Superlattices and Microstructures, Vol. 23, No. 3/4, 1998

Nanoelectronic implementations of reversible and quantum logic

S. BANDYOPADHYAY, A. BALANDIN
Department of Electrical Engineering, University of Nebraska, Lincoln, NE 68588-0511, U.S.A.

V. P. ROYCHOWDHURY, F. VATAN
Department of Electrical Engineering, University of California–Los Angeles, Los Angeles, CA 90095, U.S.A.

(Received 10 December 1997)

We describe two different proposals for implementing mathematically reversible and dissipationless logic in *nanoelectronic* systems. Both are amenable to quantum computation and use interacting single electrons housed in quantum dots to elicit logic functions. In these systems, qubit errors accruing from decoherence events can be partially remedied by quantum error control coding. We present some new results on burst-correcting quantum codes that can address *correlated* errors in nanostructures.

Key words: quantum dots, single electronics, quantum computing, error control coding.

1. Introduction

Microelectronic logic gates of present-day vintage dissipate about 1 pJ of energy per switching cycle. The Semiconductor Industry Association's National Technology Roadmap projects that by the year 2007, the dynamic power dissipated in CMOS devices will be 600 nW per logic gate with a gate density of 10^7 cm^{-2}, corresponding to a dissipation of 30 W cm^{-2} of chip area [1]. Assuming that CMOS will exhibit a switching delay of $\sim$10 ps, the energy dissipated in a switching cycle will be about 6×10^{-18} J. Single-electron transistors and related devices are predicted to have similar energy dissipation [2]. At this time, these figures are still far above the $kT \ln 2$ ($T = 300$ K) classical limit for *irreversible* logic set forth by Landauer in his seminal 1961 paper [3].

It is natural to ask from the perspective of a solid-state device engineer if power dissipation is vital. Fifteen years ago, removal of 1000 W cm^{-2} was demonstrated in a silicon chip [4]. Unfortunately, heat sinking technology has not kept pace with solid-state circuits technology and heat removal continues to be a problem. It appears that by the year 2007, the gate density may be constrained to 10^{10} gates/cm^2 from mere heat sinking considerations. Engineering denser device density will require either more efficient heat removal techniques, or less energy dissipation per logic gate. It is the latter objective that stimulates research in quasi- or fully reversible logic devices and motivates this paper. In reversible logic gates, the energy dissipated in a logic

0749–6036/98/030445 + 20 $25.00/0 sm970562

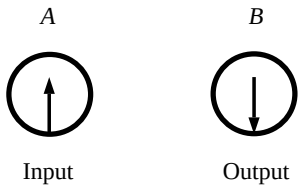


Fig. 1. Two exchange-coupled electrons in two quantum dots A and B. The ground state of this system is antiferromagnetic; the spin orientation of one electron is antiparallel to that of the other. If spin is used to encode logic bits, then this system acts as an inverter if we consider one quantum dot (A) as the input port and the other (B) as the output port. The spin orientation in A can be aligned by a SPSTM tip thus enabling a 'write' operation. The spin orientation in B can be read by a SPSTM tip thus enabling a 'read' operation. The same system can act as a quantum inverter since the ground-state wavefunction is an entangled Einstein–Podolsky–Rosen state and each quantum dot can exist in a coherent superposition of 'upspin' and 'downspin' states.

swing could approach zero†. This could certainly mitigate the technological problems associated with efficient heat sinking.

In the past, there have been concrete proposals for various versions of reversible logic that dissipate less than $kT \ln 2$ amount of energy per switching cycle. They include schemes described by [8–10, 7, 11, 12]. None of these proposals envisioned *nanoelectronic* implementation. Recently, a nanoelectronic version of a classical but reversible gate based on single-electron parametron has appeared in the literature [13]. We have proposed a nanoelectronic implementation of classical irreversible logic [14] where the energy dissipation could approach (but not fall below) $kT \ln 2$. Nanoelectronic versions of quantum gates have also appeared in the literature [15]. Here we propose and examine two nanoelectronic versions of reversible logic and quantum gate which can be potentially dissipationless. The first is an inverter based on two spin-coupled single electrons in adjacent quantum dots. The second is a Toffoli–Fredkin gate [7] based on three Coulomb-coupled single electrons in three quantum dots. The latter is based on ideas proposed by Lloyd [16] and implements a locally connected architecture capable of both classical reversible computation and quantum bit (qubit) manipulation. In principle, such an architecture can result in a functionally complete quantum computer.

2. Spin-coupled inverter

Consider two single electrons housed in closely spaced quantum dots as shown in Fig. 1. We will assume that there is only one size-quantized level in each dot. A weak magnetic field H_z is applied globally to define a spin polarization direction. The ground state of this two-electron system is antiferromagnetic [17] with the two spins antiparallel (one spin will be aligned along the magnetic field and the other opposite to it). If spin polarization is used to encode binary bits such that up-spin represents binary bit 1 and down-spin binary bit 0, then the spin polarization of one electron is the logic complement of that of the other when the system is in ground state. This can be the basis of an inverter. We can orient the spin polarization in one dot (with a local magnetic field) to conform to the input bit and the output will automatically be the inverse of the input.

† In his 1961 paper, Landauer showed that logical irreversibility leads to physical irreversibility and energy dissipation. Logical reversibility implies that the input to a logic gate can be deduced from the output and not just the other way around (i.e. the logical function is mathematically invertible). The minimum energy dissipated in a logically irreversible step is $kT \ln 2$. We will designate any system where the energy dissipated is less than $kT \ln 2$ as a physically reversible (dissipationless) system. Strictly speaking, they must also be logically reversible. It is of course understood that logically reversible gates (e.g. an inverter) do not necessarily have to be dissipationless (all present-day CMOS inverters dissipate energy during switching), but they could *in principle* be dissipationless. We will avoid the term 'conservative logic' in this paper since it has different meanings in different contexts. Fredkin and Toffoli [7] used conservation to indicate 'bit conservation' rather than purely energy conservation and pointed out that logical reversibility and conservation are independent properties. There are computing machinery that are logically reversible but not bit conservating [5] and vice versa [6].

The Hubbard Hamiltonian for this system is

$$\mathcal{H} = \sum_{i\sigma}[\epsilon_0 n_{i\sigma} + g\mu_B H_i \,\mathrm{sign}(\sigma)] + \sum_{\langle ij\rangle} t_{ij}[c^+_{i\sigma}c_{j\sigma} + h.c] + \sum_i U_i n_{i\uparrow}n_{i\downarrow} + \sum_{\langle ij\rangle\alpha\beta} J_{ij}c^+_{i\alpha}c_{i\beta}c^+_{j\beta}c_{j\alpha} + H_z\sum_{i\sigma} g\mu_B n_{i\sigma}\,\mathrm{sign}(\sigma) \tag{1}$$

where the first term denotes the electron energy in the ith dot (H_i is a z-directed magnetic field applied selectively to the ith dot with, say, a spin-polarized scanning tunneling microscope (SPSTM) tip, to orient its spin polarization), the second term denotes the hopping between the dots, the third term is the Coulomb repulsion within the ith dot, the fourth term is the exchange interaction between nearest-neighbor dots, and the last term is the Zeeman splitting induced by the globally applied magnetic field H_z directed along the z-direction.

Molotkov and Nazin [18] simplified this Hamiltonian to the Heisenberg model which yields

$$\mathcal{H} = J\sum_{\langle ij\rangle}\sigma_{zi}\sigma_{zj} + J\sum_{\langle ij\rangle}\left[\sigma_{xi}\sigma_{xj} + \sigma_{yi}\sigma_{yj}\right] + \sum_{input\ dots}\sigma_{zi}h^{input}_{zi} \qquad (J>0) \tag{2}$$

where we have neglected the global magnetic field H_z and the Coulomb repulsion U_i.† The quantity J is the exchange splitting and h^{input}_{zi} is the Zeeman splitting caused by the local magnetic field applied with an SPSTM tip to the ith dot to orient the spin(s) of its electron(s).

The above Hamiltonians describe any number of dots, each containing any number of electrons. Here, we are concerned with the special case of just two dots each containing only one electron. We will call these two dots A and B, where A is the input dot (whose spin polarization is set by an external SPSTM tip to conform to the input bit) and B is the output dot. Let us consider the case when the input bit corresponds to 'upspin'.

In the basis of two electron states, the Hamiltonian in eqn (2) can be written as

$$\begin{array}{c} \begin{array}{cccc} |\downarrow\downarrow\rangle & |\downarrow\uparrow\rangle & |\uparrow\downarrow\rangle & |\uparrow\uparrow\rangle \end{array} \\ \begin{pmatrix} h_A+J & 0 & 0 & 0 \\ 0 & h_A-2J & 2J & 0 \\ 0 & 2J-h_A & -2J & 0 \\ 0 & 0 & 0 & -h_A+J \end{pmatrix} \end{array} \begin{array}{l} |\downarrow\downarrow\rangle \\ |\downarrow\uparrow\rangle \\ |\uparrow\downarrow\rangle \\ |\uparrow\uparrow\rangle \end{array}$$

where h_A is the Zeeman splitting caused by the externally applied local magnetic field in input dot A.

The eigenenergies and eigenstates of the above Hamiltonian are found by diagonalizing

Eigenenergies	Eigenstates
$h_A + J$	$\|\downarrow\downarrow\rangle$
$-J+\sqrt{h_A^2+4J^2}$	$\sqrt{\frac{1}{2}\left(1+\frac{h_A}{\sqrt{h_A^2+4J^2}}\right)}\|\uparrow\downarrow\rangle + \sqrt{\frac{1}{2}\left(1-\frac{h_A}{\sqrt{h_A^2+4J^2}}\right)}\|\downarrow\uparrow\rangle$
$-J-\sqrt{h_A^2+4J^2}$	$\sqrt{\frac{1}{2}\left(1-\frac{h_A}{\sqrt{h_A^2+4J^2}}\right)}\|\uparrow\downarrow\rangle - \sqrt{\frac{1}{2}\left(1+\frac{h_A}{\sqrt{h_A^2+4J^2}}\right)}\|\downarrow\uparrow\rangle$
$-h_A + J$	$\|\uparrow\uparrow\rangle$

† Recently, Bychkov *et al*. (A. M. Bychkov, L. A. Openov and I. A. Semenikin, JETP LeH., **66**, 298 (1997)) studied some aspects of this system using the full Hubbard Hamiltonian. Their results are qualitatively identical to ours.

In the absence of any applied local magnetic field (h_A = 0), the ground state energy is -3J and the ground-state wavefunction is $\frac{1}{2}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ which is an entangled Einstein–Podolsky–Rosen state. Neither the input dot nor the output dot has a definite spin polarization.

In [19], we showed that if the system is initially in the ground state and a local magnetic field is applied to the input dot A at time t=0 to align its spin polarization to the 'up' state, then unitary evolution of the system according to

$$\psi(t) = \exp[-i\mathcal{H}t/\hbar]\psi(0), \tag{3}$$

mandates that the wavefunction at time t, is given by

$$\psi(t) = c_2(t)|\uparrow\downarrow\rangle + c_3(t)|\downarrow\uparrow\rangle \tag{4}$$

where

$$\begin{aligned} c_2(t) &= \frac{e^{iJt/\hbar}}{\sqrt{2}}\left[\cos(\omega t) - i\left(\frac{h_A}{\hbar\omega} + \sqrt{1 - \frac{h_A^2}{\hbar^2\omega^2}}\right)\sin(\omega t)\right] \\ c_3(t) &= -\frac{e^{iJt/\hbar}}{\sqrt{2}}\left[\cos(\omega t) - i\left(\frac{h_A}{\hbar\omega} - \sqrt{1 - \frac{h_A^2}{\hbar^2\omega^2}}\right)\sin(\omega t)\right] \end{aligned} \tag{5}$$

and $\hbar\omega = \sqrt{h_A^2 + 4J^2}$.

If the system was to act as an inverter, it should ultimately reach the state $|\uparrow\downarrow\rangle$. This desired state however is not an eigenstate of the system. Consequently, the system will continue to evolve to a different state unless a 'read' operation collapses the wavefunction as soon as the desired state is reached. The time to reach the desired state, which we will designate the switching time, is given by

$$\tau_d = \frac{h}{4\sqrt{h_A^2 + 4J^2}}. \tag{6}$$

Note that this time must be much shorter than $\hbar/kT$ in order to maintain reasonable coherence in quantum computing [20]. This can be achieved by making $J >> kT$. For 100 Å diameter dots separated by 1 eV high and 20 Å wide barriers, the exchange splitting J can be on the order of 100 meV in semiconductors.

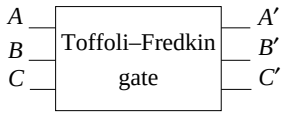
If the inverter's initial state is the ground state, then it is possible to switch the inverter *completely* (i.e. $c_2(\tau_d) = 1$, $c_1(\tau_d) = c_3(\tau_d) = c_4(\tau_d) = 0$) if $h_A = 2J$. However, if the initial state is not the ground state, then the inverter can never switch completely to the desired state (i.e. $c_2(\tau_d) < 1$). Nonetheless, we can still define a switching time as the delay that elapses before the closest approach to the desired state (in other words the time required to reach the maximum value of c_2). This switching time is still given by eqn (6). This equation also shows that the inverter will 'switch' in a finite time *even if* the switching energy $h_A \to 0$. However, the 'switching' is ephemeral since the system will continue to evolve unitarily unless a read operation collapses the wavefunction at the right juncture.

In this system, there is no dissipation whatsoever except during the read operation. Therefore, the product of dissipated energy and switching delay (necessary to complete the computation) can obviously be zero. The product of applied energy and switching delay is

$$h_A\tau_d = \frac{hh_A}{4\sqrt{h_A^2 + 4J^2}}. \tag{7}$$

We immediately see that any energy-time uncertainty that might have been expected is violated

$$h_A\tau_d < \frac{\hbar}{2} \qquad \text{if } h_A < \frac{2J}{\sqrt{\pi^2 - 1}}. \tag{8}$$



A	B	C	A'	B'	C'
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

Fig. 2. The Toffoli–Fredkin gate and its truth table.

Thus we can violate the uncertainty by making h_A arbitrarily small (and yet switching in a finite time). It should be emphasized that h_A is the energy applied to switch the inverter and is not necessarily *dissipated*. Even if it were completely dissipated, the above equation would still clearly show that there is no energy-time uncertainty limitation on (dissipated) energy-delay product, contrary to the popular view espoused in [21, 22]. Landauer agrees that there is no limit imposed by the uncertainty principle as far as dissipated energy is concerned [23]. In fact, concrete and detailed classical models of dissipationless computation have been provided by several authors [7–11] and numerous quantum-mechanical models of dissipationless computation have also been forwarded starting with the early work of Benioff [24, 25]. These models require no dissipated energy, but usually do require input energy to switch. What we see in the pathological example above is that there is no energy-time uncertainty limit even when the energy concerned is the *applied energy* rather than the dissipated energy. Computation can proceed by applying arbitrarily small energy to initiate the process.

3. Coulomb coupled quantum dots for Toffoli–Fredkin gate and quantum computation

In the previous section, we described a quantum inverter. An inverter however is not a universal gate. The Toffoli–Fredkin gate is a mathematically (and hence physically) reversible three-bit *universal* gate with three inputs A, B, C and three outputs A', B' and C'. The truth table for this gate is shown in Fig. 2.

In this gate, $A' = A$ and $B' = B$. The bit $C' = \bar{C}$ only if $A = B = 1$. Otherwise, $C' = C$.

A physical realization of the Toffoli–Fredkin gate that is most easily amenable to nanoelectronic adaptations was proposed by Lloyd [16] expanding on ideas set forth earlier by Mahler *et al*. [26]. The Lloyd architecture consists of an array of three weakly coupled quantum systems A, B and C. Each system can exist in one of two energy states E_0^i and E_1^i ($i \in A, B, C$) which represent logic 0 and 1. Furthermore, A, B, C are distinct systems such that the resonant energies $\hbar\omega_i = E_1^i - E_0^i$ are different for each of them ($\omega_A \neq \omega_B \neq \omega_C$). A π_i pulse is a radiation that obeys the condition

$$\frac{1}{\hbar}\int \vec{\mu}_B^i \cdot \hat{e}\mathcal{E}(t)dt = \pi \tag{9}$$

where $\vec{\mu}_B^i$ is the induced dipole moment between the ground state and excited state of the ith system, $\hat{e}$ is the polarization unit vector of the incident radiation and $\mathcal{E}(t)$ is the magnitude of the pulse envelope at time t. Such a pulse flips the ith system from the excited state to the ground state and vice versa. It is assumed that the duration of this pulse is much shorter than the inverse of the spontaneous decay rate from the excited to the ground state.

Because of the nearest-neighbor interaction between A, B and C, the resonant energies $\hbar\omega_i$ for each of

them is no longer unique and depends on whether its nearest neighbors are in the excited or ground state. Thus

$$\begin{aligned}\omega_A &\rightarrow \omega_0^A, \omega_1^A \\ \omega_B &\rightarrow \omega_{00}^B, \omega_{01}^B, \omega_{10}^B, \omega_{11}^B \\ \omega_C &\rightarrow \omega_0^C, \omega_1^C. \end{aligned} \tag{10}$$

Here, the subscripts on the right-hand side refer to the states of the corresponding system's nearest neighbor(s). For instance, ω_{00}^B is the resonant frequency of system B when its two neighbors A and C are both in their ground states.

A Toffoli gate can be realized by shining a π pulse with frequency ω_{11}^B. The state of B is inverted only if both A and C are in their excited states. This characteristic realizes the truth table of a Toffoli gate.

In order to perform the computation, one needs to connect various Toffoli gates. This can be realized without physical wires if we have a linear array consisting of units ABC, ABC, ... Compuation is performed by first initializing the array to the input with appropriate sequence of π pulses and then applying another series of π pulses to complete the computation. This methodology was described in detail in [16].

The above system can also be used to perform quantum computation if both π and $\pi/2$ pulses are used. A $\pi_i/2$ pulse puts the ith system in a state $1/\sqrt{2}(|1\rangle - |0\rangle)$ which is a 'qubit' in the coherent superposition of bits 1 and 2. By using an appropriate pulse train, one can perform quantum computation.

Landauer's criticism of this scheme is two-fold. First, it is not truly dissipationless unless the π or $\pi/2$ pulses can be recycled. This would also require that they are not distorted by interaction with the system. Second, interaction with the environment will cause errors and error correction will require dissipation. In principle, the latter objection is no longer tenable in view of the recent advances in quantum error control coding [31, 33, 32]. Errors can be corrected by 'software' rather than 'hardware'. Of course, this is done at the expense of increased memory and a larger system may decohere more quickly than a smaller system. We will address the issue of error correction later in this paper.

Landauer's first criticism is much more difficult to rebut. Photon recycling is not an unheard of concept in solid state systems [27–30] but it is difficult. The requirement that the pulse shape remain undistorted in any wave guide is a tall order. This would require the wave guide to have specific nonlinearities so that the pulses essentially become solitons. At this time, we do not have a suitable design for such a recycler.

In the remainder of this paper, we will examine a specific implementation of Lloyd's generic ideas and provide a concrete example of a Toffoli–Fredkin gate. This example is suitable for nanoelectronics.

3.1. Nanoelectronic version of a Toffoli–Fredkin gate

Consider an array of three quantum dots with high barriers (Fig. 3). Each houses a single conduction band electron.

For high enough barriers, we can neglect any overlap between the wavefunctions of electrons in adjacent dots, and write the many-body wavefunction of the three-electron system as a product of three single-particle wavefunctions in the Hartree approximation

$$\Psi_{n,k,l} \equiv \Psi_{n,k,l}(x_1, x_2, x_3) = \psi_n(x_1)\phi_k(x_2)\chi_l(x_3), \tag{11}$$

where $\psi_n(x_1)$, $\phi_k(x_2)$, and $\chi_l(x_3)$ are the single-electron envelope functions for the first, second and third dots, respectively. Subscripts $n,\ k,\ l$ denote conduction subband levels. We assume that each dot has two bound states in the conduction band so that each electron can occupy either ground state ($n = 1, k = 1$, or $l = 1$) or the excited state ($n = 2, k = 2$, or $l = 2$). These two states encode logic bits 1 and 0.

Owing to Coulomb interaction, the resonant frequency for transitions between the excited and ground states

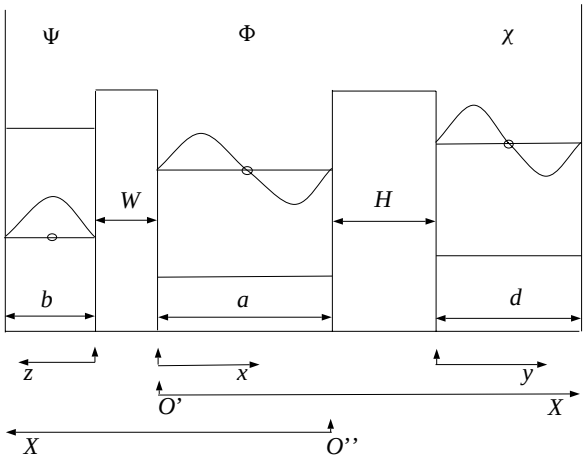


Fig. 3. The potential profile for a three-dot system showing the wavefunction envelopes for the ground and excited states.

in one dot depends on whether the electron(s) in the neighboring dot(s) are in the excited or ground state. For the central dot, this means that $\omega_{11} \neq \omega_{10} \neq \omega_{01} \neq \omega_{00}$. This forms the basis of a Toffoli–Fredkin gate. Note that in reality, a single gate only requires that ω_{11} be distinct. However, arbitrary data manipulation requires that all ω's be distinct.

Let us calculate the resonant transition frequency of the central quantum well as a function of two adjacent wells' states. We denote the widths of the well as d, a, and b (see Fig. 3) and will refer to them as the 'left' well (L), the 'central' well (C), and the 'right' well (R), respectively. The barier thicknesses are W and H. The first-order perturbation corrections to the energy of the k subband of the C well are given by the expression

$$E_{n,k,l} = E_k + \langle \Psi_{n,k,l} | V(x_3 - x_2) | \Psi_{n,k,l} \rangle + \langle \Psi_{n,k,l} | V(x_1 - x_2) | \Psi_{n,k,l} \rangle, \tag{12}$$

where $V(x_i - x_j)$ is the Coulomb interaction terms, x_i are absolute coordinates of electrons belonging to different wells, m^* is the effective mass of the conduction band electron, E_k is the unperturbed confined energy which is given for the square well potential by a regular expression

$$E_k = \frac{k^2 \pi^2 \hbar^2}{2m^* a^2}. \tag{13}$$

To simplify the calculation, we define a set of local coordinate systems (see Fig. 3). Substituting in eqn (11), the electron envelope functions for the square well potential (written in local coordinates), can be rewritten as

$$\Psi_{n,k,l} = \sqrt{\frac{2}{d}} \sin\left(\frac{\pi n z}{d}\right) \sqrt{\frac{2}{a}} \sin\left(\frac{\pi k x}{a}\right) \sqrt{\frac{2}{b}} \sin\left(\frac{\pi l y}{b}\right). \tag{14}$$

The distance between electrons in the R and C wells (in O′ coordinate system) is $x_3 - x_2 = a + W + y - x$, while the distance between electrons in the L and C wells (in O″ coordinate system) is $x_1 - x_2 = a + H + z - x$. With the limits of integrations determined by the well boundaries, eqn (12) now reads

$$E_{n,k,l} = \frac{\pi^2 \hbar^2 k^2}{2m^* a^2} + \frac{e^2}{\pi \epsilon^* ab} \int_{x=0}^{a} \int_{y=0}^{b} \frac{\sin^2(\pi k x/a) \sin^2(\pi l y/b)}{a + W + y - x} \, dx \, dy + \frac{e^2}{\pi \epsilon^* ad} \int_{x=0}^{a} \int_{z=0}^{d} \frac{\sin^2(\pi k x/a) \sin^2(\pi n z/d)}{a + H + z - x} \, dx \, dz, \tag{15}$$

where $\epsilon^* = f_b \epsilon_b + f_w \epsilon_w$ is an effective dielectric constant of the system, f_b (f_w) and ϵ_b (ϵ_w) are the volume

fraction and dielectric constant of the barrier (well) material, respectively. Note that with this definition ϵ^* is a function of well width when the barrier thickness is fixed.

The energy of the transition between the first excited state ($k = 2$) and the ground state ($k = 1$) in the central well can now be written as a function of the principal numbers n and l of the neighboring wells:

$$\Delta E_{n,l} = \frac{3\pi^2\hbar^2}{2m^*a^2} + \frac{e^2}{\pi\epsilon^* ab}\int_{x=0}^{a}\int_{y=0}^{b}\frac{\sin(3\pi x/a)\sin(\pi x/a)\sin^2(\pi l y/b)}{a+W+y-x}\,dx\,dy + \frac{e^2}{\pi\epsilon^* ad}\int_{x=0}^{a}\int_{z=0}^{d}\frac{\sin(3\pi kx/a)\sin(\pi kx/a)\sin^2(\pi nz/d)}{a+H+z-x}\,dx\,dz. \tag{16}$$

Here we have utilized some trigonometrical equalities to simplify the result of the subtraction $\Delta E_{n,l} = E_{n,2,l} - E_{n,1,l}$.

In order to be able to build a conditional quantum gate (or the Toffoli–Fredkin gate), the transition energy $\Delta E_{n,l}$ should be different for all possible quantum state $\{|n\rangle, |l\rangle\}$: $\Delta E_{1,2} \neq \Delta E_{2,1} \neq \Delta E_{1,1} \neq \Delta E_{2,2}$. Obviously, the two states which are most difficult to resolve are $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$. For convenience, we write here explicitly the energy difference between these two states

$$\Delta E_{1,2} - \Delta E_{2,1} = \frac{e^2}{\pi\epsilon^* a}\int_{x=0}^{a}\left(\int_{y=0}^{b}\frac{\sin(3\pi x/a)\sin(\pi x/a)\sin(3\pi y/b)\sin(\pi y/b)}{b(a+W+y-x)}\,dy \times \int_{z=d}^{0}\frac{\sin(3\pi kx/a)\sin(\pi kx/a)\sin(\pi z/d)\sin(3\pi z/d)}{d(a+H+z-x)}\,dz\right)dx. \tag{17}$$

To derive eqn (17), we used the fact that $\sin^2(2\pi y/b) - \sin^2(\pi y/b) = \sin(3\pi y/b)\sin(\pi y/b)$, and changed the limits of integration. For the special case when $W = H$, eqn (17) can be further simplified by substitution of variable in the integrand to

$$\Delta E_{1,2} - \Delta E_{2,1} = \frac{e^2}{\pi\epsilon^* a}\int_{x=0}^{a}\int_{u=d}^{b}\frac{d\sin(3\pi u/b)\sin(\pi u/b) + b\sin(3\pi u/d)\sin(\pi u/d)}{bd(a+H+u-x)} \times \sin(3\pi kx/a)\sin(\pi kx/a)\,du\,dx. \tag{18}$$

It is easy to see from eqn (18) that when the thicknesses of two peripheral wells and barriers are equal ($d = b$ and $W = H$), the states $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ are degenerate and can not be resolved. This is a direct result of the symmetry of the system and can be easily guessed without mathematical consideration. A more interesting consequence of eqns (17) and (18) is that there exists a ratio of b/d ($\neq 1$) such that the integral in (18) vanishes, and the states are degenerate again. The physical origin of this additional degeneracy will be discussed later. One should find optimum values of well thicknesses b and d such that the states $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ are resolved.

3.2. Resonant energies in Coulomb coupled dots

In calculating resonant energies in Coulomb coupled dots, we will concentrate mostly on two material systems. The first is InAs characterized by light electron effective mass $m^*(\text{InAs}) = 0.023m_o$ and strong dielectric screening $\epsilon(\text{InAs}) = 14.6$ (m_o is the free electron mass). The second is CdS which is characterized by heavy electron effective mass $m^*(\text{CdS}) = 0.21m_o$ and relatively weak dielectric screening ($\epsilon(\text{CdS}) = 5.4$ for the frequencies close to band gap resonance and $\epsilon(\text{CdS})$ approaches 3.1 for the infrared region relevant to intraband transitions). Ordered and regimented arrays of InAs and CdS dots uniformly dispersed in an alumina matrix are being self-assembled in our laboratories [34]. These are realistic systems that are relatively easy to produce.

In order to find optimum values of peripheral well thicknesses, we will calculate transition energy $\Delta E_{n,l}$ as a function of the R well thickness b while fixing the L well thickness d and using it as a parameter. For

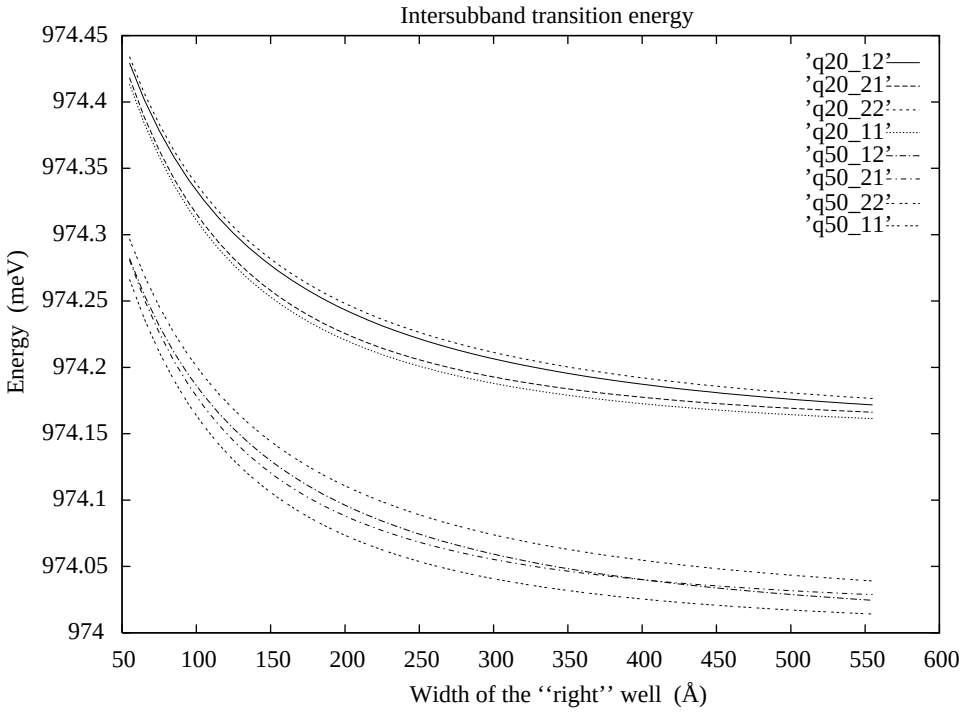


Fig. 4. Energy of the transition between the first excited and ground states in the 'central well' as a function of the width of the 'right' well. The upper family of curves corresponds to the 'left' well width of 20 Å, the lower one corresponds to the 'left' well width of 50 Å. The results are shown for all four possible combination of states in the two extremal wells. Material parameters for InAs have been used.

simplicity, the thickness of the left barrier will be assumed to be equal to that on the right ($W = H$). These thicknesses will be assumed to be 20 Å unless otherwise stated. This value of the barrier thickness guarantees negligible barrier penetration of the wavefunction.

In Fig. 4, we present the energy of the transition between the first excited state and the ground state in the C well as a function of the R well width (b). The curves are shown for InAs quantum wells. The thickness of the C well is 100 Å. The L well width is varied over two values: 20 Å and 50 Å. It is interesting to note that the splittings between different states attain maximum values when b is in the range 150–170 Å. Moreover, the states $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ are degenerate not only at $b = d = 50$ Å but also at $b \approx 400$ Å. At first, this may appear surprising. The physical origin of the additional degeneracy lies in the fact that Coulomb perturbation to the transition energies depends on the distance between particles as well as on the electron envelopes which serve as weight functions in the integrand in eqn (18). Consequently, at some values of $b/d \neq 1$ the integration over u in eqn (18) vanishes.

In order to examine the behavior of the worst resolved states $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$, we plot separately the difference in transition energy between these two states as a function of the R well thickness (see Fig. 5). The L well thickness is chosen to be 55 Å (solid line), 105 Å (dashed line), and 505 Å (dotted line). As one can see, the average splitting is very small for this system and represents a fraction of meV at its maximum. Each curve has an additional degeneracy ($\Delta E_{1,2} - \Delta E_{2,1} = 0$) at $b/d \neq 1$ which should be avoided while designing the logic gate. Since $\Delta E_{1,2} - \Delta E_{2,1}$ does not depend on m^* (see eqn (7)) and strongly depends on ϵ^*, one can expect that the resolution of the $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ states will be better for CdS and any other

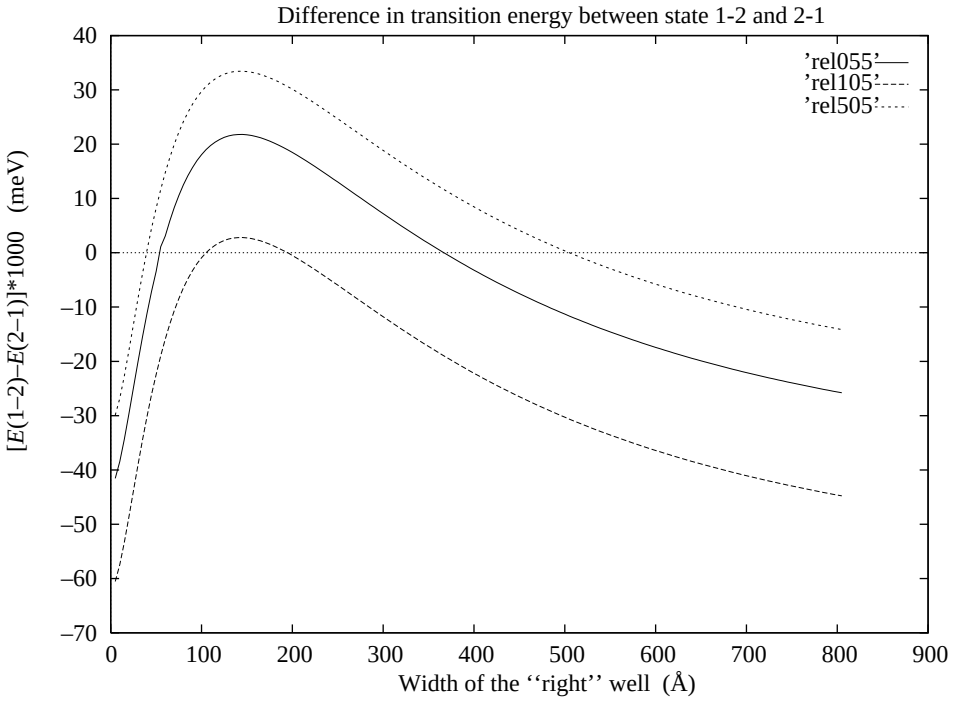


Fig. 5. The difference in transition energy $\Delta E_{1,2} - \Delta E_{2,1}$ as a function of the width of the 'right' well. The results are shown for three different values of the width of the 'left' well. The material parameters used for calculation correspond to InAs.

system with lower dielectric constant. This is indeed the case, and it is clearly seen in Fig. 6. The splitting between states is an order of magnitude higher for the CdS system compared to the InAs system.

It is intuitively clear that in order to increase the energy difference between $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ states, one should introduce higher asymmetry into the system. Apart from varying the R well thickness, it is possible to break the symmetry by changing the barrier thickness (see Fig. 6). One can notice that increasing the width of one of the barriers decreases the energy separation between $\{|1\rangle, |1\rangle\}$ and $\{|2\rangle, |2\rangle\}$ states but increases it for $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ states. The degeneracies ($b = 50$ Å and $b \approx 400$ Å), for the uniform barrier system, disappear for a system with different barriers. This is of course also desirable from architectural considerations. Another potential way of increasing the energy splitting between $\{|1\rangle, |2\rangle\}$ and $\{|2\rangle, |1\rangle\}$ states is through engineering the potential profile. One well can be rectangular and the other parabolic. This may be achieved through dopant grading.

4. Quantum error correction codes: Software countermeasures against decoherence

One serious drawback of solid-state systems is the short coherence time for electrons. It has recently been demonstrated that the electron coherence time saturates to about 1 ns in most solids as the temperature is decreased towards 0 K [35]. This would have seriously dampened prospects for solid state implementation of quantum computers were it not for the recent advances in quantum error control coding.

The theory of quantum error correction is now an active area of research [31–33, 36–38]. Various techniques regarding construction of quantum error correcting codes based on classical codes have been proposed [31–33, 38]. Here, we briefly review the process of error-correction for quantum information, and then present some new results on the design of codes for the case where decoherence events are *correlated*. Correlation

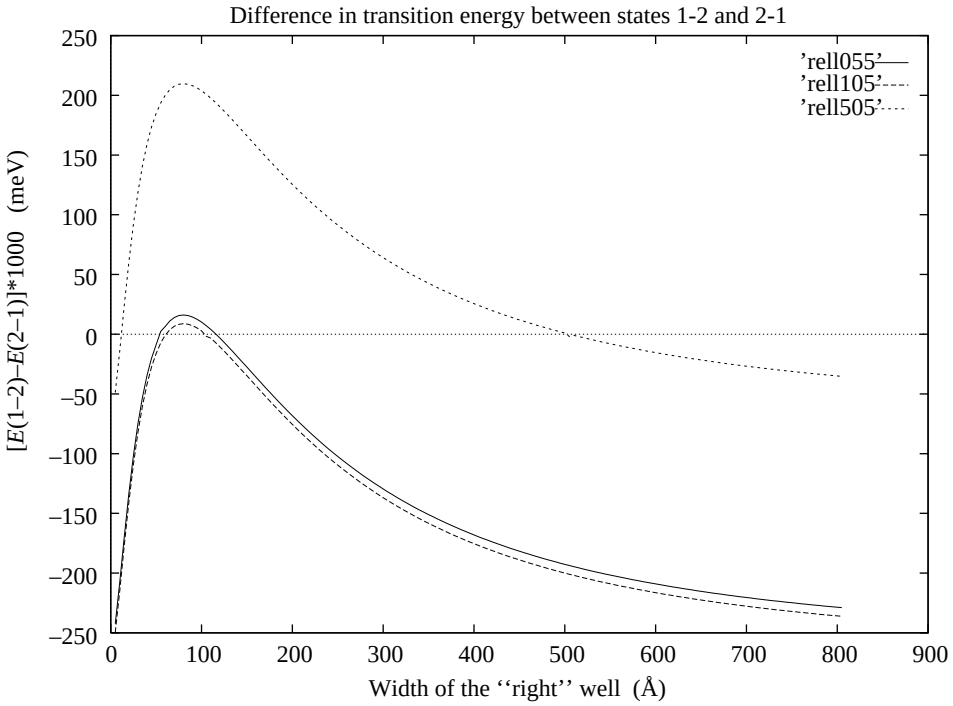


Fig. 6. The difference in transition energy $\Delta E_{1,2} - \Delta E_{2,1}$ as a function of the width of the 'right' well. The results are shown for three different values of the width of the 'left' well. The material parameters used for this calculation correspond to CdS.

between decoherence events is a more physical and realistic assumption in nanoelectronic systems (such as the quantum-dot version of the Toffoli–Fredkin gate or the spin inverter) since the spatial separation between dots is typically much smaller than the radiation wavelength or phonon wavelength causing decoherence. In fact, inelastic scattering that affect a large number of dots equally (when the offending phonon's wavelength spans several dots) may not cause serious decoherence. This model contrasts with the usual assumption in recent work that decoherence events of individual qu-bits are independent. The results are briefly presented here, and the associated proofs and details are documented in [39].

4.1. A basic review

Noise is an unavoidable feature of any physical system. In classical systems, it can be viewed as arising due to the interaction between those degrees of freedom of a physical system pertinent to a measurement and their interaction with other known and/or unknown degrees of freedom, in a random manner. For example, in a classical communication channel, a perfectly correlated input signal appears noisy at the output due to interaction of the channel with unintended external radiation during signal propagation. Here, the degrees of freedom that are pertinent to the communication channel are the electronic signals carrying the binary 0 and 1 values, while the undesired degrees of freedom—which interact with the channel—correspond to that of the external radiation.

In quantum systems, there are two sources for signal noise: (i) interaction of the pertinent degrees of freedom of the physical system with that of the external world as discussed in the previous paragraph, and (ii) due to the probabilistic nature of quantum physics. The second component is present even in the absence of interaction with external degrees of freedom (of course, only until a measurement is made). An example where this is

manifested is the shot noise in current flowing across a barrier. In this section, though we deal with qubits, which are quantum systems, we will be concerned only with correcting errors arising due to interaction of the system with external degrees of freedom. Typical examples of such external degrees of freedom are the phonon and photon fields.

Model:

The desired degrees of freedom of a quantum computer with N bits are the 2^N orthonormal states $|I\rangle \sim |x_1 x_2 \ldots x_{2^N}\rangle$ where, $x_1, x_2, \ldots, x_{2^N} \in \{0, 1\}$. The undesired degrees of freedom, which comprise all degrees of freedom other than the 2^N mentioned states are labeled $|e_1\rangle$, $|e_2\rangle$, ..., and will hence forth be referred to as the environment. The environment states, as will appear in the rest of this section, are not necessarily orthogonal to one another or normalized to unity. The most general model for decoherence is one where an initially unentangled state of the computer and the environment $|\phi\rangle \otimes |e\rangle$, upon interaction with the environment, evolves to a state where each of the basis states of the computer is entangled with a state of the environment,

$$|\phi\rangle \otimes |e\rangle = \left(\sum_{j=1}^{2^N} a_j |j\rangle \right) |e\rangle \rightarrow \sum_{j=1}^{2^N} a_j |e_j\rangle \otimes |j\rangle. \tag{19}$$

If the various states $|e_j\rangle$ are identical, we simply have the initial state. The degree of decoherence would depend on the correlation between the various environment states. An error that maximally entangles the states of the computer with those of the environment would be hopeless to correct. In the classical case this corresponds to a situation where almost all bits have flipped, clearly a hopeless case for classical error correction. The probability for such an event is, however, very small and it is sufficient to design codes that correct errors in only a small fraction of the total number of bits.

Independent qubit decoherence model (IQD model): Each qubit interacts with a seperate environment and decoheres as (we drop the outer product symbol between the states of the computer and the environment),

$$|0\rangle_j |e\rangle \rightarrow |e_1\rangle |0\rangle_j + |e_2\rangle |1\rangle_j \tag{20}$$

$$|1\rangle_j |e\rangle \rightarrow |e_3\rangle |0\rangle_j + |e_4\rangle |1\rangle_j \ , \tag{21}$$

where the subscript j denotes the jth qubit. From a physical view point, each qubit can be considered to interact with an independent environment if the inter qubit distance is much larger than the correlation length of the environment.

4.2. Spatially correlated qubit errors and burst-correcting quantum codes

The IQD model is a valid assumption when the spatial separation of qubits in a quantum register is larger than the correlation length of the reservoir (or source of decoherence). Whether this condition is met or not will depend on specific physical models for quantum computers. The two main hardware proposals for quantum computers are the ion trap model [40] and the polymer chain model [16]. The exact nature of decoherence in these models is not well understood but we would expect the IQD model to break down in the polymer chain model where qubits are only a few angstroms apart. Interaction with phonons whose spatial extent would be several atoms long will result in correlated decoherence of spatially continuous qubits. Reference [41] provided the first step in studying the effect of decoherence by assuming different models for interaction of qubits and the reservoir. Specifically, the effect of decoherence on a two-qubit system under circumstances when the IQD model is valid and when the correlation length of the reservoir is larger than the separation of the two qubits were studied. An important conclusion was that the second model for decoherence (i.e. where the correlation length is larger than the separation of qubits) leads to superdecoherence and subdecoherence of certain off-diagonal elements of the density matrix in comparison with the IQD model.

If the details of the decoherence mechanism of qubits are known, then it might be possible to build more efficient error correcting codes compared with the IQD model. In classical error correction, it is well known that magnetic tapes used for storage are usually defective over length scales corresponding to a few bits. Then it is sufficient to code information on the tape so as to correct only spatially continuous errors. Similarly, in a classical communication channel, disturbances of the channel over short time periods lead to random single errors while disturbances over longer time periods lead to temporally continuous errors at the receiver. Such errors are called burst errors and the corresponding error-correcting codes have significantly higher rates (see, e.g. [42]).

In this paper, we discuss a quantum analog of burst-error-correcting codes. These codes would be important (i) when the coherence length of the reservoir is large enough to cause decoherence of spatially contiguous bits to be dominant, (ii) in storing of quantum information on a string of qubits (this case is similar to the magnetic tape case mentioned above; uninteded impurities here may perturb the energy levels of a few contiguous qubits) and (iii) in communication of quantum information where entangled qubits would be temporally transported over an appropriate communication channel [37].

We described different schemes for constructing quantum burst-correcting codes. As expected, these classes of codes are more efficient than codes that protect against random errors. More specifically, to protect against burst errors of width b (where b is a fixed constant), it is enough to map $n - \log n - O(b)$ qubits to n qubits, while in the case of t random errors at least $n - t \log n$ qubits should be mapped to n qubits (the best construction so far maps $n - (t+1)\log n - O(1)$ qubits to n qubits). Only the results and the associated steps are summarized here, and all the proofs can be found in [39].

4.2.1. Basic concepts and definitions

In this section we provide basic definitions and notations about quantum error-correcting codes. We shall also describe various methods for constructing these codes; these techniques will be used in Sections 4.2.3 for constructing several different kinds of burst-correcting quantum codes.

A sequence of amplitude errors in qubits $i_1, \ldots, i_t$ of a block of n qubits can be represented by the unitary operator X_α, where the binary vector α of length n has 1 components only at positions $i_1, \ldots, i_t$. Thus, for the basis $|v_1\rangle, \ldots, |v_{2^n}\rangle$ of the 2^n-dimensional Hilbert space of n qubits, we have

$$X_\alpha |v_i\rangle = |v_i + \alpha\rangle . \tag{22}$$

Similarly, a sequence of phase errors can be written as

$$Z_\beta |v_i\rangle = (-1)^{v_i \cdot \beta} |v_i\rangle , \tag{23}$$

where the binary vector β represents the positions of errors, and $v_i \cdot \beta$ is the inner product of two binary vectors modulo 2. Note that

$$Z_\beta X_\alpha = (-1)^{\alpha \cdot \beta} X_\alpha Z_\beta . \tag{24}$$

Since we will be concerned with sets of errors with special structures, it is useful for us to consider a general setting, where a set $\mathcal{E}$ of possible errors of the form $\pm X_\alpha Z_\beta$ is fixed (a similar approach is followed in [43]). Let $\overline{\mathcal{E}}$ be the set of the pairs (α, β) such that either $X_\alpha Z_\beta$ or $-X_\alpha Z_\beta$ is in $\mathcal{E}$. For example, the result of the entanglment of introducing at most t *random* errors in a state $|x\rangle$ can be repesented as $\pm X_\alpha Z_\beta |x\rangle$, where $\mathrm{wt}(\alpha \cup \beta) \leq t$ †. Therefore, in this case $\overline{\mathcal{E}} = \{ (\alpha, \beta) \mid \mathrm{wt}(\alpha \cup \beta) \leq t \}$. We will use the following notations:

$$\overline{\mathcal{E}}_X = \{ \alpha \in \{0,1\}^n \mid (\alpha, \beta) \in \overline{\mathcal{E}} \text{ for some } \beta \in \{0,1\}^n \} \cup \{\mathbf{0}\},$$
$$\overline{\mathcal{E}}_Z = \{ \beta \in \{0,1\}^n \mid (\alpha, \beta) \in \overline{\mathcal{E}} \text{ for some } \alpha \in \{0,1\}^n \} \cup \{\mathbf{0}\}.$$

† Here $\mathrm{wt}(c)$ denotes the weight of the binary vector c, i.e. the number of 1-components of c; and the binary vector $\alpha \cup \beta$ is the result of component-wise or operation of α and β, for example $(011010) \cup (000110) = (011110)$.

For example, in the above example where $\mathcal{E}$ is the set of at most t (random) errors, both $\overline{\mathcal{E}}_X$ and $\overline{\mathcal{E}}_Z$ are equal to $\{ c \in \{0,1\}^n \mid \mathrm{wt}(c) \leq t \}$. The following result gives a necessary and sufficient condition for a set of quantum states to constitute a quantum code.

THEOREM 4.1([37, 43]). A 2^k-dimensional subspace $\mathcal{Q}$ of $\mathbb{C}^{2^n}$ is an $((n, 2^k))$ error-correcting quantum code mapping k qubits to n qubits that protect against all errors in $\mathcal{E}$ if for every orthonormal basis $|x_1\rangle, \ldots, |x_{2^k}\rangle$ of $\mathcal{Q}$ and every $e, e' \in \mathcal{E}$

$$\langle x_i \mid ee' \mid x_j \rangle = 0, \qquad \text{if } i \neq j, \tag{25}$$

$$\langle x_i \mid ee' \mid x_i \rangle = \langle x_j \mid ee' \mid x_j \rangle. \tag{26}$$

If for all i, $\langle x_i \mid ee' \mid x_i \rangle = 0$, then the quantum code is said to be *non-degenerate*.

In [33, 32] it is shown how to use classical error-correcting codes to build quantum codes. Although they stated their results when errors are (random) errors of weight at most t, their construction can easily be generalized for any set $\mathcal{E}$ of errors. Before we state this result, we reiterate a definition concerning classical codes. Let $\mathcal{C}$ be a subspace of $\{0,1\}^n$, and $\mathcal{F}$ be a subset of $\{0,1\}^n$. We say $\mathcal{C}$ has the ability to correct every error from $\mathcal{F}$ (or simply, $\mathcal{C}$ *has* $\mathcal{F}$*-correcting ability*) if and only if every two different elements e_1 and e_2 of $\mathcal{F}$ belong to different cosets of $\mathcal{C}$; or equivalently, $e_1 + e_2 \notin \mathcal{C}$.

THEOREM 4.2. Let $\mathcal{E}$ be a set of possible quantum errors. If there are $[n, k]$ classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ (with $2k > n$) such that ${\mathcal{C}_2}^{\perp} \subseteq \mathcal{C}_1$ and $\mathcal{C}_1$ has $\overline{\mathcal{E}}_X$-correcting ability and $\mathcal{C}_2$ has $\overline{\mathcal{E}}_Z$-correcting ability, then there is an $((n, 2^{2k-n}))$ quantum code that has $\mathcal{E}$-correcting ability.

A special case of the above theorem is when $\mathcal{C}_1 = \mathcal{C}_2$; thus we have the following corollary.

COROLLARY 4.3. Let $\mathcal{E}$ be a set of possible quantum errors. If there is an $[n, k]$ classical code $\mathcal{C}$ (with $2k > n$) such that $\mathcal{C}$ is weakly self-dual (i.e., $\mathcal{C}^{\perp} \subseteq \mathcal{C}$) and $\mathcal{C}$ has both $\overline{\mathcal{E}}_X$-correcting ability and $\overline{\mathcal{E}}_Z$-correcting ability, then there is an $((n, 2^{2k-n}))$ quantum code that has $\mathcal{E}$-correcting ability.

It is possible to generalize the above construction even for the case when $\mathcal{C}$ is not weakly self-dual.

THEOREM 4.4. Let $\mathcal{E}$ be a set of possible quantum errors. Suppose that there is an $[n, k]$ classical code $\mathcal{C}$ such that $\mathcal{C}$ has $\overline{\mathcal{E}}_X$-correcting ability and $\mathcal{C}^{\perp}$ has $\overline{\mathcal{E}}_Z$-correcting ability. Let $\mathcal{D} = \{e + e' \mid e, e' \in \overline{\mathcal{E}}_X\}$. Then there is a quantum code that maps $n - k - \lceil \log_2 |\mathcal{D}| \rceil$ qubits to n qubits and has $\mathcal{E}$-correcting ability.

In [44, 38] a general method for describing and constructing quantum error-correcting codes is proposed. Consider unitary operators $e_1 = X_{\alpha_1} Z_{\beta_1}, \ldots, e_k = X_{\alpha_k} Z_{\beta_k}$, such that ${e_i}^2 = I$ (the identity operator) and $e_i e_j = e_j e_i$, for all i and j (i.e. $\alpha_i \cdot \beta_i = 0$ and $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$, where the inner products are modulo 2). Consider the $k \times (2n)$ matrix

$$H = \left(\begin{array}{c|c} \alpha_1 & \beta_1 \\ \vdots & \vdots \\ \alpha_k & \beta_k \end{array} \right). \tag{27}$$

Suppose the matrix H has full rank over GF(2). Then the set of the vectors $|x\rangle$ in $\mathbb{C}^{2^n}$ such that $e_i |x\rangle = |x\rangle$, for all $1 \leq i \leq k$, form an $(n-k)$-dimensional quantum code. The following theorem connects the error-correcting ability of this code with the properties of the dual space of H in $\{0,1\}^{2n}$.

THEOREM 4.5([44]). Let $\mathcal{E}$ be a set of quantum errors. Suppose the $k \times (2n)$ matrix H in *(27)* is totally singular, i.e. $\alpha_i \cdot \beta_i = 0$ and $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$ for all i and j. Let $\mathcal{C}$ denote the $[2n, k]$ binary code with H as its generator matrix. Then the space of the vectors $|x\rangle$ such that $X_{\alpha_i} Z_{\beta_i} |x\rangle = |x\rangle$, for all $1 \leq i \leq k$, is an $((n, 2^{n-k}))$ quantum code that has $\mathcal{E}$-correcting ability if for every $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \overline{\mathcal{E}}$ either $(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \in \mathcal{C}$ or $H \cdot (\beta_1 + \beta_2 \mid \alpha_1 + \alpha_2)^T \neq 0$.

4.2.2. Some results on binary cyclic codes

We construct different burst-correcting quantum codes (each with different dimensions) by utilizing Theorems 4.2, 4.4 and 4.5 when the underlying classical codes are cyclic. In this section we provide necessary facts and results concerning binary cyclic codes.

A linear subspace $\mathcal{C}$ of $\{0,1\}^n$ is called a *cyclic code* if $\mathcal{C}$ is closed under the cyclic shift operator, i.e. whenever $(c_0, c_1, \ldots, c_{n-1})$ is in $\mathcal{C}$ then so is $(c_{n-1}, c_0, \ldots, c_{n-2})$. When dealing with cyclic codes, it is much easier to identify each binary vector with a polynomial over the binary field $F_2 = \{0,1\}$. For this, we correspond to the vector $c = (c_0, c_1, \ldots, c_{n-1})$ in ${F_2}^n$ the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ in $F_2[x]$. For example, the vector $(1,0,0,1,1,0)$ corresponds to the polynomial $1 + x^3 + x^4$.

One of the basic properties of a cyclic code $\mathcal{C}$ is that $\mathcal{C}$ is generated by one of its codewords; in the sense that there is a codeword in $\mathcal{C}$, represented by the polynomial $g(x)$, such that every codeword $c(x) \in \mathcal{C}$ is a multiple of $g(x)$, i.e. $c(x) = q(x) \cdot g(x)$ for some polynomial $q(x)$. Here the identity $c(x) = q(x) \cdot g(x)$ holds in the quotient ring $F_2[x]/(x^n + 1)$, i.e. we identify $q(x) \cdot g(x)$ with $q(x) \cdot g(x) \bmod (x^n + 1)$. It is well known that if the polynomial $g(x)$ generates the cyclic code $\mathcal{C}$ of length n, then $g(x)$ is a factor of $x^n + 1$. (For more details see, e.g. [45].)

Some more useful notations. The *reciprocal* of a polynomial $f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + a_m x^m$, with $a_m \neq 0$, is $f^\star(x) = a_m + a_{m-1}x + \cdots + a_1 x^{m-1} + a_0 x^m$, which is obtained from $f(x)$ by reversing the order of the coefficients. Then $f^\star(x) = x^m f(x^{-1})$. The *exponent* of the polynomial $f(x) \in F_2[x]$ is the least integer s such that $f(x)$ divides $x^s + 1$.

We start with stating some easy facts about cyclic codes.

LEMMA 4.6. Let $\mathcal{C}$ be cyclic code of length n generated by the polynomial $g(x) = 1 + \alpha_1 x + \cdots + \alpha_{k-1}x^{k-1} + x^k$ in $F_2[x]$.

(a) If $w(x) = x^j + a_1 x^{j+1} + \cdots + a_{\ell-1}x^{j+\ell-1} + x^{j+\ell}$ is in $\mathcal{C}$, then $\ell \geq k$.

(b) If $w \in \mathcal{C}$, $w \neq 0$ and w contains a block of m consecutive 0's, then $m < n - k$.

In the next theorem we formulate a necessary condition for a cyclic code to be self-dual.

THEOREM 4.7. Let a polynomial $g(x)$ of degree k ($k \leq n/2$) generate a cyclic code $\mathcal{C}$ of length n. Let $g(x) = g_1(x) \cdots g_m(x)$ be a decomposition of $g(x)$ to irreducible polynomials. If the reciprocal of any of $g_i(x)$ is not among $g_1(x), \ldots, g_m(x)$ (especially, none of the $g_i(x)$ is self-reciprocal), then $\mathcal{C}$ is weakly self-dual, i.e. $\mathcal{C}^\perp \subseteq \mathcal{C}$.

Now we give some results on cyclic codes that correct burst errors. A *burst of width b* is a vector in $\{0,1\}^n$ whose only nonzero components are among b successive components, the first and the last of which are nonzero. (The last component c_{n-1} of the vector $(c_0, c_1, \ldots, c_{n-1})$ is understood to be adjacent to c_0.) As mentioned in the previous section, we say a linear code $\mathcal{C}$ has *burst-correcting ability b* if for every bursts w_1 and w_2 of width $\leq b$ we have $w_1 + w_2 \notin \mathcal{C}$. The following theorem gives a simple criterion for a cyclic code to have burst-correcting ability.

THEOREM 4.8. Let $\mathcal{C}$ be a cyclic code generated by the polynomial $g(x)$ of degree k. If $k \geq \frac{n}{2} + b$, then $\mathcal{C}$ has burst-correcting ability b.

The following theorem by Fire [46] and Melas and Gorog [47] (see also [42]) gives a general method to construct interesting burst-correcting cyclic codes.

THEOREM 4.9. Let $q(x)$ generate an $[n', k']$ code that has burst-correcting ability b. Let $p(x)$ be an irreducible polynomial of degree $\geq b$ and exponent e such that $(p(x), q(x)) = 1$ (i.e. $p(x)$ and $q(x)$ have no common factor). Then the cyclic code $\mathcal{C}$ of length $n = en'$ generated by $c(x) = q(x)p(x)$ has burst-correcting ability b.

In the following theorem we construct a small burst-correcting code. The interesting property of this code is that it is *weakly self-dual*; the property which is not addressed by the previous theorem.

THEOREM 4.10. The polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^9$ generates a cyclic [21, 12] code $\mathcal{C}$ which has burst-correcting ability $b = 4$. Moreover, $\mathcal{C}$ is weakly self-dual.

To utilize Theorem 4.9 for producing cyclic weakly self-dual codes that correct $b > 4$ bursts, we need to start with small cyclic weakly self-dual codes with burst-correcting ability b. It appears to be hard to find such codes with optimal, or near optimal, length. But it is possible to construct small cyclic weakly self-dual codes that correct *random* t errors. In the next lemma we give a construction for such codes. Although in this way we do not get optimal codes, the result is enough to rise to an infinite class of burst-correcting codes.

LEMMA 4.11. For any t, there is a binary cyclic weakly self-dual $[n, k, 2t + 1]$ code with $n = 2^m - 1$ and $k = n - tm$, where $n > 2(2t - 1)^2$.

4.2.3. Explicit construction of burst-correcting quantum codes

The *quantum burst-correcting codes* are defined naturally. Consider the set $\mathcal{E}$ of quantum errors such that both $\overline{\mathcal{E}_X}$ and $\overline{\mathcal{E}_Z}$ are bursts of width $\leq b$. Then any quantum code that has $\mathcal{E}$-correcting ability is called a b-burst-correcting code.

First we show that there is a two-dimensional quantum code of length $n = 15$ which corrects burst errors of width $b = 3$. From the table given in [48], it follows that to correct $t = 3$ (random) errors one qubit should be mapped to at least 17 qubits.

We consider the cyclic [15, 9] code $\mathcal{C}$ generated by $1 + x^3 + x^4 + x^5 + x^6$. As it is noted in [42], this code corrects $b = 3$ burst errors. We show that the dual of this code has the same burst-correcting ability.

The dual code $\mathcal{C}^\perp$ is generated by the polynomial $1 + x + x^4 + x^5 + x^6 + x^9$. So the following is a generator matrix for $\mathcal{C}^\perp$:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

We want to show that if b_1 and b_2 are two burst of width ≤ 3 and $b_1 \neq b_2$, then $b_1 + b_2 \notin \mathcal{C}^\perp$. First note that $b_1 + b_2$ contains a block of at least five consecutive zeros. Then w.l.o.g. we can assume $b_1 + b_2 = (000000\star\star\cdots\star)$ or $b_1 + b_2 = (000001\star\star\cdots\star)$. If $b_1 + b_2 \in \mathcal{C}^\perp$, then in the first case we would have $b_1 + b_2 = 0$, i.e. $b_1 = b_2$ which contradicts the assumption $b_1 \neq b_2$; and in the second case $b_1 + b_2 = (000001100111001)$ which is not sum of two bursts of width ≤ 3. This completes the proof that $\mathcal{C}^\perp$ corrects bursts of width 3.

Now we show that the all-one vector $\mathbf{1}$ is not in coset of any vector of the form $b_1 + b_2$, where b_1 and b_2 are bursts of width ≤ 3. Assume, by contradiction, that $\mathbf{1} + b_1 + b_2 \in \mathcal{C}^\perp$. Since $b_1 + b_2$ has a block of at least five consecutive zeros, $\mathbf{1} + b_1 + b_2$ is either $(111110\star\star\cdots\star)$ or $(111111\star\star\cdots\star)$. In the first case $\mathbf{1} + b_1 + b_2$ is (111110111010001) and in the second case it is (111111011101000). So $b_1 + b_2$ is either (000001000101110) or (000000100010111); which in neither case can be the sum of two bursts of width ≤ 3.

So the desired quantum code consists of $|0_L\rangle = \sum_{c\in\mathcal{C}} |c\rangle$ and $|1_L\rangle = \sum_{c\in\mathcal{C}} |c + \mathbf{1}\rangle$.

In fact, there is a 3-burst-correcting quantum code with smaller length. This is a [13, 1, 5] code. The stabilizer of this code is defined by a quadratic residue code over GF(4) $= \{0, 1, \omega, \overline{\omega} = \omega^2\}$ with $g(x) = (1 + x)g_1(x)$ as its generator polynomial, where $g_1(x) = 1 + \overline{\omega}x + \omega x^3 + \overline{\omega}x^5 + x^6$ (see [48] for details on quantum codes

defined by codes over GF(4)). Here it is enough to show that the cyclic code $\mathcal{C}$ (over GF(4)) generated by the polynomial $g_1(x)$ is a 3-burst-correcting code. Suppose the nonzero polynomial $q(x)$ (of degree ≤ 12) represents a codeword in $\mathcal{C}$ that is a sum of two bursts of width ≤ 3. Then at least seven coefficients of $q(x)$ are zero. Therefore, without loss of generality, we can assume $q(x) = 1 + a_1x + \cdots + a_8x^8$. Hence $q(x) = (1 + ax + bx^2)g_1(x)$, for some $a, b \in$ GF(4). But for any a and b the corresponding $q(x)$ is not a sum of two bursts of width ≤ 3.

Now we show the existence of infinite classes of quantum burst-correcting codes.

THEOREM 4.12. If there is a binary $[n, k]$ code $\mathcal{C}$ (with $k < \frac{n}{2}$) such that $\mathcal{C}$ and $\mathcal{C}^{\perp}$ both have burst-correcting ability b, then there is an $((n, 2^K))$ quantum code with $K = n - k - 2\lceil \log n \rceil - b$ that corrects all burst errors of width b.

COROLLARY 4.13. There are $((n, 2^k))$ quantum codes with $n = (2^m - 1)(2b - 1)$ and $k = n - m - 2\lceil \log n \rceil - 3b + 1$ having burst-correcting ability b.

For fixed constant b, the above result gives a family of quantum codes of length n and dimension $n - 3\log n - O(1)$ having burst-correcting ability b. In the next theorem we show for $b \leq 4$ we can construct burst-correcting quantum codes with dimension $n - 2\log n - O(1)$.

THEOREM 4.14. For every $m \geq 7$, there is an $((n, 2^k))$ quantum code with $n = 21(2^m - 1)$ and $k = n - 2m - 18$ having burst-correcting ability $b = 4$.

By utilizing Lemma 4.11, we can get a similar result for the case $b > 4$. The following theorem shows how to construct $((n, 2^K))$ quantum codes, with $K = n - 2\log n - O(b)$, for constant burst-width b; note however that the constant, $O(b)$, in the preceding expression could be a large function of b.

THEOREM 4.15. For every b, there is an $((n, 2^k))$ quantum b-burst-correcting code, where $n = (2^{m'} - 1)(2^m - 1)$, $k = n - 2m - 2bm'$, $2^{m'} > 2(2b - 1)^2$ and $m > m'$.

4.2.4. Bounds and a new scheme for construction

In this section we present general upper and lower bounds for maximum dimension of a quantum burst-correcting code.

THEOREM 4.16. Let $\mathcal{E}$ be a set of errors, and $\mathcal{D} = \{e + e' \mid e, e' \in \mathcal{E}\}$. Let 2^k be the maximum of dimension of any non-degenerate quantum code of length n that has $\mathcal{E}$-correcting ability. Then

$$n - \log_2 |\mathcal{D}| \leq k \leq n - \log_2 |\mathcal{E}|.$$

COROLLARY 4.17. Let 2^k be the maximum of dimension of any non-degenerate quantum code of length n which has burst-correcting ability b. Then

$$n - 2\log_2 n - 2b \leq k \leq n - \log_2(n - b + 2) - 2b - 3.$$

Next we present a new scheme for constructing quantum codes from classical linear codes. By utilizing this method, for fixed constant b, we obtain b-bursts-correcting quantum codes of length n with dimension $n - \log_2 n - O(1)$. These are almost optimal codes (compare with the bound given in Corollary 4.17).

THEOREM 4.18. If there is a $(3b + 1)$-burst correcting binary $[n, k]$ cyclic code $\mathcal{C}$ such that $\mathcal{C}$ is weakly self-dual, then there is a b-burst-correcting $((n, 2^k))$ quantum code.

Proof. Suppose the $(n-k) \times n$ matrix H is a parity check matrix for $\mathcal{C}$. Let $H^{\rightarrow m}$ denote the matrix that is obtained from H by shifting (cyclically) the columns m times to the right. Note that $H^{\rightarrow m}$ is also a parity check matrix of $\mathcal{C}$, because $\mathcal{C}$ is cyclic. Now, consider the stabilizer defined by the matrix

$$G = \left[H + H^{\rightarrow b} \mid H + H^{\rightarrow 2b+1}\right].$$

It is easy to check that G is indeed a totally singular matrix. Suppose $e = (e_1 \mid e_2)$ and $e' = (e'_1 \mid e'_2)$ are bursts of width $\leq b$, and $e \neq e'$. Let

$$w = e_1 + e'_1 + (e_1 + e'_1)^{\rightarrow b} + e_2 + e'_2 + (e_2 + e'_2)^{\rightarrow 2b+1},$$

where $e^{\rightarrow b}$ denotes the vector obtained by cyclically shifting e to the right b times. Then it is easy to check that $w \neq 0$ and w is the sum of two bursts of width $\leq 3b+1$. So $w \notin \mathcal{C}$ and

$$G \cdot (e + e')^T = H \cdot w^T \neq 0.$$

Now the theorem follows from Theorem 4.5. □

To apply the above theorem, we need weakly self-dual b-burst-correcting binary codes with arbitrary length. For $b \leq 4$, Theorem 4.10 gives explicit construction of such codes. In general, we can apply the following theorem.

THEOREM 4.19([49]) . For every b and for every square-free polynomial $e(x)$ of degree $b-1$ and of index m_e such that $e(0) \neq 0$ and for every sufficiently large $m \equiv 0 (\mathrm{mod}\ m_e)$, a primitive polynomial $p(x)$ of degree m exists such that $e(x)p(x)$ generates a b-burst-correcting code of length $n = 2^m - 1$ and dimension $k = n - m - b$.

To get weakly self-dual codes, choose $e(x)$ to be any primitive polynomial of degree $b-1$. Then $e(x)p(x)$ generates a weakly self-dual b-burst-correcting code, because no primitive polynomial is self-reciprocal. Thus we get the following bound for burst-correcting quantum codes.

THEOREM 4.20. For every b and for sufficiently large $n = 2^m - 1$ (where $m \equiv 0 (\mathrm{mod}\ m_b)$ for some fixed integer m_b depending only on b), there are b-burst-correcting quantum codes of length n and dimension $n - m - 3b + 1$.

5. Conclusion

In this paper, we have discussed specific examples of physical *nanoelectronic* models for reversible and quantum gates. Since these systems are vulnerable to ubiquitous decohering perturbations, we have also studied a number of quantum error control codes that can correct some of the errors arising from decoherence. Some new results on quantum error-correcting codes have been presented. In the spirit of Landauer's untiring efforts to instil truth in advertising, we certainly admit the serious problem of decoherence, but hope that quantum error-correcting codes will pave the way towards a practical solution.

Acknowledgement—This work was supported by the Defense Advanced Research Projects Agency under contract 35918-OH.

References

[1] The Semiconductor Industry Association: National Technology Roadmap, 1994.
[2] *Single Charge Tunneling*, edited by H. Grabert and M. H. Devoret (Plenum, New York, 1992); A. N. Korotkov in *Molecular Electronics*, edited by J. Jortner and M. A. Ratner (Blackwell, Oxford, 1997).
[3] R. Landauer, IBM J. Res. Develop. **5**, 183 (1961); R. W. Keyes and R. Landauer, IBM J. Res. Develop. **14**, 152 (1970).

[4] D. B. Tuckerman and R. F. W Pease, IEEE Elec. Dev. Lett. **2**, 126 (1981).
[5] T. Toffoli, in *Seventh Colloquium in Automata, Languages and Programming*, edited by J. W. de Bakker and J. W. van Leeuwen, (Springer-Verlag, Berlin, 1980). p. 632
[6] K. Kinoshita, S. Tsutomu, and M. Jun, IEEE Trans. Computers **C-25**, 247 (1976).
[7] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. **21**, 219 (1982).
[8] C. H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).
[9] C. H. Bennett and R. Landauer, Sci. Am. **253**, 48 (1985).
[10] T. Toffoli, Math. Syst. Theor. **14**, 13 (1981).
[11] K. K. Likharev, Int. J. Theor. Phys. **21**, 311 (1982).
[12] R. Landauer, in *Der Informationsbegriff in Technik und Wissenschaft*, edited by O. G. Folberth and C. Hackl (R. Oldenbourg, München, 1986), p. 139.
[13] K. K. Likharev and A. N. Korotkov, Science **273**, 763 (1996).
[14] V. P. Roychowdhury, D. B. Janes, and S. Bandyopadhyay, Proc. IEEE **85**, 574 (1997).
[15] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995).
[16] S. Lloyd, Science **261**, 1569 (1993); S. Lloyd, Science **263**, 695 (1994).
[17] N. Ashcroft and D. Mermin, *Solid State Physics* (Saunders College, Philadelphia, 1976).
[18] S. S. Molotkov and S. N. Nazin, JETP Lett. **62**, 272 (1995).
[19] S. Bandyopadhyay and V. P. Roychowdhury, Superlat. Microstruct. **22**, 411 (1997).
[20] W. G. Unruh, Phys. Rev. **A51**, 992 (1995).
[21] R. T. Bate, in *VLSI Microstructure Science and Engineering*, edited by N. G. Einspruch, vol. 4, (Academic Press, New York, 1981).
[22] C. Mead and L. Conway, *Introduction to VLSI Systems*, Chapter IX, (Addison-Wesley, Reading, Massachusetts, 1980). p. 333.
[23] R. Landauer, Int. J. Theor. Phys. **21**, 283 (1982).
[24] P. Benioff, J. Stat. Phys. **22**, 563 (1980).
[25] P. Benioff, Int. J. Theor. Phys. **21**, 177 (1982).
[26] W. G. Teich, K. Obermeyer, and G. Mahler, Phys. Rev. **B37**, 8111 (1988); W. G. Teich and G. Mahler, Phys. Rev. **S45**, 3300 (1992); H. Korner and G. Mahler, Phys. Rev. **B48**, 2335 (1993).
[27] .B. Lush, D. H. Levi, H. F. MacMillan, R. K. Ahrenkiel, M. R. Melloch, and M. S. Lundstrom, Appl. Phys. Lett. **61**, 2440 (1992).
[28] G. B. Lush, H. F. MacMillan, B. M. Keyes, D. H. Levi, M. R. Melloch, R. K. Ahrenkiel, and M. S. Lundstrom, J. Appl. Phys. **72**, 1436 (1992).
[29] M. P. Patkar, M. S. Lundstrom, and M. R. Melloch, J. Appl. Phys. **78**, 2817 (1995).
[30] R. K. Ahrenkiel, B. M. Keyes, G. B. Lush, M. R. Melloch, M. S. Lundstrom, and H. F. MacMillan, J. Vac. Sci. and Tech. **A10**, 990 (1992).
[31] P. W. Shor, Phys. Rev. **A52**(4), 2493–2496 (1995).
[32] A. M. Steane, Phys. Rev. Lett. **77**(5), pp. 793–797 (1996).
[33] A. R. Calderbank and P. W. Shor, Good quantum error–correcting codes exit, Phys. Rev. **A54**(2), 1098–1105 (1996).
[34] S. Bandyopadhyay *et. al.*, Nanotechnology **7**, 360 (1996).
[35] P. Mohanty, E. M. Q. Jariwala, and R. A. Webb, Phys. Rev. Lett. **78**, 3366 (1997).
[36] R. Laflamme, C. Miquel, J. Pablo Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[37] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. **A54**(5), 3824–3851 (1996).
[38] D. Gottesman, Phys. Rev. **A54**(3), 1862–8168 (1996).
[39] F. Vatan, V. P. Roychowdhury, and M. P. Anantram, *Spatially correlated Qubit Errors, and Burst-Correcting Quantum Codes*, LANL e–print quant–ph/9704019.
[40] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**(20), 4091–4094 (1995).
[41] G. M. Palma, K.-A. Suominen, and A. K. Ekert, Proc. R. Soc. London **A452**, 567–584 (1996).

[42] W. W. Peterson and E. J. Weldon, Jr., *Error–Correcting Codes*, 2nd edn, MIT Press, 1972.
[43] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, LANL e–print quant–ph/9604034
[44] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction and orthogonal geometry*, LANL e–print quant–ph/9605005.
[45] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, (North–Holland, New York, 1977).
[46] P. Fire, *A Class of Multiple–Error-Correcting Binary Codes for Non–Independent Errors*, Sylvania Report RSL–E–2, Sylvania Reconnaissance Systems Laboratory, Mountain View, California, 1959.
[47] C. M. Melas and E. Gorog, IBM J. Res. Develop. **7**, 151–152, (1963).
[48] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction via codes over GF(4)*, LANL e–print quant–ph/9608006.
[49] K. A. S. Abdel–Ghaffar, R. J. McEliece, A. M. Odlyzko, and H. C. A. van Tilborg, IEEE Trans. Information Theory **IT–32**(6), 768–775 (1986)
[50] E. Rains, private communication, April 1997.