Perfect quantum-error-correction coding in 24 laser pulses

Samuel L. Braunstein
Universität Ulm, Abteilung Quantenphysik, 89069 Ulm, Germany
*and SEECS, University of Wales, Bangor, Gwynedd LL57 1UT, United Kingdom**

John A. Smolin
IBM Research Division, Yorktown Heights, New York 10598
(Received 29 April 1996; revised manuscript received 21 October 1996)

An efficient coding circuit is given for the perfect quantum-error correction of a single quantum bit (qubit) against arbitrary one-qubit errors within a five-qubit code. The circuit presented employs a double ''classical'' code, i.e., one for bit flips and one for phase shifts. An implementation of this coding circuit on an ion-trap quantum computer is described that requires 26 laser pulses. Another circuit is presented requiring only 24 laser pulses, making it an efficient protection scheme against arbitrary one-qubit errors. In addition, the performances of two error-correction schemes, one based on the quantum Zeno effect and the other using standard methods, are compared. The quantum Zeno error correction scheme is found to fail completely for a model of noise based on phase diffusion. [S1050-2947(97)03902-4]

PACS number(s): 03.65.−w, 89.70.+c, 89.80.+h, 02.70.−c

INTRODUCTION

Quantum-error-correction schemes [1–8] hold the promise of reliable storage, processing, and transfer of quantum information. They actively ''isolate'' a quantum system from perturbations, which would otherwise decohere the state [9,10]. How quickly this decoherence occurs depends, to a large extent, on what degrees of freedom are involved: single- or many-body, electronic, nuclear, etc. In principle, however, the development of quantum-error correction allows one to decouple a quantum state from arbitrary few-particle perturbations.

The decoupling in quantum error correction schemes is achieved by unitarily ''rotating'' the state into one involving a larger number of degrees of freedom. In this larger space the information about the original state is recorded only in multiparticle correlations. Thus, if only a few particles undergo decohering perturbations, the multiparticle correlations are not destroyed, but only mixed among each other. After determining which few-particle perturbation has occurred we can unmix the multiparticle correlations and hence reconstruct the original state. If, by contrast, decohering perturbations accumulate over too many particles then the multiparticle correlations are no longer isolated and the error correction begins to break down.

In this paper an efficient coding circuit for arbitrary single-quantum-bit (qubit) errors is given. Its efficiency is quantified relative to a specific quantum computer model: Cirac and Zoller's ion-trap model [11]. Next, two schemes designed to protect against single-qubit phase noise are studied. One scheme relies on the quantum Zeno effect [12,13] and uses two qubits to protect against ''slow'' perturbations of the system; the other is a more conventional quantum-error-correction scheme [6,7,14] that requires three qubits to protect against arbitrary single-particle dephasing. The poor behavior of the Zeno schemes is discussed and explained.

*Permanent address.

EFFICIENT CODING

Various authors [4,5,8] have presented circuits implementing five qubits that protects one qubit of quantum information. This code is described as ''perfect'' since it allows for the complete correction of arbitrary single-qubit errors. (The term qubit [15] represents the amount of ''quantum'' information stored in an arbitrary two-state quantum system.) In this section a simpler version of the Laflamme *et al.* coding circuit [5] is presented. We discuss the structure of the circuit and consider its efficiency. The measure of efficiency used [16] is the number of laser pulses required to implement the scheme on an ion-trap quantum computer. A second circuit yielding a slightly different version of this code was found by a computer search and is the most efficient circuit so far constructed for one-bit encoding.

Figure 1 shows our simplification of the five-bit coding circuit of Laflamme *et al.* [5]. This circuit uses single-particle rotations

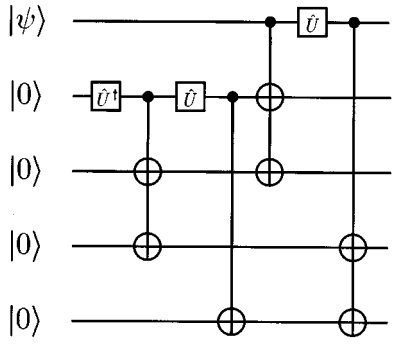
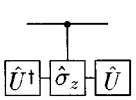


FIG. 1. Efficient quantum five-qubit error correction circuit. The system starts at the left and is successively processed through each of the elementary gates proceeding from left to right. Here the qubit $|\psi\rangle$ is rotated into a protective five-particle state by the unitary operations represented by the elements of this circuit. The three-qubit gates shown are simply pairs of controlled-NOT gates.

$$\hat{U}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\ , \tag{1}$$

represented by the square ''one-qubit'' gates in the circuit and two-particle controlled-NOT gates

$$\oplus = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \equiv \quad ; \tag{2}$$



here the $\oplus$ notation is chosen because of the equality of the controlled-NOT operation and the mathematical exclusive-OR operation. The conditional $\hat{\sigma}_z$ operation itself is given by

$$\equiv \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}\ . \tag{3}$$

Here these elements are represented in the basis where $|0\rangle=\binom{1}{0}, |1\rangle=\binom{0}{1}$, and

$$\begin{aligned}|00\rangle&=(1,0,0,0)^{\mathrm{T}}\ ,\\ |01\rangle&=(0,1,0,0)^{\mathrm{T}}\ ,\\ |10\rangle&=(0,0,1,0)^{\mathrm{T}}\ ,\\ |11\rangle&=(0,0,0,1)^{\mathrm{T}}\ ,\end{aligned} \tag{4}$$

etc. Decoding is executed by running the coding circuitry backward, finally recovering the original state after a few extra operations [5,17].

The circuit in Fig. 1 has an interesting structure: The coding initially entangles four auxiliary particles and then executes a double ''classical'' code on the state to be protected. This ''stores'' the degrees of freedom of $|\psi\rangle$ in the correlations of a five-particle entangled state. The classical codes each consist of a simple triple redundancy of the qubit on the upper line of Fig. 1: The first classical code may be interpreted as protecting against random bit flips and the second against random phase shifts. This double code was motivated by theorem 6 of Steane [6]. He found, however, that such double coding required a minimum of seven qubits for a *linear* quantum code. The circuit in Fig. 1 produces a code that is not linear [5].

To see that the above circuit reproduces the Laflamme *et al.* code it is sufficient to consider how this circuit acts on an arbitrary qubit $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$. With the auxiliary qubits initially in the states $|0\rangle$ the circuit generates the superposition

$$\begin{aligned}&\alpha(|00000\rangle+|00110\rangle+|01001\rangle-|01111\rangle+|10011\rangle\\ &\quad+|10101\rangle+|11010\rangle-|11100\rangle)+\beta(|00011\rangle-|00101\rangle\\ &\quad-|01010\rangle-|01100\rangle-|10000\rangle+|10110\rangle+|11001\rangle\\ &\quad+|11111\rangle)\\ &=\alpha(|b_2\rangle|00\rangle+|b_5\rangle|01\rangle+|b_7\rangle|10\rangle+|b_4\rangle|11\rangle)\\ &\quad+\beta(|b_1\rangle|11\rangle-|b_6\rangle|10\rangle+|b_8\rangle|01\rangle-|b_2\rangle|00\rangle),\end{aligned} \tag{5}$$

where the $|b_j\rangle$ are the three-particle Bell states defined by Laflamme *et al.* [5]. Here we have dropped the normalization constant. This code is clearly idential to the Laflamme *et al.* code up to the relabeling of the Bell states.

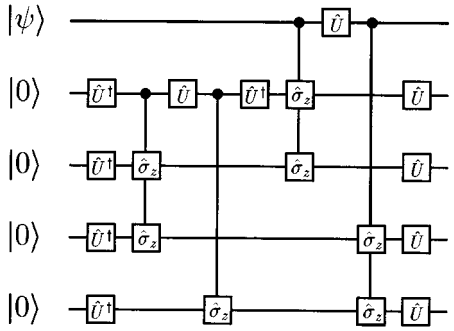


FIG. 2. Circuit from Fig. 1 rewritten in terms of the gate primitives of an ion-trap quantum computer [11]. The single two-qubit gate is the conditional $\hat{\sigma}_z$ operation defined in Eq. (2) and pairs of them are drawn as three-qubit gates. Each single-qubit rotation requires one laser pulse, the two-qubit gate requires three pulses, and the three-qubit gates, if implemented as single elements, require only four laser pulses each [16]. This circuit, therefore, uses a total of 26 laser pulses.

How efficient is this coding scheme? One measure is obtained by asking how many ''clock cycles'' are required to execute the scheme on a quantum computer. The most promising device, at least for relatively small numbers of two-state systems, is a linear ion-trap model suggested by Cirac and Zoller [11]. In this model the basic clock frequency is limited by that of the center-of-mass mode of the trapped ions as they undergo coupled oscillations. This limitation arises from the requirement that the laser linewidths be narrower than the lowest vibrational mode of the ions, thus ensuring that only the correct energy levels are addressed by the laser pulses. The energy-time uncertainty relation therefore implies that the duration of the laser pulses must exceed the inverse frequency of this lowest vibrational mode. We then conclude that for ion-trap computers the number of laser pulses required to complete a particular algorithm is a reasonable measure of its efficiency [18].

Rather than directly using the circuit in Fig. 1, we optimize it for the particular primitive instruction set of the ion-trap quantum computer in the manner shown in Fig. 2. (Note that the three-qubit operations, the controlled double $\hat{\sigma}_z$ operations, require only four laser pulses each, as demonstrated in the Appendix.)

A simple counting of the requirements for the circuit of Fig. 2 yields 26 laser pulses. By contrast the original circuit of Laflamme *et al.* [5] appears to require at least 41 laser pulses. Another scheme using six two-qubit controlled-NOT gates and five one-bit gates was mentioned in Ref. [8]; its unoptimized form requires 35 laser pulses [19].

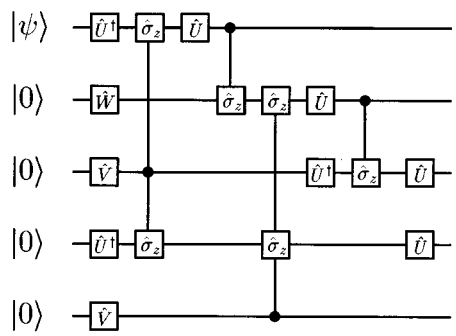


FIG. 3. Best known circuit for encoding a single qubit in a five-qubit error correction code. As shown, 24 laser pulses would be required to implement this circuit on an ion-trap quantum computer.

It is worth noting here that short of trying all possible circuits it is not known in general how to determine the optimal circuit. Much of the optimization achieved here is actually hidden in the choice of the circuit in Fig. 1, where a number of rearrangements were tried by hand to yield the ''simplest'' circuit. More efficient circuits than shown in Fig. 2 can be found by computer search. In fact, we show our current best in Fig. 3, where we define two new one-bit operations

$$\hat{V}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}, \quad \hat{W}=\hat{V}\hat{U}^{\dagger} \ . \tag{6}$$

As shown, it requires only 24 laser pulses, not counting further speedups such as paralleling the operation of several of its one-bit gates.

An alternative method of error correction has been suggested by Vaidman *et al.* [13]. Its operation involves a circuit that can provide only error detection *not* error correction; however, by sufficiently rapid operation of the circuit the quantum Zeno effect allows it to ''turn off'' the relatively slow errors. Using the quantum Zeno effect it corrects for *small* single-particle perturbations of the system rather than the arbitrary single-particle errors of the standard schemes. Nonetheless, quantum Zeno error correction has the advantage of only requiring four qubits. Further, we find that the coding and decoding may each be executed using as few as 16 laser pulses with possibly only one extra for the auxiliary qubit resetting. How effective are these error correction schemes that rely on the quantum Zeno effect? We shall now evaluate their performance for correcting phase-diffusion noise.

ZENO VERSUS STANDARD QUANTUM-ERROR CORRECTION

In this section we compare the performance of Zeno and standard methods for quantum-error correction. Rather than considering the schemes discussed in the preceding section, however, we study simpler schemes that protect only against one-qubit dephasing. In particular, we compare a compact two-qubit code given by Chuang and Laflamme [12], and independently by Vaidman *et al.* [13] versus a standard three-qubit code [6,7,14]. The two-qubit scheme relies on the quantum Zeno effect to correct for *small* deviations in the system's state, whereas the three-qubit code can correct for

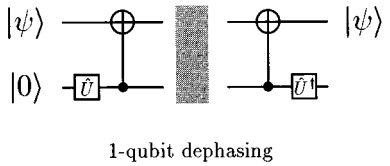


FIG. 4. Quantum Zeno error correction scheme [12,13]. Both coding and decoding circuits are shown. (The shaded region represents one-qubit dephasing.)

arbitrary one-qubit dephasing. How do these schemes compare?

Figures 4 and 5 show complete coding and decoding circuits for both schemes. Clearly, the Zeno scheme uses fewer resources and requires fewer gates to operate so it has a distinct implementational advantage over the more conventional schemes.

Our model for dephasing assumes that the phase in each qubit undergoes an independent random walk according to

$$\alpha|0\rangle+\beta|1\rangle\rightarrow\alpha|0\rangle+\beta e^{i\phi(t)}|1\rangle \tag{7}$$

(up to normalization), where the perturbing phases $\phi(t)$ are given by the Ito stochastic calculus [20] with

$$\begin{aligned}\phi(0)&=0,\\ \langle\langle d\phi(t)\rangle\rangle&=0,\\ \langle\langle d\phi(t)\ d\phi(t')\rangle\rangle&=2\delta(t-t')dt,\end{aligned} \tag{8}$$

etc., where $d\phi(t)$ is the Ito differential and the doubled angular brackets represent stochastic averages. Equation (7) therefore describes our model of the shaded regions in Figs. 4 and 5.

How do each of the above error correction circuits work if applied only after the dephasing has acted for a time t? Delaying the decoding circuit in Fig. 4 for a time t after the coding yields

$$\hat{\rho}_0\equiv\begin{pmatrix}|\alpha|^2 & \overline{\beta\alpha}\\ \overline{\alpha\beta} & |\beta|^2\end{pmatrix}\rightarrow\begin{pmatrix}|\alpha|^2 & e^{-t}\,\overline{\beta\alpha}\\ e^{-t}\,\overline{\alpha\beta} & |\beta|^2\end{pmatrix} \ , \tag{9}$$

where $\hat{\rho}_0$ is the initial density matrix for the qubit $|\psi\rangle$; i.e., there is no improvement using the Zeno error correction scheme for this model of noise even for short times. A similar result was noted by Chuang and Laflamme [12]. By contrast, a delay for time t in circuit 5 before decoding yields

$$\hat{\rho}_0\rightarrow(2+3e^{-t}-e^{-3t})\ \hat{\rho}_0/4+(2+e^{-3t}-3e^{-t})\ \hat{\sigma}_x\ \hat{\rho}_0\ \hat{\sigma}_x/4, \tag{10}$$

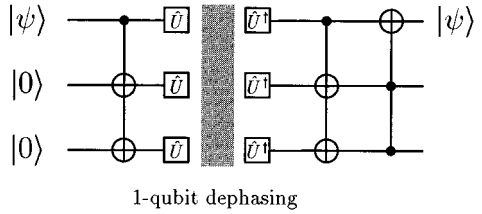


FIG. 5. Standard quantum one-bit dephasing correction scheme [14]. Both coding and decoding circuits are shown.

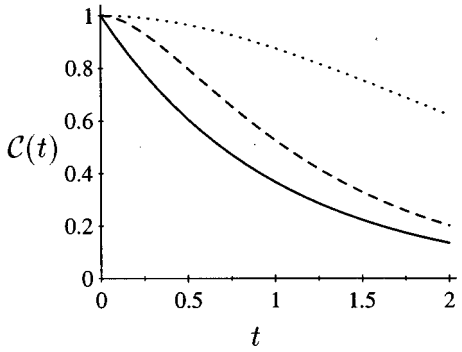


FIG. 6. Measure of coherence for no error correction (solid line), the Zeno error correction scheme of Fig. 4 at time t (solid line), the three-qubit scheme of Fig. 5 at time t (dashed line, representing the lower bound), and the tenfold repetition of the three-qubit scheme by time t (dotted line, representing the lower bound).

with $\hat{\sigma}_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ being one of the standard Pauli matrices.

A measure of (relative) coherence between a pair of states is given by the absolute value of the off-diagonal terms in the density matrix $\hat{\rho}(t)$ [21],

$$\mathcal{C}(t) \left| \frac{\langle 1|\hat{\rho}(t)|0\rangle}{\langle 1|\hat{\rho}_0(t)|0\rangle} \right| . \tag{11}$$

The two-qubit Zeno error correction scheme yields

$$\mathcal{C}_{\text{2-qubit}}(t) = e^{-t} , \tag{12}$$

whereas the standard three-qubit scheme has a coherence bounded by its worst case

$$\mathcal{C}_{\text{3-qubit}}(t) \geqslant (3e^{-t} - e^{-3t})/2 . \tag{13}$$

Finally, we note that n evenly spaced repetitions in a time t of an error correction scheme will yield an improved coherence $\mathcal{C}$ according to

$$\mathcal{C}^{n \text{ shot}}(t) = [\mathcal{C}(t/n)]^n . \tag{14}$$

The performances of the Zeno two-qubit scheme, conventional three-qubit scheme, and a tenfold repetition of the latter are displayed in Fig. 6.

Why does the Zeno-error-correction scheme fail to work for the noise model of Eq. (7) even at short times? Put simply, the random-walk model for dephasing implies that the expected deviation of the phase grows as $\sqrt{t}$ instead of t. The error therefore accumulates too quickly for the Zeno scheme.

The random-walk model of noise really has two time scales: the typical time between random steps and the much longer dephasing time. The stochastic calculus approach assumes that the former of these time scales is so short as to be negligible. This means that in this model of noise, no matter how quickly we operate the Zeno-error-correction scheme many stochastic steps have occurred. The averaging over these many random steps in phase produces a pertubabtion that overwhelms the linear correction to the state. However, the Zeno-error-correction schemes discussed above [12,13] require that the change in the system's state be dominated by linear terms. The implications are that phase diffusion is *not* corrected by these Zeno-error-correction schemes unless they are repeatedly used at a rate faster than the typical time between random steps of the phase: the phase-diffusion time itself is already much too slow. How fast does this need to be in practice? That depends on the detailed source of the phase diffusion: For instance, it might be relatively slow (though still faster than the phase diffusion time) when the principle source of noise is due to external mechanical noise. Other models, however, are very much faster: Unruh's [9] study of decoherence due to vacuum fluctuations in the electromagnetic field coupling to a qubit yielded a time scale comparable to x-ray frequencies.

It is worth mentioning two error ''stabilization'' schemes that utilize the Zeno effect: Zurek [23] has outlined a scheme that averages several copies of a computation and Berthiaume *et al.* [24,25] have considered in some detail a scheme that projects several copies of a computation to the symmetric state. Because these schemes evenly spread errors over several copies of a computation rather than attempt to correct them it may be that they circumvent the problem with dephasing discussed here. We leave this question open for further study.

Quantum-error correction of arbitrary single-qubit errors is rather costly of computing resources: a minimum of five qubits and possibly 24 laser pulses for coding (decoding being only slightly more expensive [17]). This might be compared with the resources required to execute a moderate unprotected calculation; Beckman *et al.* [16] show that the Shor algorithm could be implemented on 6 trapped ions using only 38 laser pulses to factor the number 15 [22]. Alternate error correction schemes based on the quantum Zeno effect are much more efficient to implement. However, they fail for simple models of decoherence, such as the model of phase diffusion considered here.

CONCLUSION

In conclusion, because error correction is virtually as expensive as the simplest error-correction-free computations, it appears unlikely that full quantum-error correction will be implemented for computational purposes in the first few generations of quantum computers. Instead, quantum-error correction will probably initially play an important role in the long-term storage of quantum information: implementing a true quantum memory.

ACKNOWLEDGMENTS

The authors thank the ISI for giving them the opportunity to collaborate; S.L.B. appreciates the support of the Alexander von Humboldt Foundation and discussions with N. Cohen and D. DiVincenzo.

APPENDIX: QUANTUM NETWORKS ON ION TRAPS

In this appendix we describe how controlled double $\hat{\sigma}_z$ operations may be performed in four laser pulses on a Cirac-Zoller ion-trap quantum computer [11]. These operations are the *three-qubit* operations seen in Fig. 2. Labeling the ground and excited states of ion i as $|g\rangle_i$ and $|e\rangle_i$, respectively, and the Fock state of the center-of-mass vibrational mode of the trap as $|n\rangle_{\text{c.m.}}$, we summarize two important operations: A

suitably tuned π pulse on ion i yields the operation [11,16]

$$\hat{W}^{(i)}_{\rm phon}: \quad \begin{cases} |g\rangle_i|0\rangle_{\rm c.m.} \rightarrow |g\rangle_i|0\rangle_{\rm c.m.} \\ |g\rangle_i|1\rangle_{\rm c.m.} \rightarrow -i|e\rangle_i|0\rangle_{\rm c.m.} \\ |e\rangle_i|0\rangle_{\rm c.m.} \rightarrow -i|g\rangle_i|1\rangle_{\rm c.m.} \\ |e\rangle_i|1\rangle_{\rm c.m.} \rightarrow |e\rangle_i|1\rangle_{\rm c.m.} \ , \end{cases} \tag{A1}$$

whereas a differently tuned 2π pulse on ion j yields [11,16]

$$\hat{V}^{(j)}: \quad \begin{cases} |g\rangle_j|0\rangle_{\rm c.m.} \rightarrow |g\rangle_j|0\rangle_{\rm c.m.} \\ |g\rangle_j|1\rangle_{\rm c.m.} \rightarrow -|g\rangle_j|1\rangle_{\rm c.m.} \\ |e\rangle_j|0\rangle_{\rm c.m.} \rightarrow |e\rangle_j|0\rangle_{\rm c.m.} \\ |e\rangle_j|1\rangle_{\rm c.m.} \rightarrow |e\rangle_j|1\rangle_{\rm c.m.} \ . \end{cases} \tag{A2}$$

Finally, another appropriately tuned π pulse on ion j yields [11,16]

$$\hat{V}^{(j)}_{\rm phon}: \quad \begin{cases} |g\rangle_j|0\rangle_{\rm c.m.} \rightarrow |g\rangle_j|0\rangle_{\rm c.m.} \\ |g\rangle_j|1\rangle_{\rm c.m.} \rightarrow -i|e'\rangle_j|0\rangle_{\rm c.m.} \\ |e\rangle_j|0\rangle_{\rm c.m.} \rightarrow |e\rangle_j|0\rangle_{\rm c.m.} \\ |e\rangle_j|1\rangle_{\rm c.m.} \rightarrow |e\rangle_j|1\rangle_{\rm c.m.} \ , \end{cases} \tag{A3}$$

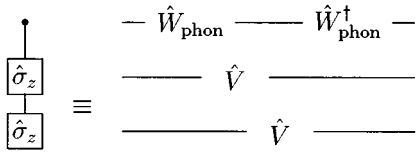
where $|e'\rangle_j$ is a *different* excited state of ion j.

Using these operations and taking the trap's vibrational mode intially in the ground state $|0\rangle_{\rm c.m.}$ we find

$$\hat{W}^{(i)\dagger}_{\rm phon}\hat{V}^{(k)}\hat{V}^{(j)}\hat{W}^{(i)}_{\rm phon}: \quad |\epsilon\rangle_i|\eta_1\rangle_j|\eta_2\rangle_k \rightarrow (-1)^{\eta_1\epsilon} \times (-1)^{\eta_2\epsilon}|\epsilon\rangle_i|\eta_1\rangle_j|\eta_2\rangle_k . \tag{A4}$$

This completes the construction of the controlled double $\hat{\sigma}_z$ operation. We note that this construction requires only four laser pulses as opposed to the six required to perform the two controlled $\hat{\sigma}_z$ operations separately.

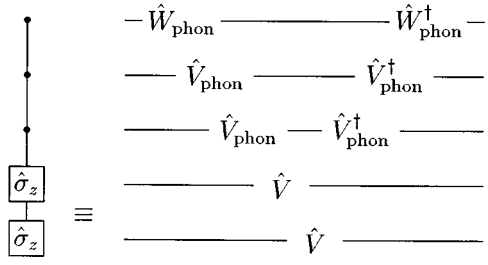
In order to see how to generalize this approach let us introduce a different notation. We start by labeling the states to be acted on by $|\epsilon_1, \epsilon_2, \ldots, \eta_1, \eta_2, \ldots\rangle$, where the ϵ_j represents the jth control bit and η_k represents the kth controlled bit. When only a single of either kind of bit occurs we drop the corresponding subscript. Then we introduce a *space-time* diagram of events on the ion trap to replace the usual circuit notation. In these space-time diagrams the horizontal lines represent the world lines of the ions (in an exactly analogous way that they do in the usual circuits). Finally, we superpose on these world lines the events corresponding to an appropriately tuned laser on each ion. In this way Eq. (A4) becomes



$$= (-i)^{\epsilon}(-1)^{\bar{\eta}_1\epsilon}(-1)^{\bar{\eta}_2\epsilon}(+i)^{\epsilon} = (-1)^{\eta_1\epsilon}(-1)^{\eta_2\epsilon} , \tag{A5}$$

where $\overline{\eta} \equiv (1-\eta)$. Reading from left to right, this circuit decomposes to $\hat{W}^{(1)\dagger}_{\rm phon}\hat{V}^{(3)}\hat{V}^{(2)}\hat{W}^{(1)}_{\rm phon}$, where now we must explicitly add the numbers of the ions. Since these circuits only involve conditional phase changes it is sufficient to ask what phases accumulate as we operate the various pulses. We see that whenever there is an *even* number of phases to be flipped (i.e., an even number of $\hat{V}$ pulses) the phases accumulated from pulses on the control bits are unwanted and need to be canceled by applying the inverse operation the second time around. In particular, here we apply $\hat{W}^{\dagger}_{\rm phon}$ the second time since we applied $\hat{W}_{\rm phon}$ the first. Similarly, below where we make use of $\hat{V}_{\rm phon}$ for a second and further control bit, we must use $\hat{V}^{\dagger}_{\rm phon}$ the second time whenever there is an even number of bits to have their phases flipped (i.e., an even number of $\hat{V}$'s).

We now give two more example constructions

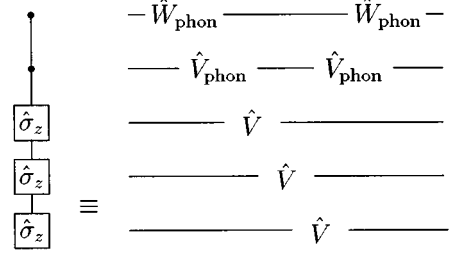


$$= (-i)^{\epsilon_1}(-i)^{\bar{\epsilon}_2\epsilon_1}(-i)^{\bar{\epsilon}_3\epsilon_2\epsilon_1}(-1)^{\bar{\eta}_1\epsilon_3\epsilon_2\epsilon_1} \times (-1)^{\bar{\eta}_2\epsilon_3\epsilon_2\epsilon_1}(+i)^{\bar{\epsilon}_3\epsilon_2\epsilon_1}(+i)^{\bar{\epsilon}_2\epsilon_1}(+i)^{\epsilon_1} = (-1)^{\eta_1\epsilon_3\epsilon_2\epsilon_1}(-1)^{\eta_2\epsilon_3\epsilon_2\epsilon_1} , \tag{A6}$$

which correspond to the series of laser pulses

$$\hat{W}^{(1)\dagger}_{\rm phon}\hat{V}^{(2)\dagger}_{\rm phon}\hat{V}^{(3)\dagger}_{\rm phon}\hat{V}^{(5)}\hat{V}^{(4)}\hat{V}^{(3)}_{\rm phon}\hat{V}^{(2)}_{\rm phon}\hat{W}^{(1)}_{\rm phon} , \tag{A7}$$

and as a final example



$$= (-i)^{\epsilon_1}(-i)^{\bar{\epsilon}_2\epsilon_1}(-1)^{\bar{\eta}_1\epsilon_2\epsilon_1} \times (-1)^{\bar{\eta}_2\epsilon_2\epsilon_1}(-1)^{\bar{\eta}_3\epsilon_2\epsilon_1}(-i)^{\bar{\epsilon}_2\epsilon_1}(-i)^{\epsilon_1} = (-1)^{\eta_1\epsilon_2\epsilon_1}(-1)^{\eta_2\epsilon_2\epsilon_1}(-1)^{\eta_3\epsilon_2\epsilon_1} , \tag{A8}$$

which correspond to the series of laser pulses

$$\hat{W}^{(1)}_{\rm phon}\hat{V}^{(2)}_{\rm phon}\hat{V}^{(5)}\hat{V}^{(4)}\hat{V}^{(3)}\hat{V}^{(2)}_{\rm phon}\hat{W}^{(1)}_{\rm phon} . \tag{A9}$$

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[3] A. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[4] J.A. Smolin, in *Joint Mathematics Meetings of the AMS, Orlando, 1996* (Ref. [8]).
[5] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[6] A. M. Steane, Proc. R. Soc. London (to be published).
[7] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. **54**, 3824 (1996).
[9] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).
[10] R. Landauer, Philos. Trans. R. Soc. London, Ser. A **353**, 367 (1996).
[11] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[12] I. L. Chuang and R. Laflamme (unpublished).
[13] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A **54**, 1745 (1996).
[14] S. L. Braunstein (unpublished).
[15] R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994); B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
[16] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A **54**, 1034 (1996).
[17] Just how many extra operations are required to complete decoding depends on whether it is done by added circuitry or by external observation of the state of the auxiliary qubits. When the necessity of reinitializing the auxiliary qubits is included it appears that as few as three extra ''clock cycles'' should be required for the external-observation schemes since most of the operations act only one single particle and so could probably be executed in parallel.
[18] Indeed, it is likely that many of the operations can be run in parallel. For instance, if the blocks of unitary operations at the beginning and ending of Fig. 2 are executed in parallel then the entire circuit would be completed in only 20 clock cycles.
[19] Optimization depends on the detailed structure of the circuit, which was not given in Ref. [8].
[20] C. W. Gardiner, *Handbook of Stochastic Methods* (Springer-Verlag, Berlin, 1983); L. Arnold, *Stochastic Differential Equations* (Wiley, New York, 1973).
[21] S. L. Braunstein, Phys. Rev. A **45**, 6803 (1992).
[22] The smallest number for which Shor's algorithm strictly applies is 15.
[23] W. H. Zurek, Phys. Rev. Lett. **53**, 391 (1984).
[24] A. Berthiaume, D. Deutsch, and R. Jozsa, in *Proceedings of the Workshop on Physics and Computation—PhysComp94* (IEEE Computer Society, Dallas, 1994).
[25] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello (unpublished).