stability for even one ion. Of course, this argument can be regarded as too simplistic because the requirements on phase stability can be reduced by invoking error correction[39]; however, this comes at the cost of increased overhead[18]. For qubit levels with a transition frequency in the microwave regime, local oscillators of the required phase stability exist, but the optical path lengths between the driving lasers and each of the interaction regions must be stable at the nanometre level over the course of the computation[13], a daunting task for a 10 cm QCCD device.

On the other hand, as the logic levels of a DFS-encoded qubit are degenerate, we do not need phase synchronization at all to perform a logic operation within the DFS. Operations in the DFS are also independent of the optical path lengths of the driving lasers, because the phases $\Delta\phi_{12}$, $\Delta\phi_{34}$ in equations (2) and (5) depend only on the distance between the two ions comprising a logical qubit. The universal gate-set constructed above allows us to perform highly parallel computations in the DFS without synchronization between gates separated in time or space. Similar considerations would apply to other quantum computing architectures. □

doi:10.1038/nature00784.

1. Shor, P. W. in *Proc. 35th Annu. Symp. on the Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society, Los Alamitos, 1994).
2. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79,** 325–328 (1997).
3. Cirac, J. I. & Zoller, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74,** 4091–4094 (1995).
4. DiVincenzo, D. P. in *Scalable Quantum Computers* (eds Braunstein, S. L. & Lo, H. K.) 1–14 (Wiley-VCH, Berlin, 2001).
5. Monroe, C. *et al.* Resolved-sideband Raman cooling of a bound atom to the 3D zero-point energy. *Phys. Rev. Lett.* **75,** 4011–4014 (1995).
6. King, B. E. *et al.* Cooling the collective motion of trapped ions to initialize a quantum register. *Phys. Rev. Lett.* **81,** 1525–1528 (1998).
7. Roos, C. *et al.* Quantum state engineering on an optical transition and decoherence in a Paul trap. *Phys. Rev. Lett.* **83,** 4713–4716 (1999).
8. Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. & Wineland, D. J. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.* **75,** 4714–4717 (1995).
9. Sackett, C. A. *et al.* Experimental entanglement of four particles. *Nature* **404,** 256–259 (2000).
10. Nägerl, H. C. *et al.* Laser addressing of individual ions in a linear ion trap. *Phys. Rev. A* **60,** 145–148 (1999).
11. Blatt, R. & Zoller, P. Quantum jumps in atomic systems. *Eur. J. Phys.* **9,** 250–256 (1988).
12. Rowe, M. A. *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409,** 791–794 (2001).
13. Wineland, D. J. *et al.* Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *J. Res. NIST* **103,** 259–328 (1998).
14. Hughes, R. J., James, D. F. V., Knill, E. H., Laflamme, R. & Petschek, A. G. Decoherence bounds on quantum computation with trapped ions. *Phys. Rev. Lett.* **77,** 3240–3243 (1996).
15. Enzer, D. G. *et al.* in *Experimental Implementation of Quantum Computation '01* (ed. Clark, R.) (Rinton, Princeton, 2001).
16. Pellizzari, T., Gardiner, S. A., Cirac, J. I. & Zoller, P. Decoherence, continuous observation, and quantum computing: A cavity QED model. *Phys. Rev. Lett.* **75,** 3788–3791 (1995).
17. DeVoe, R. G. Elliptical ion traps and trap arrays for quantum computation. *Phys. Rev. A* **58,** 910–914 (1998).
18. Steane, A. M. & Lucas, D. M. Quantum computing with trapped ions, atoms and light. *Fortsch. Phys.* **48,** 839–858 (2000).
19. Cirac, J. I. & Zoller, P. A scalable quantum computer with ions in an array of microtraps. *Nature* **404,** 579–581 (2000).
20. Steane, A. *et al.* Speed of ion-trap quantum-information processors. *Phys. Rev. A* **62,** 042305 (2000).
21. Sørensen, A. & Mølmer, K. Entanglement and quantum computation with ions in thermal motion. *Phys. Rev. A* **62,** 022311 (2000).
22. Paul, W. Electromagnetic traps for charged and neutral particles. *Rev. Mod. Phys.* **62,** 531–540 (1990).
23. Turchette, Q. A. *et al.* Heating of trapped ions from the quantum ground state. *Phys. Rev. A* **61,** 063418 (2000).
24. Kielpinski, D.. *Entanglement and Decoherence in a Trapped-ion Quantum Register.* Thesis, Univ. Colorado (2001); available at ⟨http://www.boulder.nist.gov/timefreq/ion/qucomp/papers.htm⟩.
25. Rowe, M. A. *et al.* Transport of quantum states and separation of ions in a dual RF ion trap. Preprint quant-ph/0205094 at ⟨http://xxx.lanl.gov⟩ (2002).
26. Guthöhrlein, G. R., Keller, M., Hayasaka, K., Lange, W. & Walther, H. A single ion as a nanoscopic probe of an optical field. *Nature* **414,** 49–51 (2001).
27. Kielpinski, D. *et al.* Sympathetic cooling of trapped ions for quantum logic. *Phys. Rev. A* **61,** 032310 (2000).
28. Morigi, G. & Walther, H. Two-species Coulomb chains for quantum information. *Eur. Phys. J. D* **13,** 261–269 (2001).
29. Larson, D. J., Bergquist, J. C., Bollinger, J. J., Itano, W. M. & Wineland, D. J. Sympathetic cooling of trapped ions: A laser-cooled two-species nonneutral ion plasma. *Phys. Rev. Lett.* **57,** 70–73 (1986).
30. Rohde, H. *et al.* Sympathetic ground-state cooling and coherent manipulation with two-ion crystals. *J. Opt. B* **3,** S34–S41 (2001).
31. Blinov, B. B. *et al.* Sympathetic cooling of trapped Cd^+ isotopes. Preprint quant-ph/0112084 at ⟨http://xxx.lanl.gov⟩ (2001).
32. Lidar, D. A., Chuang, I. L. & Whaley, K. B. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.* **81,** 2594–2597 (1998).
33. Duan, L. M. & Guo, G. C. Reducing decoherence in quantum-computer memory with all quantum bits coupling to the same environment. *Phys. Rev. A* **57,** 737–741 (1998).
34. Kielpinski, D. *et al.* A decoherence-free quantum memory using trapped ions. *Science* **291,** 1013–1015 (2001).
35. Sørensen, A. & Mølmer, K. Quantum computation with ions in thermal motion. *Phys. Rev. Lett.* **82,** 1971–1974 (1999).
36. van Enk, S. J. The physical meaning of phase and its importance for quantum teleportation. *J. Mod. Opt.* **48,** 2049–2054 (2001).
37. Steane, A. The ion-trap quantum information processor. *Appl. Phys. B* **64,** 623–643 (1997).
38. Young, B. C., Cruz, F. C., Itano, W. M. & Bergquist, J. C. Visible lasers with subhertz linewidths. *Phys. Rev. Lett.* **82,** 3799–3802 (1999).
39. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* 425–493 (Cambridge Univ. Press, Cambridge, 2000).

Acknowledgements

We acknowledge the experimental contributions of the NIST Ion Storage group, and also J. Beall for assistance with microfabrication. We thank D. Leibfried and M.A. Rowe for comments on the manuscript. D.K. and D.J.W. were supported by the US National Security Agency (NSA), Advanced Research and Development Activity (ARDA) and the Office of Naval Research. C.M. was supported by the US NSA, ARDA and the National Science Foundation ITR programme.

Correspondence and requests for materials should be addressed to D.K. (e-mail: utonium@mit.edu).

3. Duc, P.-A., Brinks, E., Wink, J. E. & Mirabel, I. F. Gas segregation in the interacting system Arp 105. *Astron. Astrophys.* **326,** 537–553 (1997).
4. Duc, P.-A. & Mirabel, I. G. Young tidal dwarf galaxies around the gas-rich disturbed lenticular NGC 5291. *Astron. Astrophys.* **333,** 813–826 (1998).
5. Brouillet, N., Henkel, C. & Baudry, A. Detection of an intergalactic molecular complex? *Astron. Astrophys.* **262,** L5–L8 (1992).
6. Walter, F. & Heithausen, A. The discovery of a molecular complex in the tidal arms near NGC 3077. *Astrophys. J.* **519,** L69–L72 (1999).
7. Smith, B. J. & Higdon, J. L. A search for CO(1–0) emission from the tidal structures of interacting and merging galaxies. *Astron. J.* **108,** 837–843 (1994).
8. Smith, B. J., Struck, C., Kenney, J. D. P. & Jogee, S. The molecule-rich tail of the peculiar galaxy NGC 2782 (Arp 215). *Astron. J.* **117,** 1237–1248 (1999).
9. Zwicky, F. Multiple galaxies. *Ergenisse Exakten Naturwissenschaften* **29,** 344–385 (1956).
10. Schweizer, F. in *Structure and Properties of Nearby Galaxies* (eds Berkhuijsen, E. M. & Wielebinski, R.) 279–284 (Riedel, Dordrecht, 1978).
11. Hibbard, J. E. & van Gorkom, J. H. HI, HII, and R-Band observations of a galactic merger sequence. *Astron. J.* **111,** 655–695 (1996).
12. Duc, P.-A. & Mirabel, I. F. in *Galaxy Interactions at Low and High Redshift* (eds Barnes, J. & Sanders, D.) 61–70 (IAU Symp. 186, Kluwer, Dordrecht, 1997).
13. Barnes, J. E. & Hernquist, L. Formation of dwarf galaxies in tidal tails. *Nature* **360,** 715–717 (1992).
14. Duc, P.-A. *et al.* The interacting system NGC 2992/3 (Arp 245). *Astron. J.* (submitted).
15. Taylor, C. L., Kobulnicky, H. A. & Skillman, E. D. CO emission in low-luminosity, HI-rich galaxies. *Astron. J.* **116,** 2746–2756 (1998).
16. Kennicutt, R. C. Jr Star formation in galaxies along the Hubble sequence. *Annu. Rev. Astron. Astrophys.* **36,** 189–232 (1998).
17. Guélin, M. *et al.* 1.3 mm emission in the disk of NGC 891: Evidence of cold dust. *Astron. Astrophys.* **279,** L37–L40 (1993).
18. Braine, J., Combes, F. & Van Driel, W. NGC 4414: A flocculent galaxy with a high gas surface density. *Astron. Astrophys.* **280,** 451–467 (1993).
19. Hollenbach, D. & MCKee, C. F. Molecule formation and infrared emission in fast interstellar shocks. III—results for J shocks in molecular clouds. *Astrophys. J.* **342,** 306–336 (1989).
20. Neininger, N., Guélin, M., Garcia-Burillo, S., Zylka, R. & Wielebinski, R. Cold dust and molecular line emission in NGC 4565. *Astron. Astrophys.* **310,** 725–736 (1996).
21. Dumke, M. *et al.* the interstellar medium in the edge-on galaxy NGC 5907. Cold dust and molecular line emission. *Astron. Astrohys.* **325,** 124–134 (1997).
22. Braine, J. *et al.* Gas and dust in the active spiral galaxy NGC 3079. *Astron. Astrophys.* **326,** 963–975 (1997).
23. Sage, L. J. The properties and origins of molecular gas in the lenticular galaxies NGC 404, 4710 and 5195. *Astron. Astrophys.* **239,** 125–136 (1990).
24. Arp, H. Atlas of peculiar galaxies. *Astrophys. J. Suppl. Ser.* **14,** 1–20 (1966).
25. Fritze-v.Alvensleben, U. & Duc, P.-A. in *The Magellanic Clouds and other Dwarf Galaxies* (eds Braun, J. M. & Richtler, T.) 141–145 (Proceedings of the Workshop of the Graduiertenkolleg Bonn-Bochum, Shaker, Aachen, 1998).

Correspondence and requests for materials should be addressed to J.B. (e-mail: Jonathan.Braine@observ.u-bordeaux.fr).

Geometric quantum computation using nuclear magnetic resonance

Jonathan A. Jones*†, Vlatko Vedral*, Artur Ekert* & Giuseppe Castagnoli‡

* *Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK*
† *Oxford Centre for Molecular Sciences, New Chemistry Laboratory, South Parks Road, Oxford OX1 3QT, UK*
‡ *Elsag, Via Puccini 2, 1615 Genova, Italy*

A significant development in computing has been the discovery[1] that the computational power of quantum computers exceeds that of Turing machines. Central to the experimental realization of quantum information processing is the construction of fault-tolerant quantum logic gates. Their operation requires conditional quantum dynamics, in which one sub-system undergoes a coherent evolution that depends on the quantum state of another sub-system[2]; in particular, the evolving sub-system may acquire a conditional phase shift. Although conventionally dynamic in origin, phase shifts can also be geometric[3,4]. Conditional geometric (or 'Berry') phases depend only on the geometry of the path executed, and are therefore resilient to certain types of errors; this suggests the possibility of an intrinsically fault-tolerant way of performing quantum gate operations. Nuclear magnetic resonance techniques have already been used to demonstrate both simple quantum information processing[5–9] and geometric phase shifts[10–12]. Here we combine these ideas by performing a nuclear magnetic resonance experiment in which a conditional Berry phase is implemented, demonstrating a controlled phase shift gate.

Any quantum computation can be built out of simple operations involving only one or two quantum bits (qubits)[13]. A particularly simple two-qubit gate in many experimental implementations, such as nuclear magnetic resonance (NMR)[14], is the controlled phase shift. This may be achieved using a conditional Berry phase, and thus quantum geometrical phases can form the basis of quantum computation. We will use spin half nuclei as an example to demonstrate the feasibility of this approach, but the basic idea is general. In our experiments the state of one spin determines the Berry phase acquired by the other spin.

Suppose that a spin half nucleus undergoes a conical evolution with cone angle θ. Then the Berry phase is simply $\gamma = \pm\frac{1}{2}\Omega = \pm\pi(1-\cos\theta)$ where the $\pm$ signs depend on whether the system is in the eigenstate aligned with or against the field, and Ω is the solid angle subtended by the conical circuit. We note that any deformation of the path of the spin which preserves this solid angle leaves the phase unchanged. Thus the phase is not affected by the speed with which the path is traversed; nor is it very sensitive to random fluctuations about the path.

Berry phases can be conveniently demonstrated in an NMR experiment[15] by working in a rotating frame. We consider an ensemble of spin half particles in a magnetic field, B_0, aligned along the z-axis; their precession frequency is then given by the Larmor frequency, ω_0. If the spins are irradiated by a circularly polarized radio-frequency field, B_1, at a frequency ω_{rf}, the total hamiltonian (neglecting relaxation) may be written in the rotating frame as $H = (\omega_0 - \omega_{rf})I_z + \omega_1 I_x$, where, following conventional NMR practice, the hamiltonian is described in product operator notation[16] and the field strengths are written in terms of their corresponding Larmor frequencies.

When $|\omega_1| \ll |\omega_0 - \omega_{rf}|$ the hamiltonian lies close to the z-axis, while when $|\omega_1| \gg |\omega_0 - \omega_{rf}|$, the hamiltonian lies close to the x-axis. If radio-frequency radiation is applied far from resonance, the system is effectively quantized along the z-axis, and if the radio frequency is swept towards resonance ($\omega_{rf} = \omega_0$), the effective hamiltonian rotates from the z-axis towards the x-axis. If the frequency sweep is applied adiabatically then the spin will follow the hamiltonian. Next, a circular motion can be imposed by adiabatically varying the phase of the radio frequency. When the hamiltonian returns to the x-axis the frequency sweep may be reversed, so that the spin returns to its original state, aligned along the z-axis. The Berry phase acquired in this cyclic process is $\pm\pi$. If the radio-frequency field is not swept all the way to resonance, but only to some final value ω_f, the hamiltonian ends at some angle to the z-axis, and so circuits with arbitrary cone angles can be implemented. A similar case occurs if the frequency sweep is replaced by an amplitude sweep, in which the radio frequency is always applied away from resonance, and its amplitude is raised smoothly from zero to some final value, ω_1.

This situation arises naturally in a system of two weakly coupled spins, I and S. For simplicity we consider a heteronuclear system, so that ω_I and ω_S are very different, and only one spin (say I) is close to resonance. The two transitions of I (corresponding to the two possible states of spin S) will be split by $\pm\pi J$, and so will have different resonance offsets. After an amplitude sweep the orientation of the effective hamiltonian depends on the resonance offset, and so θ (and hence the Berry phase acquired) will depend on the state of spin S. This permits a conditional Berry phase to be applied to spin I, where the size of the phase shift is controlled by spin S. If the radio frequency is applied at a frequency δ (measured in Hz)

away from the transition frequency of spin I when spin S (the control spin) is in state 0, and ν_1 is the maximum radio-frequency field strength (also in Hz), then the differential Berry phase shift

$$\Delta\gamma = \gamma_1 - \gamma_0 = \pm\pi\left[\frac{\delta + J}{\sqrt{(\delta + J)^2 + \nu_1^2}} - \frac{\delta}{\sqrt{\delta^2 + \nu_1^2}}\right]$$

depends only on δ, ν_1 and J; it is independent of how the process is carried out as long as it is slow enough to be adiabatic, but rapid compared with the decoherence times (T_1 and T_2).

In addition to the geometric phases, there will also be additional dynamic phases, which do depend on experimental details. In principle these could be calculated and corrected for, but this is not practical as a result of B_1 inhomogeneity. The radio-frequency field strength will vary over the sample, and so different nuclei will acquire different dynamic phases; averaging over the sample will result in extensive dephasing. This can be overcome using a conventional spin echo approach: the pulse sequence is applied twice, with the second application surrounded by a pair of 180° pulses applied to spin I. This has the effect of completely refocusing the dynamic phase, and thus refocusing any inhomogeneity in it. We note that this approach will only be successful if the dynamic phase terms are the same during the two halves of the spin echo, and thus it is important that any variation in these terms occurs on a timescale that is long compared with the echo time. In our experiments minor variations in the dynamic phase arising from the effects of molecular diffusion within the slightly inhomogeneous B_1 field are visible as a small loss in signal intensity. Similarly it is important to ensure that refocusing pulses are applied reliably, which is relatively simple within NMR. These issues must be considered when seeking to apply this approach with other experimental techniques.

This procedure would also cancel out the geometric phase, but this can be sidestepped by performing the radio-frequency phase sweep in the opposite direction, thus negating the geometric phase, so that the two geometric terms add together while the dynamic phases cancel out. Cancellation of dynamic phases arising from the natural evolution of spin S, could also be achieved by incorporating the sequence within another spin echo, involving 180° pulses applied to S. Similarly, in more complex spin systems, contributions to the geometric phase which depend on the states of other spins can be cancelled by the judicious application of further spin echoes. It might seem that this approach would require an exponentially large number of refocusing pulses, but this is not true, as nuclear spin–spin coupling is a local effect, so that couplings between distant nuclei can be safely neglected. It should also be possible to use efficient refocusing schemes[17] based on Hadamard matrices, thus allowing the number of refocusing pulses to be further reduced.

In order to measure the sizes of γ_0 and γ_1 it is convenient to apply the Berry phase shifts to a spin I in a coherent superposition of states, created by an initial 90° pulse. The pulse sequence (Fig. 1) then generates Berry phases that are determined by examining the final phases of the magnetization. As the two states of spin I acquire equal and opposite phases, and the pulse sequence contains two separate periods in which phase shifts are generated, the total phase change observed is 4γ, with a maximum value of 720°. A range of controlled Berry phases can be generated by choosing appropriate values of δ and ν_1 (J is fixed by the chemical system). For a given value of δ/J the controlled phase will rise and then fall as ν_1 is increased. This approach will be most robust when the desired $\Delta\gamma$ occurs at the maximum of this curve, as the dependence on the size of δ is then reduced to second order. For the particular case of a controlled π shift, the basis of the controlled-NOT gate[14], this occurs at $\delta = 1.058J$ and $\nu_1 = 2.112J$.

NMR experiments were performed at 25 °C using a homebuilt 500 MHz (^{1}H frequency) NMR spectrometer at the OCMS, with two power ranges for ^{1}H pulses. Hard pulses were applied using high power ($\nu_1 < 25.8$ kHz), while adiabatic sweeps were performed using low power ($\nu_1 < 774$ Hz). Radio-frequency amplitude and phase-calibration tables (available on most modern NMR spectrometers) permit the radio-frequency power level to be varied in a phase-coherent manner. The sample was prepared by dissolving 100 mg of 99% ^{13}C-labelled $CHCl_3$ in 0.2 ml of 99.96% $CDCl_3$, and placing this in a Shigemi microtube. The single ^{1}H nucleus was used as spin I, while the ^{13}C nucleus was used as spin S; for this system $J_{IS} = 209.2$ Hz. Spin–spin relaxation times (measured using Carr–Purcell–Meiboom–Gill sequences and averaging over the two components of each doublet) were 3.9 s for ^{1}H and 0.3 s for ^{13}C; the spin–lattice relaxation times (measured by inversion-recovery) were 7.6 s for ^{1}H and 25.3 s for ^{13}C. Experiments were performed with $\delta = 221.3$ Hz, and ν_1 was varied between zero and its maximum value. Amplitude and phase sweeps were implemented using 200 linear steps of 100 μs, giving a total pulse sequence length of about 120 ms. The phases of the two ^{1}H resonances were determined by fitting the free induction decay using home-written software. Reference phases were obtained as described in Fig. 1 (legend). The results are shown in Fig. 2; clearly the measured phases lie close to the theoretically predicted values. The controlled Berry phase rises smoothly to a broad maximum at 180°, and then slowly falls back towards zero. In order to investigate the effects of a breakdown in the adiabatic criterion, some measurements were repeated with faster sweeps. With a sweep step size of 50 μs (data not shown) the

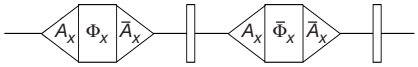


Figure 1 Pulse sequence used to demonstrate controlled Berry phases. Triangles indicate adiabatic radio-frequency amplitude sweeps, from 0 to ν_1 (A_x) or from ν_1 to 0 ($\bar{A}_x$); rectangles indicate slow rotations of the radio-frequency phase at constant amplitude. The phase rotation runs from 0° to 360° (Φ_x) or from 360° to 0° ($\bar{\Phi}_x$). Narrow rectangles correspond to hard $180°_y$ pulses. As the absolute phase of an NMR signal is undefined, it is essential to obtain a reference signal against which experimental phases can be measured. The simplest approach is to use the signal from a single 90° pulse, and a more subtle approach is to use this pulse sequence with the $\bar{\Phi}_x$ sequence replaced by Φ_x. In principle these should give the same result, but in practice minor differences are seen as a result of radio-frequency inhomogeneity and the effects of the long radio-frequency pulses on the NMR probe and pre-amplifier.

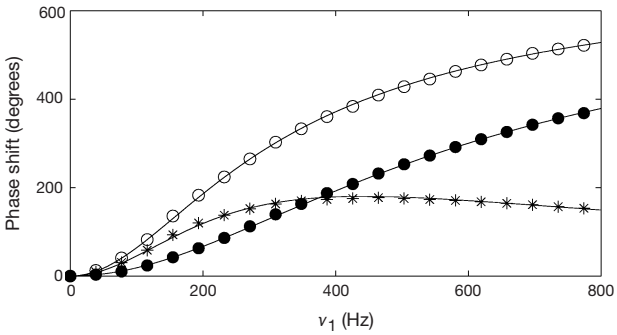


Figure 2 Experimental values for the Berry phases γ_0, γ_1, and the controlled Berry phase difference, $\Delta\gamma$, as a function of the maximum radio-frequency field strength ν_1. Experimental points are shown by filled circles (γ_0), empty circles (γ_1) and stars ($\Delta\gamma$); theoretical values are shown as smooth curves. Variability in the experimental points (estimated by repetition) was about ±2°; in a few cases the deviation of the measured data points from their theoretical values was greater than this, indicating the existence of as yet unidentified systematic errors. The signal strength observed after a phase gate was about 90% of that observed without a phase gate. This signal loss of about 10% is too great to arise simply from relaxation; more detailed experiments (data not shown) suggest that the main source of signal loss is the effect of diffusion. When considering the overall fidelity of the gate it is also necessary to include effects arising from spin S; these are dominated by the relatively rapid spin–spin (T_2) relaxation of the ^{13}C nucleus.

results were similar to, but not quite as good as, those obtained with the slower sweep. Below 50 μs the loss of adiabaticity is severe and major distortions are observed. The step size should not be increased too far beyond the adiabatic threshold, as this will increase the effects of decoherence.

The conditional Berry phase gate demonstrated here depends only on the geometry of the path, and is completely independent of how the motion is performed as long as it is adiabatic; hence this kind of computation may be called geometric quantum computation. While this approach has no particular advantage over more conventional methods in NMR quantum computation, the basis idea is general, and could be applied in other implementations. Some of the methods described here have been partly covered in previous theory papers (such as refs 18 and 19), but there have been no previous experimental demonstrations. This new approach to quantum gates may become important, as it is naturally resilient to certain types of errors. In particular, suppose that the qubit, in addition to the circular motion which implements the geometric phase, also undergoes a random motion about its path due to some unwanted interaction with the environment. Such noisy motion leaves the total area approximately unchanged (although it changes details of the path), and so will not be reflected in the final Berry phase. Geometric phases thus offer the potential of performing quantum computations in a manner which is naturally tolerant of some types of fault. Further generalizations to non-abelian Berry phases, if implemented, may open entirely new possibilities for robust quantum information processing[20,21]. □

Received 22 July; accepted 14 December 1999.

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41,** 303–332 (1999).
2. Barenco, A., Deutsch, D., Ekert, A. & Jozsa, R. Conditional quantum dynamics and logic gates. *Phys. Rev. Lett.* **74,** 4083–4086 (1995).
3. Berry, M. V. Quantal phase factors accompanying adiabatic changes. *Proc. R. Soc. Lond. A* **392,** 45–57 (1984).
4. Shapere, A. & Wilczek, F. *Geometric Phases in Physics* (World Scientific, Singapore, 1989).
5. Cory, D. G., Fahmy, A. F. & Havel, T. F. Ensemble quantum computing by NMR spectroscopy. *Proc. Natl Acad. Sci. USA* **94,** 1634–1639 (1997).
6. Gershenfeld, N. A. & Chuang, I. L. Bulk spin-resonance quantum computation. *Science* **275,** 350–356 (1997).
7. Jones, J. A. & Mosca, M. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *J. Chem. Phys.* **109,** 1648–1653 (1998).
8. Chuang, I. L., Gershenfeld, N. & Kubinec, M. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.* **80,** 3408–3411 (1998).
9. Cory, D. G., Price, M. D. & Havel, T. F. Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing. *Physica D* **120,** 82–101 (1998).
10. Suter, D., Chingas, G., Harris, R. & Pines, A. Berry's phase in magnetic resonance. *Mol. Phys.* **61,** 1327–1340 (1987).
11. Goldman, M., Fleury, V. & Guéron, M. NMR frequency shift under sample spinning. *J. Magn. Reson. A* **118,** 11–20 (1996).
12. Jones, J. A. & Pines, A. Geometric dephasing in zero-field magnetic resonance. *J. Chem. Phys.* **106,** 3007–3016 (1997).
13. Deutsch, D., Barenco, A. & Ekert, A. Universality in quantum computation. *Proc. R. Soc. Lond. A* **449,** 669–677 (1995).
14. Jones, J. A., Hansen, R. H. & Mosca, M. Quantum logic gates and nuclear magnetic resonance pulse sequences. *J. Magn. Reson.* **135,** 353–360 (1998).
15. Ernst, R. R., Bodenhausen, G. & Wokaun, A. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon, Oxford, 1987).
16. Sørensen, O. W., Eich, G. W., Levitt, M. H., Bodenhausen, G. & Ernst, R. R. Product operator-formalism for the description of NMR pulse experiments. *Prog. Nucl. Magn. Reson. Spectrosc.* **16,** 163–192 (1983).
17. Jones, J. A. & Knill, E. Efficient refocussing of one spin and two spin interactions for NMR quantum computation. *J. Magn. Reson.* **141,** 322–325 (1999).
18. Pellizzari, T., Gardiner, S. A., Cirac, J. I. & Zoller, P. Decoherence, continuous observation, and quantum computing: a cavity QED model. *Phys. Rev. Lett.* **75,** 3788–3791 (1995).
19. Averin, D. V. Adiabatic quantum computation with Cooper pairs. *Solid State Commun.* **105,** 659–664 (1998).
20. Kitaev, A. Y. Fault tolerant quantum computation with anyons. Preprint http://arxiv.org/quant-ph/9707021.
21. Preskill, J. Fault tolerant quantum computation. Preprint http://arxiv.org/quant-ph/9712048.

Acknowledgements

We thank N. Soffe for helpful discussions. J.A.J. and A.E. thank the Royal Society of London and Starlab (Riverland NV) for financial support.

Correspondence and requests for materials should be addressed to J.A.J. (e-mail: jonathan.jones@qubit.org).

Reduction in the surface energy of liquid interfaces at short length scales

C. Fradin*, A. Braslau*, D. Luzet*, D. Smilgies†, M. Alba*, N. Boudet†, K. Mecke‡ & J. Daillant*§

** Service de Physique de l'Etat Condensé, CEA Saclay, F-91191 Gif-sur-Yvette Cedex, France*

† European Synchrotron Radiation Facility, BP 220, F-38043 Grenoble Cedex, France

‡ Theoretische Physik, Bergische Universität Wuppertal, D-42097 Wuppertal, Germany

§ LURE, Centre Universitaire Paris-sud, bâtiment 209D, PB 34, F-91898 Orsay Cedex, France

Liquid–vapour interfaces, particularly those involving water, are common in both natural and artificial environments. They were first described as regions of continuous variation of density[1], caused by density fluctuations within the bulk phases[2–4]. In contrast, the more recent capillary-wave model[5,6] assumes a step-like local density profile across the liquid–vapour interface, whose width is the result of the propagation of thermally excited capillary waves. The model has been validated for length scales of tenths of micrometres and larger[7,8], but the structure of liquid surfaces on submicrometre length scales—where the capillary theory is expected to break down—remains poorly understood. Here we report grazing-incidence X-ray scattering experiments that allow for a complete determination of the free surface structure and surface energy for water and a range of organic liquids. We observe a large decrease of up to 75% in the surface energy of submicrometre waves that cannot be explained by capillary theory, but is in accord with the effects arising from the non-locality of attractive intermolecule interactions as predicted by a recent density functional theory[9]. Our data, and the results of comparable measurements on liquid solutions, metallic alloys, surfactants, lipids and wetting films should thus provide a stringent test for any new theories that attempt to describe the structure of liquid interfaces with nanometre-scale resolution.

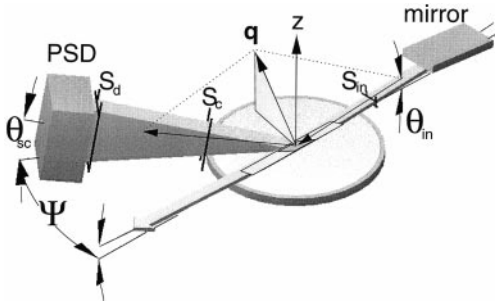


Figure 1 Schematic view of the experiment. The Teflon trough (inner diameter is 330 mm) is mounted on an active antivibration system under a helium atmosphere saturated with the vapour of the liquid under study. The monochromatic incident beam is first extracted from the polychromatic beam of the undulator source using a two-crystal diamond (111) monochromator. Higher harmonic light is eliminated using two platinum-coated glass mirrors, also used to fix the grazing angle of incidence θ_{in}. The incident and scattered beams travel through vacuum paths and the scattered signal is collected in a vertically mounted position sensitive detector (PSD). The size of the incident beam is fixed by a 265 μm × 250 μm slit, S_{in}. The horizontal resolution of the experiment is fixed by the slits S_c, 380 μm in width and S_d, 545 μm in width, placed at 213 mm and 844 mm from the sample respectively, as well as by the illuminated area seen by the detector (dark grey parallelogram in centre of circle). The scattered beam is defined by the angles Ψ and θ_{sc}. **q** is the wavevector transfer.

A One-Way Quantum Computer

Article *in* Physical Review Letters · June 2001

DOI: 10.1103/PhysRevLett.86.5188 · Source: PubMed

2 authors, including:

Robert Raussendorf
University of British Columbia - Vancouver
75 PUBLICATIONS **8,420** CITATIONS

SEE PROFILE

A One-Way Quantum Computer

Robert Raussendorf and Hans J. Briegel
Theoretische Physik, Ludwig-Maximilians-Universität München, Germany
(Received 25 October 2000)

We present a scheme of quantum computation that consists entirely of one-qubit measurements on a particular class of entangled states, the cluster states. The measurements are used to imprint a quantum logic circuit on the state, thereby destroying its entanglement at the same time. Cluster states are thus one-way quantum computers and the measurements form the program.

DOI: 10.1103/PhysRevLett.86.5188 PACS numbers: 03.67.Lx, 03.65.Ud

A quantum computer promises efficient processing of certain computational tasks that are intractable with classical computer technology [1]. While basic principles of a quantum computer have been demonstrated in the laboratory [2], scalability of these systems to a large number of qubits [3], essential for practical applications such as the Shor algorithm, represents a formidable challenge. Most of the current experiments are designed to implement sequences of highly controlled interactions between selected particles (qubits), thereby following models of a quantum computer as a (sequential) network of quantum logic gates [4,5].

Here we propose a different model of a scalable quantum computer. In our model, the entire resource for the quantum computation is provided initially in the form of a specific entangled state (a so-called cluster state [6]) of a large number of qubits. Information is then written onto the cluster, processed, and read out from the cluster by one-particle measurements only. The entangled state of the cluster thereby serves as a universal "substrate" for any quantum computation. Cluster states can be created efficiently in any system with a quantum Ising-type interaction (at very low temperatures) between two-state particles in a lattice configuration.

We consider two- and three-dimensional arrays of qubits that interact via an Ising-type next-neighbor interaction [6] described by a Hamiltonian $H_{\mathrm{int}} = g(t) \times \sum_{\langle a,a'\rangle} \frac{1+\sigma_z^{(a)}}{2} \frac{1-\sigma_z^{(a')}}{2} \cong -\frac{1}{4} g(t) \sum_{\langle a,a'\rangle} \sigma_z^{(a)} \sigma_z^{(a')}$ [7] whose strength $g(t)$ can be controlled externally. A possible realization of such a system is discussed below. A qubit at site a can be in two states $|0\rangle_a \equiv |0\rangle_{z,a}$ or $|1\rangle_a \equiv |1\rangle_{z,a}$, the eigenstates of the Pauli phase flip operator $\sigma_z^{(a)}$ $[\sigma_z^{(a)}|i\rangle_a = (-1)^i |i\rangle_a]$. These two states form the computational basis. Each qubit can equally be in an arbitrary superposition state $\alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. For our purpose, we initially prepare all qubits in the superposition $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, an eigenstate of the Pauli spin flip operator σ_x $[\sigma_x|\pm\rangle = \pm|\pm\rangle]$. H_{int} is then switched on for an appropriately chosen finite time interval T, where $\int_0^T dt\, g(t) = \pi$, by which a unitary transformation S is realized. Since H_{int} acts uniformly on the lattice, entire clusters of neighboring particles become entangled in one single step. The quantum state $|\Phi\rangle_C$, the state of a cluster (C) of neighboring qubits, which is thereby created provides in advance all entanglement that is involved in the subsequent quantum computation. It has been shown [6] that the cluster state $|\Phi\rangle_C$ is characterized by a set of eigenvalue equations

$$\sigma_x^{(a)} \bigotimes_{a' \in ngbh(a)} \sigma_z^{(a')} |\Phi\rangle_C = \pm |\Phi\rangle_C \,, \qquad (1)$$

where $ngbh(a)$ specifies the sites of all qubits that interact with the qubit at site $a \in C$. The eigenvalues are determined by the distribution of the qubits on the lattice. The equations (1) are central for the proposed computation scheme. As an example, a measurement on an individual qubit of a cluster has a random outcome. On the other hand, Eqs. (1) imply that any two qubits at sites $a, a' \in C$ can be projected into a Bell state by measuring a subset of the other qubits in the cluster. This property will be used to define quantum channels that allow us to propagate quantum information through a cluster.

We show that a cluster state $|\Phi\rangle_C$ can be used as a substrate on which any quantum circuit can be imprinted by one-qubit measurements. In Fig. 1 this scheme is illustrated. For simplicity, we assume that in a certain region of the lattice each site is occupied by a qubit. This requirement is not essential as will be explained below [see (d)]. In the first step of the computation, a subset of qubits is measured in the basis of σ_z which effectively removes them. In Fig. 1 these qubits are denoted by " ⊙."

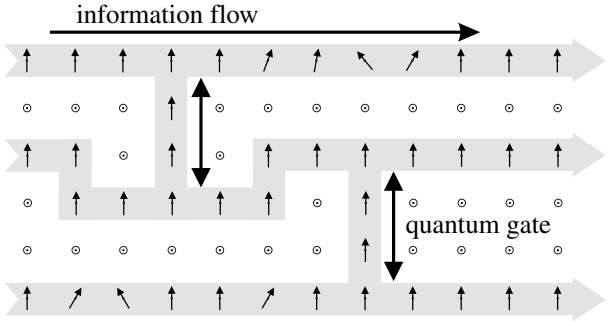


FIG. 1. Quantum computation by measuring two-state particles on a lattice. Before the measurements the qubits are in the cluster state $|\Phi\rangle_C$ of (1). Circles ⊙ symbolize measurements of σ_z, vertical arrows are measurements of σ_x, while tilted arrows refer to measurements in the x-y plane.

 0031-9007/01/86(22)/5188(4)$15.00

The state $|\Phi\rangle_C$ is thereby projected into a tensor product $|\mu\rangle_{C\setminus\mathcal{N}} \otimes |\tilde{\Phi}\rangle_{\mathcal{N}}$ consisting of the state $|\mu\rangle_{C\setminus\mathcal{N}}$ of all measured particles (subset $C\setminus\mathcal{N}$) on one side and an entangled state $|\tilde{\Phi}\rangle_{\mathcal{N}}$ of yet unmeasured particles (subset $\mathcal{N} \subset C$), on the other side. These unmeasured particles define a "network" $\mathcal{N}$ corresponding to the shaded structure in Fig. 1. The state $|\tilde{\Phi}\rangle_{\mathcal{N}}$ of the network is related to a cluster state $|\Phi\rangle_{\mathcal{N}}$ on $\mathcal{N}$ by a local unitary transformation which depends on the set of measurement results μ. More specifically, $|\tilde{\Phi}\rangle_{\mathcal{N}}$ satisfies Eqs. (1)—with C replaced by the subcluster $\mathcal{N}$—except for a possible difference in the sign factors, which are determined by the measurement results μ.

To process quantum information with this network, it suffices to measure its particles in a certain order and in a certain basis. Quantum information is thereby propagated horizontally through the cluster by measuring the qubits on the wire while qubits on vertical connections are used to realize two-bit quantum gates. The basis in which a certain qubit is measured depends in general on the results of preceding measurements. The processing is finished once all qubits except the last one on each wire have been measured. At this point, the results of previous measurements determine in which basis these "output" qubits need to be measured for the final readout. We note that, in the entire process, only one-qubit measurements are required. The amount of entanglement therefore decreases with every measurement [8] and all entanglement involved in the process is provided by the initial resource, the cluster state. This is different from the scheme of Ref. [11], which uses Bell measurements (capable of producing entanglement) to realize quantum gates.

In the following, we show that any quantum logic circuit can be implemented on a cluster state. The purpose of this is twofold. First, it serves as an illustration of how to implement a particular quantum circuit in practice. Second, in showing that any quantum circuit can be implemented on a sufficiently large cluster we demonstrate the universality of the proposed scheme. For pedagogical reasons we first explain a scheme with one essential modification with respect to the proposed scheme: before the entanglement operation S, certain qubits are selected as input qubits and the input information is written onto them, while the remaining qubits are prepared in $|+\rangle$. This step weakens the scheme since it affects the character of the cluster state as a genuine resource. It can, however, be avoided [see (e)]. Points (a) to (c) are concerned with the basic elements of a quantum circuit, quantum gates, and wires, point (d) with the composition of gates to circuits.

(a) Information propagation in a wire for qubits. A qubit can be teleported from one site of a cluster to any other site. In particular, consider a chain of an odd number of qubits 1 to n prepared in the state $|\psi_{\text{in}}\rangle_1 \otimes |+\rangle_2 \otimes \cdots \otimes |+\rangle_n$ and subsequently entangled by S. The state that was originally encoded in qubit 1, $|\psi_{\text{in}}\rangle$, is now delocalized and can be transferred to site n by performing σ_x measurements (basis $\{|+\rangle_j = |0\rangle_{x,j}, |-\rangle_j = |1\rangle_{x,j}\}$) at qubit sites $j = 1, \ldots, n-1$ with measurement outcomes $s_j \in \{0, 1\}$. The resulting state is $|s_1\rangle_{x,1} \otimes \cdots \otimes |s_{n-1}\rangle_{x,n-1} \otimes |\psi_{\text{out}}\rangle_n$. The output state $|\psi_{\text{out}}\rangle$ is related to the input state $|\psi_{\text{in}}\rangle$ by a unitary transformation $U_\Sigma \in \{1, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$ which depends on the outcomes of the σ_x measurements at sites 1 to $n-1$. A similar argument can be given for an even number of qubits. The effect of U_Σ can be accounted for at the end of a computation as shown below [see (d)]. It is noteworthy that not all classical information gained by the σ_x measurements needs to be stored to identify the transformation U_Σ. Instead, U_Σ is determined by the values of only two classical bits which are updated with every measurement.

(b) An arbitrary rotation $U_R \in \text{SU}(2)$ can be achieved in a chain of five qubits. Consider a rotation in its Euler representation $U_R(\xi, \eta, \zeta) = U_x(\zeta)U_z(\eta)U_x(\xi)$, where $U_x(\alpha) = \exp(-i\alpha\frac{\sigma_x}{2}), U_z(\alpha) = \exp(-i\alpha\frac{\sigma_z}{2})$. Initially, the first qubit is in some state $|\psi_{\text{in}}\rangle$, which is to be rotated, and the other qubits are in $|+\rangle$; i.e., their common state reads $|\Psi\rangle_{1,\ldots,5} = |\psi_{\text{in}}\rangle_1 \otimes |+\rangle_2 \otimes |+\rangle_3 \otimes |+\rangle_4 \otimes |+\rangle_5$. After the five qubits are entangled by S they are in the state $S|\Psi\rangle_{1,\ldots,5} = 1/2|\psi_{\text{in}}\rangle_1|0\rangle_2|-\rangle_3|0\rangle_4|-\rangle_5 - 1/2|\psi_{\text{in}}\rangle_1|0\rangle_2|+\rangle_3|1\rangle_4|+\rangle_5 - 1/2|\psi^*_{\text{in}}\rangle_1|1\rangle_2|+\rangle_3|0\rangle_4|-\rangle_5 + 1/2|\psi^*_{\text{in}}\rangle_1|1\rangle_2|-\rangle_3|1\rangle_4|+\rangle_5$, where $|\psi^*_{\text{in}}\rangle = \sigma_z|\psi_{\text{in}}\rangle$. Now, the state $|\psi_{\text{in}}\rangle$ can be rotated by measuring qubits 1 to 4, while it is teleported to site 5 at the same time. The qubits $1, \ldots, 4$ are measured in appropriately chosen bases $\mathcal{B}_j(\alpha_j) = \{\frac{|0\rangle_j + e^{i\alpha_j}|1\rangle_j}{\sqrt{2}}, \frac{|0\rangle_j - e^{i\alpha_j}|1\rangle_j}{\sqrt{2}}\}$ whereby the measurement outcomes $s_j \in \{0, 1\}$ for $j = 1, \ldots, 4$ are obtained. Here, $s_j = 0$ means that qubit j is projected into the first state of $\mathcal{B}_j(\alpha_j)$. The resulting state is $|s_1\rangle_{\alpha_1,1} \otimes |s_2\rangle_{\alpha_2,2} \otimes |s_3\rangle_{\alpha_3,3} \otimes |s_4\rangle_{\alpha_4,4} \otimes |\psi_{\text{out}}\rangle_5$ with $|\psi_{\text{out}}\rangle = U|\psi_{\text{in}}\rangle$. For the choice $\alpha_1 = 0$ (measuring σ_x of qubit 1) the rotation U has the form $U = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}U_R[(-1)^{s_1+1}\alpha_2, (-1)^{s_2}\alpha_3, (-1)^{s_1+s_3}\alpha_4]$. In summary, the procedure to implement an arbitrary rotation $U_R(\xi, \eta, \zeta)$, specified by its Euler angles ξ, η, ζ is (i) measure qubit 1 in $\mathcal{B}_1(0)$; (ii) measure qubit 2 in $\mathcal{B}_2((-1)^{s_1+1}\xi)$; (iii) measure qubit 3 in $\mathcal{B}_3((-1)^{s_2}\eta)$; (iv) measure qubit 4 in $\mathcal{B}_4((-1)^{s_1+s_3}\zeta)$. In this way the rotation U'_R is realized: $U'_R(\xi, \eta, \zeta) = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}U_R(\xi, \eta, \zeta)$. The extra rotation $U_\Sigma = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}$ can be accounted for at the end of the computation, as is described below in (d).

(c) To perform the gate $\text{CNOT}(c, t_{\text{in}} \to t_{\text{out}}) = |0\rangle_{cc}\langle 0| \otimes 1^{(t_{\text{in}}\to t_{\text{out}})} + |1\rangle_{cc}\langle 1| \otimes \sigma_x^{(t_{\text{in}}\to t_{\text{out}})}$ between a control qubit c and a target qubit t, four qubits, arranged as depicted Fig. 2a, are required. During the action of the gate, the target qubit t is transferred from t_{in} to t_{out}. The following procedure has to be implemented. Let qubit 4 be the control qubit. First, the state $|i_1\rangle_{z,1} \otimes |i_4\rangle_{z,4} \otimes |+\rangle_2 \otimes |+\rangle_3$ is prepared and then the entanglement operation S is performed. Second, σ_x of qubits 1 and 2 is measured. The measurement results

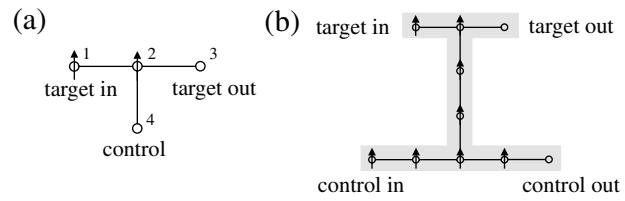


FIG. 2. Realization of a CNOT gate by one-particle measurements. See text.

$s_j \in \{0, 1\}$ correspond to projections of the qubits j into $|s_j\rangle_{x,j}$, $j = 1, 2$. The quantum state created by this procedure is $|s_1\rangle_{x,1} \otimes |s_2\rangle_{x,2} \otimes U_{\Sigma}^{(34)} |i_4\rangle_{z,4} \otimes |i_1 + i_4 \bmod 2\rangle_{z,3}$, where $U_{\Sigma}^{(34)} = \sigma_z^{(3)^{s_1+1}} \sigma_x^{(3)^{s_2}} \sigma_z^{(4)^{s_1}}$. The input state is thus acted upon by the CNOT and successive σ_x and σ_z rotations $U_{\Sigma}^{(34)}$, depending on the measurement results s_1, s_2. These unwanted extra rotations can again be accounted for as described in (d). For practical purposes it is more convenient if the control qubit is, as the target qubit, transferred to another site during the action of the gate. When a CNOT is combined with other gates to form a quantum circuit it will be used in the form shown in Fig. 2b.

To explain the working principle of the CNOT gate we, for simplicity, refer to the minimal implementation with four qubits. The minimal CNOT can be viewed as a wire from qubit 1 to qubit 3 with an additional qubit, No. 4, attached. From the eigenvalue equations (1) it can now be derived that, if qubit 4 is in an eigenstate $|i_4\rangle_{z,4}$ of σ_z, then the value of $i_4 \in \{0, 1\}$ determines whether a unit wire or a spin flip σ_x (modulo the same correction $U_{\Sigma}^{(3)}$ for both values of i_4) is being implemented. In other words, once σ_x of qubits 1 and 2 have been measured, the value i_4 of qubit 4 controls whether the target qubit is flipped or not.

(d) Quantum circuits. The gates described—the CNOT and arbitrary one-qubit rotations—form a universal set [5]. In the implementation of a quantum circuit on a cluster state the site of every output qubit of a gate overlaps with the site of an input qubit of a subsequent gate. Because of this, the entire entanglement operation can be performed at the beginning. To see this, compare the following two strategies. Given a quantum circuit implemented on a network $\mathcal{N}$ of qubits which is divided into two consecutive circuits, circuit 1 is implemented on network $\mathcal{N}_1$ and circuit 2 is implemented on network $\mathcal{N}_2$, and $\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2$. There is an overlap $\mathcal{O} = \mathcal{N}_1 \cap \mathcal{N}_2$ which contains the sites of the output qubits of circuit 1 (these are identical to the sites of the input qubits of circuit 2). The sites of the readout qubits form a set $\mathcal{R} \subset \mathcal{N}_2$. Strategy (i) consists of the following steps: (1) write input and entangle all qubits on $\mathcal{N}$; (2) measure qubits $\in \mathcal{N} \backslash \mathcal{R}$ to implement the circuit. Strategy (ii) consists of (1) write input and entangle the qubits on $\mathcal{N}_1$, (2) measure the qubits in $\mathcal{N}_1 \backslash \mathcal{O}$. This implements the circuit on $\mathcal{N}_1$ and writes the intermediate output to $\mathcal{O}$; (3) entangle the qubits on $\mathcal{N}_2$; (4) measure all qubits in $\mathcal{N}_2 \backslash \mathcal{R}$. Steps 3 and 4 implement the circuit 2 on $\mathcal{N}_2$. The measurements on $\mathcal{N}_1 \backslash \mathcal{O}$ commute with the entanglement operation restricted to $\mathcal{N}_2$, since they act on different subsets of particles. Therefore the two strategies are mathematically equivalent and yield the same results. It is therefore consistent to entangle in a single step at the beginning and perform all measurements afterwards.

Two further points should be addressed in connection with circuits. First, the randomness of the measurement results does not jeopardize the function of the circuit. Depending on the measurement results, extra rotations σ_x and σ_z act on the output qubit of every implemented gate. By use of the relations $U_R(\xi, \eta, \zeta) \sigma_z^s \sigma_x^{s'} = \sigma_z^s \sigma_x^{s'} U_R((-1)^s \xi, (-1)^{s'} \eta, (-1)^s \zeta)$, and $\mathrm{CNOT}(c, t) \sigma_z^{(t)^{s_t}} \sigma_z^{(c)^{s_c}} \sigma_x^{(t)^{s'_t}} \sigma_x^{(c)^{s'_c}} = \sigma_z^{(t)^{s_t}} \sigma_z^{(c)^{s_c + s_t}} \sigma_x^{(t)^{s'_c + s'_t}} \sigma_x^{(c)^{s'_c}} \mathrm{CNOT}(c, t)$, these extra rotations can be pulled through the network to act upon the output state. There they can be accounted for by adjusting the measurement basis for the final readout. The above relations imply that for a rotation $U_R(\xi, \eta, \zeta)$—different from the CNOT gate—the accumulated extra rotations U_Σ at the input side of U_R need to be determined before the measurement bases that realize U_R can be specified. This introduces a partial temporal ordering of the measurements on the whole cluster. Second, quantum circuits can also be implemented on irregular clusters. In that case, qubits may be missing which are required for the standard implementation of the circuit. This can be compensated by a large flexibility in shape of the gates and wires. The components can be bent and stretched to fit to the cluster structure as long as the topology of the circuit implementation does not change. Irregular clusters are found in lattices with a finite site occupation probability $0 < p < 1$. In such a situation, the possibility of *universal* quantum computation is closely linked to the phenomenon of percolation. For p above a certain critical value p_c, which depends on the dimension of the lattice, an infinitely extended cluster exists that may be used as the carrier of the quantum circuit. In two dimensions, for example, exactly one such cluster C exists. Suppose this cluster is divided into two subclusters C_1 and C_2 by a one-dimensional cut $\mathcal{O} = C_1 \cap C_2$. It can be shown, e.g., by using Russo's formula [12] from percolation theory that, for any cut $\mathcal{O}$, $|\mathcal{O}| = \infty$. Therefore there is no upper bound, in principle, to the "capacity" of the cluster, i.e., to the number of qubits that can be processed across such a cut.

(e) Full scheme. It is important to note that the step of writing the input information onto the qubits before the cluster is entangled was introduced only for pedagogical reasons. For illustration of this point consider a chain of five qubits in the state $S|+\rangle_1 \otimes |+\rangle_2 \otimes \cdots \otimes |+\rangle_5$. Clearly, there is no local information on any of the qubits. However, by measuring qubits 1 to 4 along suitable directions, qubit 5 can be projected into any desired state (modulo U_Σ). What is used here is the knowledge that the

resource has been prepared with qubit 1 in the state $|+\rangle_1$ before the entanglement operation. By the four measurements, this qubit is then rotated as described in (b). In order to use qubit 5 for further processing, the five-qubit chain considered here should, of course, be part of a larger cluster such that particle 5 is still entangled with the remaining network, after particles 1 to 4 have been measured. The method of preparing the input state remains the same, in this case, as explained in (d). In a similar manner any desired input state can be prepared if the rotations are replaced by a circuit preceding the proper circuit for computation. In summary, no input information needs to be written to the qubits before they are entangled. Cluster states are thus a genuine resource for quantum computation via measurements only.

For a cluster of a given *finite* size, the number of computational steps may be too large to fit on the cluster. In this case, the computation can be split into consecutive parts, for each of which there is sufficient space on the cluster. The modified procedure consists then of repeatedly (re)entangling the cluster and imprinting the actual part of the circuit—by measuring all of the lattice qubits except the ones carrying the intermediate quantum output—until the whole calculation is performed. This procedure has also the virtue that qubits involved in the later part of a calculation need not be protected from decoherence for a long time while the calculation is still being performed at a remote place of the cluster. Standard error-correction techniques [13,14] may then be used on each part of the circuit to stabilize the computation against decoherence.

A possible implementation of such a quantum computer uses neutral atoms stored in periodic micropotentials [15–18] where Ising-type interactions can be realized by controlled collisions between atoms in neighboring potential wells [16,18]. This system combines small decoherence rates with a high scalability. The question of scalability is linked to the percolation phenomenon, as mentioned earlier. For a site occupation probability above the percolation threshold, there exists a cluster which is bounded in size only by the trap dimensions. For optical lattices in three dimensions, single-atom site occupation with a filling factor of 0.44 has been reported [19] which is significantly above the percolation threshold of 0.31 [20]. As in other proposed implementations for quantum computing, the addressability of single qubits in the lattice is, however, still a problem. (For recent progress, see Ref. [21]). Recently, it has also been shown that implementations based on arrays of capacitively coupled quantum dots may be used to realize an Ising-type interaction [22].

In conclusion, we have described a new scheme of quantum computation that consists entirely of one-qubit measurements on a particular class of entangled states, the cluster states. The measurements are used to imprint a quantum circuit on the state, thereby destroying its entanglement at the same time. Cluster states are thus one-way quantum computers and the measurements form the program.

We thank D. E. Browne, D. P. DiVincenzo, A. Schenzle, and H. Wagner for helpful discussions. This work was supported by the Deutsche Forschungsgemeinschaft.

[1] C. H. Bennett and D. P. DiVincenzo, Nature (London) **404**, 247 (2000).
[2] See Ref. [1] for a recent review.
[3] J. I. Cirac and P. Zoller, Nature (London) **404**, 579 (2000).
[4] D. Deutsch, Proc. R. Soc. London **425**, 73 (1989).
[5] A. Barenco *et al.,* Phys. Rev. A **52**, 3457 (1995).
[6] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[7] The second Hamiltonian is of the standard Ising form. The symbol "≅" means that the states generated from a given initial state, under the action of these Hamiltonians, are identical up to a local rotation on certain qubits. We use the first Hamiltonian to make the computational scheme more transparent. The conclusions drawn in the paper are, however, the same for both Hamiltonians.
[8] By the "amount of entanglement" contained in the resource, we mean any measure that satisfies the criteria of an entanglement monotone [9]. For cluster states, the entanglement can be calculated, e.g., in terms of the Schmidt measure of Ref. [10].
[9] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[10] J. Eisert and H.-J. Briegel, quant-ph/0007081.
[11] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[12] See, e.g., G. Grimmett, *Percolation* (Springer-Verlag, New York, 1989).
[13] A. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[14] A. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[15] G. K. Brennen *et al.,* Phys. Rev. Lett. **82**, 1060 (1999).
[16] D. Jaksch *et al.,* Phys. Rev. Lett. **82**, 1975 (1999).
[17] T. Calarco *et al.,* Phys. Rev. A **61**, 022304 (2000).
[18] H.-J. Briegel *et al.,* J. Mod. Opt. **47**, 415 (2000).
[19] M. T. DePue *et al.,* Phys. Rev. Lett. **82**, 2262 (1999).
[20] J. M. Ziman, *Models of Disorder* (Cambridge University Press, Cambridge, United Kingdom, 1979).
[21] R. Scheunemann *et al.,* Phys. Rev. A **62**, 051801(R) (2000).
[22] T. Tanamoto, quant-ph/0009030.

Quantum computing in molecular magnets

Michael N. Leuenberger & Daniel Loss

Department of Physics and Astronomy, University of Basel, Klingelbergstrasse 82, 4056 Basel, Switzerland

Shor and Grover demonstrated that a quantum computer can outperform any classical computer in factoring numbers[1] and in searching a database[2] by exploiting the parallelism of quantum mechanics. Whereas Shor's algorithm requires both superposition and entanglement of a many-particle system[3], the superposition of single-particle quantum states is sufficient for Grover's algorithm[4]. Recently, the latter has been successfully implemented[5] using Rydberg atoms. Here we propose an implementation of Grover's algorithm that uses molecular magnets[6, 7, 8, 9, 10], which are solid-state systems with a large spin; their spin eigenstates make them natural candidates for single-particle systems. We show theoretically that molecular magnets can be used to build dense and efficient memory devices based on the Grover algorithm. In particular, one single crystal can serve as a storage unit of a dynamic random access memory device. Fast electron spin resonance pulses can be used to decode and read out stored numbers of up to 10^5, with access times as short as 10^{-10} seconds. We show that our proposal should be feasible using the molecular magnets Fe_8 and Mn_{12}.

Suppose we want to find a phone number in a phone book consisting of $N=2^n$ entries. Usually it takes $N/2$ queries on average to be successful. Even if the N entries were encoded binary, a classical computer would need approximately $\log_2 N$ queries to find the desired phone number[2]. But the computational parallelism provided by the superposition and interference of quantum states enables the Grover algorithm to reduce

the search to one single query[2]. Here we will show that this query can be implemented in terms of a unitary transformation applied to the single spin of a molecular magnet. Such molecular magnets, forming identical and largely independent units, are embedded in a single crystal so that the ensemble nature of such a crystal provides a natural amplification of the magnetic moment of a single spin. However, for the Grover algorithm to succeed, it is necessary to find ways to generate arbitrary superpositions of spin eigenstates. For spins larger than 1/2 this turns out to be a highly non-trivial task as spin excitations induced by magnetic dipole transitions in conventional electron spin resonance (ESR) can occur only in discrete steps of one $\hbar$ (Planck's constant divided by 2π), that is, single steps by two or more $\hbar$ values are excluded by selection rules. To circumvent such physical limitations we propose an unusual scenario which, in principle, allows the controlled generation of arbitrary spin superpositions through the use of multifrequency coherent magnetic radiation in the microwave and radiofrequency range. In particular, we will show by means of the *S*-matrix and time-dependent high-order perturbation theory that by using advanced ESR techniques it is possible to coherently populate and manipulate many spin states simultaneously by applying one single pulse of a magnetic a.c. field containing an appropriate number of matched frequencies. This a.c. field creates a nonlinear response of the magnet via multiphoton absorption processes involving particular sequences of σ and π photons which allows the encoding and, similarly, the decoding of states. Finally, the subsequent read-out of the decoded quantum state can be achieved by means of pulsed ESR techniques. These exploit the non-equidistance of energy levels which is typical of molecular magnets. The method we propose here is interesting in its own right since there has never been an experimental or theoretical attempt, to our knowledge, that shows that the states of spin systems with $s > 1/2$ can be coherently populated.

We implement the Grover algorithm in the single-spin representation with the level spectrum of a spin system as shown in Fig. 1. First, a strong magnetic field in *z*

direction must be applied in order to prepare the initial state $|y_0\rangle = |s\rangle$. Then this field is reduced almost to zero (up to the bias δH_z) in such a way that all $|m\rangle$-states are localized, say, on the left side of the potential barrier. Thus, the magnetic moment pointing along the *z* axis assumes its maximum value and the single spin of a molecular magnet is described by the hamiltonian $H_{\rm spin} = H_{\rm a}+V$ (see Fig. 1). To mark specific states, with a certain occupation amplitude (including phases), we could apply weak oscillating transverse magnetic fields $\mathbf{H}_\perp$ to induce multiphoton transitions via virtual states, which can usually be calculated in perturbation theory in $\mathbf{H}_\perp$. However, the Grover algorithm requires that all the *k*-photon transitions, $k = 1,2,...,s\text{-}1$, have (approximately) the same amplitudes (and possibly different phases). Thus, this would require that all terms of power $V^1, V^2, \ldots, V^{s-1}$ must be of comparable magnitude. Obviously, perturbation theory breaks down in such a case.

To bypass this problem, in our method, all the transition amplitudes between the states $|s\rangle$ and $|m\rangle$, $m=1,2,...,s\text{-}1$, are of the same order in perturbation *V*. This allows us to use perturbation theory. It works only if the energy levels are not equidistant, which is typically the case in molecular magnets owing to anisotropies (in contrast to, for example, a harmonic oscillator potential). In general, if we choose to work with the states $m = m_0, m_0+1,...,s\text{-}1$, where $m_0 = 1,2,...,s\text{-}1$, we have to go up to *n*th order in perturbation, where $n = s\text{-}m_0$ is the number of computational states used for the Grover search algorithm (see below), to obtain the first non-vanishing contribution. Figure 2 shows the transitions for $s = 10$ and $m_0 = 5$. The *n*th-order transitions correspond to the nonlinear response of the spin system to strong magnetic fields. Thus, a coherent magnetic pulse of duration *T* is needed with a discrete frequency spectrum $\{\omega_m\}$, say, for Mn_{12} between 20 and 300 GHz and a single low-frequency ω_0 around 100 MHz (for pulse shaping techniques see ref. 11 and references therein). The low-frequency field

$\mathbf{H}_z(t) = H_0(t)\cos(\omega_0 t)\boldsymbol{e}_z$, applied along the easy-axis, couples to the spin of the molecular magnet through the hamiltonian

$$V_{\rm low}(t) = g\mu_B\, H_0(t)\cos(\omega_0\, t)S_z \qquad (1)$$

where $\hbar w_0 << e_{m_0} - e_{m_0+1}$ and $\boldsymbol{e}_z$ is the unit vector pointing along the z axis. The π photons[12] of $V_{\rm low}$ supply the necessary energy for the resonance condition (see below). They give rise to virtual transitions with $\Delta m = 0$, that is, they do not transfer any angular momentum, see Fig. 2.

The perturbation hamiltonian for the high-frequency transitions from $|s\rangle$ to virtual states that are just below $|m\rangle$, $m = m_0,...,s\text{-}1$, given by the transverse fields $\mathbf{H}_\perp^-(t) = \sum_{m=m_0}^{s-1} H_m(t)\left[\cos(w_m t + \Phi_m)\mathbf{e}_x - \sin(w_m t + \Phi_m)\mathbf{e}_y\right]$, reads

$$\begin{aligned} V_{\rm high}(t) &= \sum_{m=m_0}^{s-1} g m_{\rm B} H_m(t)\left[\cos(w_m t + \Phi_m)S_x - \sin(w_m t + \Phi_m)S_y\right] \\ &= \sum_{m=m_0}^{s-1} \frac{g m_{\rm B} H_m(t)}{2}\left[e^{i(w_m t+\Phi_m)}S_+ + e^{-i(w_m t+\Phi_m)}S_-\right] \end{aligned} \qquad (2)$$

with phases Φ_m (see below), where we have introduced the unit vectors $\boldsymbol{e}_x$ and $\boldsymbol{e}_y$ pointing along the x and y axis, respectively. These transverse fields rotate clockwise and thus produce left circularly polarized σ^- photons which induce only transitions in the left well (see Fig. 1). In general, absorption (emission) of σ^- photons gives rise to $\Delta m = -1$ ($\Delta m = +1$) transitions, and vice versa in the case of σ^+ photons. Anti-clockwise rotating magnetic fields of the form $\mathbf{H}_\perp^+(t) = \sum_{m=m_0}^{s-1} H_m(t)\left[\cos(w_m t + \Phi_m)\mathbf{e}_x + \sin(w_m t + \Phi_m)\mathbf{e}_y\right]$ can be used to induce spin transitions only in the right well (see Fig. 1). In this way, both wells can be accessed independently.

Next we calculate the quantum amplitudes for the transitions induced by the magnetic a.c. fields (see Fig. 2) by evaluating the S-matrix perturbatively. The jth-order

term of the perturbation series of the *S*-matrix in powers of the total perturbation hamiltonian $V(t) = V_{\text{low}}(t)+V_{\text{high}}(t)$ is expressed by

$$S_{m,s}^{(j)} = \left(\frac{1}{i\hbar}\right)^j \prod_{k=1}^{j-1} \int_{-\infty}^{\infty} dt_k \int_{-\infty}^{\infty} dt_j \Theta(t_k - t_{k+1}) U(\infty, t_1) V(t_1) U(t_1, t_2) V(t_2) \ldots V(t_j) U(t_j, -\infty), \quad (3)$$

which corresponds to the sum over all Feynman diagrams of order *j*, and where $U(t,t_0) = e^{-iH(t-t_0)/\hbar}$ is the free propagator, $\Theta(t)$ is the Heavyside function. The total *S*-matrix is then given by $S = \sum_{j=0}^{\infty} S^{(j)}$. The high-frequency virtual transition changing *m* from *s* to *s*-1 is induced by the frequency $\omega_{s-1} = \omega_{s-1,s}-(n-1)\omega_0$. The other high frequencies ω_m, $m = m_0,\ldots,s-2$, of the high-frequency fields H_m mismatch the level separations by ω_0, that is, $\hbar\omega_m = \varepsilon_m-\varepsilon_{m+1}+\hbar\omega_0$, see Fig. 2. As the levels are not equidistant, it is possible to choose the low and high frequencies in such a way that $S_{m,s}^{(j)} = 0$ for $j < n$, in which case the resonance condition is not satisfied, that is, energy is not conserved. In addition, the higher-order amplitudes $\left|S_{m,s}^{(j)}\right|$ are negligible compared to $\left|S_{m,s}^{(n)}\right|$ for $j > n$. Using rectangular pulse shapes, $H_k(t) = H_k$, if $-T/2 < t < T/2$, and 0 otherwise, for $k = 0$ and $k \geq m_0$, we obtain after lengthy but straightforward calculation ($m \geq m_0$)

$$S_{m.s}^{(n)} = \sum_F \Omega_m \frac{2p}{i}\left(\frac{gm_B}{2\hbar}\right)^n \frac{\prod_{k=m}^{s-1} H_k e^{i\Phi_k} H_0^{m-m_0} p_{m,s}(F)}{(-1)^{q_F} q_F! r_s(F)! w_0^{n-1}} \times d^{(T)}\left(w_{m,s} - \sum_{k=m}^{s-1} w_k - (m-m_0)w_0\right), \quad (4)$$

where $\Omega_m = (m-m_0)!$ is the symmetry factor of the Feynman diagrams *F* (see Fig. 2), $q_F = m-m_0-r_s(F)$, $p_{m,s}(F) = \prod_{k=m}^{s} \langle k|S_z|k\rangle^{r_k(F)} \prod_{k=m}^{s-1} \langle k|S_-|k+1\rangle$, $r_k(F) = 0,1,2,\ldots \leq m-m_0$ is the number of π transitions directly above or below the state $|k\rangle$, depending on the particular Feynman diagram *F*, and $d^{(T)}(w) = \frac{1}{2p}\int_{-T/2}^{+T/2} e^{iwt} dt = \sin(wT/2)/pw$ is the delta-function of width $1/T$, ensuring overall energy conservation (resonance condition) for $\omega T >> 1$. The duration *T* of the magnetic pulses must be shorter than the lifetimes τ_d of the states $|m\rangle$ (see Fig. 1). For illustration, we now focus on the case $s = 10$, $m_0 = 5$, and thus $n = 5$, described by $S_{m,10}^{(5)}$, since this is most relevant for the molecular magnets

Mn_{12} and Fe_8 (see Fig. 2). In general, the Grover algorithm requires that the levels are simultaneously populated with roughly equal amplitudes, that is, $\left|S^{(n)}_{m,s}\right| \approx \left|S^{(n)}_{s-1,s}\right|$, $\forall m \geq m_0$, from which we can deduce the required field amplitudes using equation (4)

$$|H_8/H_0|=0.04,\ |H_7/H_0|=0.25,\ |H_6/H_0|=0.61,\ |H_5/H_0|=1.12 \qquad (5)$$

This means that the fields H_0 and H_9, and the frequency ω_0 can be chosen independently. We note particularly that the amplitudes H_k do not differ too much from each other, which can be traced back to partial cancellations in equation (4) owing to the factor $(-1)^{q_F}$. This fact is most useful for applications.

Next, we estimate the transition rate needed to coherently populate the five levels with one single pulse with $V_{\text{low}} + V_{\text{high}}$. As $[\delta^{(T)}(\omega)]^2 \approx (T/2\pi)\delta^{(T)}(\omega)$, the transition rate $w_{m,s} = \left|S^{(n)}_{m,s}\right|^2 / T$ from $|10\rangle$ to $|5\rangle$ at resonance (with $\delta^{(T)}(0) = T/2\pi$) reads

$$w_{5,10} = T\left(\frac{gm_B}{2\hbar}\right)^{10}\left|\frac{H_5 H_6 H_7 H_8 H_9 p_{5,10}}{4! w_0^4}\right|^2, \qquad (6)$$

where $p_{5,10} = \prod_{k=5}^{9}\langle k|S_-|k+1\rangle$. We then insert the parameters $\omega_0 = 5\times10^8$ s^{-1}, $T = 10^{-7}$ s, $H_0 = H_9 = 20$ G giving the transition rate $w_{5,10} = 9\times10^6$ s^{-1}, which is of the order of τ_d, that is, $Tw_{5,10} = 1$. For our purpose it is sufficient to choose $Tw_{5,10} << 1$. If $\omega_0 = 5\times10^7$ s^{-1}, $T = 10^{-7}$ s, $H_0 = H_9 = 2$ G, we obtain the transition rate $w_{5,10} = 9\times10^4$ s^{-1}, thus $Tw_{5,10} \approx 0.01$. Thus we have shown that the required amplitudes and frequencies of the fields given in equation (1) and (2) are experimentally accessible.

We adapt now the Grover scheme[5] to describe the quantum computational read-in and decoding of the quantum data register ***a***. For simplicity we set the relative phase $\Phi_0 = 0$ of the low-frequency field $\mathbf{H}_z(t)$; see equation (1).

(1) Read-in. We start from the ground state $|s\rangle$ as initial state. Then, in order to introduce the desired phases Φ_m for each state $|m\rangle$ we need to irradiate the system with a coherent magnetic pulse of duration T containing the n high-frequency fields $H_m[\cos(\omega_m t+\Phi_m)\boldsymbol{e}_x - \sin(\omega_m t+\Phi_m)\boldsymbol{e}_y]$ (see equation (2)) with $\Phi_m = \sum_{k=s-1}^{m+1}\Phi_k + j_m$ (φ_m

are the relative phases), and the low-frequency field $\mathbf{H}_z(t)$ (see equation (1)), yielding $S^{(n)}_{m_0,s} = \ldots = S^{(n)}_{s-2,s} = S^{(n)}_{s-1,s} = \pm h$, $\eta>0$, that is, $\varphi_m = 0,\pi$, depending on the number to be encoded. For example, to encode the number $13_{10}=1101_2$ in Fig. 2, we need $\varphi_9 = \varphi_8 = \varphi_7 = 0$ and $\varphi_6 = \varphi_5 = \pi$, where the states $m = 9,8,7,6,5$ represent the binary digits $2^0,2^1,2^2,2^3,2^4$, respectively. We note that $S^{(n)}_{m,s}$ can be either positive or negative, depending on the explicit Feynman diagrams F. In this way one can prepare the quantum data register $\boldsymbol{a} = (a_s, a_{s-1}, \ldots, a_{m_0})$, where the bits $a_s = 1$, $a_m = \pm\eta$ are the amplitudes of the state $|y\rangle = \sum_{m=m_0}^{s} a_m |m\rangle$. This pulse performs a unitary transformation up to order η, that is, $U_{m,s} + O(h^2) = S^{(n)}_{m,s}$. In this way an arbitrary integer between 0 and 2^n can be stored.

(2) Decoding. In order to decode the phase information stored in the data register $\boldsymbol{a}$, a universal single pulse (see equations (1) and (2)) leading to $S^{(n)}_{m_0,s} = \ldots = S^{(n)}_{s-2,s} = S^{(n)}_{s-1,s} = -h$ must be applied, which performs approximately a unitary transformation for $\eta << 1$. The accumulated error is about $n\eta^2$, which must be kept smaller than 1. Because $\eta > \eta_0 > 0$, with η_0 given by the precision of the detection, we require that $n << 1/h_0^2$. We note that this decoding works also if the bits a_m, with $\eta_0 < |a_m| << 1$, have different amplitudes (but still of similar magnitude). This pulse amplifies the flipped bits, which have amplitude $-\eta$, and suppresses the rest of the bits with amplitude $+\eta$. For the example shown in Fig. 2 the relative phases in equation (2) must be set $\varphi_9 = \varphi_7 = \varphi_5 = 0$ and $\varphi_8 = \varphi_6 = \pi$ (irrespective of $\boldsymbol{a}$).

(3) Read-out. Once a state has been marked and amplified, that is, decoded, we must be able to read out this information physically. This task can be accomplished by standard spectroscopy with, say, pulsed ESR, where the circularly polarized radiation can now be incoherent because we need the absorption intensity of only one pulse. Full spectral analysis of Mn_{12} have been performed with ESR[13] and neutron scattering[14]. Thus, we can assume that the spectrum is known. Now, irradiation of the magnet with a single pulse of duration T containing the frequencies $\omega_{m-1,m}$, $m = s\text{-}2,\ldots,m_0$, induces transitions that are described by the first-order amplitudes $S^{(1)}_{m-1,m}$ (higher-order multiphoton effects

can now be neglected for sufficiently small fields). For instance, let us assume that the state $|7\rangle$ is marked, that is, populated. Then, we would observe stimulated emission for the transitions from $|7\rangle$ to $|8\rangle$ at the frequency $\omega = \omega_{7,8}$ and stimulated absorption of approximately the same intensity for the transition from $|7\rangle$ to $|6\rangle$ at $\omega = \omega_{6,7}$, which uniquely identifies the marked level, because the levels are not equidistant. Generally, if the states $|m_1\rangle, |m_2\rangle, \ldots, |m_k\rangle$, where $1 \le k \le n$, are marked, the following absorption/emission intensity in leading order is measured:

$$I_{s-2}^{m_0} = \sum_{i=1}^{k} \left(\left| S^{(1)}_{m_i-1,m_i} \right|^2 + \left| S^{(1)}_{m_i+1,m_i} \right|^2 \right). \qquad (7)$$

This spectrum identifies all the marked states unambiguously. We emphasize that the entire Grover algorithm (read-in, decoding, read-out) requires three subsequent pulses each of duration T with $t_d > T > w_0^{-1} > w_m^{-1}, w_{m,m\pm1}^{-1}$. This gives a 'clock-speed` of about 10 GHz for Mn_{12}, that is, the entire process of read-in, decoding, and read-out can be performed within about 10^{-10} s.

Finally, so far we have used only the left well of the potential in Fig. 1. As both wells can be accessed separately during read-in, decoding and read-out by magnetic fields that rotate either clockwise or anti-clockwise, a single molecular magnet represents a two-digit number. Every digit can store $N = 2^{s-1}$ elements at most, which allows us to store a number between 0 and $2^{2s-2} = 2.6\times10^5$ in a single crystal made of molecular magnets with spin $s = 10$. If $M > 2$ phases can be distinguished for φ_m (depending on the experimental resolution)[5], a number between 0 and M^{2s-2} can be stored in a single crystal of molecular magnets with spin s. We note that the experimental overhead required by the Grover search algorithm involves only the control of $\log_M N$ frequencies, which, once available, can decode any number between 1 and N by means of a single magnetic pulse. Our proposal for implementing Grover's algorithm works not only for molecular magnets but for any electron or nuclear spin system with non-equidistant energy levels. Although such spin systems cannot be scaled

to arbitrarily large spin *s* — the larger a spin becomes, the faster it decoheres and the more classical its behavior will be — we can use such spin systems of given *s* to great advantage in building dense and highly efficient memory devices.

Received 24 November 2000; accepted 14 February 2001.

1. Shor, P. in *Proc. 35th Ann. Symp. Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, Los Alomitos, 1994).

2. Grover, L. K. Quantum Computers Can Search Arbitrarily Large Databases by a Single Query. *Phys. Rev. Lett.* **79**, 4709–4712 (1997).

3. Lloyd, S. Quantum search without entanglement. *Phys. Rev. A* **61**, R 010301-1–010301-4 (1999).

4. Ekert, A. K. & Jozsa, R. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.* **68**, 733–753 (1996).

5. Ahn, J., Weinacht, T. C. & Bucksbaum, P. H. Information Storage and Retrieval Through Quantum Phase. *Science* **287**, 463–465 (2000).

6. Thiaville, A. & Miltat, J. MAGNETISM: Small Is Beautiful. *Science* **284**, 1939–1940 (1999).

7. Thomas, L., Lionti, F., Ballou, R., Gatteschi, D., Sessoli, R. & Barbara, B. Macroscopic quantum tunnelling of magnetization in a single crystal of nanomagnets. *Nature* **383**, 145–147 (1996).

8. Friedman, J. R., Sarachik, M. P., Tejada, J. & Ziolo, R. Macroscopic Measurement of Resonant Magnetization Tunneling in High-Spin Molecules. *Phys. Rev. Lett.* **76**, 3830–3833 (1996).

9. Sangregorio, C., Ohm, T., Paulsen, C., Sessoli, R. & Gatteschi, D. Quantum Tunneling of the Magnetization in an Iron Cluster Nanomagnet. *Phys. Rev. Lett.* **78**, 4645–4648 (1997).

10. Wernsdorfer, W., Sessoli, R., Caneschi, A., Gatteschi, D. & Cornia, A. Nonadiabatic

Landau-Zener tunneling in Fe_8 molecular nanomagnets. *Europhys. Lett.* **50**, 552–558 (2000).

11. Fitzgerald, R. Pulse shaping improves efficiency of soft X-ray harmonic generation. *Phys. Today* **53**, 24 (2000).

12. Cohen-Tannoudji, C., Diu, B., Laloë, F. Quantum Mechanics, Vol. 2, 1323–1339 (Wiley, New York).

13. Barra, A. L., Gatteschi, D. & Sessoli, R. High-frequency EPR spectra of a molecular nanomagnet: Understanding quantum tunneling of the magnetization. *Phys. Rev. B* 56, 8192–8198 (1997).

14. Mirebeau, I., Hennion, M., Casalta, H., Andres, H., Güdel, H. U., Irodova, A. V. & Caneschi, A. Low-Energy Magnetic Excitations of the Mn_{12}-Acetate Spin Cluster Observed by Neutron Scattering. *Phys. Rev. Lett.* 83, 628–631 (1999).

15. Leuenberger, M. N. & Loss, D. Spin tunneling and phonon-assisted relaxation in Mn_{12}-acetate. *Phys. Rev. B* **61**, 1286–1302 (2000).

16. Leuenberger, M. N. & Loss, D. Incoherent Zener tunneling and its application to molecular magnets. *Phys. Rev. B* **61**, 12200–12203 (2000).

Acknowledgements

We thank G. Salis and J. Schliemann for useful comments. This work has been supported in part by the Swiss NSF and by the European Union Molnanomag network.

Correspondence should be addressed to D. L. (e-mail: Daniel.Loss@unibas.ch).

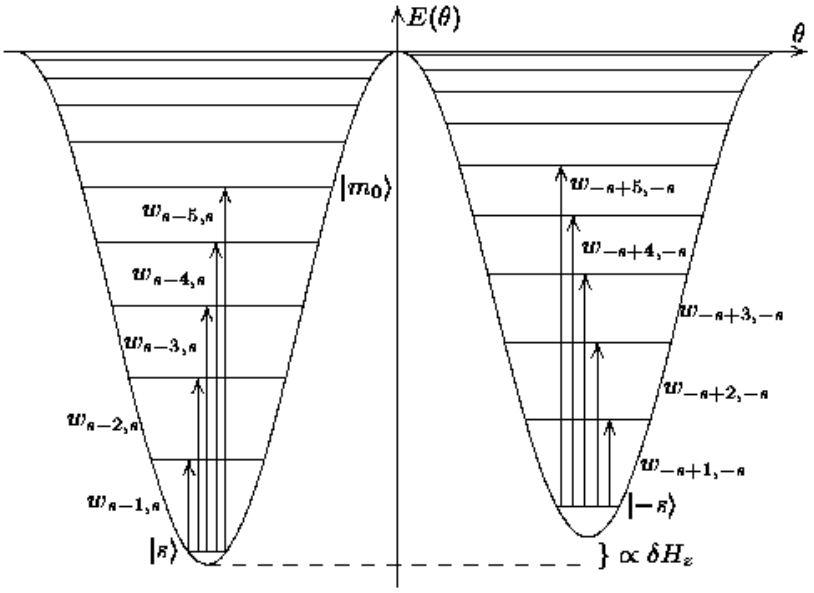


Figure 1 Double well potential seen by the spin due to magnetic anisotropies in Mn_{12}. Arrows depict transitions between spin eigenstates driven by the external magnetic field **H** (see below).

Molecular magnets have the important advantage that they can be grown naturally as single crystals of up to 10–100 μm length containing about 10^{12} to 10^{15} (largely) independent units so that only minimal sample preparation is required. The molecular magnets behave like single spins, for example, Mn_{12} (refs 7, 8) and Fe_8 (refs 9, 10) have a spin $s = 10$ ground state. Thus, they can be described by a single-spin hamiltonian of the form $H_{\rm spin} = H_{\rm a} + V + H_{\rm sp} + H_{\rm T}$[15,16], where $H_{\rm a} = -AS_z^2 - BS_z^4$ represents the magnetic anisotropy ($A >> B > 0$), that is, the easy axis of the spin lies along the z direction. The Zeeman term $V = g\mu_{\rm B}\mathbf{H}\cdot\mathbf{S}$ describes the coupling between the external magnetic field **H** and the spin **S** of length s. The calculational states are given by the $2s+1$ eigenstates $|m\rangle$ of $H_{\rm a} + g\mu_{\rm B}\delta H_z S_z$ with eigenenergies $\varepsilon_m = -Am^2 - Bm^4 + g\mu_{\rm B}\delta H_z m$, $-s \le m \le s$. The corresponding classical anisotropy potential energy $E(\theta) = -As\cos^2\theta - Bs\cos^4\theta + g\mu_{\rm B}\delta H_z s\cos\theta$, shown here, is obtained by the substitution $S_z = s\cos\theta$, where θ is the polar spherical angle. We have introduced the notation $\hbar\omega_{m,m'} = \varepsilon_{m'} - \varepsilon_m$. The hamiltonian $H_{\rm T}$ induces tunnelling between (quasi) degenerate $|m\rangle$-states with tunnel splitting energy $E_{mm'}$. However, applying a bias field δH_z such that $g\mu_{\rm B}\delta H_z > E_{mm'}$, tunnelling can be completely suppressed and thus $H_{\rm T}$ can be neglected[15,16]. We also assume temperatures of below 1 K such that transitions due to spin-

phonon interactions (H_{sp}) can also be neglected. In this regime, the level lifetime in Fe_8 and Mn_{12} is estimated to be about $\tau_d = 10^{-7}$s, limited mainly by hyperfine and/or dipolar interactions[10,15,16].

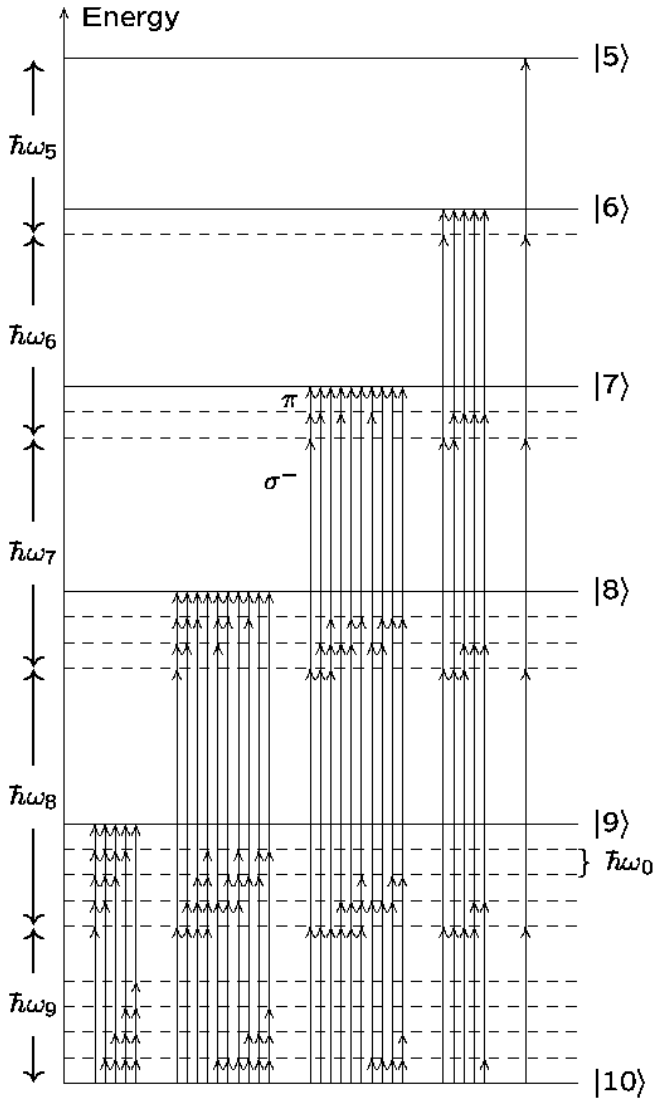


Figure 2 Feynman diagrams *F* that contribute to $S^{(5)}_{m,s}$ for $s = 10$ and $m_0 = 5$ describing transitions (of 5th order in *V*) in the left well of the spin system (see Fig. 1). The blue (red) arrows indicate the transitions induced by the high-(low-)frequency magnetic fields H_m (H_0) shown in equation (2) (equation (1)). Whereas the H_m fields transfer angular momentum to the spin of the molecular magnet by means of σ^- photons, the H_0 field provides only energy without angular momentum by means of π photons. In this way all the transition amplitudes $S^{(5)}_{m,s}$ are of similar

magnitude (see text). We note that $S_{m,s}^{(j)} = 0$ for $j < n$, and $\left|S_{m,s}^{(j)}\right| << \left|S_{m,s}^{(n)}\right|$ for $j > n$. For example, the transition from $|10\rangle$ to $|7\rangle$ arises from the absorption of five photons in total, comprising three σ^- photons and two π photons. Since it does not matter in which order the five photons are absorbed, there are $\binom{5}{2} = 10$ different kinds of diagrams. Also, it is essential that the levels are not equidistant; if they are, this scheme for multiphoton absorption does not work, because then resonances can occur already in lower order of the *S*-matrix leading to incoherent populations of the levels. There is a global phase factor due to the unperturbed time evolution of the spin system, given by $e^{-ie_m(t-t_0)/\hbar}$, which can be easily accounted for and thus shall be ignored here. For a first test of the nonlinear response described here, we can irradiate the molecular magnet with an a.c. field of frequency $\omega_{s-1,s}/2$, which gives rise to a two-photon absorption and thus to a Rabi oscillation between the states $|s\rangle$ and $|s-1\rangle$. We note that for stronger magnetic fields it is in principle possible to generate superpositions of Rabi oscillations between the states $|s\rangle$ and $|s-1\rangle$, $|s\rangle$ and $|s-2\rangle$, $|s\rangle$ and $|s-3\rangle$, and so on (to be published elsewhere).

A scheme for efficient quantum computation with linear optics

E. Knill*, R. Laflamme* & G. J. Milburn†

* *Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 87545, USA*
† *Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Australia*

Quantum computers promise to increase greatly the efficiency of solving problems such as factoring large integers, combinatorial optimization and quantum physics simulation. One of the greatest challenges now is to implement the basic quantum-computational elements in a physical system and to demonstrate that they can be reliably and scalably controlled. One of the earliest proposals for quantum computation is based on implementing a quantum bit with two optical modes containing one photon. The proposal is appealing because of the ease with which photon interference can be observed. Until now, it suffered from the requirement for non-linear couplings between optical modes containing few photons. Here we show that efficient quantum computation is possible using only beam splitters, phase shifters, single photon sources and photo-detectors. Our methods exploit feedback from photo-detectors and are robust against errors from photon loss and detector inefficiency. The basic elements are accessible to experimental investigation with current technology.

Quantum information processing (QIP) uses quantum mechanics for information storage, communication and computation. It enables large improvements in computational efficiency and communication security by exploiting the superposition principle and non-classical correlations of quantum mechanics. Examples include Shor's quantum algorithm for factoring large integers[1], Grover's algorithm for accelerating combinatorial searches[2] and quantum cryptography for secure communication[3,4]. Initial concern that quantum coherence may be too fragile to be exploited has been dispelled by theoretical work showing that noise and decoherence are not fundamental obstacles to the implementation of QIP[5–10]. Consequently, increasing effort is being devoted towards physically realizing quantum computers, and there are many proposals for implementing the necessary quantum devices. Examples of promising technologies include ion traps, quantum dots, Josephson junctions, nuclear spins in silicon and nuclear spins in molecules[11].

Quantum effects are particularly easy to observe in optical systems, and it is therefore not surprising that one of the earliest proposals for QIP uses photons to implement quantum logic[12]. Optical systems currently constitute the only realistic proposal for long-distance quantum communication and underlie experimental implementations of quantum cryptography[13–15]. Until now the main obstacle to scalable optical QIP was the apparent need for nonlinear couplings between optical modes. Achieving such couplings at sufficient strengths is possible in principle but is technically difficult[16]. As a result, other proposals[17–19] for using linear optics to benchmark quantum algorithms require exponentially large physical resources.

Here we show the surprising[20] result that linear optics is sufficient for efficient QIP with photons. Efficiency in the sense of the theory of computation means with polynomial resources, and we achieve low linear resources. Our proposal for QIP with linear optics requires single photon sources (implementable with active linear optics[21]), beam splitters, phase shifters, photo-detectors, and feedback from photo-detector outputs. A quantum bit (qubit) is realized by one photon in two optical modes (such as horizontal or vertical polarization). Efficient QIP is established by means of three results, each of which constitutes a breakthrough in linear optics QIP. The first result implies that non-deterministic quantum computation[22] is possible with linear optics. It is based on a non-linear sign shift between two qubits that uses two additional photons and post-selection. The sign shift succeeds with probability 1/16, and whether or not it succeeded is known. Although there are no practical applications of non-deterministic quantum computation, it implies that linear optics has features not available to classical deterministic or probabilistic computation. The second result shows that the probability of success of the quantum gates can be increased arbitrarily close to one. The result is based on using entangled states prepared non-deterministically and quantum teleportation[23,24]. Thus quantum computation is possible in principle with linear optics. The resources needed to make the probability of success close to one with these methods are extremely demanding. The third result shows that with quantum coding, the resources for obtaining accurate encoded qubits are very efficient with respect to the accuracy achieved, thus completing the goal of efficient linear optics quantum computation (LOQC). The coding methods can be adapted to make LOQC fault-tolerant for photon loss, detector inefficiency and phase decoherence. As a result, LOQC can be robustly implemented with resources low enough to suggest practical scalability, making it as promising a technology for QIP as are other proposals.

Bosonic qubits and optical elements

The fundamental units of QIP are qubits, the quantum generalizations of classical bits. A qubit's state space consists of all superpositions $\alpha|0\rangle + \beta|1\rangle$ ($|\alpha|^2 + |\beta|^2 = 1$) of the basic states $|0\rangle$ and $|1\rangle$. A set of qubits can be realized by independent two-state subsystems of a physical system. Bosonic qubits are defined by states of optical modes. An optical mode is a physical system whose state space consists of superpositions of the number states $|n\rangle$, where $n = 0, 1, 2, \ldots$ gives the number of photons in the mode. When we consider several qubits or modes, we use labels to distinguish between them. For example, $|20\rangle_{lm}$ (short for $|2\rangle_l|0\rangle_m$) is a state where modes l and m have two and zero photons, respectively. The basic states of a bosonic qubit encoded in modes l_1 and l_2 are $|0\rangle \rightarrow |0\rangle_{l_1}|1\rangle_{l_2}$ and $|1\rangle \rightarrow |1\rangle_{l_1}|0\rangle_{l_2}$. For comprehensive treatments of quantum optics and QIP, see the references[25–27].

In addition to instances of an ideal quantum system, a complete implementation of a quantum computer requires a means for state preparation, the ability to apply sufficiently powerful quantum gates, and a readout method. To process information, these elements are combined in quantum networks (see Box 1). The initial state is the vacuum state $|\mathbf{0}\rangle$, in which there are no photons in any of

the modes to be used. The basic element that adds photons to the initial state is a single photon source. It can be used to set the state of any given mode to the one-photon state $|1\rangle$. It is sufficient to be able to prepare this state non-deterministically. This means that the state preparation has a non-zero probability of success, and whether or not it succeeded is known.

The simplest optical elements are phase shifters and beam splitters. These elements generate the evolutions implementable by passive linear optics. These evolutions preserve the total photon number, and can be described by their effects on each mode's creation operator, which is defined by $\mathbf{a}^{(l)\dagger}|n\rangle_l = \sqrt{n+1}|n+1\rangle_l$. Let U be the unitary operator applied to a state by such an evolution. Using $U|\mathbf{0}\rangle = |\mathbf{0}\rangle$ gives $U\mathbf{a}^{(l)\dagger}|\mathbf{0}\rangle = U\mathbf{a}^{(l)\dagger}U^\dagger U|\mathbf{0}\rangle = U\mathbf{a}^{(l)\dagger}U^\dagger|\mathbf{0}\rangle = \Sigma_k u_{kl}\mathbf{a}^{(k)\dagger}|\mathbf{0}\rangle$. The coefficients u_{kl} introduced by these equations define a matrix u that must be unitary. Conversely, for every unitary u there is a sequence of phase shifters and beam splitters that implements the corresponding operation up to a global phase[28]. For a named optical element X, let $u(X)$ be the unitary matrix associated with X according to the above rules. The unitary matrix associated with phase shifter $\mathbf{P}_\theta$ is $u(\mathbf{P}_\theta) = e^{i\theta}$. The unitary matrix associated with beam splitter $\mathbf{B}_{\theta,\phi}$ is

$$u(\mathbf{B}_{\theta,\phi}) = \begin{pmatrix} \cos(\theta) & -e^{i\phi}\sin(\theta) \\ e^{-i\phi}\sin(\theta) & \cos(\theta) \end{pmatrix} \quad (1)$$

We define $\mathbf{B}_\theta = \mathbf{B}_{\theta,0}$.

Phase shifters and beam splitters applied to a bosonic qubit's modes preserve the qubit state space. Their effect can therefore be expressed in the qubit basis using the standard Pauli operators σ_x, σ_y and σ_z. For example, $\mathbf{P}_\theta^{(1)}$ applies $\exp(-i\sigma_z\theta/2)$ up to a global phase shift, and $\mathbf{B}_\theta^{(12)}$ applies $\exp(-i\sigma_y\theta)$. It follows that all one-qubit rotations can be implemented with linear optics. To achieve the full power of quantum computation we require a two-qubit gate such as the conditional sign flip c–z defined by $|a\rangle|b\rangle \rightarrow (-1)^{ab}|a\rangle|b\rangle$, where $a, b = 0,1$ and labels have been omitted.

Readout is accomplished by measuring a mode with a photo-detector, which destructively determines whether one or more photons are present in a mode. We assume that photo-detectors can be applied at any time and that the measurement result can be used to control other optical elements. We need a photon counter, which destructively counts the number of photons in a mode. An approximate photon counter that suffices for our purposes can be designed by using beam splitters and multiple photo-detectors. To measure a mode, we can use beam splitters to distribute the mode's photons evenly over N modes and use a photo-detector on each. The desired count is the number of detectors that 'see' photons. The probability of undercounting given that the photon number is k is at most $k(k-1)/(2N)$. For LOQC, $k \leqslant 4$.

Nondeterministic conditional sign flip

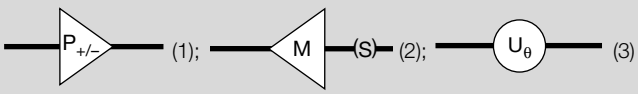
LOQC is based on a series of non-deterministic operations with increasing probability of success. The first operation is a non-deterministic nonlinear sign change on one mode defined by the operation NS: $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \rightarrow \alpha_0|0\rangle + \alpha_1|1\rangle - \alpha_2|2\rangle$ (with probability 1/4), and can be implemented using the optical network of Fig. 1. Its main features are the use of two ancilla modes with one prepared photon and post-selection based on measuring the ancillas. This procedure can be experimentally verified using techniques similar to those used in a recent Greenberger–Horne–Zeilinger (GHZ) experiment[29] (see Supplementary Information). A conditional sign flip c–$z_{1/16}$ that succeeds with probability 1/16 can be

Box 1

Quantum gates and networks

Quantum information processing (QIP) is accomplished by applying quantum gates and measurements to prepared qubits. The gates evolve the state according to the laws of quantum mechanics. The power of QIP depends on the ability to implement enough evolutions using the available gates. If all unitary evolutions can be approximated up to a global phase, the set of gates is called universal. Standard quantum computation relies on universal gate sets where each gate acts on one or two qubits. One such gate set consists of the one-qubit rotations $U_\phi = \exp(-i\sigma_u\phi/2)$, $U = X, Y$ or Z, where ϕ can be restricted to $\phi = 45°$; and either the conditional sign flip (see text) or one of the 90° rotations $(UV)_{90°}^{(12)} = \exp(-i\pi\sigma_u^{(1)}\sigma_v^{(2)}/4)$, with $U, V = X, Y$ or Z.

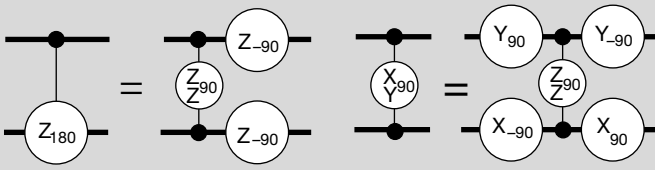
A sequence of state preparations, quantum gates and measurements is called a quantum network. Quantum networks can be depicted by time–space diagrams, with time lines of qubits given by lines running from left to right, and gates by elements that intercept the lines. Our conventions for depicting one qubit gates are:



(1) is a preparation gate, with $P = X, Y$ or Z corresponding to preparations of σ_x, σ_y or σ_z eigenstates. For example, if $P_\pm = Z_+$, the $|0\rangle$ state is prepared. (2) is a measurement gate, where $M = X, Y$ or Z corresponds to measurements in the eigenbasis of σ_x, σ_y or σ_z. The symbol S denotes the measurement outcome, which can be +1 or –1. (3) is a one-qubit rotation around $U = X, Y$ or Z by angle ϕ (in degrees by default). Two-qubit gates are denoted by

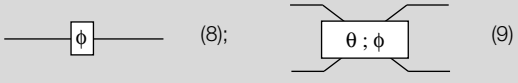
(4) is a conditional sign change by phase χ and applies χ only to the state $|11\rangle$. (5) is a $(ZY)_{90°}^{(12)}$ rotation.

Many of the gates are equivalent up to one-qubit rotations. Here are some equivalences used in the text:



(7) expresses one gate by conjugating another by $Y_{-90°}^{(1)}$ and $X_{90°}^{(2)}$.

Optical networks are similar to quantum networks except that the basic systems are optical modes. The basic elements of an optical network drawing are:



(8) shows a phase shifter $\mathbf{P}_\phi$ and (9) a beam splitter $\mathbf{B}_{\theta,\phi}^{(12)}$, where mode 1 is the top mode. If $\phi = 0$, only angle θ may be given in a diagram. State preparation is like (1), with $P_\pm$ replaced by 0 or 1, for the number of photons inserted into the mode. Measurement is like (2), with M replaced by $\mathbf{n}$ and S by R, for the number of photons detected.

implemented with two independent applications of the operation NS as shown in Fig. 2.

Quantum gates by teleportation

Quantum teleportation has proved to be a very versatile tool in QIP[23,24]. Here we use it to increase the probability of success of coupling gates by reducing the implementation of c–z to a state preparation problem. A basic quantum teleportation protocol $\mathbf{T}_1$ for transferring the state $\alpha_0|0\rangle_1 + \alpha_1|1\rangle_1$ of mode 1 to mode 3 begins by adjoining the 'entangled' ancilla state $|t_1\rangle_{23} = |01\rangle_{23} + |10\rangle_{23}$ (normalization constants omitted). Next, modes 1 and 2 are measured in the basis $|01\rangle_{12} \pm |10\rangle_{12}$, $|00\rangle_{12} \pm |11\rangle_{12}$ (a Bell basis). The measurement consists of two steps. The first determines the parity p of the number of photons in modes 1 and 2 (parity measurement). The second determines the sign s in the superposition. Consider the case where p is odd. If $s =$ '+', the state of mode 3 is $\alpha_0|0\rangle_3 + \alpha_1|1\rangle_3$. If $s =$ '–', the state is $\alpha_0|0\rangle_3 - \alpha_1|1\rangle_3$, which can be restored to the initial state by using a phase shifter. For even p, the situation is similar except that $|0\rangle_3$ and $|1\rangle_3$ are flipped (and cannot easily be un-flipped using linear optics). The key property of quantum teleportation is that the input state appears in mode 3 up to a simple transformation without having interacted with mode 3.

The basic teleportation protocol can be implemented in linear optics with success probability 1/2 by applying a balanced beam splitter to modes 1 and 2 and then measuring the number of photons in the two modes. This partial Bell (or teleportation) measurement ($\mathbf{BM}_1$) determines the parity, and if it is odd, the sign. Using this method, it is possible to implement a conditional sign flip c–$z_{1/4}$ that succeeds with probability 1/4 (Fig. 3).

To reliably detect photon loss (in the single photon sources, in transmission or by undercounting in detectors), we give another method, $\mathbf{RT}_1$, for teleporting a bosonic qubit with success probability 1/2, which is shown in Fig. 4. The method for obtaining c–$z_{1/4}$ using $\mathbf{T}_1$ works with $\mathbf{RT}_1$, giving c–$z_{r,1/4}$ with identical failure behaviour (see the caption of Fig. 3). The implementation is in the Supplementary Information.

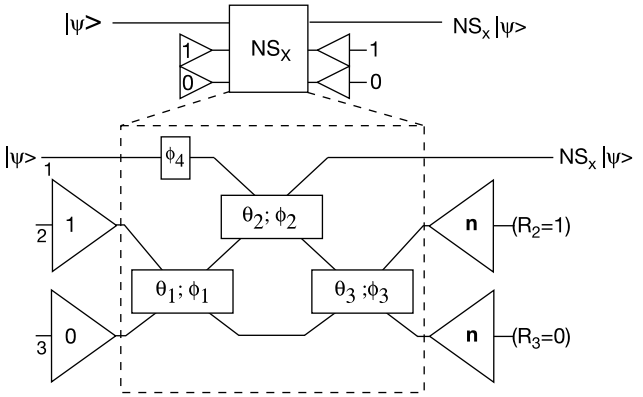


Figure 1 Nonlinear phase shifts on one mode. The numbers at the beginning of the horizontal mode line are their labels. The outlined optical element is abbreviated in future figures by using the top diagram as indicated. The output is accepted only if the photon counters detect one photon in mode 2 and none in mode 3. The subscript x in the top diagram is the phase shift applied and depends on the choice of phases in the optical elements. NS as defined in the text corresponds to $x = -1$ and requires $\theta_1 = 22.5°$, $\phi_1 = 0°$, $\theta_2 = 65.5302°$, $\phi_2 = 0°$, $\theta_3 = -22.5°$, $\phi_3 = 0°$ and $\phi_4 = 180°$. The probability of success is 0.25. Exact expressions for the angles of NS can be determined from the 3×3 unitary matrix u associated with the optical elements[28]:

$$u = \begin{pmatrix} 1 - 2^{1/2} & 2^{-1/4} & (3/2^{1/2} - 2)^{1/2} \\ 2^{-1/4} & 1/2 & 1/2 - 1/2^{1/2} \\ (3/2^{1/2} - 2)^{1/2} & 1/2 - 1/2^{1/2} & 2^{1/2} - 1/2 \end{pmatrix}.$$

A shift of $|2\rangle_1$ by $x = \exp(i\pi/2)$ is obtained by setting $\theta_1 = 36.53°$, $\phi_1 = 88.24°$, $\theta_2 = 62.25°$, $\phi_2 = -66.52°$, $\phi_3 = -36.53°$, $\phi_3 = -11.25°$ and $\phi_4 = 102.24°$. The probability of success is 0.18082.

Near-deterministic quantum teleportation and operations

To improve the probability of successful teleportation to $1 - 1/(n+1)$, we generalize the prepared entanglement by defining $|t_n\rangle_{1\ldots(2n)} = \Sigma_{j=0}^{n} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}$. The notation $|a\rangle^j$ means $|a\rangle|a\rangle\ldots, j$ times. The modes are labelled from 1 to $2n$, left to right. The state exists in the space of n bosonic qubits, where the kth qubit is encoded in modes $n+k$ and k (in that order). Using the qubit bases, the state $|t_n\rangle$ is $\Sigma_{j=0}^{n}|o\rangle^j|1\rangle^{n-j}$. This representation can be used to obtain linear size quantum networks (which are implementable in LOQC) for preparing the state.

A procedure for teleporting the state $\alpha_0|0\rangle_0 + \alpha_1|1\rangle_0$ using $|t_n\rangle$ applies the measurement $\mathbf{BM}_n$, which consists of the $n+1$ point Fourier transform $\hat{\mathbf{F}}_{n+1}$ followed by measurement of modes $0\ldots n$. $\hat{\mathbf{F}}_{n+1}$ is determined by $u(\hat{\mathbf{F}}_{n+1})_{kl} = \omega^{kl}/\sqrt{n+1}$, where $\omega = \exp(i2\pi/(n+1))$ and $k, l \in 0\ldots n$. It has efficient linear optics implementations[30,31].

Suppose $\mathbf{BM}_n$ detects k photons altogether. We claim that if $0 < k < n+1$, then the teleported state appears in mode $n+k$ and only needs to be corrected by applying a phase shift. The modes $2n-l$ are in state 1 for $0 \leqslant l < (n-k)$ and can be reused in future preparations requiring single photons. The modes $2n-l$ are in state 0 for $n-k < l < n$. If $k = 0$ we learn that the input state was $|0\rangle_0$ and if $k = n+1$, that it was $|1\rangle_0$. The probability of these two events is $1/(n+1)$, regardless of the input. Both the necessary correction and which mode we teleported to are unknown until after the measurement.

The construction of c–$z_{1/4}$ and c–$z_{r,1/4}$ can be generalized using near-deterministic teleportation. To obtain a conditional sign flip c–$z_{n^2/(n+1)^2}$ that succeeds with probability $n^2/(n+1)^2$, the prepared entanglement consists of two copies of $|t_n\rangle$ modified by applied c–z operations as follows

$$|cs_n\rangle = \sum_{i,j=0}^{n} (-1)^{(n-i)(n-j)} |1\rangle^i|0\rangle^{n-i}|0\rangle^j|1\rangle^{n-i}|1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j} \quad (2)$$

$$= \sum_{i,j=0}^{n} (-1)^{(n-i)(n-j)} |o\rangle^i|1\rangle^{n-i}|o\rangle^j|1\rangle^{n-j} \quad (3)$$

where the bosonic qubit encoding introduced earlier for $|t_n\rangle$ has been used for the second identity. The teleportation measurements involve the first modes of the two qubits to which c–z is to be

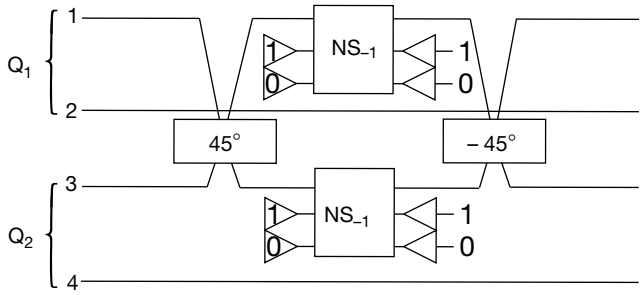


Figure 2 Conditional sign flip implemented with NS operations. Q_1 and Q_2 refer to the bosonic qubits encoded in modes 1, 2, and 3, 4, respectively. Consider the effect of the first beam splitter: When both qubits are in state $|1\rangle$, modes 1 and 3 are in the state $|11\rangle_{13}$, which transforms to $|20\rangle_{13} + |02\rangle_{13}$. In none of the other cases do two photons appear in the same mode. Thus $NS^{(1)}$ and $NS^{(3)}$ have the desired effect. Both of these operations must succeed, so c–$z_{1/16}$ succeeds with probability 1/16.

applied, and modes $1\ldots n$ and $2n+1\ldots 2n+n$ (left to right order), respectively. An additional phase correction is needed after the measurement, depending on which modes the output appears in.

To ensure detection of photon loss, the state $|\mathrm{rt}_n\rangle$, which generalizes $|\mathrm{rt}_1\rangle$, can be used: $|\mathrm{rt}_n\rangle = \Sigma_{j=}^{n}|0\rangle^{j}|1\rangle^{n-j}|0\rangle^{n-j}|1\rangle^{j}$, written in terms of the qubit encoding. As before, the total number of photons in the modes measured for teleportation is now fixed (at $n+1$), and any deviation from this results in a detected loss error. The state needed for the loss-detecting implementation of c–z, c–$z_{r,n^2/(n+1)^2}$ is:

$$|\mathrm{rcs}_n\rangle = \sum_{i,j=0}^{n}(-1)^{(n-i)(n-j)}|0\rangle^{i}|1\rangle^{n-i}|0\rangle^{n-i}|1\rangle^{i}|0\rangle^{j}|1\rangle^{n-j}|0\rangle^{n-j}|1\rangle^{j} \quad (4)$$

The failure-by-measurement behaviour for c–$z_{n^2/(n+1)^2}$ and c–$z_{r,n^2/(n+1)^2}$ can be made the same as that for c–$z_{1/4}$ (see Fig. 3).

Applications of the techniques introduced so far include near-deterministic non-destructive parity measurements, a method for

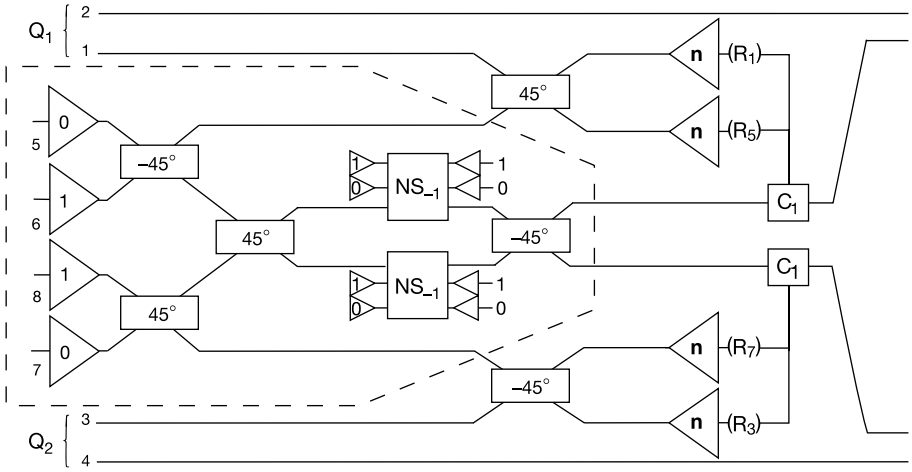


Figure 3 Conditional sign flip with success probability 1/4. The method may be derived as follows[24]: To implement c–z on two bosonic qubits in modes 1, 2 and 3, 4, respectively, we can teleport the first modes of each qubit to two new modes (labelled 6 and 8) and then apply c–z to the new modes. When using the basic teleportation protocol ($\mathbf{T}_1$), we may need to apply a sign correction. Since this commutes with c–z, it is possible to apply c–z to the prepared state before performing the measurements, reducing the implementation of c–z to a state-preparation (outlined) and two teleportations. The two teleportation measurements each succeed with probability 1/2, giving a net success probability of 1/4. The correction operations C_1 consist of applying the phase shifter $\mathbf{P}_{180°}$ when required by the measurement outcomes. The state preparation needs to be attempted 16 times on average before success, which corresponds to 32 attempted NS operations (without taking advantage of the ability to avoid an attempt if the first one in a pair failed).

The implementation of c–$z_{1/4}$ fails if one of the two teleportation measurements does not succeed. The following properties hold for failure of c–$z_{1/4}$: (1) the failed teleportation measurements result in an unintentional Z measurement of the corresponding bosonic qubit (2). The teleportation measurements fail independently. (Alternatively, to improve efficiency, one may attempt the measurements sequentially, so as not to perform the second one if the first one fails.) (3) By reintroducing a photon if necessary, the measurements can be assumed to be non-destructive. (4) By applying a phase shifter if necessary, it can be arranged that the effect on the successfully teleported qubit is as if the c–z operation succeeded before the unintentional measurement.

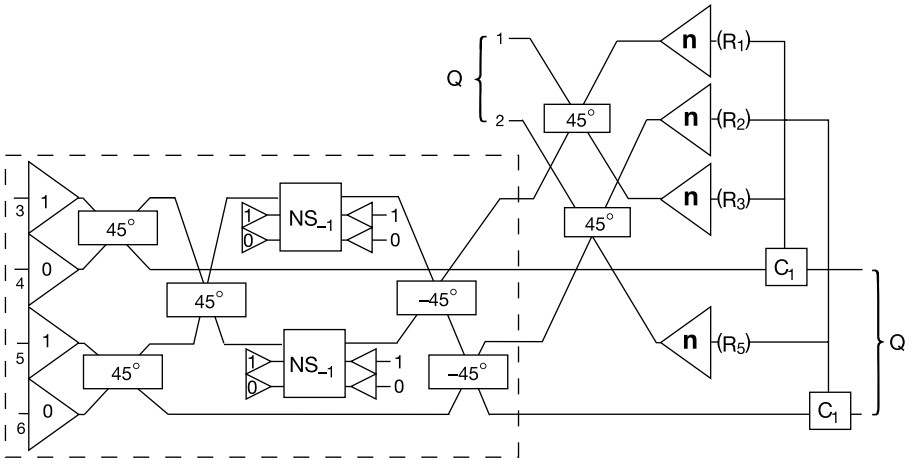


Figure 4 Teleportation with loss detection ($\mathbf{RT}_1$). The outlined box prepares the state $|\mathrm{rt}\rangle_{3456} = |01\rangle_{34}|10\rangle_{56} + |10\rangle_{34}|01\rangle_{56}$ using non-deterministic gates. This teleportation protocol has been experimentally tested[44,45], using down conversion with post-selection for preparing $|\mathrm{rt}_1\rangle$ instead of the preparation network shown above. Given $|\mathrm{rt}_1\rangle$, the protocol succeeds with probability 1/2. The pair of NS operations implements a c–$z_{1/16}$ on bosonic qubits encoded in modes 3, 4 and 5, 6, respectively. Thus 32 NS attempts are needed on average before successfully obtaining $|\mathrm{rt}_1\rangle$. Without loss, the number of photons in modes 1, 2, 3, 5 is two. Thus, loss is detected if $R_1 + R_2 + R_3 + R_5 \neq 2$. The teleportation succeeds if $R_1 + R_3 = 1$ and $R_2 + R_5 = 1$, in which case the qubit reappears in modes 4, 6. Failure not due to loss results in a Z measurement of the teleported qubit. Loss of a photon in the incoming qubit or from detector inefficiency is always detected. Assuming no loss in the prepared state or the detectors, $\mathbf{RT}_1$ detects if the input is not a bosonic qubit state (a leakage event) and returns a bosonic qubit. This is necessary for scalable quantum information processing (QIP).

creating entanglement by local measurements of uncorrelated photons shared with beam splitters, and nearly unconditional quantum teleportation and Bell-state measurements with linear optics.

The proof of the claim of this section, the teleportation network for the case $n = 2$, networks for preparing $|cs_2\rangle$ and $|rt_2\rangle$ and descriptions of the applications are in the Supplementary Information.

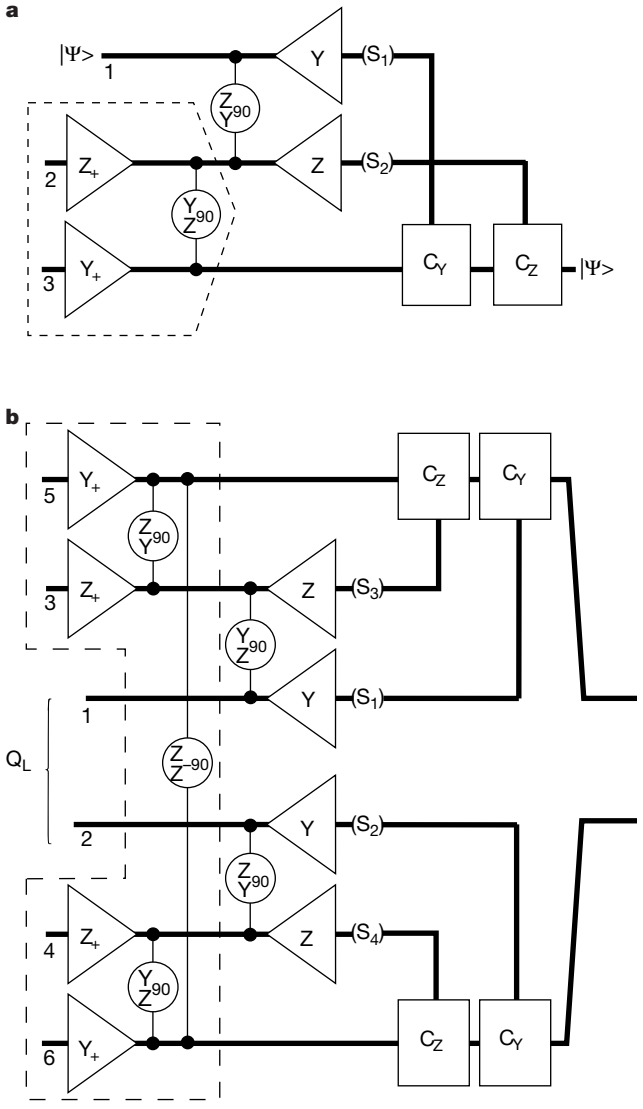


Figure 5 Teleportation networks for the code χ_2. **a**, Teleportation satisfying that failures of the teleportation step result at worst in a Z-measurement of qubit 1. The networks are based on a variation of the teleportation protocol that exploits the flexibility in the choices for initial states, rotations and measurements to ensure that it behaves well with respect to measurement failures. The correction operations are $C_Z = X_{180°}$ if $S_2 = 1$ and $C_Y = Z_{180°}$ if $S_1 = 1$. The state preparation is outlined and outputs a state denoted by $|tx_2\rangle$. **b**, Teleportation for applying $(Z^{(L)})_{90°}$. If $S_3S_4 = -1$, the phase needs to be corrected with a $Z_{180°}$ on both qubits. The prepared state (outlined) is obtained by applying $(ZZ)_{90°}$ to the destination qubits of two copies of $|tx_2\rangle$. The method for applying $(Z^{(L_1)}Z^{(L_2)})_{90°}$ is similar, using four copies instead. Both teleportations are attempted. The procedure can only fail with the logical qubit measured in Z. For simplicity, the following failure protocol can be used: If both teleportations fail in any way, we measure the qubits in Z on purpose (if that has not already happened), thus inducing a logical Z measurement. If only one fails, we ensure that the corresponding qubit is measured in Z, then follow the recovery protocol of Fig. 6 using the successfully teleported qubit. With this failure protocol, the logical failure probability for the $Z^{(L)}$ and $Z^{(L_1)}Z^{(L_2)}$ rotations is $f_2 = (1-(1-f)^2)^2 + 2(1-(1-f)^2)(1-f)^2 f_r$ with $f_r = f/(1-f(1-f))$ the probability of recovery failure (Fig. 6). Thus $f_2 < f$ whenever $f < 1/6.43$.

Boosting success with quantum codes

Exponential improvements in the probability of success for gates and state preparation can be obtained by exploiting quantum codes and the failure behaviour of $c{-}z_{n^2/(n+1)^2}$. As a result, n need not be large and the difficulty of preparing states such as $|cs_n\rangle$ or $|rcs_n\rangle$ is lessened. We give a method based on a two-qubit code, χ_2. This method can be used to define logical qubits with greatly improved success probabilities and robustness, provided that the given qubits are sufficiently controllable. As a result it is possible to iterate the method to efficiently achieve essentially perfect QIP. This iteration is known as concatenation and underlies the accuracy-threshold theorems of fault-tolerant quantum computation[6–9].

From now on, we use qubit based quantum networks and rely on the following list of operations implementable in LOQC with bosonic qubits according to the techniques of the previous sections: (1) X, Y and Z eigenstate (eigenvalue +1 or −1) preparation; (2) X, Y and Z measurements; (3) $X_{180°}$, $Y_{180°}$ and $Z_{180°}$ rotations; (4) X_ϕ rotations; (5) $Z_{90°}$ rotation; (6) $(Z^{(1)}Z^{(2)})_{90°}$ rotation. For the moment we assume that the optical elements, single-photon sources and photon counters are error-free. Operations (1) to (4) always succeed. The $(Z^{(1)}Z^{(2)})_{90°}$ rotation fails independently on qubits 1 and 2 with probability f. If $c{-}z_{n^2/(n+1)^2}$ is used, then $f = 1/(n+1)$. The $Z_{90°}$ rotation always succeeds in LOQC, although after the first encoding it fails with probability f. A qubit on which an operation fails is measured in Z after the rotation has been applied. The $Y_{90°}$, $(YZ)_{90°}$ and $(YY)_{90°}$ rotations can be implemented by conjugation of $Z_{90°}$ or $(ZZ)_{90°}$ with failure-free X rotations. The failure mode of these rotations is similar to that for the $(ZZ)_{90°}$ rotation, with commuting Y measurements replacing Z measurements.

To encode a qubit we define its logical states $|0\rangle_L$ and $|1\rangle_L$ by $|0\rangle_L = |00\rangle + |11\rangle$ and $|1\rangle_L = |01\rangle + |10\rangle$. This is an instance of a stabilizer code[32–35]. In this context it is convenient to use the abbreviation $U = \sigma_u$ for $U = X, Y, Z$. With encoding qubits labelled 1, 2, the logical X, Y and Z operators are given by $X^{(L)} = X^{(1)} =_L X^{(2)}$, $Z^{(L)} = Z^{(1)}Z^{(2)} =_L -Y^{(1)}Y^{(2)}$ and $Y^{(L)} = Y^{(1)}Z^{(2)} =_L Z^{(1)}Y^{(2)}$, where we introduced the notation $=_L$ to denote identity when restricted to the code space spanned by $|0\rangle_L$, $|1\rangle_L$. To destructively measure one of the logical operators, it suffices to measure each qubit; it is straightforward to obtain nondeterministic state preparation networks (see the Supplementary Information). Any rotation $X_\phi^{(L)}$ can be implemented by applying $X_\phi^{(1)}$ or $X_\phi^{(2)}$. The 180° logical rotations can be applied by using the corresponding 180° rotations directly on the qubits, a feature satisfied by all stabilizer codes[36]. For example, to apply $Y_{180°}^{(L)}$ apply both $Y_{180°}^{(1)}$ and $Z_{180°}^{(2)}$.

The logical operations introduced so far can be done without failure. To implement the $Z_{90°}^{(L)}$ and $(ZZ)_{90°}^{(L_1L_2)}$ rotations with failure probabilities much less than f requires the teleportation networks shown in Fig. 5, which have the property that at worst, the teleported qubit is measured in Z. As described in the captions of Figs 5 and 6, the failure probability f_z of these logical rotations satisfies $f_z < O(f^2)$ and $f_z < f$ whenever $f < 1/6.43$.

The methods can be improved in three ways: first, by better exploiting the flexibility in state preparation and responses to failures; second, by using classical linear codes like the repetition codes; and third, by encoding more than one qubit into one block. With these techniques it is possible to achieve $f_z < f$ for $f < 1/2$ (see Supplementary Information).

Scalability and resource requirements

A scalable information processing system requires that one can deal with errors that occur in the physical implementation. For LOQC, dominant sources of errors are photon loss (at the single photon source or during processing), detector inefficiency (which can be

viewed as photon loss) and phase errors. Photon loss can be dealt with by using the loss-detecting implementations of c–z. The probability f_l of loss for an LOQC operation can be predicted from the characteristics of the optical devices. The possibility of loss introduces a new failure mode, where nothing is known about what happened to the state of the qubit. This is the erasure model of errors[37]. A good implementation of LOQC ensures that $f_l \ll f$, so that we can first improve f using the techniques already discussed, and then deal with the problem of erasures. Compensating for erasures is much easier than dealing with general errors, with pessimistic estimates of $f_l \lesssim 0.01$ (ref. 38) for quadratic improvements. Unlike photon loss, phase errors are not detected by the networks discussed so far. Happily, phase-error correction can be integrated into the methods for reducing f using codes that generalize χ_2 based on classical repetition codes. These codes can correct unknown phase errors in up to half the qubits. More details on erasure and phase error correcting codes are in the Supplementary Information.

The methods introduced so far suffice for implementing accurate quantum gates on logical qubits in the presence of intrinsic failures of LOQC, and sufficiently low photon loss and phase errors. Scalable quantum computation is possible provided that any remaining errors in the logical operations fall below a threshold. There is evidence that the relevant threshold may be above 0.0001 (D. Gottesman and J. Preskill, unpublished work). Achieving such low error is experimentally challenging for any device, although optimism is justified by the observations that many of the errors are due to improper calibration of classical control parameters, and these are often controllable well below the estimated threshold. An example is pulse phase in nuclear magnetic resonance. Another reason for optimism is that at least for quantum communication, the threshold is well above 0.01 (ref. 39). As all viable proposals for long-distance quantum communication are based on optics, this may be the first scalable application of LOQC.

Resources contributing toward a logical quantum gate based on LOQC can be counted in two ways: as total and as conditional resources. The total resources are given by the number of optical operations required on average. This depends on the success probabilities of the component state preparations and the desired success probability for the logical operations. As most of the resources are used in independent state preparation steps, an implementation of LOQC can be based on massively parallel state factories. It is thus natural to consider the conditional resources, which are the number of optical operations that successfully contribute toward a logical quantum gate. Their significance is that the error of an operation conditional on success can be estimated by multiplying the conditional error of the optical elements by the conditional resource count. Detailed resource analyses are yet to be done. However, it can be shown that failure probabilities below 5% can be achieved using only two iterations of χ_2, requiring about 300 successful c–$z_{9/16}$ operations per logical two-qubit gate[38].

An implementation of LOQC requires careful mode matching, rapidly controllable delay lines or good synchronization of pulses, tunable beam splitters and phase shifters, single photon sources and high-efficiency fast photo-detectors for single photon detection. Speed is needed to be able to select successful state preparations before photon loss becomes too large. Tunable optical elements can be made using polarizers and polarizing beam splitters. Non-deterministic single photon sources can be constructed with parametric down converters[21], although a better method is to use one of the schemes for single photon sources that have recently been proposed[40,41]. The best photon counters currently have efficiencies of about 0.9 at optical frequencies[42]. This is sufficient for experimentally implementing the basic elements of LOQC. Higher efficiencies are required for implementing the more complex teleportation and quantum gate operations with sufficiently low error conditional on success.

The preliminary resource counts discussed above imply large but not excessive resource overheads per reliable quantum gate. The need for robustness requires non-trivial resource overheads in all implementations of QIP, so this suggests that scalable quantum computation using LOQC is comparable in complexity to other proposals. LOQC has the advantage in several respects. In particular, there is no need for low temperature for the basic optical elements (except perhaps in the single photon sources and the photo-detectors, depending on implementation), and photons naturally maintain their coherence over timescales that are long compared to the basic control operations. Furthermore, the sources of noise are better understood and do not depend on difficult-to-predict or difficult-to-measure thermal interactions. However, all proposals until now, including LOQC, require that various technologies can be made to work together to obtain high fidelities in operations.

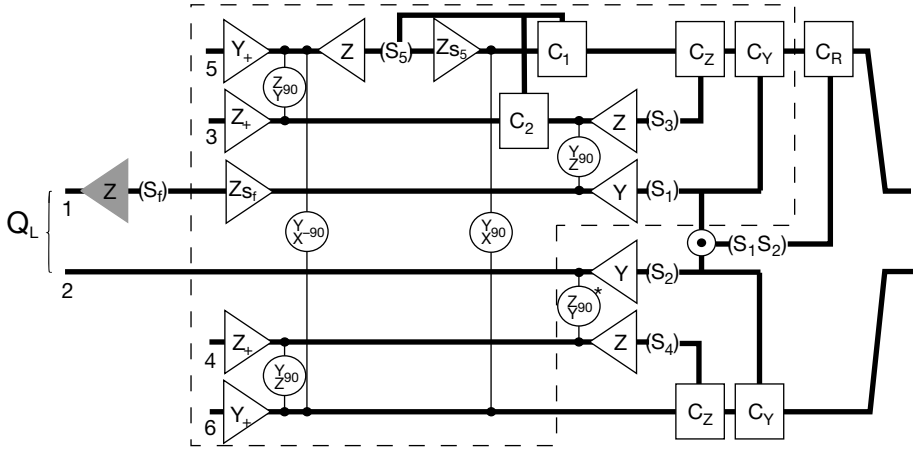


Figure 6 Recovery from Z measurement. A state is prepared using two instances of $|\mathrm{tx}_2\rangle$ modified by projecting with $I + XX$. The gates C_1 and C_2 correct for measuring $S_5 = -1$ by applying $C_1 = Z_{180°}$ to qubit 5 and $C_2 = X_{180°}$ to qubit 3. The two teleportations are then attempted. The network assumes that we need to recover from a Z measurement of qubit 1 (shown in grey). In this case, qubit 1 can be absorbed into a state preparation; which one depends on the measurement outcome. This avoids being affected by failures in the top teleportation. The parts of the network which can be performed in a non-deterministic state preparation are outlined. An XX measurement of the teleported qubits becomes recorded in the teleportation measurements. The recovered state is obtained by applying $C_R = Z_{180°}$ if $S_1S_2 = -1$. If the pre-measurement coupling gate marked by an asterisk fails with a Y-measurement only, then we can retry the recovery process using a new prepared state. The probability of this failure event is $f(1-f)$, so the total failure probability f_r of recovery satisfies $f_r = f + f(1+f)f_r$, whence $f_r = f/(1-f(1-f))$.

Discussion

Linear optics was believed to be insufficient for quantum computation because every implementable evolution can be understood in terms of a small unitary matrix, contrary to expectations of exponential complexity. Furthermore, passive linear optics does not involve particle interactions other than those imposed by statistics and can be understood in terms of classical wave mechanics. There is, however, a hidden non-linearity in LOQC (in the photo-detectors) and our techniques effectively transfer this non-linearity to the bosonic qubits, thus enabling universal quantum computation.

There are other options for implementing LOQC. Particularly interesting is an idea[43] that involves encoding qubits in the phase space of a mode. Universal computation in this system requires active linear optics and a nonlinearly prepared state, but has the advantage of being intrinsically robust against errors involving shifts in the canonically conjugate variables. It may be possible to combine approaches to achieve robust and efficient LOQC even more easily. □

Received 24 July; accepted 13 November 2000.

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26,** 1484–1509 (1997).
2. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79,** 325–328 (1997).
3. Wiesner, S. Conjugate coding. *(Original Manuscript ~ 1969) Sigact News* **15,** 78–88 (1983).
4. Bennett, C., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **5,** 3–28 (1992).
5. Shor, P. W. in *Proceedings of the 37th Symposium on the Foundations of Computer Science (FOCS)* 56–65 (IEEE Press, Los Alamitos, 1996).
6. Aharonov, D. & Ben-Or, M. in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)* 176–188 (ACM Press, New York, 1996).
7. Kitaev, A. Y. Quantum computations: algorithms and error correction. *Russian Math. Surv.* **52,** 1191–1249 (1997).
8. Knill, E., Laflamme, R. & Zurek, W. H. Resilient quantum computation. *Science* **279,** 342–345 (1998).
9. Preskill, J. Reliable quantum computers. *Proc. R. Soc. Lond. A* **454,** 385–410 (1998).
10. Steane, A. Efficient fault-tolerant quantum computing. *Nature* **399,** 124–126 (1999).
11. Experimental proposals for quantum computation. (Special focus issue) *Fort. Phys.* **48,** 767–1138 (2000).
12. Milburn, G. J. Quantum optical Fredkin gate. *Phys. Rev. Lett.* **62,** 2124–2127 (1988).
13. Hughes, R. J., Morgan, G. L. & Peterson, C. G. Quantum key distribution over a 48 km optical fibre network. *J. Mod. Optics* **47,** 533–547 (2000).
14. Tittle, W., Brendel, J., Gisin, N. & Zbinden, H. Long-distance Bell-type tests using energy-time entangled photons. *Phys. Rev. A* **59,** 4150–4163 (1999).
15. Townsend, P., Rarity, J. & Tapster, P. Single photon interference in 10 km long optical fibre interferometer. *Electron. Lett.* **29,** 1291–1293 (1993).
16. Turchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H. & Kimble, H. J. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.* 4710–4713 (1995).
17. Cerf, N. J., Adami, C. & Kwiat, P. G. Optical simulation of quantum logic. *Phys. Rev. A* **57,** R1477–R1480 (1998).
18. Howell, J. C. & Yeazell, J. A. Reducing the complexity of linear optics quantum circuits. *Phys. Rev. A* **61,** 052303/1–5 (2000).
19. Kwiat, P. G., Mitchell, J. R., Schwindt, P. D. D. & White, A. G. Grover's search algorithm: An optical approach. *J. Mod. Optics* **47,** 257–266 (2000).
20. Lütkenhaus, N., Calsamiglia, J. & Suominen, K.-A. Bell measurements for teleportation. *Phys. Rev. A* **59,** 3295–3300 (1999).
21. Hong, C. K. & Mandel, L. Experimental realization of a localized one-photon state. *Phys. Rev. Lett.* **56,** 58–60 (1986).
22. Adleman, L. M., DeMarrais, U. & Huang, M.-D. A. Quantum computability. *SIAM J. Comput.* **26,** 1524–1540 (1997).
23. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
24. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402,** 390–393 (1999).
25. Walls, D. F. & Milburn, G. J. *Quantum Optics* (Springer, Berlin, 1994).
26. Aharonov, D. in *Annual Reviews of Computational Physics VI* (ed. Stauffer, D.) (World Scientific, Singapore, 1999).
27. DiVincenzo, D. The physical implementation of quantum computation. *Fort. Phys.* **48,** 771–793 (2000).
28. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of an discrete unitary operator. *Phys. Rev. Lett.* **73,** 58–61 (1994).
29. Bouwmeester, D., Pan, J.-W., Daniell, M., Weinfurter, H. & Zeilinger, A. Observation of three-photon Greenberger-Horne-Zeilinger entanglement. *Phys. Rev. Lett.* **82,** 1345–1349 (1999).
30. Weihs, G., Reck, M., Weinfurter, H. & Zeilinger, A. All-fiber three-path Mach-Zehnder interferometer. *Opt. Lett.* **21,** 302–304 (1996).
31. Cormen, T. H., Leiserson, C. E. & Rivest, R. L. *Introduction to Algorithms* 795 (MIT Press, Cambridge, MA, 1990).
32. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52,** 2493–2496 (1995).
33. Steane, A. Multiple particle interference and quantum error correction. *Proc. R. Soc. Lond. A* **452,** 2551–2577 (1996).
34. Calderbank, A., Rains, E., Shor, P. & Sloane, N. Quantum error correction and orthogonal geometry. *Phys. Rev. A* **78,** 405–408 (1997).
35. Gottesman, D. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A* **54,** 1862–1868 (1996).
36. Gottesman, D. A theory of fault-tolerant quantum computation. *Phys. Rev. A* **57,** 127–137 (1998).
37. Grassl, M., Beth, T. & Pellizari, T. Codes for the quantum erasure channel. *Phys. Rev. A* **56,** 33–38 (1997).
38. Knill, E., Laflamme, R. & Milburn, G. Thresholds for linear optics quantum computation. Preprint quant-ph/0006120 at ⟨xxx.lanl.gov⟩ (2000).
39. Dür, W., Briegel, H.-J., Cirac, J. I. & Zoller, P. Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59,** 169–181 (1999).
40. Kim, J., Benson, O., Kan, H. & Yamamoto, Y. A single-photon turnstile device. *Nature* **397,** 500–503 (1999).
41. Foden, C. L., Talyanskii, V. I., Milburn, G. J., Leadbeater, M. L. & Pepper, M. High frequency acousto-electric single photon source. *Phys. Rev. A* **62,** 011803(R)/1–4 (2000).
42. Takeuchi, S., Yamamoto, Y. & Hogue, H. H. Development of a high-quantum-efficiency single-photon counting system. *Appl. Phys. Lett.* **74,** 1063–1065 (1999).
43. Gottesman, D., Kitaev, A. & Preskill, J. Encoding a qubit in an oscillator. Preprint quant-ph/0008040 at ⟨xxx.lanl.gov⟩ (2000).
44. Bouwmeester, D., Pan, J., Mattle, K., Eibl, M., Weinfurter, H. & Zeilinger, A. Experimental quantum teleportation. *Nature* **390,** 575–579 (1997).
45. Boschi, D., Branca, S., Martini, F. D., Hardy, L. & Popescu, S. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels. *Phys. Rev. Lett.* **80,** 1121–1125 (1998).

Supplementary information is available on *Nature*'s World-Wide Web site (http://www.nature.com) or as paper copy from the London editorial office of *Nature*.

Acknowledgements

We thank P. Kwiat and A. White for help and discussions.

Correspondence and requests for materials should be sent to E. Knill (e-mail: knill@lanl.gov).

Fault-tolerant quantum computation by anyons

A. Yu. Kitaev

L.D.Landau Institute for Theoretical Physics,
117940, Kosygina St. 2
e-mail: kitaev@itp.ac.ru

February 1, 2008

Abstract

A two-dimensional quantum system with anyonic excitations can be considered as a quantum computer. Unitary transformations can be performed by moving the excitations around each other. Measurements can be performed by joining excitations in pairs and observing the result of fusion. Such computation is fault-tolerant by its physical nature.

A quantum computer can provide fast solution for certain computational problems (e.g. factoring and discrete logarithm [1]) which require exponential time on an ordinary computer. Physical realization of a quantum computer is a big challenge for scientists. One important problem is decoherence and systematic errors in unitary transformations which occur in real quantum systems. From the purely theoretical point of view, this problem has been solved due to Shor's discovery of fault-tolerant quantum computation [2], with subsequent improvements [3, 4, 5, 6]. An arbitrary quantum circuit can be simulated using imperfect gates, provided these gates are close to the ideal ones up to a constant precision δ. Unfortunately, the threshold value of δ is rather small[1]; it is very difficult to achieve this precision.

Needless to say, *classical* computation can be also performed fault-tolerantly. However, it is rarely done in practice because classical gates are reliable enough. Why is it possible? Let us try to understand the easiest thing — why classical information can be stored reliably on a magnetic media. Magnetism arise from spins of individual atoms. Each spin is quite sensitive to thermal fluctuations. But the spins interact with each other and tend to be oriented in the same direction. If some spin flips to the opposite direction, the interaction forces it to flip back to the direction of other spins. This process is quite similar to the standard error correction procedure for the repetition code. We may say that errors are being corrected at the physical level. Can we propose something similar in the quantum case? Yes, but it is not so simple. First of all, we need a quantum code with local stabilizer operators.

I start with a class of stabilizer quantum codes associated with lattices on the torus and other 2-D surfaces [6, 8]. Qubits live on the edges of the lattice whereas the stabilizer operators correspond to the vertices and the faces. These operators can be put together to make up a

[1] Actually, the threshold is not known. Estimates vary from 1/300 [7] to 10^{-6} [4].

Hamiltonian with local interaction. (This is a kind of penalty function; violating each stabilizer condition costs energy). The ground state of this Hamiltonian coincides with the protected space of the code. It is 4^g-fold degenerate, where g is the genus of the surface. The degeneracy is persistent to local perturbation. Under small enough perturbation, the splitting of the ground state is estimated as $\exp(-aL)$, where L is the smallest dimension of the lattice. This model may be considered as a quantum memory, where stability is attained at the physical level rather than by an explicit error correction procedure.

Excitations in this model are anyons, meaning that the global wavefunction acquires some phase factor when one excitation moves around the other. One can operate on the ground state space by creating an excitation pair, moving one of the excitations around the torus, and annihilating it with the other one. Unfortunately, such operations do not form a complete basis. It seems this problem can be removed in a more general model (or models) where the Hilbert space of a qubit have dimensionality > 2. This model is related to Hopf algebras.

In the new model, we don't need torus to have degeneracy. An n-particle excited state on the plane is already degenerate, unless the particles (excitations) come close to each other. These particles are nonabelian anyons, i.e. the degenerate state undergoes a nontrivial unitary transformation when one particle moves around the other. Such motion ("braiding") can be considered as fault-tolerant quantum computation. A measurement of the final state can be performed by joining the particles in pairs and observing the result of fusion.

Anyons have been studied extensively in the field-theoretic context [9, 10, 11, 12, 13]. So, I hardly discover any new about their algebraic properties. However, my approach differs in several respects:

- The model Hamiltonians are different.
- We allow a generic (but weak enough) perturbation which removes *any* symmetry of the Hamiltonian.[2]
- The language of ribbon and local operators (see Sec. 5.2) provides unified description of anyonic excitations and long range entanglement in the ground state.

An attempt to use *one-dimensional* anyons for quantum computation was made by G. Castagnoli and M. Rasetti [14], but the question of fault-tolerance was not considered.

1 Toric codes and the corresponding Hamiltonians

Consider a $k \times k$ square lattice on the torus (see fig. 1). Let us attach a spin, or qubit, to each edge of the lattice. (Thus, there are $n = 2k^2$ qubits). For each vertex s and each face p, consider operators of the following form

$$A_s = \prod_{j \in \mathrm{star}(s)} \sigma_j^x \qquad B_p = \prod_{j \in \mathrm{boundary}(p)} \sigma_j^z \tag{1}$$

These operators commute with each other because $\mathrm{star}(s)$ and $\mathrm{boundary}(p)$ have either 0 or 2 common edges. The operators A_s and B_p are Hermitian and have eigenvalues 1 and -1.

[2] Some local symmetry still can be established by adding unphysical degrees of freedom, see Sec. 3.

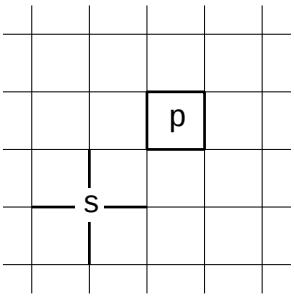


Figure 1: Square lattice on the torus

Let $\mathcal{N}$ be the Hilbert space of all $n = 2k^2$ qubits. Define a *protected subspace* $\mathcal{L} \subseteq \mathcal{N}$ as follows[3]

$$\mathcal{L} \;=\; \Big\{\, |\xi\rangle \in \mathcal{N} \;:\;\; A_s|\xi\rangle = |\xi\rangle,\;\; B_p|\xi\rangle = |\xi\rangle \text{ for all } s,p \,\Big\} \tag{2}$$

This construction gives us a definition of a quantum code $\mathrm{TOR}(k)$, called a *toric code* [6, 8]. The operators A_s, B_p are the *stabilizer operators* of this code.

To find the dimensionality of the subspace $\mathcal{L}$, we can observe that there are two relations between the stabilizer operators, $\prod_s A_s = 1$ and $\prod_p B_p = 1$. So, there are $m = 2k^2 - 2$ independent stabilizer operators. It follows from the general theory of additive quantum codes [15, 16] that $\dim \mathcal{L} = 2^{n-m} = 4$.

However, there is a more instructive way of computing $\dim \mathcal{L}$. Let us find the algebra $\mathbf{L}(\mathcal{L})$ of all linear operators on the space $\mathcal{L}$ — this will give us full information about this space. Let $\mathcal{F} \subseteq \mathbf{L}(\mathcal{N})$ be the algebra of operators generated by A_s, B_p. Clearly, $\mathbf{L}(\mathcal{L}) \cong \mathcal{G}/\mathcal{I}$, where $\mathcal{G} \supseteq \mathcal{F}$ is the algebra of all operators which commute with A_s, B_p, and $\mathcal{I} \subset \mathcal{G}$ is the ideal generated by $A_s - 1$, $B_p - 1$. The algebra $\mathcal{G}$ is generated by operators of the form

$$Z \;=\; \prod_{j \in c} \sigma_j^z \qquad\qquad X \;=\; \prod_{j \in c'} \sigma_j^x$$

where c is a loop (closed path) on the lattice, whereas c' is a cut, i.e. a loop on the dual lattice (see fig. 2). If a loop (or a cut) is contractible then the operator Z is a product of B_p, hence $Z \equiv 1 \pmod{\mathcal{I}}$. Thus, only non-contractible loops or cuts are interesting. It follows that the algebra $\mathbf{L}(\mathcal{L})$ is generated by 4 operators Z_1, Z_2, X_1, X_2 corresponding to the loops c_{z1}, c_{z2} and the cuts c_{x1}, c_{x2} (see fig. 2). The operators Z_1, Z_2, X_1, X_2 have the same commutation relations as σ_1^z, σ_2^z, σ_1^x, σ_2^x. We see that each quantum state $|\xi\rangle \in \mathcal{L}$ corresponds to a state of 2 qubits. Hence, the protected subspace $\mathcal{L}$ is 4-dimensional.

In a more abstract language, the algebra $\mathcal{F}$ corresponds to 2-boundaries and 0-coboundaries (with coefficients from $\mathbb{Z}_2$), $\mathcal{G}$ corresponds to 1-cycles and 1-cocycles, and $\mathbf{L}(\mathcal{L})$ corresponds to 1-homologies and 1-cohomologies.

There is also an explicit description of the protected subspace which may be not so useful but is easier to grasp. Let us choose basis vectors in the Hilbert space $\mathcal{N}$ by assigning a label $z_j = 0, 1$ to each edge j. [4] The constraints $B_p|\xi\rangle = |\xi\rangle$ say that the sum of the labels at the boundary of a face should be zero (mod 2). More exactly, only such basis vectors contribute to

[3] We will show that this subspace is really protected from certain errors. Vectors of this subspaces are supposed to represent "quantum information", like codewords of a classical code represent classical information.

[4] 0 means "spin up", 1 means "spin down". The Pauli operators σ_z, σ_x have the standard form in this basis.

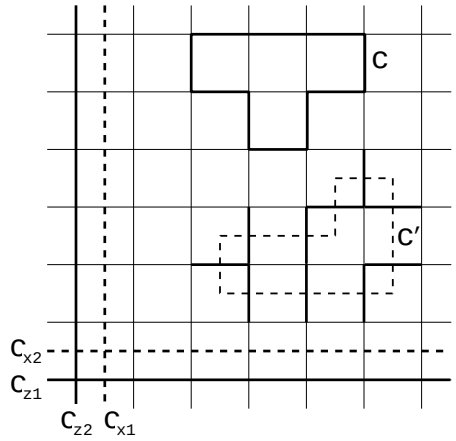


Figure 2: Loops on the lattice and the dual lattice

a vector from the protected subspace. Such a basis vector is characterized by two topological numbers: the sums of z_j along the loops c_{z1} and c_{z2}. The constraints $A_p|\xi\rangle = |\xi\rangle$ say that all basis vectors with the same topological numbers enter $|\xi\rangle$ with equal coefficients. Thus, for each of the 4 possible combinations of the topological numbers v_1, v_2, there is one vector from the protected subspace,

$$|\xi_{v_1,v_2}\rangle \;=\; 2^{-(k^2-1)/2} \sum_{z_1,\ldots,z_n} |z_1,\ldots,z_n\rangle \quad : \quad \sum_{j\in c_{z1}} z_j = v_1, \quad \sum_{j\in c_{z2}} z_j = v_2 \tag{3}$$

Of course, one can also create linear combinations of these vectors.

Now we are to show that the code TOR(k) detects $k-1$ errors[5] (hence, it corrects $\lfloor \frac{k-1}{2} \rfloor$ errors). Consider a multiple error

$$E \;=\; \sigma(\alpha_1,\ldots,\alpha_n;\,\beta_1,\ldots,\beta_n) \;=\; \prod_j (\sigma_j^x)^{\alpha_j} \prod_j (\sigma_j^z)^{\beta_j} \qquad (\alpha_j,\beta_j = 0,1)$$

This error can not be detected by syndrome measurement (i.e. by measuring the eigenvalues of all A_s, B_j) if and only if $E \in \mathcal{G}$. However, if $E \in \mathcal{F}$ then $E|\xi\rangle = |\xi\rangle$ for every $|\xi\rangle \in \mathcal{L}$. Such an error is not an error at all — it does not affect the protected subspace. The bad case is when $E \in \mathcal{G}$ but $E \notin \mathcal{F}$. Hence, the support of E should contain a non-contractible loop or cut. It is only possible if $|\operatorname{Supp}(E)| \geq k$. (Here $\operatorname{Supp}(E)$ is the set of j for which $\alpha_j \neq 0$ or $\beta_j \neq 0$).

One may say that the toric codes have quite poor parameters. Well, they are not "good" codes in the sense of [17]. However, the code TOR(k) corrects *almost any* multiple error of size $O(k^2)$. (The constant factor in $O(\ldots)$ is related to the percolation problem). So, these codes work if the error rate is constant but smaller than some threshold value. The nicest property of the codes TOR(k) is that they are *local check codes*. Namely,

1. Each stabilizer operators involves bounded number of qubits (at most 4).

2. Each qubit is involved in a bounded number of stabilizer operators (at most 4).

[5] In the theory of quantum codes, the word "error" is used in a somewhat confusing manner. Here it means a single qubit error. In most other cases, like in the formula below, it means a multiple error, i.e. an arbitrary operator $E \in \mathbf{L}(\mathcal{N})$.

3. There is no limit for the number of errors that can be corrected.

Also, at a constant error rate, the unrecoverable error probability goes to zero as $\exp(-ak)$.

It has been already mentioned that error detection involves syndrome measurement. To correct the error, one needs to find its characteristic vector $(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n)$ out of the syndrome. This is the usual error correction scheme. A new suggestion is to perform error correction at the physical level. Consider the Hamiltonian

$$H_0 \;=\; -\sum_s A_s \;-\; \sum_p B_p \tag{4}$$

Diagonalizing this Hamiltonian is an easy job because the operators A_s, B_p commute. In particular, the ground state coincides with the protected subspace of the code TOR(k); it is 4-fold degenerate. All excited states are separated by an energy gap $\Delta E \geq 2$, because the difference between the eigenvalues of A_s or B_p equals 2. This Hamiltonian is more or less realistic because in involves only *local* interactions. We can expect that "errors", i.e. noise-induced excitations will be removed automatically by some relaxation processes. Of course, this requires cooling, i.e. some coupling to a thermal bath with low temperature (in addition to the Hamiltonian (4)).

Now let us see whether this model is stable to perturbation. (If not, there is no practical use of it). For example, consider a perturbation of the form

$$V \;=\; -\vec{h}\sum_j \vec{\sigma}_j \;-\; \sum_{j<p} J_{jp}(\vec{\sigma}_j, \vec{\sigma}_p)$$

It is important that the perturbation is local, i.e. each term of it contains a small number of σ (at most 2). Let us estimate the energy splitting between two orthogonal ground states of the original Hamiltonian, $|\xi\rangle \in \mathcal{L}$ and $|\eta\rangle \in \mathcal{L}$. We can use the usual perturbation theory because the energy spectrum has a gap. In the m-th order of the perturbation theory, the splitting is proportional to $\langle\xi|V^m|\eta\rangle$ or $\langle\xi|V^m|\xi\rangle - \langle\eta|V^m|\eta\rangle$. However, both quantities are zero unless V^m contains a product of σ_j^z or σ_j^x along a non-contractible loop or cut. Hence, the splitting appears only in the $\lceil k/2 \rceil$-th or higher orders. As far as all things (like the number of the relevant terms in V^m) scale correctly to the thermodynamic limit, the splitting vanishes as $\exp(-ak)$. A simple physical interpretation of this result is given in the next section. (Of course, the perturbation should be small enough, or else a phase transition may occur).

Note that our construction is not restricted to square lattices. We can consider an arbitrary irregular lattice, like in fig. 6. Moreover, such a lattice can be drawn on an arbitrary 2-D surface. On a compact orientable surface of genus g, the ground state is 4^g-fold degenerate. In this case, the splitting of the ground state is estimated as $\exp(-aL)$, where L is the smallest dimension of the lattice. We see that the ground state degeneracy depends on the surface topology, so we deal with *topological quantum order*. On the other hand, there is a finite energy gap between the ground state and excited states, so all spatial correlation functions decay exponentially. This looks like a paradox — how do parts of a macroscopic system know about the topology if all correlations are already lost at small scales? The answer is that there is long-range entanglement [6] which can not be expressed by simple correlation functions like $\langle\sigma_j^a\sigma_l^b\rangle$. This entanglement reveals itself in the excitation properties we are going to discuss.

[6] Entanglement is a special, purely quantum form of correlation.

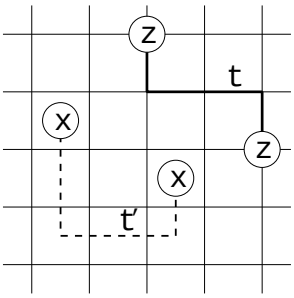


Figure 3: Strings and particles

2 Abelian anyons

Let us classify low-energy excitations of the Hamiltonian (4). An eigenvector of this Hamiltonian is an eigenvector of all the operators A_s, B_p. An *elementary excitation*, or *particle* occurs if only one of the constraints $A_s|\xi\rangle = |\xi\rangle$, $B_p\xi\rangle = |\xi\rangle$ is violated. Because of the relations $\prod_s A_s = 1$ and $\prod_p B_p = 1$, it is impossible to create a single particle. However, it is possible to create a two-particle state of the form $|\psi^z(t)\rangle = S^z(t)|\xi\rangle$ or $|\psi^x(t')\rangle = S^x(t')|\xi\rangle$, where $|\xi\rangle$ is an arbitrary ground state, and

$$S^z(t) \;=\; \prod_{j\in t} \sigma_j^z \qquad\qquad S^x(t') \;=\; \prod_{j\in t'} \sigma_j^x \tag{5}$$

(see fig. 3). In the first case, two particles are created at the endpoints of the "string" (non-closed path) t. Such particles live on the vertices of the lattice. We will call them z-type particles, or "electric charges". Correspondingly, x-type particles, or "magnetic vortices" live on the faces. The operators $S^z(t)$, $S^x(t')$ are called *string operators*. Their characteristic property is as follows: they commute with every A_s and B_p, except for few ones (namely, 2) corresponding to the endpoints of the string. Note that the state $|\psi^z(t)\rangle = S^z(t)|\xi\rangle$ depends only on the homotopy class of the path t while the operator $S^z(t)$ depends on t itself.

Any configuration of an even number of z-type particles and an even number of x-type particles is allowed. We can connect them by strings in an arbitrary way. Each particle configuration defines a 4^g-dimensional subspace in the global Hilbert space $\mathcal{N}$. This subspace is independent of the strings but a particular vector $S^{a_1}(t_1)\cdots S^{a_m}(t_m)|\xi\rangle$ depends on $t_1,\ldots,t_m$. If we draw these strings in a topologically different way, we get another vector in the same 4^g-dimensional subspace. Thus, the strings are unphysical but we can not get rid of them in our formalism.

Let us see what happens if these particles move around the torus (or other surface). Moving a z-type particle along the path c_{z1} or c_{z2} (see fig. 2) is equivalent to applying the operator Z_1 or Z_2. Thus, we can operate on the ground state space by creating a particle pair, moving one of the particles around the torus, and annihilating it with the other one. Thus we can realize some quantum gates. Unfortunately, too simple ones — we can only apply the operators σ_z and σ_x to each of the 2 (or $2g$) qubits encoded in the ground state.

Now we can give the promised physical interpretation of the ground state splitting. In the presence of perturbation, the two-particle state $|\psi^z(t)\rangle$ is not an eigenstate any more. More exactly, both particles will propagate rather than stay at the same positions. The propagation process is described by the Schrödinger equation with some effective mass m_z. (x-type particles have another mass m_x). In the non-perturbed model, $m_z = m_x = \infty$. There are no real particles

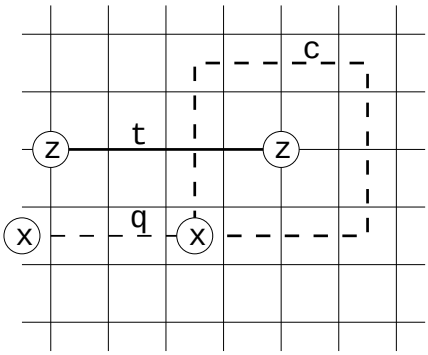


Figure 4: An x-type particle moving around a z-type particle

in the ground state, but they can be created and annihilate virtually. A virtual particle can tunnel around the torus before annihilating with the other one. Such processes contribute terms $b_{z1}Z_1$, $b_{z2}Z_2$, $b_{x1}X_1$, $b_{x2}X_2$ to the ground state effective Hamiltonian. Here $b_{\alpha i} \sim \exp(-a_\alpha L_i)$ is the tunneling amplitude whereas $a_\alpha \sim \sqrt{2m\Delta E}$ is the imaginary wave vector of the tunneling particle.

Next question: what happens if we move particles around each other? (For this, we don't need a torus; we can work on the plane). For example, let us move an x-type particle around a z-type particle (see fig. 4). Then

$$|\Psi_{\text{initial}}\rangle \;=\; S^z(t)\,|\psi^x(q)\rangle\;, \qquad\qquad |\Psi_{\text{final}}\rangle \;=\; S^x(c)\,S^z(t)\,|\psi^x(q)\rangle \;=\; -|\Psi_{\text{initial}}\rangle$$

because $S^x(c)$ and $S^z(t)$ anti-commute, and $S^x(c)|\psi^x(q)\rangle = |\psi^x(q)\rangle$. We see that the global wave function (= the state of the entire system) acquires the phase factor -1. It is quite unlike usual particles, bosons and fermions, which do not change their phase in such a process. Particles with this unusual property are called *abelian anyons*. More generally, abelian anyons are particles which realize nontrivial one-dimensional representations of (colored) braid groups. In our case, the phase change can be also interpreted as an Aharonov-Bohm effect. It does not occur if both particles are of the same type.

Note that abelian anyons exist *in real solid state systems*, namely, they are intrinsicly related to the fractional quantum Hall effect [18]. However, these anyons have different braiding properties. In the fractional quantum Hall system with filling factor p/q, there is only one basic type of anyonic particles with (real) electric charge $1/q$. (Other particles are thought to be composed from these ones). When one particle moves around the other, the wave function acquires a phase factor $\exp(2\pi i/q)$.

Clearly, the existence of anyons and the ground state degeneracy have the same nature. They both are manifestations of a topological quantum order, a hidden long-range order that can not be described by any local order parameter. (The existence of a local order parameter contradicts the nature of a quantum code — if the ground state is accessible to local measurements then it is not protected from local errors). It seems that the anyons are more fundamental and can be used as a universal probe for this hidden order. Indeed, *the ground state degeneracy on the torus follows from the existence of anyons* [19]. Here is the original Einarsson's proof applied to our two types of particles.

We derived the ground state degeneracy from the commutation relations between the operators Z_1, Z_2, X_1, X_2. These operators can be realized by moving particles along the loops

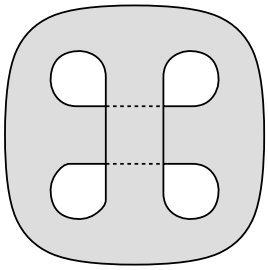


Figure 5: A fly-over crossing geometry for a 2-D electron layer

c_{z1}, c_{z2}, c_{x1}, c_{x2}. These loops only exist on the torus, not on the plane. Consider, however, the process in which an x-type particle and a z-type particle go around the torus and then trace their paths backward. This corresponds to the operator $W = X_1^{-1} Z_1^{-1} X_1 Z_1$ which can be realized on the plane. Indeed, we can deform particles' trajectories so that one particle stays at rest while the other going around it. Due to the anyonic nature of the particles, $W = -1$. We see that X_1 and Z_1 anti-commute.

The above argument is also applicable to the fractional quantum Hall anyons [19]. The ground state on the torus is q-fold degenerate, up to the precision $\sim \exp(-L/l_0)$, where l_0 is the magnetic length. This result does not rely on the magnetic translational symmetry or any other symmetry. Rather, it relies on the existence of the energy gap in the spectrum (otherwise the degeneracy would be unstable to perturbation). Note that holes (=punctures) in the torus do not remove the degeneracy unless they break the nontrivial loops c_{x1}, c_{x2}, c_{z1}, c_{z2}. The fly-over crossing geometry (see fig. 5) is topologically equivalent to a torus with 2 holes, but it is almost flat. In principle, such structure can be manufactured [7], cooled down and placed into a perpendicular magnetic field. This will be a sort of quantum memory — it will store a quantum state forever, provided all anyonic excitation are frozen out or localized. Unfortunately, I do not know any way this quantum information can get in or out. Too few things can be done by moving abelian anyons. All other imaginable ways of accessing the ground state are uncontrollable.

3 Materialized symmetry: is that a miracle?

Anyons have been studied extensively in the gauge field theory context [9, 10, 11, 13]. However, we start with quite different assumptions about the Hamiltonian. A gauge theory implies a gauge symmetry which can not be removed by external perturbation. To the contrary, our model is stable to *arbitrary* local perturbations. It is useful to give a field-theoretic interpretation of this model. The edge labels z_j (measurable by σ_j^z) correspond to a $\mathbb{Z}_2$ vector potential, whereas σ_j^x corresponds to the electric field. The operators A_s are local gauge transformations whereas B_p is the magnetic field on the face p. The constraints $A_s|\xi\rangle = |\xi\rangle$ mean that the state $|\xi\rangle$ is gauge-invariant. Violating the gauge invariance is energetically unfavorable but not forbidden. The Hamiltonian (which includes H_0 and some perturbation V) need not obey the gauge symmetry. The constraints $B_p|\xi\rangle = |\xi\rangle$ mean that the gauge field corresponds to a flat connection. These constraints are not strict either.

[7] It is not easy. How will the two layers (the two crossing "roads", one above the other) join in a single crystal layout?

Despite the absence of symmetry in the Hamiltonian $H = H_0 + V$, our system exhibits two conservation laws: electric charge and magnetic charge (i.e. the number of vortices) are both conserved *modulo* 2. In the usual electrodynamics, conservation of electric charge is related to the local (=gauge) $\mathbf{U}(1)$ symmetry. In our case, it should be a local $\mathbb{Z}_2$ symmetry for electric charges and another $\mathbb{Z}_2$ symmetry for magnetic vortices. So, our system exhibits a *dynamically created* $\mathbb{Z}_2 \times \mathbb{Z}_2$ symmetry which appears only at large distances where individual excitations are well-defined.

Probably, the reader is not satisfied with this interpretation. Really, it creates a new puzzle rather than solve an old one. What is this mysterious symmetry? How do symmetry operators look like at the microscopic level? The answer sounds as nonsense but it is true. This symmetry (as well as any other local symmetry) can be found in *any* Hamiltonian if we introduce some unphysical degrees of freedom. So, the symmetry is not actually being created. Rather, an artificial symmetry becomes a real one.

The new degrees of freedom are spin variables $v_s, w_p = 0, 1$ for each vertex s and each face p. The vertex spins will stay in the state $2^{-1/2}\Big(|0\rangle + |1\rangle\Big)$ whereas the face spins will stay in the state $|0\rangle$. So, all the extra spins together stay in a unique quantum state $|\zeta\rangle$. Obviously, $\sigma_s^x|\zeta\rangle = |\zeta\rangle$ and $\sigma_p^z|\zeta\rangle = |\zeta\rangle$, for every vertex s and every face p. From the mathematical point of view, we have simply defined an embedding of the space $\mathcal{N}$ into a larger Hilbert space $\mathcal{T}$ of all the spins, $|\psi\rangle \mapsto |\psi\rangle \otimes |\zeta\rangle$. So we may write $\mathcal{N} \subseteq \mathcal{T}$. We will call $\mathcal{N}$ the *physical space* (or subspace), $\mathcal{T}$ the *extended space*. Physical states (i.e. vectors $|\psi\rangle \in \mathcal{N}$) are characterized by the equations

$$\sigma_s^x|\psi\rangle \;=\; |\psi\rangle \;, \qquad \sigma_p^z|\psi\rangle \;=\; |\psi\rangle$$

for every vertex s and face p.

Now let us apply a certain unitary transformation U on the extended space $\mathcal{T}$. This transformation is just a change of the spin variables, namely

$$v_s \;\mapsto\; v_s \;, \qquad z_j \;\mapsto\; z_j \,+ \sum_{s=\text{endpoint}(j)} v_s \;, \qquad w_p \;\mapsto\; w_p \,+ \sum_{j\in\text{boundary}(p)} z_j \tag{6}$$

(all sums are taken *modulo* 2). The physical subspace becomes $\mathcal{N}' = U\mathcal{N}$. Vectors $|\psi\rangle \in \mathcal{N}'$ are invariant under the following symmetry operators

$$P_s \;=\; U\sigma_s^x U^\dagger \;=\; \sigma_s^x\, A_s \qquad\qquad Q_p \;=\; U\sigma_p^z U^\dagger \;=\; \sigma_p^z\, B_p \tag{7}$$

The transformed Hamiltonian $H' = UHU^\dagger$ commutes with these operators. It is defined up to the equivalence $P_s \equiv 1$, $Q_p \equiv 1$. In particular,

$$H_0' \;=\; U\, H_0\, U^\dagger \;=\; H_0' \;\equiv\; -\sum_s \sigma_s^x \,- \sum_p \sigma_p^z \tag{8}$$

In the field theory language, the vertex variables v_s (or the operators σ_s^z) are a Higgs field. The operators P_s are local gauge transformations. Thus, an arbitrary Hamiltonian can be written in a gauge-invariant form if we introduce additional Higgs fields. Of course, it is a very simple observation. The real problem is to understand how the artificial gauge symmetry "materialize", i.e. give rise to a physical conservation law.

Electric charge at a vertex s is given by the operator σ_s^x. The total electric charge on a compact surface is zero[8] because $\prod_s \sigma_s^x \equiv 1$. This is not a physically meaningful statement as it is. It is only meaningful if there are discrete charged particles. Then the charge is also conserved locally, in every scattering or fusion process. It is difficult to formulate this property in a mathematical language, but, hopefully, it is possible. (The problem is that particles are generally smeared and can propagate. Physically, particles are well-defined if they are stable and have finite energy gap). Alternatively, one can use various local and nonlocal order parameters to distinguish between phases with an unbroken symmetry, broken symmetry or confinement.

The artificial gauge symmetry materialize for the Hamiltonian (8) but this is not the case for every Hamiltonian. Let us try to describe possible symmetry breaking mechanisms in terms of local order parameters. If the gauge symmetry is broken then there is a nonvanishing vacuum average of the Higgs field, $\phi(s) = \langle \sigma_s^z \rangle \neq 0$. Electric charge is not conserved any more. In other words, there is a Bose condensate of charged particles. Although the second $\mathbb{Z}_2$ symmetry is formally unbroken, free magnetic vortices do not exist. More exactly, magnetic vortices are confined. (The duality between symmetry breaking and confinement is well known [25]). It is also possible that the second symmetry is broken, then electric charges are confined. From the physical point of view, these two possibilities are equivalent: there is no conservation law in the system.[9]

An interesting question is whether magnetic vortices can be confined without the gauge symmetry being broken. Apparently, the answer is "no". The consequence is significant: electric charges and magnetic vortices can not exist without each other. It seems that materialized symmetry needs better understanding; as presented here, it looks more like a miracle.

4 The model based on a group algebra

From now on, we are constructing and studying nonabelian anyons which will allow universal quantum computation.

Let G be a finite (generally, nonabelian) group. Denote by $\mathcal{H} = \mathbb{C}[G]$ the corresponding group algebra, i.e. the space of formal linear combinations of group elements with complex coefficients. We can consider $\mathcal{H}$ as a Hilbert space with a standard orthonormal basis $\Big\{ |g\rangle : g \in G \Big\}$. The dimensionality of this space is $N = |G|$. We will work with "spins" (or "qubits") taking values in this space.[10] *Remark*: This model can be generalized. One can take for $\mathcal{H}$ any finite-dimensional Hopf algebra equipped with a Hermitian scalar product with certain properties. However, I do not want to make things too complicated.

To describe the model, we need to define 4 types of linear operators, L_+^g, L_-^g, T_+^h, T_-^h acting on the space $\mathcal{H}$. Within each type, they are indexed by group elements, $g \in G$ or $h \in G$. They act as follows

$$\begin{array}{rclcrcl} L_+^g|z\rangle &=& |gz\rangle & & T_+^h|z\rangle &=& \delta_{h,z}\,|z\rangle \\ L_-^g|z\rangle &=& |zg^{-1}\rangle & & T_-^h|z\rangle &=& \delta_{h^{-1},\,z}\,|z\rangle \end{array} \qquad (9)$$

[8] Strictly speaking, the electric charge is not a numeric quantity; rather, it is an irreducible representation of the group $\mathbb{Z}_2$. "Zero" refers to the identity representation.

[9] The two possibilities only differ if an already materialized symmetry breaks down at much large distances (lower energies).

[10] In the field theory language, the value of a spin can be interpreted as a G gauge field. However, we do *not* perform symmetrization over gauge transformations.

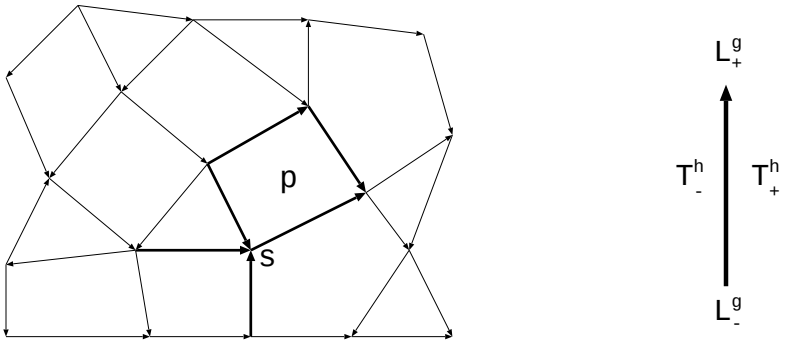


Figure 6: Generic lattice and the orientation rules for the operators $L^g_\pm$ and $T^h_\pm$

(In the Hopf algebra context, the operators L^g_+, L^g_-, T^h_+, T^h_- correspond to the left and right multiplications and left and right comultiplication, respectively). These operators satisfy the following commutation relations

$$\begin{aligned} L^g_+\, T^h_+ &= T^{gh}_+\, L^g_+ & \qquad L^g_+\, T^h_- &= T^{hg^{-1}}_-\, L^g_+ \\ L^g_-\, T^h_+ &= T^{hg^{-1}}_+\, L^g_- & \qquad L^g_-\, T^h_- &= T^{gh}_-\, L^g_- \end{aligned} \tag{10}$$

Now consider an arbitrary lattice on an arbitrary orientable 2-D surface, see fig. 6. (We will mostly work with a plane or a sphere, not higher genus surfaces). Corresponding to each edge is a spin which takes values in the space $\mathcal{H}$. Arrows in fig. 6 mean that we choose some orientation for each edge of the lattice. (Changing the direction of a particular arrow will be equivalent to the basis change $|z\rangle \mapsto |z^{-1}\rangle$ for the corresponding qubit). Let j be an edge of the lattice, s one of its endpoints. Define an operator $L^g(j,s) = L^g_\pm(j)$ as follows. If s is the origin of the arrow j then $L^g(j,s)$ is $L^g_-(j)$ (i.e. L^g_- acting on the j-th spin), otherwise it is $L^g_+(j)$. This rule is represented by the diagram at the right side of fig. 6. Similarly, if p is the left (the right) ajacent face of the edge j then $T^h(j,p)$ is T^h_- (resp. T^h_+) acting on the j-th spin.

Using these notations, we can define local gauge transformations and magnetic charge operators corresponding to a vertex s and an adjacent face p (see fig. 6). Put

$$\begin{aligned} A_g(s,p) &= A_g(s) = \prod_{j\in \mathrm{star}(s)} L^g(j,s) \\ B_h(s,p) &= \sum_{h_1\cdots h_k = h} \prod_{m=1}^{k} T^{h_m}(j_m,p) \end{aligned} \tag{11}$$

where $j_1,\ldots,j_k$ are the boundary edges of p listed in the counterclockwise order, starting from, and ending at, the vertex s. (The sum is taken over all combinations of $h_1,\ldots,h_k \in G$, such that $h_1\cdots h_k = h$. Order is important here!). Although $A_g(s,p)$ does not depend on p, we retain this parameter to emphasize the duality between $A_g(s,p)$ and $B_h(s,p)$. [11] These operators generate an algebra $\mathcal{D} = \mathbf{D}(G)$, Drinfield's quantum double [20] of the group algebra $\mathbb{C}[G]$. It will play a very important role below. Now we only need two symmetric combinations of $A_g(s,p)$ and $B_h(s,p)$, namely

$$A(s) = N^{-1}\sum_{g\in G} A_g(s,p) \qquad\qquad B(p) = B_1(s,p) \tag{12}$$

[11] In the Hopf algebra setting, $A_g(s,p)$ does depend on p.

where $N = |G|$. Both $A(s)$ and $B(p)$ are projection operators. ($A(s)$ projects out the states which are gauge invariant at s, whereas $B(p)$ projects out the states with vanishing magnetic charge at p). The operators $A(s)$ and $B(p)$ commute with each other.[12] Also $A(s)$ commutes with $A(s')$, and $B(p)$ commutes with $B(p')$ for different vertices and faces. In the case $G = \mathbb{Z}_2$, these operators are almost the same as the operators (1), namely $A(s) = \frac{1}{2}(A_s + 1)$, $B(p) = \frac{1}{2}(B_p + 1)$. [13]

At this point, we have only defined the global Hilbert space $\mathcal{N}$ (the tensor product of many copies of $\mathcal{H}$) and some operators on it. Now let us define the Hamiltonian.

$$H_0 \;=\; \sum_s (1 - A(s)) \;+\; \sum_p (1 - B(p)) \tag{13}$$

It is quite similar to the Hamiltonian (4). As in that case, the space of ground states is given by the formula

$$\mathcal{L} \;=\; \Big\{\, |\xi\rangle \in \mathcal{N} \;:\;\; A(s)|\xi\rangle = |\xi\rangle,\;\; B(p)|\xi\rangle = |\xi\rangle \text{ for all } s, p \,\Big\} \tag{14}$$

The corresponding energy is 0; all excited states have energies ≥ 1.

It is easy to work out an explicit representation of ground states similar to eq. (3). The ground states correspond 1-to-1 to flat G-connections, defined up to conjugation, or superpositions of those. So, the ground state on a sphere is not degenerate. However, particles (excitations) have quite interesting properties even on the sphere or on the plane. (We treat the plane as an infinitely large sphere). The reader probably wants to know the answer first, and then follow formal calculations. So, I give a brief abstract description of these particles. It is a mixture of general arguments and details which require verification.

The particles live on vertices or faces, or both; in general, one particle occupies a vertex and an adjacent face same time. A combination of a vertex and an adjacent face will be called a *site*. Sites are represented by dotted lines in fig. 7. (The dashed lines are edges of the dual lattice).

Consider n particles on the sphere pinned to particular sites $x_1, \ldots, x_n$ at large distances from each other. The space $\mathcal{L}[n] = \mathcal{L}(x_1, \ldots, x_n)$ of n-particle states has dimensionality $N^{2(n-1)}$, including the ground state.[14] Not all these states have the same energy. Even more splitting occurs under perturbation, but some degeneracy still survive. Of course, we assume that the perturbation is local, i.e. it can be represented by a sum of operators each of which acts only on few spins. To find the residual degeneracy, we will study the action of such *local operators* on the space $\mathcal{L}[n]$. Local operators generate a subalgebra $\mathcal{P}[n] \subseteq \mathbf{L}(\mathcal{L}[n])$. Elements of its center, $\mathcal{C}[n]$, are conserved classical quantities; they can be measured once and never change. (More exactly, they can not be changed by local operators). As these classical variables are locally measurable, we interpret them as particle's types. It turns out that the types correspond 1-to-1 to irreducible representations of the algebra $\mathcal{D}$, the quantum double. Thus, each particle can belong to one of these types. The space $\mathcal{L}[n]$ and the algebra $\mathcal{P}[n]$ split accordingly:

$$\mathcal{L}[n] \;=\; \bigoplus_{d_1,\ldots,d_n} \mathcal{L}_{d_1,\ldots,d_n} \qquad \mathcal{P}[n] \;=\; \bigoplus_{d_1,\ldots,d_n} \mathcal{P}_{d_1,\ldots,d_n} \qquad \Big(\, \mathcal{P}_{d_1,\ldots,d_n} \subseteq \mathbf{L}(\mathcal{L}_{d_1,\ldots,d_n}) \,\Big) \tag{15}$$

[12] This is not obvious. Use the commutation relations (10) to verify this statement.

[13] Here A_s and B_p are the notations from Sec. 1; we will not use them any more.

[14] The absence of particle at a given site is regarded as a particle of special type.

where d_m is the type of the m-th particle. The "classical" subalgebra $\mathcal{C}[n]$ is generated by the projectors onto $\mathcal{L}_{d_1,\ldots,d_n}$.

But this is not the whole story. The subspace $\mathcal{L}_{d_1,\ldots,d_n}$ splits under local perturbations from $\mathcal{P}_{d_1,\ldots,d_n}$. By a general mathematical argument,[15] this algebra can be characterized as follows

$$\mathcal{L}_{d_1,\ldots,d_n} \;=\; \mathcal{K}_{d_1,\ldots,d_n} \otimes \mathcal{M}_{d_1,\ldots,d_n} \qquad\qquad \mathcal{P}_{d_1,\ldots,d_n} \;=\; \mathbf{L}(\mathcal{K}_{d_1,\ldots,d_n}) \tag{16}$$

The space $\mathcal{K}_{d_1,\ldots,d_n}$ corresponds to local degrees of freedom. They can be defined independently for each particle. So, $\mathcal{K}_{d_1,\ldots,d_n} = \mathcal{K}_{d_1} \otimes \cdots \otimes \mathcal{K}_{d_n}$, where $\mathcal{K}_{d_m}$ is the space of "subtypes" (internal states) of the m-th particle. Like the type, the subtype of a particle is accessible by local measurements. However, it can be changed, while the type can not.

The most interesting thing is the *protected space* $\mathcal{M}_{d_1,\ldots,d_n}$. It is not accessible by local measurements and is not sensitive to local perturbations, unless the particles come close to each other. This is an ideal place to store quantum information and operate with it. Unfortunately, the protected space does not have tensor product structure. However, it can be described as follows. Associated with each particle type a is an irreducible representation $\mathcal{U}_d$ of the quantum double $\mathcal{D}$. Consider the product representation $\mathcal{U}_{d_1} \otimes \cdots \otimes \mathcal{U}_{d_n}$ and split it into components corresponding to different irreducible representations. The protected space is the component corresponding to the identity representation.

If we swap two particles or move one around the other, the protected space undergoes some unitary transformation. Thus, the particles realize some multi-dimensional representation of the braid group. Such particles are called *nonabelian anyons*. Note that braiding does not affect the local degrees of freedom. If two particles fuse, they can annihilate or become another particle. The protected space becomes smaller but some classical information comes out, namely, the type of the new particle. So, the we can do measurements on the protected space. Finally, if we create a new pair of particles of definite types, it always comes in a particular quantum state. So, we have a standard toolkit for quantum computation (new states, unitary transformations and measurements), except that the Hilbert space does not have tensor product structure. Universality of this toolkit is a separate problem, see Sec. 7.

Our model gives rise to the same braiding and fusion rules as gauge field theory models [10, 11]. The existence of local degrees of freedom (subtypes) is a new feature. These degrees of freedom appear because there is no explicit gauge symmetry in our model.

5 Algebraic structure

5.1 Particles and local operators

This subsection is also rather abstract but the claims we do are concrete. They will be proven in Sec. 5.4.

As mentioned above, the ground state of the Hamiltonian (13) is not degenerate (on the sphere or on the plane regarded as an infinitely large sphere). Excited states are characterized by their energies. The energy of an eigenstate $|\psi\rangle$ is equal to the number of constraints $(A(s)-1)|\psi\rangle = 0$ or $(B(p)-1)|\psi\rangle = 0$ which are violated. Complete classification of excited states is a difficult problem. Instead of that, we will try to classify *elementary* excitations, or particles.

[15] $\mathcal{P}_{d_1,\ldots,d_n}$ is a subalgebra of $\mathbf{L}(\mathcal{L}_{d_1,\ldots,d_n})$ with a trivial center, closed under Hermitian conjugation.

Let us formulate the problem more precisely. Consider a few excited "spots" separated by large distances. Each spot is a small region where some of the constrains are violated. The energy of a spot can be decreased by local operators but, generally, the spot can not disappear. Rather, it shrinks to some minimal excitation (which need not be unique). We will see (in Sec. 5.4) that any excited spot can be transformed into an excitation which violates at most 2 constraints, $A(s) - 1 \equiv 0$ and $B(p) - 1 \equiv 0$, where s is an arbitrary vertex, and p is an adjacent face. Such excitations are be called *elementary excitations*, or *particles*. Note that definition of elementary excitations is a matter of choice. We could decide that an elementary excitation violates 3 constraints. Even with our definition, the "space of elementary excitations" is redundant.

By the way, the space of elementary excitations is not well defined because such an excitation does not exist alone. More exactly, the only one-particle state on the sphere is the ground state. (This can be proven easily). The right thing is the space of two-particle excitations, $\mathcal{L}(a,b)$. Here $a = (s,p)$ and $b = (s',p')$ are the sites occupied by the particles. (Recall that a site is a combination of a vertex and an adjacent face). The projector onto $\mathcal{L}(a,b)$ can be written as $\prod_{r\neq s,s'} A(r) \prod_{l\neq p,p'} B(l)$. Note that introducing a third particle (say, c) will not give more freedom for any of the two. Indeed, b and c can fuse without any effect on a.

Let us see how local operators act on the space $\mathcal{L}(a,b)$. In this context, a local operator is an operator which acts only on spins near a (or near b). Besides that, it should preserve the subspace $\mathcal{L}(a,b) \subseteq \mathcal{N}$ and its orthogonal complement. ($\mathcal{N}$ is the space of all quantum states). Example: the operators $A_g(a)$ and $B_h(a)$, where $a = (s,p)$, commute with $A(r)$, $B(l)$ for all $r \neq s$ and $l \neq p$. Hence, they commute with the projector onto the subspace $\mathcal{L}(a,b)$. These operators generate an algebra $\mathcal{D}(a) \subset \mathbf{L}(\mathcal{N})$. It will be shown in Sec. 5.4 that $\mathcal{D}(a)$ includes *all* local operators acting on the space $\mathcal{L}(a,b)$, and the action of $\mathcal{D}(a)$ on $\mathcal{L}(a,b)$ is *exact* (i.e. different operators act differently).

Actually, the algebra $\mathcal{D}(a) = \mathcal{D}$ does not depend on a, only the embedding $\mathcal{D} \to \mathbf{L}(\mathcal{N})$ does. This algebra is called the *quantum double* of the group G and denoted by $\mathbf{D}(G)$. Its structure is determined by the following relations between the operators $A_g = A_g(a)$ and $B_h = B_h(a)$

$$A_f\, A_g \;=\; A_{fg} \qquad\qquad B_h\, B_i \;=\; \delta_{h,i}\, B_h \qquad\qquad A_g\, B_h \;=\; B_{ghg^{-1}} A_g \tag{17}$$

The operators $D_{(h,g)} = B_h A_g$ form a linear basis of $\mathcal{D}$. (In [10, 11] these operators were denoted by ${}^{h}\!\llcorner_{g}$). The following multiplication rules hold

$$D_{(h_1,g_1)} D_{(h_2,g_2)} \;=\; \delta_{h_1,\, g_1 h_2 g_1^{-1}}\, D_{(h_1,\, g_1 g_2)}$$

This identity can be also written in a symbolic tensor form, with h and g being combined into one index:

$$D_{\boldsymbol{m}}\, D_{\boldsymbol{n}} \;=\; \Omega^{\boldsymbol{k}}_{\boldsymbol{mn}}\, D_{\boldsymbol{k}} \qquad\qquad \Omega^{(h,g)}_{(h_1,g_1)\,(h_2,g_2)} \;=\; \delta_{h_1,\, g_1 h_2 g_1^{-1}}\; \delta_{h,h_1}\; \delta_{g,\, g_1 g_2} \tag{18}$$

(summation over $\boldsymbol{k}$ is implied). Actually, $\mathcal{D}$ is not only an algebra, it is a quasi-triangular Hopf algebra, see Secs. 5.2, 5.3.

Note that $\mathcal{D} = \mathcal{D}(a)$ is closed under Hermitian conjugation (in $\mathbf{L}(\mathcal{N})$) which acts as follows

$$A_g^\dagger \;=\; A_{g^{-1}} \qquad\qquad B_h^\dagger \;=\; B_h \qquad\qquad D_{(h,g)}^\dagger \;=\; D_{(g^{-1}hg,\, g^{-1})} \tag{19}$$

Thus, $\mathcal{D} = \mathcal{D}(a)$ is a finite-dimensional C^*-algebra. Hence it has the following structure

$$\mathcal{D} \;=\; \bigoplus_d \mathbf{L}(\mathcal{K}_d) \tag{20}$$

where d runs over all irreducible representations of $\mathcal{D}$. We can interpret d as particle's type.[16] The absence of particle corresponds to a certain one-dimensional representation called the *identity representation*. More exactly, the operators $D_{(h,g)}$ act on the ground state $|\xi\rangle$ as follows

$$D_{\boldsymbol{k}}\,|\xi\rangle \;=\; \varepsilon_{\boldsymbol{k}}\,|\xi\rangle \qquad\qquad \text{where} \quad \varepsilon_{(h,g)} \;=\; \delta_{h,1} \tag{21}$$

The "space of subtypes", $\mathcal{K}_d$ actually characterize the redundancy of our definition of elementary excitations. However, this redundancy is necessary to have a nice theory of ribbon operators (see Sec. 5.2).

Irreducible representations of $\mathcal{D}$ can be described as follows [10]. Let $u \in G$ be an arbitrary element, $C = \{gug^{-1} : g \in G\}$ its conjugacy class, $E = \{g \in G : gu = ug\}$ its centralizer. There is one irreducible representation $d = (C, \chi)$ for each conjugacy class C and each irreducible representation χ of the group E (see below). It does not matter which element $u \in C$ is used to define E. The conjugacy class C can be interpreted as magnetic charge whereas χ corresponds to electric charge. For example, consider the group S_3 (the permutation group of order 3). It has 3 conjugacy classes of order 1, 2 and 3, respectively. So, the algebra $\mathbf{D}(S_3)$ has irreducible representations of dimensionalities 1,1,2; 2,2,2; 3,3.

The simplest case is when χ is the identity representation, i.e. the particle carries only magnetic charge but no electric charge. Then the subtypes can be identified with the elements of C, i.e. the corresponding space (denoted by $\mathcal{B}_C$) has a basis $\{|v\rangle : v \in C\}$. The local operators act on this space as follows

$$D_{(h,g)}|v\rangle \;=\; \delta_{h,\,gvg^{-1}}\,|gvg^{-1}\rangle \tag{22}$$

Now consider the general case. Denote by $W_f = W_f^{(\chi)}$ the irreducible action of $f \in E$ on an appropriate space $\mathcal{A}_\chi$. Choose arbitrary elements $q_v \in G$ such that $q_v u q_v^{-1} = v$ for each $v \in C$. Then any element $g \in G$ can be uniquely represented in the form $g = q_v f$, where $v \in C$ and $f \in E$. We can define a unique action of $\mathcal{D}$ on $\mathcal{B}_C \otimes \mathcal{A}_\chi$, such that

$$\begin{aligned} B_h\Big(|v\rangle \otimes |\eta\rangle\Big) \;&=\; \delta_{h,v}\,|v\rangle \otimes |\eta\rangle \\ A_{q_v f}\Big(|u\rangle \otimes |\eta\rangle\Big) \;&=\; |v\rangle \otimes W_f|\eta\rangle \qquad\qquad (v \in C,\ f \in E) \end{aligned} \tag{23}$$

More generally, $D_{(h,g)}\Big(|v\rangle \otimes |\eta\rangle\Big) \;=\; \delta_{h,\,gvg^{-1}}\,|gvg^{-1}\rangle \otimes W_f|\eta\rangle$, where $f = q_v(q_{gvg^{-1}})^{-1}g$. This action is irreducible.

5.2 Ribbon operators

The next task is to construct a set of operators which can create an arbitrary two-particle state from the ground state. I do not know how to deduce an expression for such operators; I will

[16] *Caution.* The local operators should not be interpreted as symmetry transformations. The true symmetry transformations, so-called *topological operators*, will be defined in Sec. 6. Mathematically, they are described by the same algebra $\mathcal{D}$, but their action on physical states is different.

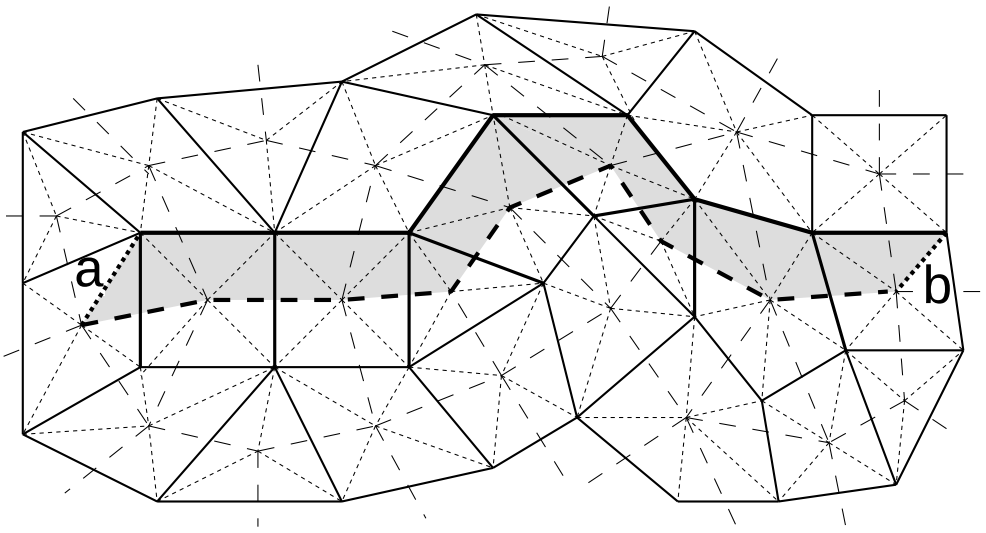


Figure 7: A ribbon on the lattice

just give an answer and explain why it is correct. In the abelian case (see Sec. 2) there were two types of such operators which corresponded to paths on the lattice and the dual lattice, respectively. In the nonabelian case, we have to consider both types of paths together. Thus, the operators creating a particle pair are associated with a *ribbon* (see fig. 7). The ribbon connects two sites at which the particles will appear (say, $a = (s, p)$ and $b = (s', p')$). The corresponding operators act on the edges which constitute one side of the ribbon (solid line), as well as the edges intersected by the other side (dashed line).

For a given ribbon t, there are N^2 *ribbon operators* $F^{(h,g)}(t)$ indexed by $g, h \in G$. They act as follows[17]

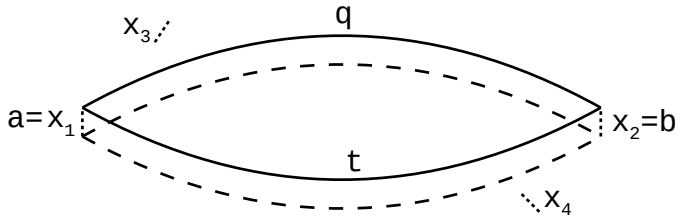
$$
\begin{array}{lll}
 & \overset{x_1}{\leftarrow} \overset{x_2}{\leftarrow} \overset{x_3}{\leftarrow} & \\
F^{(h,g)}(t) & \begin{array}{ccc} \uparrow y_1 & \uparrow y_2 & \uparrow y_3 \end{array} & = \\
 & \overset{x_1}{\leftarrow} \overset{x_2}{\leftarrow} \overset{x_3}{\leftarrow} & \\
= \quad \delta_{g,\, x_1 x_2 x_3} & \begin{array}{ccc} \uparrow hy_1 & \uparrow x_1^{-1} h x_1\, y_2 & \uparrow (x_1 x_2)^{-1} h (x_1 x_2)\, y_3 \end{array} &
\end{array}
\tag{24}
$$

These operators commute with every projector $A(r)$, $B(l)$, except for $r = s, s'$ and $l = p, p'$. This is the first important property of ribbon operators.

The operators $F^{(h,g)}(t)$ depend on the ribbon t. However, their action on the space $\mathcal{L}(a, b)$

[17] Horizontal and vertical arrows are the two types of edges. Each of the two diagrams (6 arrows with labels) stand for a particular basis vector

depends only on the *topological class* of the ribbon This is also true for a multi-particle excitation space $\mathcal{L}(x_1, \ldots, x_n)$. More exactly, consider two ribbons, t and q, connecting the sites $x_1 = a$ and $x_2 = b$ The actions of $F^{(h,g)}(t)$ and $F^{(h,g)}(q)$ on $\mathcal{L}(x_1, \ldots, x_n)$ coincide provided none of the



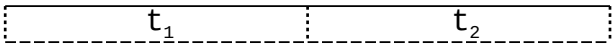
sites $x_3, \ldots, x_n$ lie on or between the ribbons. This is the second important property of ribbon operators. We will write $F^{(h,g)}(t) \equiv F^{(h,g)}(q)$, or, more exactly, $F^{(h,g)}(t) \overset{M}{\equiv} F^{(h,g)}(q)$, where $M = \{x_1, \ldots, x_n\}$.

Linear combination of the operators $F^{(h,g)}(t)$ are also called ribbon operators. They form an algebra $\mathcal{F}(t) \cong \mathcal{F}$. The multiplication rules are as follows

$$F^{\boldsymbol{m}}(t)\, F^{\boldsymbol{n}}(t) \;=\; \Lambda^{\boldsymbol{mn}}_{\boldsymbol{k}}\, F^{\boldsymbol{k}}(t) \qquad\qquad \Lambda^{(h_1,g_1)\,(h_2,g_2)}_{(h,g)} \;=\; \delta_{h_1 h_2, h}\; \delta_{g_1,g}\; \delta_{g_2,g} \tag{25}$$

(summation over $\boldsymbol{m}$ and $\boldsymbol{n}$ is implied).

Any ribbon operator on a long ribbon $t = t_1 t_2$ (see figure below) can be represented in terms of ribbon operators corresponding to its parts, t_1 and t_2



$$F^{\boldsymbol{k}}(t_1 t_2) \;=\; \Omega^{\boldsymbol{k}}_{\boldsymbol{mn}}\, F^{\boldsymbol{m}}(t_1)\, F^{\boldsymbol{n}}(t_2) \qquad\qquad \Omega^{(h,g)}_{(h_1,g_1)\,(h_2,g_2)} \;=\; \delta_{g,\, g_1 g_2}\; \delta_{h_1,h}\; \delta_{h_2,\, g_1^{-1} h g_1} \tag{26}$$

(Note that $F^{\boldsymbol{m}}(t_1)$ and $F^{\boldsymbol{n}}(t_2)$ commute because the ribbons t_1 and t_2 do ton overlap). By some miracle, the tensor $\Omega^{\star}_{\star\star}$ is the same as in eg. (18). From the mathematical point of view, eq. (26) defines a linear mapping $\Delta(t_1, t_2) :\ \mathcal{F}(t_1, t_2) \to \mathcal{F}(t_1) \otimes \mathcal{F}(t_2)$, or just $\Delta : \mathcal{F} \to \mathcal{F}$. Such a mapping is called a *comultiplication*.

The comultiplication rules (26) allow to give another definition of ribbon operators which is nicer than eq. (24). Note that a ribbon consists of triangles of two types (see fig. 7). Each triangle corresponds to one edge. More exactly, a triangle with two dotted sides and one dashed side corresponds to a combination of an edge and its endpoint, say, i and r. Similarly, a triangle with a solid side corresponds to a combination of an edge and one of the adjacent faces, say, j and l. Each triangle can be considered as a short ribbon. The corresponding ribbon operators are

$$F^{(h,g)}(i,r) \;=\; \delta_{g,1}\, L^h(i,r) \qquad\qquad F^{(h,g)}(j,l) \;=\; T^{g^{-1}}(j,l)$$

The ribbon operators on a long ribbon can be constructed from these ones.

It has been already mentioned that the multiplication in $\mathcal{D}$ and the comultiplication in $\mathcal{F}$ are defined by the same tensor $\Omega^{\star}_{\star\star}$. Actually, $\mathcal{D}$ and $\mathcal{F}$ are Hopf algebras dual to each other.

(For general account on Hopf algebras, see [21, 22, 23]). The multiplication in $\mathcal{F}$ corresponds to a comultiplication in $\mathcal{D}$ defined as follows

$$\Delta(D_{\boldsymbol{k}}) \;=\; \Lambda_{\boldsymbol{k}}^{\boldsymbol{mn}}\, D_{\boldsymbol{m}} \otimes D_{\boldsymbol{n}} \tag{27}$$

(More explicitly, $\Delta(D_{(h,g)}) = \sum_{h_1 h_2 = h} D_{(h_1,g)} \otimes D_{(h_2,g)}$). The unit element of $\mathcal{F}$ is $1_{\mathcal{F}} = \varepsilon_{\boldsymbol{k}} F^{\boldsymbol{k}}$, where $\varepsilon_{\boldsymbol{k}}$ are given by eq. (21); the tensor $\varepsilon_\star$ also defines a counit of $\mathcal{D}$ (i.e. the mapping $\varepsilon : \mathcal{D} \to \mathbb{C}$: $\varepsilon(D_{\boldsymbol{k}}) = \varepsilon_{\boldsymbol{k}}$). The unit of $\mathcal{D}$ and the counit of $\mathcal{F}$ are given by

$$\mathrm{e}^{(h,g)} \;=\; \delta_{g,1} \tag{28}$$

The Hopf algebra structure also includes an antipode, i.e. a mapping $S : \mathcal{D} \to \mathcal{D}$: $S(D_{\boldsymbol{k}}) = \mathrm{S}_{\boldsymbol{k}}^{\boldsymbol{m}} D_{\boldsymbol{m}}$, or $S : \mathcal{F} \to \mathcal{F}$: $S(F^{\boldsymbol{m}}) = \mathrm{S}_{\boldsymbol{k}}^{\boldsymbol{m}} F^{\boldsymbol{k}}$. The tensor $\mathrm{S}_\star^\star$ is given by the equation

$$\mathrm{S}_{(h_2,g_2)}^{(h_1,g_1)} \;=\; \delta_{g_1^{-1} h_1 g_1,\, h_2^{-1}}\; \delta_{g_1,\, g_2^{-1}} \tag{29}$$

Here is the complete list of Hopf algebra axioms.

$$\Lambda_{\boldsymbol{i}}^{\boldsymbol{lm}}\, \Lambda_{\boldsymbol{k}}^{\boldsymbol{in}} \;=\; \Lambda_{\boldsymbol{k}}^{\boldsymbol{lj}}\, \Lambda_{\boldsymbol{j}}^{\boldsymbol{mn}} \qquad\qquad \varepsilon_{\boldsymbol{i}}\, \Lambda_{\boldsymbol{k}}^{\boldsymbol{im}} \;=\; \Lambda_{\boldsymbol{k}}^{\boldsymbol{mj}}\, \varepsilon_{\boldsymbol{j}} \;=\; \delta_{\boldsymbol{k}}^{\boldsymbol{m}} \tag{30}$$

$$\Omega_{\boldsymbol{lm}}^{\boldsymbol{i}}\, \Omega_{\boldsymbol{in}}^{\boldsymbol{k}} \;=\; \Omega_{\boldsymbol{lj}}^{\boldsymbol{k}}\, \Omega_{\boldsymbol{mn}}^{\boldsymbol{j}} \qquad\qquad \mathrm{e}^{\boldsymbol{i}}\, \Omega_{\boldsymbol{in}}^{\boldsymbol{k}} \;=\; \Omega_{\boldsymbol{mj}}^{\boldsymbol{k}}\, \mathrm{e}^{\boldsymbol{j}} \;=\; \delta_{\boldsymbol{m}}^{\boldsymbol{k}} \tag{31}$$

$$\Lambda_{\boldsymbol{q}}^{\boldsymbol{lm}}\, \Omega_{\boldsymbol{kn}}^{\boldsymbol{q}} \;=\; \Omega_{\boldsymbol{ij}}^{\boldsymbol{l}}\, \Omega_{\boldsymbol{rs}}^{\boldsymbol{m}}\, \Lambda_{\boldsymbol{k}}^{\boldsymbol{ir}}\, \Lambda_{\boldsymbol{n}}^{\boldsymbol{js}} \qquad \varepsilon_{\boldsymbol{q}}\, \Omega_{\boldsymbol{kn}}^{\boldsymbol{q}} \;=\; \varepsilon_{\boldsymbol{k}}\, \varepsilon_{\boldsymbol{n}} \qquad \Lambda_{\boldsymbol{q}}^{\boldsymbol{lm}}\, \mathrm{e}^{\boldsymbol{q}} \;=\; \mathrm{e}^{\boldsymbol{l}}\, \mathrm{e}^{\boldsymbol{m}} \tag{32}$$

$$\mathrm{S}_{\boldsymbol{l}}^{\boldsymbol{k}}\, \Lambda_{\boldsymbol{p}}^{\boldsymbol{lm}}\, \Omega_{\boldsymbol{kn}}^{\boldsymbol{q}}\, \delta_{\boldsymbol{m}}^{\boldsymbol{n}} \;=\; \delta_{\boldsymbol{l}}^{\boldsymbol{k}}\, \Lambda_{\boldsymbol{p}}^{\boldsymbol{lm}}\, \Omega_{\boldsymbol{kn}}^{\boldsymbol{q}}\, \mathrm{S}_{\boldsymbol{m}}^{\boldsymbol{n}} \;=\; \varepsilon_{\boldsymbol{p}}\, \mathrm{e}^{\boldsymbol{q}} \tag{33}$$

Most of these identities correspond to physically obvious properties of ribbon operators. Eq. (30) is a statement of the usual multiplication axioms in the algebra $\mathcal{F}$, namely, $(F^{\boldsymbol{l}} F^{\boldsymbol{m}}) F^{\boldsymbol{n}} = F^{\boldsymbol{l}} (F^{\boldsymbol{m}} F^{\boldsymbol{n}})$ and $1 F^{\boldsymbol{m}} = F^{\boldsymbol{m}} 1 = F^{\boldsymbol{m}}$. The first equation in (31) (coassociativity of the comultiplication in $\mathcal{F}$) can be proven by expanding $F^{\boldsymbol{k}}(t_1 t_2 t_3)$ as $\Omega_{\boldsymbol{in}}^{\boldsymbol{k}}\, F^{\boldsymbol{i}}(t_1 t_2)\, F^{\boldsymbol{n}}(t_3)$ or $\Omega_{\boldsymbol{lj}}^{\boldsymbol{k}}\, F^{\boldsymbol{l}}(t_1)\, F^{\boldsymbol{j}}(t_2 t_3)$ — the result must be the same.[18] Eqs. (32) mean that the multiplication and comultiplication are consistent with each other. To prove the first equation in (32), expand $F^{\boldsymbol{l}}(t_1 t_2)\, F^{\boldsymbol{m}}(t_1 t_2)$ in two different ways. The second equation follows from the fact that $\varepsilon_{\boldsymbol{q}} F^{\boldsymbol{q}}(t_1 t_2)$ is the identity operator.

The antipode axiom (33) does not have explicit physical meaning. Mathematically, it is a *definition* of the tensor $\mathrm{S}_\star^\star$: the element $\gamma = \mathrm{S}_{\boldsymbol{k}}^{\boldsymbol{l}} F^{\boldsymbol{k}} \otimes D_{\boldsymbol{l}} \in \mathcal{F} \otimes \mathcal{D}$ is the inverse to the canonical element $\delta = F^{\boldsymbol{i}} \otimes D_{\boldsymbol{i}}$. The antipode have the following properties which can be derived from (30–33)

$$\mathrm{S}_{\boldsymbol{l}}^{\boldsymbol{i}}\, \mathrm{S}_{\boldsymbol{m}}^{\boldsymbol{j}}\, \Lambda_{\boldsymbol{p}}^{\boldsymbol{lm}} \;=\; \Lambda_{\boldsymbol{q}}^{\boldsymbol{ji}}\, \mathrm{S}_{\boldsymbol{p}}^{\boldsymbol{q}} \qquad\qquad \mathrm{S}_{\boldsymbol{q}}^{\boldsymbol{p}}\, \Omega_{\boldsymbol{ij}}^{\boldsymbol{q}} \;=\; \Omega_{\boldsymbol{ml}}^{\boldsymbol{p}}\, \mathrm{S}_{\boldsymbol{j}}^{\boldsymbol{m}}\, \mathrm{S}_{\boldsymbol{i}}^{\boldsymbol{l}} \tag{34}$$

[18] The coassociativity is necessary and sufficient for that. The sufficiency is rather obvious; the necessity follows from the fact that the mapping $\mathcal{F} \to \mathcal{F}(t)$ is injective, i.e. the operators $F^{\boldsymbol{k}}(t)$ with different $\boldsymbol{k}$ are linearly independent.

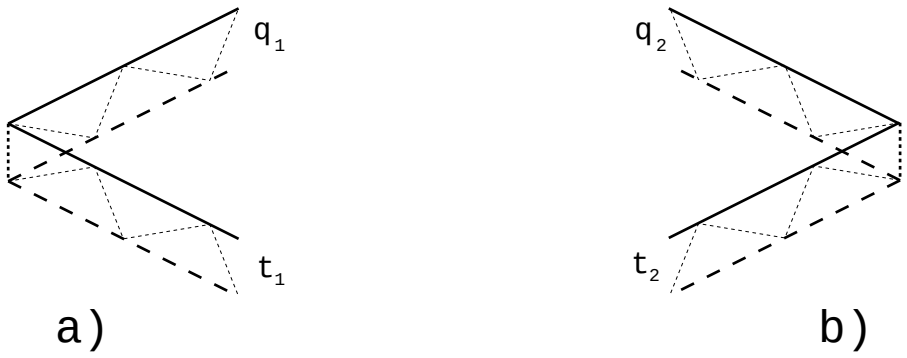


Figure 8: Two ribbons attached to the same site

Finally, we can define a so-called *skew antipode* $\tilde{\mathrm{S}}^\star_\star$ as follows

$$\tilde{\mathrm{S}}^{\boldsymbol{m}}_{\boldsymbol{i}}\ \mathrm{S}^{\boldsymbol{i}}_{\boldsymbol{n}}\ =\ \mathrm{S}^{\boldsymbol{m}}_{\boldsymbol{j}}\ \tilde{\mathrm{S}}^{\boldsymbol{j}}_{\boldsymbol{n}}\ =\ \delta^{\boldsymbol{m}}_{\boldsymbol{n}} \tag{35}$$

In our case, $\tilde{\mathrm{S}}^{\boldsymbol{m}}_{\boldsymbol{i}} = \mathrm{S}^{\boldsymbol{m}}_{\boldsymbol{i}}$, but this is not true for a generic Hopf algebra. The skew antipode have the following properties similar to (33) and (34)

$$\tilde{\mathrm{S}}^{\boldsymbol{n}}_{\boldsymbol{l}}\ \Lambda^{\boldsymbol{lm}}_{\boldsymbol{p}}\ \Omega^{\boldsymbol{q}}_{\boldsymbol{kn}}\ \delta^{\boldsymbol{k}}_{\boldsymbol{m}}\ =\ \delta^{\boldsymbol{n}}_{\boldsymbol{l}}\ \Lambda^{\boldsymbol{lm}}_{\boldsymbol{p}}\ \Omega^{\boldsymbol{q}}_{\boldsymbol{kn}}\ \tilde{\mathrm{S}}^{\boldsymbol{k}}_{\boldsymbol{m}}\ =\ \varepsilon_{\boldsymbol{p}}\,\mathrm{e}^{\boldsymbol{q}} \tag{36}$$

$$\tilde{\mathrm{S}}^{\boldsymbol{i}}_{\boldsymbol{l}}\ \tilde{\mathrm{S}}^{\boldsymbol{j}}_{\boldsymbol{m}}\ \Lambda^{\boldsymbol{lm}}_{\boldsymbol{p}}\ =\ \Lambda^{\boldsymbol{ji}}_{\boldsymbol{q}}\ \tilde{\mathrm{S}}^{\boldsymbol{q}}_{\boldsymbol{p}} \qquad\qquad \tilde{\mathrm{S}}^{\boldsymbol{p}}_{\boldsymbol{q}}\ \Omega^{\boldsymbol{q}}_{\boldsymbol{ij}}\ =\ \Omega^{\boldsymbol{p}}_{\boldsymbol{ml}}\ \tilde{\mathrm{S}}^{\boldsymbol{m}}_{\boldsymbol{j}}\ \tilde{\mathrm{S}}^{\boldsymbol{l}}_{\boldsymbol{i}} \tag{37}$$

(Note the distinction between (33) and (36), however).

The reader may be overwhelmed by a number of formal things, so let us summarize what we know by now. We have defined two algebras, $\mathcal{D}$ and $\mathcal{F}$, and their actions on the Hilbert space $\mathcal{N}$. In this context, we denote them by $\mathcal{D}(a)$ and $\mathcal{F}(t)$ because the actions depend on the site a or on the ribbon t, respectively. Operators from $\mathcal{D}(a)$ affect one particle whereas operators from $\mathcal{F}(t)$ affect two particles. The action of $\mathcal{F}(t)$ on the space of n-particle states $\mathcal{L}(x_1, \ldots, x_n)$ depends only on the topological class of the ribbon t. This space have not been found yet, even for $n = 2$. (It will be found after we learn more about local and ribbon operators). The algebra $\mathcal{F}$ is a Hopf algebra. The comultiplication allows to make up a long ribbon from parts. There is a formal duality between $\mathcal{F}$ and $\mathcal{D}$. The comultiplication in $\mathcal{F}$ is dual to the multiplication in $\mathcal{D}$. The multiplication in $\mathcal{F}$ is dual to a comultiplication in $\mathcal{D}$. (The meaning of the latter is not clear yet).

5.3 Further properties of local and ribbon operators

Let us study commutation relations between ribbon operators. Consider two ribbons attached to the same site, as shown in fig. 8 a or b. Then

$$\begin{aligned} F^{(h,g)}(t_1)\ F^{(v,u)}(q_1) &= F^{(v,u)}(q_1)\ F^{(v^{-1}hv,\,v^{-1}g)}(t_1) \\ F^{(h,g)}(t_2)\ F^{(v,u)}(q_2) &= F^{(v,u)}(q_2)\ F^{(h,\,gu^{-1}vu)}(t_2) \end{aligned}$$

In a tensor form, these equations read as follows

$$\begin{aligned} F^{\boldsymbol{m}}(t_1)\ F^{\boldsymbol{n}}(q_1) &= \mathrm{R}^{\boldsymbol{ik}}\ \Omega^{\boldsymbol{n}}_{\boldsymbol{ij}}\ \Omega^{\boldsymbol{m}}_{\boldsymbol{kl}}\ F^{\boldsymbol{j}}(q_1)\ F^{\boldsymbol{l}}(t_1) \\ F^{\boldsymbol{m}}(t_2)\ F^{\boldsymbol{n}}(q_2) &= F^{\boldsymbol{i}}(q_2)\ F^{\boldsymbol{k}}(t_2)\ \Omega^{\boldsymbol{n}}_{\boldsymbol{ij}}\ \Omega^{\boldsymbol{m}}_{\boldsymbol{kl}}\ \bar{\mathrm{R}}^{\boldsymbol{jl}} \end{aligned} \tag{38}$$

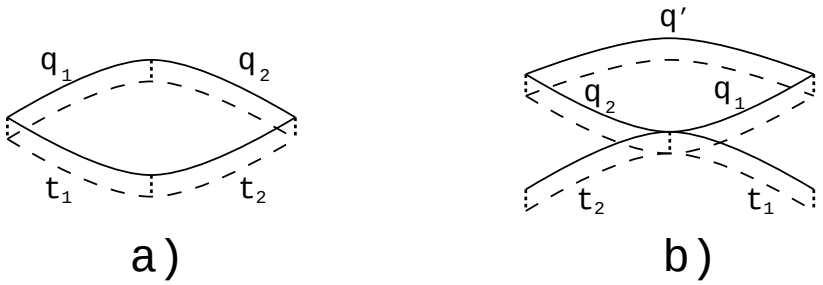


Figure 9: Checking consistency of the commutation relations

where

$$\mathrm{R}^{(h,g)(v,u)} \;=\; \delta_{h,u}\;\delta_{g,1} \qquad\qquad \bar{\mathrm{R}}^{(h,g)(v,u)} \;=\; \delta_{h^{-1},\,u}\;\delta_{g,1} \tag{39}$$

Note that

$$\bar{\mathrm{R}}^{\boldsymbol{ik}}\;\Omega^{\boldsymbol{n}}_{\boldsymbol{ij}}\;\Omega^{\boldsymbol{m}}_{\boldsymbol{kl}}\;\mathrm{R}^{\boldsymbol{jl}} \;=\; \mathrm{R}^{\boldsymbol{ik}}\;\Omega^{\boldsymbol{n}}_{\boldsymbol{ij}}\;\Omega^{\boldsymbol{m}}_{\boldsymbol{kl}}\;\bar{\mathrm{R}}^{\boldsymbol{jl}} \;=\; \mathrm{e}^{\boldsymbol{n}}\,\mathrm{e}^{\boldsymbol{m}} \tag{40}$$

To prove[19] (and to see the physical meaning of) this equation, consider the configuration shown in fig. 9b. Clearly, $F^{\boldsymbol{r}}(t_2t_1)$ and $F^{\boldsymbol{s}}(q')$ commute. On the other hand, $F^{\boldsymbol{s}}(q') \equiv F^{\boldsymbol{s}}(q_2q_1)$, so $F^{\boldsymbol{r}}(t_2t_1)$ and $F^{\boldsymbol{s}}(q_2q_1)$ commute. It follows that $\bar{\mathrm{R}}^{\boldsymbol{ik}}\,\Omega^{\boldsymbol{n}}_{\boldsymbol{ij}}\,\Omega^{\boldsymbol{m}}_{\boldsymbol{kl}}\,\mathrm{R}^{\boldsymbol{jl}} \;=\; \mathrm{e}^{\boldsymbol{n}}\mathrm{e}^{\boldsymbol{m}}$. This identity can be easily written in an invariant form, namely, $\bar{R}R \;=\; 1_{\mathcal{D}\otimes\mathcal{D}}$, where $R \;=\; \mathrm{R}^{\boldsymbol{jl}}\,D_{\boldsymbol{j}} \otimes D_{\boldsymbol{l}}$ and $\bar{R} = \bar{\mathrm{R}}^{\boldsymbol{ik}}\,D_{\boldsymbol{i}} \otimes D_{\boldsymbol{k}}$. It also implies that $R\bar{R} = 1_{\mathcal{D}\otimes\mathcal{D}}$ because the algebra $\mathcal{D}\otimes\mathcal{D}$ is finite dimensional. Thus, $\bar{R} = R^{-1}$.

The tensor $\mathrm{R}^{\star}_{\star}$ (or the element $R \in \mathcal{D}\otimes\mathcal{D}$) is called the *R-matrix*. It satisfies the following axioms

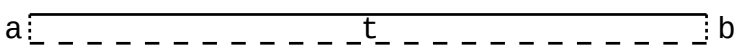
$$\Lambda^{\boldsymbol{ij}}_{\boldsymbol{k}}\;\mathrm{R}^{\boldsymbol{km}} \;=\; \mathrm{R}^{\boldsymbol{il}}\;\mathrm{R}^{\boldsymbol{jn}}\;\Omega^{\boldsymbol{m}}_{\boldsymbol{ln}} \qquad\qquad \mathrm{R}^{\boldsymbol{mk}}\Lambda^{\boldsymbol{ji}}_{\boldsymbol{k}} \;=\; \Omega^{\boldsymbol{m}}_{\boldsymbol{ln}}\;\mathrm{R}^{\boldsymbol{li}}\;\mathrm{R}^{\boldsymbol{nj}} \tag{41}$$

$$\Lambda^{\boldsymbol{ji}}_{\boldsymbol{k}} \;=\; \Omega^{\boldsymbol{i}}_{\boldsymbol{lmr}}\;\Omega^{\boldsymbol{j}}_{\boldsymbol{pns}}\;\mathrm{R}^{\boldsymbol{lp}}\;\Lambda^{\boldsymbol{mn}}_{\boldsymbol{k}}\;\bar{\mathrm{R}}^{\boldsymbol{rs}} \tag{42}$$

where $\Omega^{\boldsymbol{i}}_{\boldsymbol{lmr}} = \Omega^{\boldsymbol{i}}_{\boldsymbol{lu}}\Omega^{\boldsymbol{u}}_{\boldsymbol{mr}} = \Omega^{\boldsymbol{u}}_{\boldsymbol{lm}}\Omega^{\boldsymbol{i}}_{\boldsymbol{ur}}$. Eqs. (41) follow from (38). Conversely, these equations ensure that the commutation relation are consistent. To prove the first equation in (41), commute $F^{\boldsymbol{m}}(t_1)\,F^{\boldsymbol{i}}(q_1)\,F^{\boldsymbol{j}}(q_1)$ in two different ways. You will get $\mathrm{W}^{\boldsymbol{ijm}}_{\boldsymbol{ab}}\,F^{\boldsymbol{a}}(q_1)\,F^{\boldsymbol{b}}(t_1)$, with two different expressions for $\mathrm{W}^{\boldsymbol{ijm}}_{\boldsymbol{ab}}$. Then calculate $\mathrm{W}^{\boldsymbol{ijm}}_{\boldsymbol{ab}}\,\mathrm{e}^{\boldsymbol{a}}\,\mathrm{e}^{\boldsymbol{b}}$ using the axioms (30–32). The second equation in (41) can be proven in a similar way.

To prove eq. (42), consider the configuration shown in fig. 9a. Clearly, $F^{\boldsymbol{i}}(q_1q_2) \equiv F^{\boldsymbol{i}}(t_1t_2)$, so $F^{\boldsymbol{j}}(t_1t_2)\,F^{\boldsymbol{i}}(q_1q_2) \;\equiv\; \Lambda^{\boldsymbol{ji}}_{\boldsymbol{k}}\,F^{\boldsymbol{k}}(t_1t_2)$. On the other hand, we can first expand $F^{\boldsymbol{j}}(t_1t_2)$ and $F^{\boldsymbol{i}}(q_1q_2)$ using the comultiplication rules, and then apply the commutation relations (38). The result must be the same.

Let t be a ribbon connecting sites a and b. The local and ribbon operators commute as follows



$$F^{\boldsymbol{m}}(t)\;D_{\boldsymbol{i}}(a) \;=\; \Lambda^{\boldsymbol{jk}}_{\boldsymbol{i}}\;\Omega^{\boldsymbol{m}}_{\boldsymbol{kl}}\;D_{\boldsymbol{j}}(a)\;F^{\boldsymbol{l}}(t) \qquad\qquad D_{\boldsymbol{i}}(b)\;F^{\boldsymbol{m}}(t) \;=\; \Omega^{\boldsymbol{m}}_{\boldsymbol{lk}}\;\Lambda^{\boldsymbol{kj}}_{\boldsymbol{i}}\;F^{\boldsymbol{l}}(t)\;D_{\boldsymbol{j}}(b) \tag{43}$$

[19] This proof is not rigorous, but an interested reader can easily fix it. Anyway, you can just substitute (39) into (40) and check it directly.

These commutation relations can be also written in the form

$$\begin{aligned} D_{\boldsymbol{j}}(a)\; F^{\boldsymbol{l}}(t) &= \Lambda^{\boldsymbol{ik}}_{\boldsymbol{j}}\; \tilde{\mathrm{S}}^{\boldsymbol{n}}_{\boldsymbol{k}}\; \Omega^{\boldsymbol{l}}_{\boldsymbol{nm}}\; F^{\boldsymbol{m}}(t)\; D_{\boldsymbol{i}}(a) \\ F^{\boldsymbol{l}}(t)\; D_{\boldsymbol{j}}(b) &= \Omega^{\boldsymbol{l}}_{\boldsymbol{mn}}\; \tilde{\mathrm{S}}^{\boldsymbol{n}}_{\boldsymbol{k}}\; \Lambda^{\boldsymbol{ki}}_{\boldsymbol{j}}\; D_{\boldsymbol{i}}(b)\; F^{\boldsymbol{m}}(t) \end{aligned} \tag{44}$$

where $\tilde{\mathrm{S}}^{\star}_{\star}$ is the skew antipode (see eqs. (35,36)).

Finally, we introduce some special elements $C \in \mathcal{D}$ and $\tau \in \mathcal{F}$. The first one has a clear physical meaning: the corresponding operator $C(a) = A(a)\,B(a)$ projects out states with no particle at the site a. The element C can be represented in the form

$$C \;=\; \mathrm{c}^{\boldsymbol{i}}\, D_{\boldsymbol{i}} \qquad\qquad \text{where} \quad \mathrm{c}^{(h,g)} \;=\; N^{-1}\delta_{h,1} \tag{45}$$

It has the following properties:

$$CX \;=\; XC \;=\; \varepsilon(X)\,C \quad \text{for any } \; X \in \mathcal{D} \qquad\qquad \varepsilon(C) \;=\; 1$$

or, in tensor notations,

$$\Omega^{\boldsymbol{k}}_{\boldsymbol{ij}}\,\mathrm{c}^{\boldsymbol{i}} \;=\; \Omega^{\boldsymbol{k}}_{\boldsymbol{ji}}\,\mathrm{c}^{\boldsymbol{i}} \;=\; \varepsilon_{\boldsymbol{j}}\,\mathrm{c}^{\boldsymbol{k}} \qquad\qquad \varepsilon_{\boldsymbol{k}}\,\mathrm{c}^{\boldsymbol{k}} \;=\; 1 \tag{46}$$

The element $\tau \in \mathcal{F}$ is dual to C; it is defined as follows

$$\tau \;=\; \tau_{\boldsymbol{i}}\, F^{\boldsymbol{i}} \qquad\qquad \text{where} \quad \tau_{(h,g)} \;=\; N^{-1}\delta_{1,g} \tag{47}$$

Its properties are as follows

$$\Lambda^{\boldsymbol{ij}}_{\boldsymbol{k}}\,\tau_{\boldsymbol{i}} \;=\; \Lambda^{\boldsymbol{ji}}_{\boldsymbol{k}}\,\tau_{\boldsymbol{i}} \;=\; \mathrm{e}^{\boldsymbol{j}}\,\tau_{\boldsymbol{k}} \qquad\qquad \mathrm{e}^{\boldsymbol{k}}\,\tau_{\boldsymbol{k}} \;=\; 1 \tag{48}$$

Note that $\tau_{\boldsymbol{k}}\,\mathrm{c}^{\boldsymbol{k}} = N^{-2}$. Using these properties, we can we can derive an important consequence from the commutation relations (43)

$$\tau_{\boldsymbol{s}}\,\Omega^{\boldsymbol{s}}_{\boldsymbol{mp}}\,\mathrm{S}^{\boldsymbol{p}}_{\boldsymbol{q}}\; F^{\boldsymbol{m}}(t)\,C(a)\,F^{\boldsymbol{q}}(t) \;=\; \tau_{\boldsymbol{s}}\,\Omega^{\boldsymbol{s}}_{\boldsymbol{pm}}\,\mathrm{S}^{\boldsymbol{p}}_{\boldsymbol{q}}\; F^{\boldsymbol{q}}(t)\,C(b)\,F^{\boldsymbol{m}}(t) \;=\; N^{-2} \tag{49}$$

5.4 The space $\mathcal{L}(a,b)$

Now we are in a position to find the space $\mathcal{L}(a,b)$ and to prove the assertions from Sec. 5.1. The first assertion was that any excited spot can be transformed into one particle. It is simple if we can transform two particles into one by ribbon operators. Let us choose an arbitrary site b the excited spot to be compressed to. Let some constraint, $A(s) - 1 \equiv 0$ or $B(p) - 1 \equiv 0$, be violated. Choose any site a containing the vertex s or the face p. Connect a and b by a ribbon. By the assumption, we can clean up the site a while changing the state of b, but without violating any more constraint. We can repeat this procedure again and again to clean up the whole spot.

So, we only need to show that two particles can be transformed into one. What does it mean exactly? Physically, any transformation must be unitary, but it can involve also some external system. (Otherwise, it is impossible to "decrease entropy", i.e. to convert many states into fewer). On the other hand, it is clear that unitarity is not relevant to this problem. However, we should exclude degenerate transformations, such as multiplication by the zero operator. So, it is better to reformulate the assertion as follows: any two-particle state (plus some other

excitations far away) can be obtained from one-particle states (plus the same excitations far away). Let $|\psi\rangle \in \mathcal{L}(a,b,\ldots)$ be such a two-particle state. We are going to use the formula (49). Let

$$G_{\boldsymbol{q}} \;=\; N^2\,\tau_{\boldsymbol{s}}\,\Omega^{\boldsymbol{s}}_{\boldsymbol{mp}}\,\mathrm{S}^{\boldsymbol{p}}_{\boldsymbol{q}}\;F^{\boldsymbol{m}}(t) \qquad\qquad |\eta^{\boldsymbol{q}}\rangle \;=\; C(a)\,F^{\boldsymbol{q}}(t)\,|\psi\rangle \tag{50}$$

Then $|\psi\rangle = G_{\boldsymbol{q}}\,|\eta^{\boldsymbol{q}}\rangle$. The states $|\eta^{\boldsymbol{q}}\rangle$ belong to $\mathcal{L}(b,\ldots)$, i.e. do not contain excitation at a. This is exactly what we need.

The other two assertions were about the action of local operators on the space $\mathcal{L}(a,b)$, so we need to find this space first. We can consider this space as a representation of the algebra $\mathcal{E} \cong \mathcal{E}(t)$ generated by the operators $D_{\boldsymbol{j}} = D_{\boldsymbol{j}}(a)$, $F^{\boldsymbol{l}} = F^{\boldsymbol{l}}(t)$ and $D'_{\boldsymbol{j}} = D_{\boldsymbol{j}}(b)$. As a linear space, $\mathcal{E} = \mathcal{D}\otimes\mathcal{F}\otimes\mathcal{D}$. (Thus, $\mathcal{E}$ has dimensionality N^6). Multiplication in $\mathcal{E}$ is defined by the commutation relations (43). We will call $\mathcal{E} \cong \mathcal{E}(t)$ the algebra of *extended ribbon operators*. It is just an algebra, not a Hopf algebra. More exactly, it is a finite-dimensional C^*-algebra. The involution (=Hermitian conjugation) is given by the formulas (cf. (19))

$$(D_{(h,g)})^\dagger \;=\; D_{(g^{-1}hg,\,g^{-1})} \qquad (F^{(h,g)})^\dagger \;=\; F^{(h^{-1},g)} \qquad (D'_{(h,g)})^\dagger \;=\; D'_{(g^{-1}hg,\,g^{-1})} \tag{51}$$

[*Remark.* Apparently, the algebra $\mathcal{E}$ will play the central role in a general theory of topological quantum order. Indeed, we were lucky to define ribbon operators separately from local operators. In the general case, ribbon operators should be mixed with local operators.]

So, we are looking for a particular representation $\mathcal{L}$ of the algebra $\mathcal{E}$. This representation must contain a special vector $|\xi\rangle$ (the ground state) such that

$$D_{\boldsymbol{k}}\,|\xi\rangle \;=\; \varepsilon_{\boldsymbol{k}}\,|\xi\rangle \qquad\qquad D'_{\boldsymbol{k}}\,|\xi\rangle \;=\; \varepsilon_{\boldsymbol{k}}\,|\xi\rangle \tag{52}$$

We start with constructing a representation $\check{\mathcal{L}}$ spanned by the vectors $|\psi^{\boldsymbol{k}}\rangle = F^{\boldsymbol{k}}\,|\xi\rangle$. (It will be proven after that $\check{\mathcal{L}} = \mathcal{L}$). We assume that the vectors $|\psi^{\boldsymbol{k}}\rangle$ are linearly independent. This need not be the case in the representation $\mathcal{L}$ but we can postulate $|\psi^{\boldsymbol{k}}\rangle$ being linearly independent in $\check{\mathcal{L}}$. Thus, $\mathcal{L}$ contains a factor-representation of $\check{\mathcal{L}}$.

The representation $\check{\mathcal{L}}$ is given by the formulas

$$D_{\boldsymbol{j}}\,|\psi^{\boldsymbol{k}}\rangle \;=\; \tilde{\mathrm{S}}^{\boldsymbol{n}}_{\boldsymbol{j}}\,\Omega^{\boldsymbol{k}}_{\boldsymbol{nm}}\,|\psi^{\boldsymbol{m}}\rangle \qquad F^{\boldsymbol{j}}\,|\psi^{\boldsymbol{k}}\rangle \;=\; \Lambda^{\boldsymbol{jk}}_{\boldsymbol{m}}\,|\psi^{\boldsymbol{m}}\rangle \qquad D'_{\boldsymbol{j}}\,|\psi^{\boldsymbol{k}}\rangle \;=\; \Omega^{\boldsymbol{k}}_{\boldsymbol{mj}}\,|\psi^{\boldsymbol{m}}\rangle \tag{53}$$

It is easy to show that this representation is irreducible. Hence, $\mathcal{L}$ contains $\check{\mathcal{L}}$, i.e. the vectors $|\psi^{\boldsymbol{k}}\rangle$ are linearly independent in $\mathcal{L}$. The scalar products between the vectors $|\psi^{\boldsymbol{k}}\rangle$ can be found from (53) and (51),

$$\langle\psi^{(v,u)}|\psi^{(h,g)}\rangle \;=\; N^{-1}\,\delta_{v,h}\,\delta_{u,g} \tag{54}$$

To prove that $\check{\mathcal{L}} = \mathcal{L}$, we use the equation (49) again. For an arbitrary two-particle state $|\psi\rangle \in \mathcal{L}$, define the vectors $|\eta^{\boldsymbol{q}}\rangle$ and operators $G_{\boldsymbol{q}}$ as in eq. (50). Then $|\psi\rangle = G_{\boldsymbol{q}}\,|\eta^{\boldsymbol{q}}\rangle$. One could say that $|\eta^{\boldsymbol{q}}\rangle \in \mathcal{L}(b)$ but, actually, the space $\mathcal{L}(b)$ is spanned by the sole vector $|\xi\rangle$. It follows that $|\psi\rangle \in \check{\mathcal{L}}$ — the assertion has been proven. Thus, the action of local and ribbon operators on the space $\mathcal{L} = \mathcal{L}(a,b)$ is given by eq. (53).

It is easy to see that the action of $\mathcal{D}(a)$ on $\mathcal{L}(a,b)$ is exact (though it is reducible). Besides that, $\mathcal{D}(a)$ is the commutant of $\mathcal{D}(b)$ in $\mathbf{L}(\mathcal{L}(a,b))$ and *vise versa*. (That is, $\mathcal{D}(a)$ consists of all operators $X \in \mathbf{L}(\mathcal{L}(a,b))$ which commute with every $Y \in \mathcal{D}(b)$). Hence, $\mathcal{D}(a)$ includes *all* local operators acting on the space $\mathcal{L}(a,b)$. Indeed, a local operator, which involves only spins near the site a, must commute with any operator acting on distant spins. Of course, there are many

such operators, but their action on the two-particle space $\mathcal{L}(a,b)$ coincides with the action of the operators from $\mathcal{D}(a)$. This is also true for a multi-particle excitation space $\mathcal{L}(x_1,\dots,x_n)$.

The space $\mathcal{L}(x_1,\dots,x_n)$ can be described as follows. Let us connect the sites $x_1,\dots,x_n$ by $n-1$ ribbons $t_1,\dots,t_{n-1}$ in an arbitrary way so that the ribbons form a tree. Then the vectors $|\psi^{\boldsymbol{k_1},\dots,\boldsymbol{k_{n-1}}}\rangle = F^{\boldsymbol{k_1}}(t_1)\dots F^{\boldsymbol{k_{n-1}}}(t_{n-1})\,|\xi\rangle$ form a basis of $\mathcal{L}(x_1,\dots,x_n)$. Choosing different ribbons means choosing a different basis. In the next section we will give another description of multi-particle excitation spaces.

6 Topological operators, braiding and fusion

Let us consider again the n-particle excitation space $\mathcal{L} = \mathcal{L}(x_1,\dots,x_n)$. The algebra $\mathbf{L}(\mathcal{L})$ includes the local operator algebras $\mathcal{D}(x_1),\dots,\mathcal{D}(x_1)$. An operator $Y \in \mathbf{L}(\mathcal{L})$ which commute with every $X \in \mathcal{D}(x_j)$ $(j=1,\dots,n)$ is called a *topological operator*. Physically, topological operators correspond to nonlocal degrees of freedom. For $n=2$, the algebra of topological operators coincides with the center of $\mathcal{D}(x_1)$ or $\mathcal{D}(x_2)$. (The two centers coincide). Hence, the only nonlocal degree of freedom is the type of either particle. (The two particles correspond to dual representations of $\mathcal{D}$; in other words, these are a particle and an anti-particle). So, there is no hidden (i.e. quantum nonlocal) degree of freedom in this case. Such hidden degrees of freedom appear for $n \geq 3$.

To describe the space $\mathcal{L}$ and operators acting on it, let us choose an arbitrary site x_0 (distinct from $x_1,\dots,x_n$) and connect it with $x_1,\dots,x_n$ by non-intersecting ribbons $t_1,\dots,t_n$, see fig. 10a. As stated above, the space $\mathcal{L}(x_0,x_1,\dots,x_n)$ is spanned by the vectors

$$|\psi^{\boldsymbol{k_1},\dots,\boldsymbol{k_n}}\rangle \;=\; F^{\boldsymbol{k_1}}(t_1)\dots F^{\boldsymbol{k_n}}(t_n)\,|\xi\rangle \tag{55}$$

The space in question, $\mathcal{L} = \mathcal{L}(x_1,\dots,x_n)$ is contained in $\mathcal{L}(x_0,x_1,\dots,x_n)$. It consists of all vectors $|\psi\rangle \in \mathcal{L}(x_0,x_1,\dots,x_n)$ which are invariant under the action of $\mathcal{D}(x_0)$ on the latter space.

The advantage of this description is that we can easily find all operators on the space $\mathcal{L}(x_0,x_1,\dots,x_n)$ which commute with $\mathcal{D}(x_1)\otimes\dots\otimes\mathcal{D}(x_n)$. These are simply operators which act on the ends of the ribbons $t_1,\dots,t_n$ attached to the site x_0. More exactly, an operator $D^{(r)}_{\boldsymbol{j}}$ $(r=1,\dots,n)$ acts on the r-th ribbon as $D'_{\boldsymbol{j}} = D_{\boldsymbol{j}}(x_0)$ (see eq.(53)), but does not affect the other ribbons,

$$\left(D^{(1)}_{\boldsymbol{j_1}}\otimes\dots\otimes D^{(n)}_{\boldsymbol{j_n}}\right)\,|\psi^{\boldsymbol{k_1},\dots,\boldsymbol{k_n}}\rangle \;=\; \Omega^{\boldsymbol{k_1}}_{\boldsymbol{m_1 j_1}}\dots\Omega^{\boldsymbol{k_n}}_{\boldsymbol{m_n j_n}}\,|\psi^{\boldsymbol{m_1},\dots,\boldsymbol{m_n}}\rangle \tag{56}$$

Thus we arrive to an interesting physical conclusion. Let us consider only one particle attached to an end of a semi-infinite ribbon (an analog of Dirac's string). Then *the topological operators act on the far end of the ribbon.*

Example. Let us see how the topological operators act on magnetic vortices. As shown in Sec. 5.1, a vortex type is characterized by a conjugacy class C of the group G. Individual topological states of the particle are characterized by particular elements $v \in C$. In terms of the notation (55), such a state can be represented as follows

$$|u,v\rangle \;=\; |C|^{1/2}\sum_{x:\;x^{-1}ux=v}|\psi^{(u,x)}\rangle$$

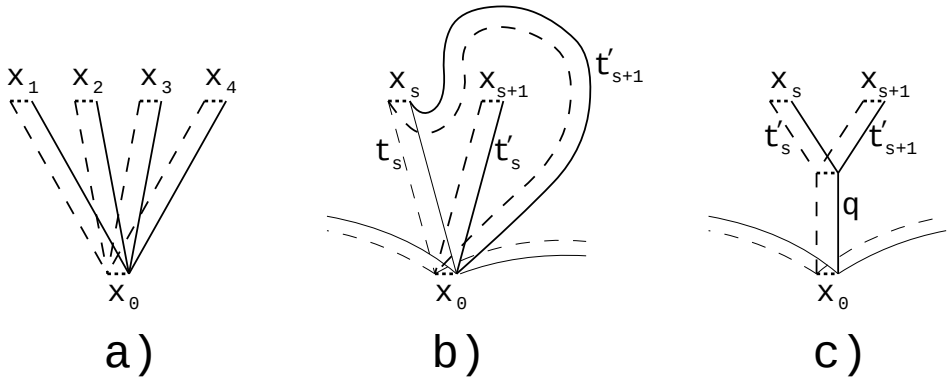


Figure 10: Braiding and fusion in terms of ribbon transformations

where $u \in C$ characterize the local state of the particle. One can easily check that $D'_{(h,g)}|u,v\rangle = \delta_{h,\,gvg^{-1}}|u,h\rangle$. This is consistent with eq. (22). Note that the local degree of freedom, u, is not affected.

How can we physically apply topological operators to particles? We can just move the particles around each other; this process is called *braiding*. Let us see what happens if we interchange two particles, x_s and x_{s+1}, counterclockwise, as shown in fig. 10b. The state $|\psi^{\cdots,\boldsymbol{k},\boldsymbol{l},\cdots}\rangle$ becomes a new state

$$|\psi^{\cdots,\boldsymbol{k},\boldsymbol{l},\cdots}\rangle_{\rm new} \;=\; \mathcal{R}_{\curvearrowleft}\,|\psi^{\cdots,\boldsymbol{k},\boldsymbol{l},\cdots}\rangle \;=\; \ldots F^{\boldsymbol{k}}(t'_s)\;F^{\boldsymbol{l}}(t'_{s+1})\ldots\,|\xi\rangle$$

To represent this state in the old basis, we should represent the operator $F^{\boldsymbol{k}}(t'_s)\,F^{\boldsymbol{l}}(t'_{s+1})$ in terms of $F^{\boldsymbol{m}}(t_s)$ and $F^{\boldsymbol{n}}(t_{s+1})$. Obviously, $F^{\boldsymbol{k}}(t'_s) = F^{\boldsymbol{k}}(t_{s+1})$; also $F^{\boldsymbol{l}}(t'_{s+1}) \equiv F^{\boldsymbol{l}}(t_s)$ as long as there is no particle at x_{s+1}, i.e. the operator $F^{\boldsymbol{k}}(t_{s+1})$ is not applied yet. Hence

$$F^{\boldsymbol{k}}(t'_s)\;F^{\boldsymbol{l}}(t'_{s+1}) \;\equiv\; F^{\boldsymbol{k}}(t_{s+1})\;F^{\boldsymbol{l}}(t_s)$$

Now we can apply the second commutation relation from (38). (Actually, we should reverse it). It follows that

$$F^{\boldsymbol{k}}(t_{s+1})\;F^{\boldsymbol{l}}(t_s) \;=\; \mathrm{R}^{\boldsymbol{ji}}\;\Omega^{\boldsymbol{l}}_{\boldsymbol{mi}}\;\Omega^{\boldsymbol{k}}_{\boldsymbol{nj}}\;F^{\boldsymbol{m}}(t_s)\;F^{\boldsymbol{n}}(t_{s+1})$$

$$\mathcal{R}_{\curvearrowleft}\,|\psi^{\cdots,\boldsymbol{k},\boldsymbol{l},\cdots}\rangle \;=\; \mathrm{R}^{\boldsymbol{ji}}\left(D^{(s)}_{\boldsymbol{i}}\otimes D^{(s+1)}_{\boldsymbol{j}}\right)\,|\psi^{\cdots,\boldsymbol{l},\boldsymbol{k},\cdots}\rangle$$

(see eq. (56)). Consequently, the counterclockwise interchange operator has the form

$$\mathcal{R}_{\curvearrowleft} \;=\; \mathrm{R}^{\boldsymbol{ji}}\,(D'_{\boldsymbol{i}}\otimes D'_{\boldsymbol{j}})\;\sigma \;=\; \sigma\;\mathrm{R}^{\boldsymbol{ij}}\,(D'_{\boldsymbol{i}}\otimes D'_{\boldsymbol{j}}) \tag{57}$$

where σ is the permutation operator, and $D'_{\boldsymbol{i}}$, $D'_{\boldsymbol{j}}$ are understood as topological operators. (Note that the operator σ permutes both topological and local degrees of freedom).

Example. Consider two magnetic vortices characterized by topological parameters $v_1, v_2 \in G$. The operator $\mathcal{R}\curvearrowleft$ acts on the state $|v_1,v_2\rangle$ as follows

$$\mathcal{R}_{\curvearrowleft}\,|v_1,v_2\rangle \;=\; |v_1v_2v_1^{-1},\,v_1\rangle \tag{58}$$

(The local parameters, u_1 and u_2, are suppressed in this formula).

Finally, let us see what happens if two particles, x_s and x_{s+1}, fuse into one. The resulting particle can be characterized by the action of topological operators on it. From this point of view, we can just glue parts of the corresponding ribbons (see fig. 10c) instead of fusing the particles themselves. Then

$$\begin{aligned} F^{\boldsymbol{k}}(t_s)\ F^{\boldsymbol{l}}(t_{s+1}) &\equiv \Omega^{\boldsymbol{k}}_{\boldsymbol{mi}}\ \Omega^{\boldsymbol{l}}_{\boldsymbol{nj}}\ \Lambda^{\boldsymbol{ij}}_{\boldsymbol{p}}\ F^{\boldsymbol{m}}(t'_s)\ F^{\boldsymbol{n}}(t'_{s+1})\ F^{\boldsymbol{p}}(q) \\ |\psi^{\dots,k,l,\dots}\rangle &\equiv \Omega^{\boldsymbol{k}}_{\boldsymbol{mi}}\ \Omega^{\boldsymbol{l}}_{\boldsymbol{nj}}\ \Lambda^{\boldsymbol{ij}}_{\boldsymbol{p}}\ F^{\boldsymbol{m}}(t'_s)\ F^{\boldsymbol{n}}(t'_{s+1})\ |\psi^{\dots,p,\dots}\rangle \\ \Lambda^{\boldsymbol{uv}}_{\boldsymbol{r}}\ D^{(s)}_{\boldsymbol{u}} \otimes D^{(s+1)}_{\boldsymbol{v}} &\equiv D'_{\boldsymbol{r}} \end{aligned}$$

where $D'_{\boldsymbol{r}}$ acts on the end of the ribbon q. Thus, fusion is described by the comultiplication in the algebra $\mathcal{D}$, see equation (27). (To avoid confusion, one should replace $D_\star$ with $D'_\star$ in that equation). The topological operator $\Delta(D'_{\boldsymbol{k}})$ acts on a particle pair as the topological operator $D'_{\boldsymbol{k}}$ on the particle resulting from fusion.

Example. Consider a pair of opposite magnetic vortices $|v,\, v^{-1}\rangle$. The operators $\Delta(D'_{\boldsymbol{k}})$ act on this state as follows

$$\Delta(D'_{(h,g)})\ |v,\, v^{-1}\rangle\ =\ \delta_{h,1}\ |gvg^{-1},\, gv^{-1}g^{-1}\rangle \tag{59}$$

It terms of the representation classification (see Sec. 5.1), this action corresponds to the pair (C, χ), where $C = \{1\}$, and χ is the adjoint representation of G. Thus, when opposite magnetic vortices fuse, the resulting particle has no magnetic charge but may have some electric charge.

7 Universal computation by anyons

(This section should be considered as an abstract of results to be presented elsewhere).

Universal quantum computation is possible in the model based on the permutation group S_5. (Unsolvability of the group seems to be important). Vortex pairs $|v,\, v^{-1}\rangle$, where v is a transposition, are used as qubits. It is possible to perform the following operations.

1. To produce pairs with zero charge. If a pair is created from the ground state, it has no charge automatically.

2. To measure the electric charge of a vortex pair destructively. For this, we should simply fuse the the pair into one particle.

3. To perform the following unitary transformation on two pairs

$$|u,\, u^{-1}\rangle \otimes |v,\, v^{-1}\rangle\ \mapsto\ |vuv^{-1},\, vu^{-1}v^{-1}\rangle \otimes |v,\, v^{-1}\rangle \tag{60}$$

   For this, we pull the first pair (as a whole) between the particles of the second pair.

4. To measure the value of v and produce an unlimited number of pure states $|v,\, v^{-1}\rangle$ for any given transposition v (say, $(1,2)$ or $(2,3)$). [At first sight, it is impossible because we can only measure the conjugacy class of a v. However, we can agree on a given state to correspond to $v = (1,2)$. Then we use it as a reference to produce an unlimited number of copies.]

The operations 3 and 4 are sufficient to perform universal classical computation. It is relatively simple to run quantum algorithms based on measurements [24]. Simulating a universal gate set is more subtle and requires *composite qubits*. That is, a usual qubit (with two distinct states) is represented by several vortex pairs.

Concluding remarks

It has been shown that anyons can arise from a Hamiltonian with local interactions but without any symmetry. These anyons can be used to perform universal quantum computation. There are still many things to do and questions to answer. First of all, it is desirable to find other models with anyons which allow universal quantum computation. (The group S_5 is quite unrealistic for physical implementation). Such models must be based on a more general algebraic structure rather than the quantum double of a group algebra. A general theory of anyons and topological quantum order is lacking. [In a sense, a general theory of anyons already exists [10]; it is based on quasi-triangular quasi-Hopf algebras. However, this theory either merely postulates the properties of anyons or connects them to certain field theories. This is quite unlike the theory of local and ribbon operators which describes both the properties of excitations and the underlying spin entanglement.] It is also desirable to formulate and prove some theorem about existence and the number of local degrees of freedom. (It seems that the local degrees of freedom are a sign that anyons arise from a system with no symmetry in the Hamiltonian). Finally, general understanding of dynamically created, or "materialized" symmetry is lacking. There one may find some insights for high energy physics. If we adopt a conjecture that the fundamental Hamiltonian or Lagrangian is not symmetric, we can probably infer some consequences about the particle spectrum.

Acknowledgements. I am grateful to J. Preskill, D. P. DiVincenzo and C. H. Bennett for interesting discussions and questions which helped me to clarify some points in my constructions. This work was supported, in part, by the Russian Foundation for Fundamental Research, grant No 96-01-01113. Part of this work was completed during the 1997 Elsag-Bailey – I.S.I. Foundation research meeting on quantum computation.

References

[1] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science*. Los Alamitos, CA: IEEE Press, pp. 124–134 (1994).

[2] P. Shor, Fault-tolerant quantum computation. In *Proceedings of the Symposium on the Foundations of Computer Science*. Los Alamitos, CA: IEEE Press (1996); e-print quant-ph/9605011.

[3] E. Knill and R. Laflamme, Concatenated quantum codes, e-print quant-ph/9608012 (1996)

[4] E. Knill, R. Laflamme and W. Zurek, Accuracy threshold for quantum computation, e-print quant-ph/9610011 (1996).

[5] D. Aharonov and M. Ben-Or, Fault tolerant quantum computation with constant error, e-print quant-ph/9611025 (1996).

[6] A. Yu. Kitaev, Quantum computing: algorithms and error correction, *Russian Math. Surveys*, to be published (1997).

[7] C. Zalka, Threshold estimate for fault tolerant quantum computing, e-print quant-ph/9612028 (1996).

[8] A. Yu. Kitaev, Quantum error correction with imperfect gates. In *Proceedings of the Third International Conference on Quantum Communication and Measurement, September 25-30, 1996*, to be published (1997).

[9] F. Wilczek, Fractional statistics and anyon superconductivity, *World Scientific*, Singapore (1990).

[10] R. Dijkgraaf, V. Pasquier and P. Roche, Quasi-Hopf algebras, group cohomology and orbifold models, *Nucl. Phys. B (Proc. Suppl.)* **18B** (1990).

[11] F. A. Bais P. van Driel and M. de Wild Propitius, Quantum symmetries in discrete gauge theories, *Phys. Lett.* **B280**, 63 (1992).

[12] F. A. Bais and M. de Wild Propitius, Discrete gauge theories, e-print hep-th/9511201 (1995).

[13] H. K. Lo and J. Preskill, Non-abelian vortices and non-abelian statistics, *Phys. Rev.* **D48**, 4821 (1993).

[14] G. Castagnoli and M. Rasetti, The notion of symmetry and computational feedback in the paradigm of steady, simultaneous quantum computation, *Int. J. of Mod. Phys.* **32**, 2335 (1993).

[15] D. Gottesman, *Phys. Rev.* **A54**, 1862 (1996).

[16] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* **78**, 405 (1997).

[17] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, e-print quant-ph/9512032 (1995)

[18] D.Arovas, J.R.Schrieffer, and F.Wilczek, Fractional statistics and the quantum Hall Effect, *Phys. Rev. Lett.* **53**, 722–723 (1984).

[19] T.Einarsson, Fractional statistics on a torus, *Phys. Rev. Lett.* **64**, 1995-1998 (1984).

[20] V. G. Drinfeld, Quantum groups. In *Proc. Int. Cong. Math. (Berkley, 1986)*, pp. 798-820 (1987).

[21] M. Sweedler, Hopf algebras, W. A. Benjamin, Inc., New York (1969).

[22] S. Majid, Quasi-triangular Hopf algebras and Yang-Baxter equation, *Intern. J. of Modern Phys.* **A5**, 1-91 (1990).

[23] C. Kassel, Quantum groups, Springer-Verlag, New York (1995).

[24] A. Yu. Kitaev, Quantum measurements and Abelian stabilizer problem, e-print quant-ph/9511026 (1995).

[25] G. t'Hooft, *Nucl. Phys.* **B138**, 1 (1978).