Basic Elements of Quantum Information Technology

Timothy P. Spiller
Networked Systems Department
HP Laboratories Bristol
HPL-97-149
December, 1997

E-mail: ts@hplb.hpl.hp.com

quantum, information, technology computing, cryptography

The marriage of quantum physics and information technology has the potential to generate radically new information processing devices. Examples are quantum cryptosystems, which provide guaranteed secure communication, and quantum computers, which manipulate data quantum mechanically and could thus solve some problems currently intractable to conventional (classical) computations. This introductory chapter serves two purposes. Firstly, I discuss some of the basic aspects of quantum physics which underpin quantum information technology (QIT). These will be used (and in some cases further expanded upon) in subsequent chapters. Secondly, and as a lead into the whole book, I outline some of the ideas of QIT and its possible uses.

Internal Accession Date Only

Basic elements of quantum information technology*

Timothy P. Spiller

Hewlett-Packard Laboratories, Bristol

Filton Road, Stoke Gifford

Bristol BS12 6QZ

United Kingdom

Telephone: +44 117 9229280 Fax: +44 117 9229285

E-Mail: ts@hplb.hpl.hp.com

Abstract

The marriage of quantum physics and information technology has the potential to generate radically new information processing devices. Examples are quantum cryptosystems, which provide guaranteed secure communication, and quantum computers, which manipulate data quantum mechanically and could thus solve some problems currently intractable to conventional (classical) computation. This introductory chapter serves two purposes. Firstly, I discuss some of the basic aspects of quantum physics which underpin quantum information technology (QIT). These will be used (and in somes cases further expanded upon) in subsequent chapters. Secondly, and as a lead into the whole book, I outline some of the ideas of QIT and its possible uses.

*To appear as Chapter 1 of *Introduction to Quantum Computation and Information*, eds. H.-K. Lo, S. Popescu and T. P. Spiller, (World Scientific Press 1998), http://www.wspc.com.sg/.

1 Introduction

Information technology (IT) can feed off quantum physics in two ways, which might loosely be termed evolutionary and revolutionary. Both are potentially very important and each one forms a currently very active and exciting research field. In the evolutionary work, quantum physics is essentially employed as a tool, so it is possible to understand and appreciate a good deal of its impact without having to get to grips with the theory itself. Conversely, in the revolutionary work quantum mechanics plays the lead role. Some knowledge of what it is about is therefore required to get a feel for the dramatic new possibilities which arise. The various chapters in this book introduce and discuss in some depth these developing areas, such as quantum cryptography and quantum computing. As will be seen, some of the most fundamental and interesting aspects of quantum mechanics play centre stage. As a primer, this chapter contains some basic discussion of these topics, in addition to an overview on some areas of QIT. Readers who have already consumed such hors-d'œuvres may care to go straight to the entrées in the later chapters.

In the *evolutionary* IT work, quantum physics is basically used to better understand and thus improve existing technology. For example, the development of smaller and faster silicon or other semiconducting devices benefits from the understanding of the quantum behaviour of electrons in such materials. A bit more radical would be the replacement of silicon transistors by superconducting Josephson junction devices.[1] Nevertheless, intrinsically quantum in nature though superconductors may be, this would still not constitute a fundamentally new technology. The superconducting benefit here would be faster digital switching and lower power consumption. However, the logical operations performed, the manipulations of the physical bits in these devices, are no different from those of existing devices. These familiar logical operations still obey the laws of classical physics, as they always have.

A genuinely radical development comes if quantum physics impacts on information technology in a second and rather different way. Instead of improved versions of what we have already, consider devices which actually *process* information—perform logical operations—according to the laws of quantum physics. Such devices, which would be part of a new *quantum information technology* (QIT), are fundamentally different from their classical counterparts. Quite unlike billiard balls, fundamental particles such as electrons can exhibit wave-like interference phenomena and two (or in principle more) of them can be intimately entangled. In a similar way, machines which store, process and transmit information (usually in the form of *bits*) quantum mechanically can do things with it that would appear totally out of character, or even impossible, for a classical machine. Of course, it's not that easy—if it were, QIT would probably have

[1] This has been tried essentially twice, by IBM and by the MITI project in Japan, but without commercial success. A third (and perhaps the final) attempt is in progress, using the new approach of rapid single flux quantum technology [1]. It remains to be seen how this will fare.

been around for a good many years by now. The problem is that measuring electrons generally shakes them up, destroying interference and entanglement. Worse still, such disruptive effects may occur whether you like it or not; they may arise from unavoidable interactions with other systems. Such behaviour is part of quantum physics in general—it is not peculiar to electrons—and so forms a barrier to the development of any form of QIT. Indeed, it is not at all clear that the decohering interactions with other systems can be avoided, and so a few years back there was substantial pessimism for practical QIT. However, recent remarkable work on *quantum error correction* has shown that the development barrier is not insurmountable [2] in some cases. This is why QIT is a growing an active research field.[3]

Even if it develops as well as current researchers can best imagine, QIT is not going to revolutionize the electronics industry in the sense of ousting existing IT. Rather, it will create new business opportunities which will grow alongside the existing ones. Instead of replacing your PC with a quantum version that merely outperforms your old one at the same tasks, it seems rather more likely that you will buy a quantum attachment, or a whole new machine, which actually does things your (or indeed any) classical machine simply cannot. The two most well-known and researched examples of quantum information processors to date are a quantum cryptosystem and a quantum factoring computer. The former enables guaranteed secure communication between two parties. The latter would enable a large composite integer to be factored, a problem which is essentially intractable on any classical computer. (It is a computationally simple task to multiply together two very large prime numbers p and q to obtain their (composite) product $N = pq$. However, it is exceedingly difficult to find the factors p and q if you are given *just* N.) The hardness of factoring forms the basis for public key cryptosystems [4] such as RSA [6]; these are very widely used today so the cracking of the factoring problem would have major implications!

I'll briefly use these two examples, cryptography and computation, to highlight how fundamental features of quantum physics come into play for QIT. First, though, we need the quantum ingredients.

---

[2] Or, at least, it is possible to tunnel through it...

[3] In addition to the discussions and references presented in this book, there exist review articles on the subject [2]−[4] which contain extensive lists of further references. Quantum information can also be found at web sites [5].

[4] For example, RSA [6] operates roughly as follows: A user wishing to receive secret messages uses two large primes p and q and *publicly* declares an encryption key of $N = pq$ and a suitable random number e, which is co-prime with $x = (p-1)(q-1)$. A sender encrypts their message m to $f = m^e \bmod N$ and transmits f. Knowing the primes p and q, it is mathematically easy for the receiver to decrypt this by evaluating $f^d \bmod N$, where $d = e^{-1} \bmod x$. However, it is extremely difficult for an eavesdropper to decrypt the transmission because they only know N and not its factors.

2 Quantum mechanics

There are five important elements of quantum mechanics which feature highly in quantum information processing.

2.1 Superposition states

Quantum systems have a much richer and more interesting existence than their classical counterparts. A single bit, the very basic building block of any classical information processor, only has a choice between two possible states, **0** or **1**. It is always in one state or the other. However, a single quantum bit, or qubit, has the luxury of an infinite choice of so-called superposition states. Nature allows it to have a part corresponding to **0** *and* a part corresponding to **1** *at the same time*, analogous to the way a musical note contains various harmonic frequencies.[5] Picture it as a classical bit being only black or white, but a qubit having every colour you like, if this helps.

In mathematical terms, the state of a quantum system (which is usually denoted by $|\psi\rangle$) is a vector in an abstract Hilbert space of possible states for the system. The space for a single qubit is spanned by a basis consisting of the two possible classical states, denoted by $|0\rangle$ and $|1\rangle$. This means that *any* state of a qubit can be decomposed into the superposition

$$|\psi\rangle = a|0\rangle \; + \; b|1\rangle \tag{1}$$

with suitable choices of the complex coefficients a and b. A familiar *representation* of the basis uses the orthogonal 2D unit vectors $\binom{0}{1}$ and $\binom{1}{0}$; in this case $|\psi\rangle$ is represented by $\binom{b}{a}$.

The value of a qubit in state $|\psi\rangle$ is uncertain; if you measure such a qubit, you cannot be sure in advance what result you will get. Quantum mechanics just gives the probabilities, from the overlaps [6] between $|\psi\rangle$ and the possible outcomes, rules due originally to Max Born. Thus the probability of getting **0** is $|\langle 0|\psi\rangle|^2 = |a|^2$ and that for **1** is $|\langle 1|\psi\rangle|^2 = |b|^2$. (Quantum states are therefore normalized; $\langle\psi|\psi\rangle = (b^* \; a^*).\binom{b}{a} = 1$ and the probabilities sum to unity.) Quantum mechanics also tells you that (assuming the system is not absorbed or totally destroyed by the action of measurement) the qubit state Eq. 1 suffers a projection to $|0\rangle$ ($|1\rangle$) when you get the result **0** (**1**). There is clearly something intrinsically irreversible about a measurement. In fact, this is

[5] Another (mathematically correct—it is sometimes called the Poincaré or Bloch sphere) analogy is to think of a globe. A classical bit can only sit at the north or the south pole, whereas a qubit is allowed to reside at any point on the surface.

[6] $\langle\eta|\psi\rangle$ is the *inner product* between the two states; $\langle\eta|$ follows from $|\eta\rangle$ by transposition and complex conjugation ($*$)—together these form Hermitian conjugation ($\dagger$). In the vector representation $\langle\psi|$ is given by $(b^* \; a^*)$ and the inner product is the familiar scalar/dot product.

not peculiar to measurement interactions and I discuss irreversibility more generally in Sec. 2.4.

As a qubit has a basis of two states, a full system of m qubits has a basis of 2^m states. These could represent the binary values from $\mathbf{0}$ to $\mathbf{2}^m - \mathbf{1}$. A classical computer with an m-bit input register can clearly only be prepared in one of these possible states and so calculations with different inputs have to be run as separate computations. However, scaling up the superposition principle of Eq. 1 to a machine with an input register of m qubits, a carefully constructed quantum computer—the reason for this qualifier will become apparent later—is thus allowed to exist in a superposition of *all* its possible classical binary states. This means that it could perform a *single* computation with its input set to a superposition of all possible classical inputs! This so-called quantum parallelism is the basis for being able to solve some problems much more quickly with a quantum processor.

2.2 Entanglement

Quantum systems are weird! Even with just two qubits, a strange and remarkable property of quantum systems raises its head. Two qubits (labelled A and B) have a basis of four states,[7] which could be written as $|0\rangle_A|0\rangle_B$, $|0\rangle_A|1\rangle_B$, $|1\rangle_A|0\rangle_B$ and $|1\rangle_A|1\rangle_B$. Consider a superposition state of just two of these,

$$|\psi\rangle_{AB} = 2^{-1/2}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) \ . \tag{2}$$

There is no way that this state can be rewritten in the factored form $|\phi\rangle_A|\chi\rangle_B$, for any crafty choice of $|\phi\rangle_A$ and $|\chi\rangle_B$. Such a form would imply that qubits A and B have definite quantum states (in their individual Hilbert spaces), independent from their partner. Consequently, for states like Eq. 2 this is not so—there exists an intimate *entanglement* between the two. Neither has a state of its own.

Entanglement plays a very important role for QIT. As such, it deserves a sizeable discussion, and this is what it gets, from Sandu Popescu in chapter two. Entanglement between two qubits, such as in Eq. 2, is well understood. However, there are still open questions on entanglement between many qubits and cases where the overall system is impure, and so has finite entropy. I give some discussion of impurity in Sec. 2.4; as will be seen, entanglement with other degrees of freedom generates entropy for the system of interest.

It is well known that the spatial separation of systems A and B when they are in an entangled state like Eq. 2 has remarkable consequences. Albert Einstein, Boris

[7] The total Hilbert space for a number of systems is given by the direct product of the individual Hilbert spaces, often denoted by the symbol $\otimes$. A complete state vector is thus a direct product of individual ones. Some authors choose to make this explicit; others, such as myself, take it as read—thus $|0\rangle_A|0\rangle_B$ denotes $|0\rangle_A \otimes |0\rangle_B$.

Podolsky and Nathan Rosen [7] started the ball rolling in 1935; John Bell [8] took it up in the sixties and proved his famous theorem—in effect that quantum mechanics as a theory is non-local. Numerous interesting and important further developments have followed in the last decade or so. One thing that *cannot* be done with the non-locality of spatially separated entangled systems (often called EPR pairs) is "faster-than-light" signalling; the irreversibility of quantum measurement ensures this. However, shared entanglement can be used for the teleportation [9] of (unknown) quantum states and superdense coding [10, 11]. This subject area, and general questions concerning quantum information theory, are addressed by Richard Jozsa in chapter three.

2.3 Reversible unitary evolution

An isolated quantum system evolves in a nice reversible manner. Schrödinger's famous equation tells us how;

$$H\ |\psi\rangle\ =\ i\hbar\ \frac{\partial|\psi\rangle}{\partial t}\ . \tag{3}$$

Here $|\psi\rangle$ is the state of the system—which might be anything from a single qubit through to some complex interacting collection of degrees of freedom—and H is the *total* Hamiltonian (the energy operator). It is important not to miss any bits of H, interactions with bits and pieces outside the defined system; [8] provided none are omitted the system is "closed" and evolves according to Eq. 3. Formally, this can be integrated to give the state at any time

$$|\psi(t)\rangle = U|\psi(0)\rangle\ , \tag{4}$$

where the unitary operator [9] is given by $U = \exp\left[-\frac{i}{\hbar}\int_0^t dt'\ H\right]$. Clearly, such evolution can be reversed by application of $U^\dagger$.

However, to make a rather less glib association with the familiar statistical mechanical idea of reversibility, it is helpful to consider a different description of quantum systems. (This broader picture can also cover irreversibility and it will be handy for the discussions later in the book where this plays a crucial role.) Consider a large number of identical and non-interacting quantum systems, where *every* member of this ensemble is in the quantum state $|\psi\rangle$. The whole ensemble can be described by a density operator,[10] given by

$$\rho = |\psi\rangle\langle\psi|\ . \tag{5}$$

[8] This could simply be coupling to the surrounding vacuum electromagnetic field, or thermal contact with some other apparatus.

[9] A unitary operator is one whose Hermitian conjugate is its inverse, so $UU^\dagger = U^\dagger U = I$ where I is the appropriate identity operator. Clearly U in Eq. 4 must be unitary to conserve the total probability; $\langle\psi(t)|\psi(t)\rangle$ must equal $\langle\psi(0)|\psi(0)\rangle$. This is ensured because the total energy is an observable and H is Hermitian; $H = H^\dagger$.

[10] In this approach, normalization gives $\langle\psi|\psi\rangle = Trace(\rho) = 1$, where $Trace$ denotes the sum of the diagonal elements. The expectation value of any observable quantity O, its average value over the ensemble, follows from $\langle O\rangle = \langle\psi|O|\psi\rangle = Trace(\rho O)$.

In the vector representation of states, ρ is a density matrix—an ensemble of qubits each in state Eq. 1 is described by $\rho = \binom{b}{a}\ (b^*\ a^*) = \binom{|b|^2\ \ ba^*}{ab^*\ \ |a|^2}$. The reason a direct statistical description of an ensemble is useful is that the *entropy* (per member of the ensemble) can be defined [12] by

$$S = -k\ Trace(\rho\ \ln \rho)\ , \tag{6}$$

where k is Boltzmann's constant. For any *pure* ensemble, where every member is in the same state (and so, from Eq. 5, $\rho^2 = \rho$), it is easy to show that the entropy vanishes. As every member is in the same state, there is no lack of knowledge, or "missing information," about such an ensemble.

The Schrödinger evolution of ρ follows from Eq. 3;

$$\frac{\partial \rho}{\partial t} = -\frac{i}{\hbar}[H, \rho]\ . \tag{7}$$

As per Eq. 4, this can be integrated to give $\rho(t) = U\rho(0)U^\dagger$. It is straightforward to show that unitary Schrödinger evolution preserves the entropy, $\partial S/\partial t = 0$. This is why such evolution is called *reversible*. The meaning is the same as in thermodynamics; the entropy of an ensemble of closed quantum systems does not change as they evolve reversibly.

It will be seen throughout this book that reversible evolution of systems is crucial for quantum information processing. Qubits have to evolve unitarily from place to place to move quantum information around. A quantum computer has to evolve reversibly, utilizing entanglement between many qubits, in order to perform tasks impossible for any classical machine. Of course, irreversibility does come into play. The only way to get answers out of quantum information processors is to make *measurements*. However, apart from these deliberate injections of irreversibility, interactions causing changes in entropy are essentially bad news, and need to be avoided.

Before moving to discuss such irreversibility, a little word of caution is in order regarding unitary operators. Generally in quantum information processing, it is handy to think of the sequences of unitary operators which have to be applied to qubits [11] to effect some desired process. However, theorists—myself included—should not get too cocky! Just because a U can be defined on paper does not necessarily mean that it is easy to implement even under laboratory conditions, let alone out in the real world! If it is effected by some piece of Hamiltonian acting for some time, errors may occur. If the Hamiltonian contains some externally applied source (like an electromagnetic pulse), in reality this may not be exactly as per the blueprint. The timings may not be quite right. The evolution may still be unitary, but it may not be that due to the desired

[11] At the most basic and universal level, these have to be on individuals and on pairs of qubits, although it may be convenient to think of more complicated many-qubit unitary "gates" which in principle break down into these basic operations.

U. Despite the discrete bases of quantum systems like qubits, general states such as Eq. 1 contain *continuous* amplitudes a and b. Incorrect unitary evolution [13, 14] thus has some analogy with the occurence of errors in classical analogue computing. Such problems cannot be ignored, as they will doubtless occur whenever QIT moves off the drawing board.

It will be clear from the chapters by Andy Steane on error correction and John Preskill on fault-tolerant computing that, over the last few years, theorists have not tried to sweep these problems under the carpet. Unitary errors, as well as non-unitary effects such as decoherence which are discussed in the next section 2.4, have to be allowed for and then overcome, in order to effect successful quantum information processing. That this can be done at all frequently surprises people, often by an amount proportional to their advance knowledge of quantum physics!

2.4 Irreversibility, measurement and decoherence

All quantum systems have a somewhat fragile existence. The only way to find out anything about a quantum state is to actually make a measurement on the system. The type of measurement you choose to make defines the set of possible results; the outcome of every measurement has to be one of these. The consequences of forcing the hand of a quantum system by measurement are that a single measurement is a truly random process and that the act of measurement imparts an *irreversible* change to the state of the system. Fragile superposition states collapse. Measuring the value of a qubit will always yield **0** or **1**—the measurement *projects* any initial state to one or other of these. For an initial superposition state such as Eq. 1 this occurs randomly with respective probabilities [12] of $|a|^2$ and $|b|^2$. There is a corresponding irreversible change to the state as it jumps to $|0\rangle$ or $|1\rangle$. Irreversibility is only avoided in the special cases when the qubit is actually in state **0** or state **1** before measurement. The upshot is that you *cannot* infer the prior state of a quantum system from the outcome of a *single* measurement—if you get **0** you have no idea if the initial state was purely this, or if it was a superposition state containing a part of this. You cannot deduce the colour of a qubit if you only see in black and white. This is not a question of experimental competence; it is a property of Nature. The fragility of quantum states is the key to a quantum cryptosystem. Sending information encoded in qubits guarantees that any eavesdropper cannot read it in transit without leaving evidence of their tampering. They will always corrupt some of the data.

Measurement of a quantum system generally requires interaction with other de-

[12] In the globe picture, measurement forces a qubit to jump at random to one of the poles, with a probability proportional to the square of the cosine of half the zenithal angle θ to that pole. In Eq. 1 the amplitudes can be parametrized in terms of this and the azimuthal angle ϕ:
$a = \exp(i\phi)\cos(\theta/2)$; $b = \sin(\theta/2)$.

grees of freedom, external to those of the system of interest (and so not included in the system Hamiltonian H). Other forms of interaction exist, too. The trendy term for additional degrees of freedom coupled to a quantum system is the *environment*—a system so coupled is referred to as "open." Its H does not tell the whole story. The irreversible nature of interactions with environments can be seen by looking at the entropy for some relevant examples.

1. Measurement: Since measuring the values of qubits projects them according to the Born rules, an initially pure ensemble $\rho_i = |\psi\rangle\langle\psi|$ with $|\psi\rangle$ given by Eq. 1 ends up as the weighted sum of pure ensembles

$$\rho_f = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1| \tag{8}$$

after measurement.[13] This is clearly not pure [14] ($\rho_f^2 \neq \rho_f$) and the entropy (Eq. 6) has increased from zero to $S = -k(|a|^2 \ln |a|^2 + |b|^2 \ln |b|^2)$.

2. Decoherence: Although entanglement *within* a large complex system is vital for quantum computing, additional entanglement with environment degrees of freedom is a real nuisance and causes unwanted irreversibility. This can be seen even in the simple example of the decoherence of an EPR pair. Consider a total pair–environment (AB–e) system initially in a state $|\Psi\rangle = |\psi\rangle_{AB}|e\rangle$, with $|\psi\rangle_{AB}$ given by Eq. 2. Suppose that an interaction with the environment generates the *additional* entanglement

$$|\Psi\rangle_f = 2^{-1/2}\left(|0\rangle_A|0\rangle_B|e_0\rangle + |1\rangle_A|1\rangle_B|e_1\rangle\right) \ . \tag{9}$$

The qubit values determine the new environment states. If the environment contains many degrees of freedom, these states will almost certainly be orthogonal (or very nearly so), $\langle e_0|e_1\rangle = 0$. Note that the environment need only couple to one or other of the pair (A or B) to do this. Clearly the total final density operator $\varrho_f = |\Psi\rangle_f\langle\Psi|_f$ is still pure; [15] however, this is not the point. Anyone trying to use the EPR pair for quantum information processing will not be using the environment as well; they may not even be aware of its intervention. The system as far as they are concerned is just A and B. The *reduced* density operator, describing an ensemble of such EPR pairs alone, is found by tracing over the environment [16] to give

$$\rho_f = Trace_e(\varrho_f) = \frac{1}{2}\left[|0\rangle_A|0\rangle_B\langle 0|_A\langle 0|_B + |1\rangle_A|1\rangle_B\langle 1|_A\langle 1|_B\right] \ . \tag{10}$$

[13] In the matrix representation this is simply $\rho_f = \left(\begin{smallmatrix} |b|^2 & 0 \\ 0 & |a|^2 \end{smallmatrix}\right)$.

[14] Extending the globe picture, a non-pure ensemble of qubits is represented by a point somewhere *inside* the surface. In particular, *diagonal* ensembles such as that of Eq. 8 lie on the axis joining the poles.

[15] The total system of EPR pair *plus* environment is *closed*, because there are no additional degrees of freedom coupled to this.

[16] $Trace_e(O)$ is effected by $\sum_k \langle k|O|k\rangle$, where the (many) states $|k\rangle$ are a complete orthonormal basis for the environment. The states in Eq. 9 decompose as $|e_i\rangle = \sum_k \alpha_i(k)|k\rangle$ for $i = 0, 1$ and their orthogonality constrains the expansion coefficients to obey $\sum_k \alpha_i^*(k)\alpha_j(k) = \delta_{ij}$.

This ensemble is not pure and has finite entropy of $S = k \ln 2$. When the environment is a large complex system containing many degrees of freedom, entanglement with it (once generated) can to all intents and purposes never be unwound. In such cases the EPR pairs effectively undergo irreversible decoherence. Clearly a similar effect can occur with much more complex systems of interest and, indeed, it will be much more likely—in effect, occur much more quickly—when there are many more components to the system (each able to couple to the environment), compared to the two of an EPR pair.

3. Thermal equilibrium: Consider the energy eigenstates of the system of interest, $H|E_j\rangle = E_j|E_j\rangle$. Independent of how it starts off—if it is being used for information processing it will be in some carefully prepared and supposedly unitarily evolving state—if the system makes contact with an environment at temperature T and attains thermal equilibrium, it decoheres. An ensemble of such systems is described by the equilibrium density operator

$$\rho_{eq} = \frac{1}{Z} \sum_j \exp(-E_j/kT) \; |E_j\rangle\langle E_j| \; . \tag{11}$$

The exponential probabilities are the well known Boltzmann factors and Z is the normalizing partition function $\sum_j \exp(-E_j/kT)$. ρ_{eq} is clearly not pure and has an entropy of $S = \overline{E}/T$, where $\overline{E}$ is the average system energy, the expectation value $Trace(\rho_{eq} H)$.

Generally speaking, irreversibility such as that in the latter two examples has to be stopped from biting before some desired unitary quantum evolution of the system has been completed.

This is the really crucial point. Although simple illustrations of irreversibility such as those just given are useful for thinking about the interactions and processes likely to generate decoherence, they don't answer the vital question: How does the typical decoherence time for a system—the inverse of the characteristic rate at which entropy grows—compare to the time needed to accomplish some useful unitary process? Actual time evolution is relevant for this, so here is another cautionary reason for not simply abstracting QIT to a list of unitary operations to be applied to a bag of qubits. The total time these operations take to run in practice is extremely important—it has to fall inside the decoherence time for that particular system. Simple error correction, or more sophisticated fault-tolerance, will more than likely lengthen the time of the desired unitary process. To gain payback, the increase in the effective decoherence time has to outstrip this.

A comprehensive discussion of the time evolution of open quantum systems, a vast subject in itself [15, 16], is clearly beyond the scope of this chapter. However, a simple introductory example is worthwhile, especially as this provides a useful model for some of the decoherence processes which occur in quantum systems relevant for QIT. Starting

with a complete system plus environment, it is possible to write down (at least formally) a very general expression for the evolution of $\rho = Trace_e(\varrho)$, assuming that the total coupled system is closed. This is extremely complicated [15, 16]; for starters it contains memory effects. The history of ρ has some say in its rate of change. Neglecting these—this is the Markovian approximation—and assuming that the interaction between the system and environment is weak enough for the Born approximation to work, it is possible to give a simple model (so-called master) equation for the system alone;

$$\frac{\partial \rho}{\partial t} = -\frac{i}{\hbar}\left[H, \rho\right] + \sum_m \left(L_m \rho L_m^\dagger - \frac{1}{2} L_m^\dagger L_m \rho - \frac{1}{2} \rho L_m^\dagger L_m \right) \ . \tag{12}$$

To re-emphasise, H is just the Hamiltonian of the system of interest. The operators L_m (which also act in the Hilbert space of this system) are the leftovers of the interaction with the environment after this has been traced out. These modify the unitary Schrödinger evolution and generate irreversibility.

The irreversible examples can be illustrated within this simple framework:

1. Measurement: Measuring the value of a qubit can be modelled using Eq. 12 with a single operator $L = \eta^{1/2} B$ where B is the bit value operator. In the matrix representation, $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and the solution is $\rho(t) = \left(\begin{smallmatrix} |b|^2 & ba^* \exp(-\eta t) \\ ab^* \exp(-\eta t) & |a|^2 \end{smallmatrix}\right)$, for a pure initial $\rho(0)$ constructed from Eq. 1. (This is in an interaction picture, setting $H = 0$.) Clearly $\rho(t)$ approaches the Eq. 8 result at large times and the rate of approach is set by the strength of the measurement interaction η. If the measurement is to look like a sharp "projection" at some timescale, η^{-1} must be very short in these units.

2. Decoherence: Qubits are frequently modelled as spin-1/2 systems and, indeed, in some cases this is an appropriate physical picture (in addition to a mathematical one). Often used operators are the Pauli matrices for the components of the spin,

$$\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \qquad \sigma_y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right) \qquad \sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) . \tag{13}$$

   Such a spin qubit subject to isotropic noise can be modelled using Eq. 12 with three operators $L_1 = \kappa^{1/2}\sigma_x$, $L_2 = \kappa^{1/2}\sigma_y$ and $L_3 = \kappa^{1/2}\sigma_z$. Besides the entropy, another quantity which can measure irreversibility and is often useful in discussions of quantum information theory is the *fidelity*, $f = \langle \psi_i | \rho(t) | \psi_i \rangle$, which compares the initial pure state $|\psi_i\rangle$ with the density operator at later times. The decoherence of a pure initial ensemble subject to isotropic noise is demonstrated by the decaying fidelity. The solution to Eq. 12 for *any* pure initial ensemble gives

$$f(t) = \frac{1}{2}\left(1 + \exp(-4\kappa t)\right) \ . \tag{14}$$

   This decay is due to that of the off-diagonal pieces of $\rho(t)$. Such damping is a generic feature of decoherence. At this level of description, then, for any physical

realization of a qubit it is vital to identify the appropriate environment coupling in order to gauge the decoherence time ($\sim \kappa^{-1}$) of the system.[17]

3. Thermal equilibrium: A photon mode coupled to a thermal bath—this might be the atoms in a laser cavity—can be modelled by Eq. 12 with two operators [16, 17], $L_1 = [(\overline{n}+1)\omega/Q]^{1/2}a$ and $L_2 = [\overline{n}\omega/Q]^{1/2}a^\dagger$. Here ω is the frequency, a ($a^\dagger$) is the photon annihilation (creation) operator (so $H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right)$), Q is the environment quality factor and $\overline{n} = [\exp(\hbar\omega/kT)-1]^{-1}$ is the thermal equilibrium photon number. For any starting condition, the photon number $a^\dagger a$ evolves according to

$$Trace\left(\rho(t)a^\dagger a\right) = \overline{n} + \left[Trace\left(\rho(0)a^\dagger a\right) - \overline{n}\right]\exp(-\omega t/Q) \qquad (15)$$

as the density operator diagonalizes to Eq. 11 with photon number eigenstates and $E_j = (j+\frac{1}{2})\hbar\omega$. Although the temperature T determines the final photon number, the timescale for evolution to this is $\sim Q/\omega$. More often than not, the timescale of a desirable unitary process will be set by the characteristic quantum frequency of the system; here this time is $\sim \omega^{-1}$. Comparing these, it is clear that high-Q systems are needed for QIT.

These last two very simple examples of decoherence illustrate the sorts of effects that have to be avoided for successful quantum information processing. Any real system will always have some level of environment coupling, so in practice this needs to be identified and a decent estimate of the relevant decoherence time made. If this compares favourably with the timescale of the unitary process to be run, all is well and good; if it doesn't, you have trouble.

I have focussed on the density operator approach to irreversibility as it is the standard one, giving a nice elegant description of ensemble average behaviour. However, QIT puts an emphasis on *individual* quantum systems, so it is worth pursuing this viewpoint a little. Certainly, it should be (made) clear that, apart from the pure ensemble case where every member is in the same state $|\psi\rangle$, a density operator does not identify with a unique ensemble. A simple example is Eq. 8 with $|a|^2 = |b|^2 = 1/2$. It could be that this ensemble is the output of bit value measurement apparatus, so each qubit *is* in state $|0\rangle$ or $|1\rangle$. However, instead it could be the result of decoherence due to isotropic noise, with all possible qubit states equally probable.[18] Both ensembles have the same density operator. Of course, you can't distinguish between these cases, or other possibilities, by making measurements; however, your actions can be detected!

[17] As an example, suppose that the spin has a magnetic moment μ and the environment is a simple white noise magnetic field $\mathbf{B}(t)$ with each component having a time-correlation of $\overline{B_i(t)B_i(s)} = B_0^2\tau\delta(t-s)$, defined by a characteristic field B_0 and a time τ. The coupling is then $\kappa \sim \mu^2 B_0^2\tau/\hbar^2$, which identifies it in terms of physical system and environment parameters.

[18] In the globe picture, there are many different ways of distributing points over the surface to achieve the same ensemble average point in the interior.

Suppose that somebody prepares one ensemble by encoding a long random bit string into the states $(|0\rangle, |1\rangle)$ and a second by doing the same but using the *alternative basis* states $(|\hat{0}\rangle, |\hat{1}\rangle)$ defined by [19]

$$|\hat{0}\rangle = 2^{-1/2}\,(|0\rangle + |1\rangle) \qquad\qquad |\hat{1}\rangle = 2^{-1/2}\,(|1\rangle - |0\rangle)\ . \tag{16}$$

In the richer state space of a qubit, these are equally good for representing zero and one; hence the labelling. Without the additional information regarding the ensembles' preparation, you simply have them both described by the same density operator, $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. If this diagonal form tempts you into thinking that you can measure in the $(|0\rangle, |1\rangle)$ basis and leave the qubits untouched, you will be mistaken, because this works for the first ensemble but not the second.[20] Don't take it personally, though, because this inability to "eavesdrop" on both ensembles is fundamental to quantum physics and forms the basis of quantum cryptography. This is outlined in Sec. 3 and discussed in more depth later in the book.

Any up to date work on open quantum systems should at least mention the quantum state approaches [16, 18, 19], as alternatives to the ensemble density operator view. These have developed considerably over the last decade. They all describe an *individual* member of an open ensemble by a state $|\psi\rangle$, which evolves stochastically—essentially there are extra bits to Eq. 3 which model the effect of the environment. The evolution is such that the average of $|\psi\rangle\langle\psi|$ over the stochastic variables gives density operator evolution consistent with the appropriate master equation. Various approaches, *unravellings* of the master equation, exist, such as quantum trajectories [16], quantum state diffusion [18] and quantum jumps [19]. The most appropriate one to use generally depends on the system and environment. Their virtue is that they are able to produce *pictures* of individual quantum systems, in keeping with the language we often use to describe them—projective measurements actually happen and thermal systems hop continually—and underpinned by the correct statistics. Such methods have proved extremely useful in mainstream quantum optics and so it seems likely that they will prove to be a very handy bag of tools for QIT modellers as well.

2.5 No cloning

Quantum systems lead a rather private existence. It is physically impossible to copy the state of a quantum system to a second identical one, leaving the original untouched. This is really a consequence of what has already been discussed; nevertheless, given its importance for QIT, it is worth stressing. From the fragility of quantum states, it

[19] On the globe, these are two points diametrically opposed on the equator. In the second basis viewpoint, *these* are now regarded as the poles. The original poles thus lie on the new equator, and there is complete symmetry between the two basis viewpoints.

[20] Clearly you should not have been tempted, since the density operator can be rewritten as $\rho = \frac{1}{2}(|\hat{0}\rangle\langle\hat{0}| + |\hat{1}\rangle\langle\hat{1}|)$.

is clear that simply measuring a system and then also placing the second system in the outcome state is useless—in general (and a copier has to work generally), neither will be in the original state. Alternatively, you might think that some subtle quantum coherent process, which *preserves* superposition states, could be devised to realize the cloning. Not so! Once again this is a property of Nature and not down to our ham-fistedness. Even if a unitary operator U_c acting on systems A and B can be arranged to copy the basis states of A to some initial state $|i\rangle_B$, so $U_c|0\rangle_A|i\rangle_B = |0\rangle_A|0\rangle_B$ and $U_c|1\rangle_A|i\rangle_B = |1\rangle_A|1\rangle_B$, it is clear that with the superposition state of Eq. 1 the result is

$$U_c|\psi\rangle_A|i\rangle_B = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B \ . \tag{17}$$

This entangled state is certainly not equal to $|\psi\rangle_A|\psi\rangle_B$, so the copying does not work in general.

The "no-cloning theorem" [20, 21] for quantum states has important implications for us. Eavesdroppers are thus unable to use cloning to try and beat a quantum cryptosystem by copying each qubit of a transmission. Similarly, it will not be possible to run off a copy of the state of a quantum computer part way through a computation, to use as backup in the event of subsequent errors. This simple approach to error correction is no good. Given this, it is not immediately obvious that any sort quantum error correction is possible. However, as you will see later in the book, recent remarkable research has shown that some forms of error correction and prolongation of quantum coherence can be done.

3 Quantum cryptography

3.1 The idea

The only cipher which is known to be mathematically secure is the one-time pad (or Vernam cipher, after Gilbert Vernam). Current public key cryptosystems rely on the *assumed* mathematical difficulty of certain operations (such as factoring in the case of RSA [6]); they are thus unable to guarantee security.[21] A one-time pad requires a random bit string, the *key*, as long as the secret message to be communicated. The key must be known only by the sender (Alice) and the receiver (Bob); "one-time" refers to the fact that any key should be used only once. To encode the message, Alice simply adds modulo 2 each bit of the key to its corresponding bit in the message. To decode, Bob simply repeats this procedure. Provided that an eavesdropper, Eve, has no information about the key, she cannot decipher the encoded message. To her it

[21] I suppose that people do not worry too much about this as it is *assumed* that the cracking of any such hard problems will happen in the academic and research community, and so will become public knowledge. Perhaps we should get suspicious if some of the top number theorists stop publishing and buy big yachts...?

will look like a random string of bits; she needs the key to crack the encoding. The security of the message thus reduces to the security of the key. Herein lies a problem, though, because if Alice and Bob share the key as ordinary classical information they cannot be *sure* that nobody else has shared their supposedly secret key. In principle, Eve can read a classical key without leaving any evidence at all of her snooping. The impact of quantum physics is to solve this problem. If Alice and Bob use qubits, they can establish a shared key which they can be sure is known only to them. They then have a guaranteed secure quantum cryptosystem because the irreversibility of quantum measurement—this is the *only* way Eve can examine the qubits—ensures that Eve *cannot* snoop without leaving evidence of this. A wider discussion of the whole area of quantum cryptology is given by Hoi-Kwong Lo in chapter four; this short section just introduces the original idea and approach.

Alice and Bob need a "quantum channel", along which qubits are sent, and a form of conventional public communication channel such as a broadcast radio system. The fundamental requirement of the public channel is that Eve cannot block all the transmissions and then replace them with her own spoof messages—if she could, she could break the security. The sacrifice of Alice and Bob's spoof-proofing is that Eve can hear their public transmissions without any effort and without revealing her presence. Where Eve has to attempt to listen in is on the quantum transmissions; this is where she gets caught.

Suppose first that Alice simply sends to Bob a random string of qubits with states $|0\rangle$ or $|1\rangle$. Knowing that he will be getting these states, Bob can measure them without introducing any irreversibility. Apparatus shortcomings aside, he gets perfect results and he and Alice have a shared random bit string. The trouble with this is that Eve can do the same! In this case the quantum channel is effectively being used classically, so Eve can listen in without being detected.

To combat this, Alice uses a second pair of states—in quantum language a second basis. These are the states $|\hat{0}\rangle$ and $|\hat{1}\rangle$ defined in Eq. 16, superpositions of the other basis states $|0\rangle$ and $|1\rangle$ (and vice versa). Bob now has a problem because if Alice sends at random one of the four states $|0\rangle$, $|1\rangle$, $|\hat{0}\rangle$ and $|\hat{1}\rangle$, he does not know what to measure! He therefore chooses at random to measure projecting onto the ($|0\rangle$,$|1\rangle$) basis, or onto the ($|\hat{0}\rangle$,$|\hat{1}\rangle$) basis. Half the time he will be okay, but half the time he will choose to measure a state which is a *superposition*, as seen in the basis in which he is measuring. These states will be irreversibly corrupted by Bob's quantum measurement, and so must be discarded. This is done by him telling Alice publicly the sequence of measurements he made (but not the results!); she then identifies which data are to be kept (which is called the raw quantum transmission—RQT) and communicates this back to Bob. On average they sacrifice half of the transmission; however, their gain is that they confound Eve.

Eve has a problem when Alice uses four states, the same problem as Bob. She

does not know what to measure, so essentially all she can do is the same as Bob, and guess. Consider just the RQT, just the data kept by Alice and Bob. For half of this Eve will guess wrongly, and measure in the opposite basis to that used by Alice and Bob. The irreversibility of quantum measurement ensures that Eve corrupts all these qubits en route to Bob. He has equal chances of recovering the correct value (sent by Alice), or getting an error, when he measures such a corrupt qubit. Eve therefore corrupts one quarter of the RQT that she intercepts; quantum physics guarantees this. Besides this original approach [22], other quantum cryptographic protocols and procedures now exist. However, they all essentially rely on the same idea:

Force Eve to undertake some guesswork as to what to measure and quantum mechanics will ensure that she leaves evidence, in the form of errors in the RQT.

By public sacrifice of a sample of the RQT, Alice and Bob can thus determine how much of this has been intercepted. If it is the lot, they bin it and try again. However, at least they know—this is why it is best to use the quantum channel to establish a secret key, rather than send the actual message. If only a part of the RQT has been read, Alice and Bob can find and eliminate the errors, and then distil from the correct data a smaller secret shared string which forms their final cryptographic key [22]. All this is done by public discussions. Even if Eve knows some of the RQT, she will still know essentially nothing about the final key. For example [22], if Eve corrupts 4% of a 2000 bit RQT, Alice and Bob are able to distil a 754 bit key, about which Eve knows less than 10^{-6} of one bit.

3.2 Experiments

Quantum cryptography is not just a pipe-dream of theoreticians. This is one area of QIT which has made it off the drawing board. There is total consensus in the field that photons—quanta of light—are the best qubits for this purpose. All the working systems use them; their polarizations or phases are used as the bit values.

The first prototype ran in 1989 at IBM,[22] [22] over a short distance under laboratory conditions. Since then, a number of groups have produced much more practical systems. Notable are those of Nicolas Gisin's group (GAP) in Geneva [24, 25] and Jim Franson's group at John Hopkins University in the US [26, 27]. GAP borrowed 23 *km* of Swiss Telecom optical fibre which runs under Lake Geneva, and ran a quantum cryptosystem down this! Franson's group has run them in free space, down lit corridors and outside in bright daylight! Between them they have addressed and solved many of the problems which lie between prototype and real, practical systems. GAP currently hold the "world record" for a quantum key, establishing a 20 *kbit* key at about 0.5 *Hz*.

[22] Charles Bennett at IBM also holds the first patent for quantum cryptosystems [23]; further refinements are also patented.

A detailed discussion on experimental quantum cryptography is given in chapter five by Hugo Zbinden.

4 Quantum computing

Whereas irreversibility is what enables quantum cryptography, it may end up being the insurmountable hurdle for useful quantum computing. Decoherence of any of the qubit components of a quantum computer may trash the running of the whole unitary algorithm. Apart from measurements *designed* into a quantum computation, which may well be made right at the end, to reveal the result, irreversibility means trouble. If you keep opening the oven door to see what is happening, or the door fits badly so heat leaks to the environment, your soufflé will flop.

Quantum computing gets its potential power from initial superposition states evolving reversibly and generating entanglement between the many components of quantum machine. The 2^m possible states of an m-bit classical register form a suitable basis, so an m-qubit register can be placed in a superposition of *all* these states. This is why certain problems may be solved "exponentially faster" by a quantum machine, in comparison to any classical machine. For a problem whose solution requires some property of the results of *all* 2^m different calculations, these have to be calculated separately in the classical case. On the other hand, if some clever manipulation can be performed on a quantum computer state (which has evolved to contain 2^m parts, corresponding to all the classical results), to yield the collective property in just one run, the solution of such a problem can be obtained with exponentially less effort! Chapter six, by Adriano Barenco, discusses details of quantum computing, from the gates and networks needed through to the types of algorithms which can usefully be run on such machines.

As decoherence rubbishes nice reversible unitary evolution, and this is vital for quantum computation, the effects of the environment have to be held at bay for the duration of any computation. Unfortunately, decoherence bites harder at bigger, more complex, quantum systems. Roughly speaking, a composite of n quantum systems decoheres n times more quickly than one of the individual members.[23] Given this, it seems unlikely that careful shielding of a quantum computer alone will render it able to perform useful calculations. Some form of active state stabilization, to preserve unitarity and prevent errors, will almost certainly be required as a useful computer will contain $n \gg 1$ qubits. Despite the "no-cloning" theorem, this can be done. The basic idea behind the procedure is the same as in classical error correction—build in redundancy and use this to protect against (some level of) errors. However, the

[23] Handwaving: In Sec. 2.4 it was seen that coherence dies like $\exp(-\kappa t)$ for a qubit where κ characterizes the coupling to the environment. Taking such a factor for each of n qubits, the effective decoherence time of the whole system is reduced to $\sim (n\kappa)^{-1}$.

implementations are more subtle because, on top of cloning being outlawed, the richer space of quantum states contains a greater variety of errors, in comparison to simple flip errors which can occur with classical bits. The first developments, independently by Peter Shor and Andy Steane, showed how a number of qubits could simply have their decoherence time lengthened, by encoding them into a greater number [28, 30, 31]. Essentially, the entropy which arises from the interactions of all the qubits with the environment is massaged into just the redundant ones, leaving the important ones unscathed. Although fine for the storage of quantum information, this is inadequate for computation, where information is *manipulated* by interactions between qubits as the system evolves. More recently, Shor [32], Steane [33] and others have addressed this problem, and shown that in principle quantum computations can be performed in a fault tolerant manner. A sample result is that provided the error probability for a single quantum operation between two qubits is $\sim 10^{-5}$, a coherent computation of $\sim 10^{12}$ such steps and involving around 80 qubits should be possible. Andy Steane (chapter seven) and John Preskill (chapter eight) discuss the important topics of error correction and fault tolerance.

4.1 Examples

Here's a list of things you might do with a quantum computer. This may not yet convince you to go and put a down payment on a machine, but it should whet your appetite for the later chapters of this book.

- **Factoring:** Given the classical cryptographic importance of factoring, the most well-known example to date of a quantum algorithm is Peter Shor's factoring algorithm [34]. Factoring of a large composite integer N is not proven to be intractable classically, but to date no good algorithms for this exist.[24] Shor's algorithm works by turning the problem into that of finding the (very large) period r of a periodic function.[25] Given r, it is a bit of elementary number theory to deduce factors of N; finding r is the hard bit.

  At least it is hard classically, because it requires a very large number of calculations, to plot the function and read off its period. Quantum mechanically, all these calculations can be performed in parallel. The clever manipulation is then to transform—apply a discrete Fourier transform—the final state to one where a single measurement will then yield r. (Actually, this is not quite true—there is a probabilistic element, so a few runs are needed, but not very many.)

[24] For example, the factoring of a 130 decimal digit number took 500 $MIPS$ *years* of computer effort, and a big supercomputer crunch at the end! (An average workstation runs at around 10 $MIPS$, million instructions per second.)

[25] $f_N(x) = y^x \bmod N$, where y is an integer coprime with N. This is a periodic function of the variable x, so $f_N(x) = f_N(x + r)$

- **Simulation:** A quantum computer would be an excellent basic research tool. It is hard to squash a sizeable Hilbert space into ordinary memory, so simulating complex interacting quantum systems on a conventional computer is really hard work. Simulating them [35] on an actual quantum machine would be much easier! Nuclear physicists, material scientists, molecular chemists and many others would queue up for time on a quantum computer, to investigate novel systems, regimes and materials inaccessible with classical modelling tools.

- **Searching and estimation:** A classical search of a random list of M items to find a particular one requires the examination of at least $M/2$ of them to have a 50% success probability. Lov Grover has shown [36] how a quantum search could find an item in only $O(M^{1/2})$ steps. In effect, using superposition states enables the examination of multiple items simultaneously. This speeds up the search, although in this case not exponentially. A similar square root improvement over classical algorithms for estimating the median of M data can be achieved in the quantum case [37].

- **Frequency standard:** As the first working quantum machines will certainly consist of only a few interacting qubits, it would be nice to find something useful that can be done with such a simple system. A possibility is to use the ideas developed for quantum error correction in something other than a computer. A frequency standard effectively relies on the coherent oscillation of a pure atomic quantum state, so it is limited by decoherence as the atom/ion interacts with its environment.[26] The problem is subtle. It is not simply one of preserving a static state; the oscillation cannot be ignored in a frequency standard! The errors are harder to remove from a time-varying state. Nevertheless, it seems that some entanglement between ions has potential benefit [38].

4.2 Experiments

Whereas quantum cryptography relies on the independent behaviour of a string of non-interacting photon qubits, *interactions between qubits* are a must for quantum computation. There are a number of candidate systems currently being researched. There is no clear favourite as yet, to mirror the use of photons for cryptography. Those jostling for position are:

1. Ions/atoms in an electromagnetic trap, interacting through their quantum vibrational motion. Their internal energy levels form qubits and external laser fields can be coupled to these.

[26] The dominant effect is dephasing, which can be described for a two state atom/ion by a single environment operator σ_z in the model given in Sec. 2.4.

2. Atoms in beams, interacting electromagnetically with cavity or travelling photons. Cavity photon number states and atomic levels (Rydberg or optical) form qubits; external fields (microwave or optical) can be coupled in.

3. Electrons in quantum dots, interacting electrostatically or possibly magnetically. The discrete levels of the confined electrons form qubits (or possibly qu*n*its) and they couple readily to external fields.

4. Spin systems, interacting through their magnetic moments. These might be in a regular lattice, or, at a smaller scale, different spins within a large molecule, the so-called NMR quantum computing [39, 40]. A static external field separates out discrete spin levels for qubits. Time dependent fields can be applied to manipulate the system; in particular, in the NMR case the technology for doing this is very well developed.

5. Superconducting systems, interacting through the quantum motion of electric charges or magnetic flux. Such systems also have discrete levels and can be probed with external currents, voltages and fluxes.

Numbers 1 and 2 took the lead in experiments. David Wineland's group [41] at NIST in Colorado have demonstrated a quantum logic operation between two qubits in an ion trap and Jeff Kimble's group [42] at Caltech have demonstrated atom-photon cavity interactions which could form the basis of a similar quantum gate.

A single two-qubit gate is clearly way short of a useful machine. However, it is worth noting that lots of these (kept quantum coherent) will be sufficient to build any quantum processor. More complex quantum gates may appear, but they are not necessary. It is known theoretically that pretty well any two-qubit gate is *universal*. Add in coherent operations applied to a single qubit—to fundamental quantum physicists these are really old hat compared to two-qubit gates—and you have the all the ingredients you need to build any quantum processor. Consequently, blueprints have already been drawn up for devices such as Shor's factoring machine. For ordinary classical (irreversible) computing, in principle just three basic gates are needed to build any processor. However, real machines usually contain many rather more complicated gates, because it is more practical and convenient to build them this way. If real quantum machines develop, they may well follow suit, using more complex tailored gates rather than being made entirely from universal building blocks.

Although ions, atoms and photons claimed the first breakthroughs for quantum gates, there is now growing interest in NMR quantum computing [39, 40], especially since the demonstration [43] of a GHZ [44] three-particle entangled state.[27] It seems very likely that logical manipulations of small numbers of NMR qubits (well within the system decoherence time) will soon be achieved; what is not so clear is how this might

[27] Eq. 9 is an example, if the environment is simply taken to be a third qubit.

be scaled to large numbers. It is also worth noting that, compared to the other options, the fabrication of complex quantum dot and superconducting systems will probably be rather easier. These may thus be crucial ingredients of future technology. Given the early stages of the work, for the meantime basic research in all of the QIT building block areas (including potential new ones) is likely to contribute to this ultimate goal. Current practical quantum computing research areas are reviewed later in this book; Thomas Pellizzari discusses optical and ionic systems in chapter nine and Isaac Chuang discusses NMR systems in chapter ten.

5 Summary and comments

Here are a few comments to take forward for the rest of the book. At the end, in chapter eleven, Charles Bennett discusses in more detail the future of QIT, some open questions and how the field may develop.

- Quantum physics has the potential to generate both evolutionary and revolutionary developments in information technology. Expect evolutionary improvements to conventional logical processing to have shorter lead times than those for the emergence of radically new forms of processor.
- The intrinsic irreversibility of quantum measurement enables guaranteed secure communications. Eavesdroppers cannot intercept quantum transmissions without corrupting some of the data, thus exposing themselves. Quantum cryptosystems use secret keys, shared quantum mechanically, as one-time pads.
- Quantum cryptosystems work in the real world, not just in sanitized laboratories. The "world record" key is 20 *kbit*, established down 23 *km* of optical fibre under Lake Geneva at 0.5 *Hz*. Much higher ($\sim 10^3$) bit rates have been achieved in shorter bursts.
- Quantum systems can exist in superposition states, which simultaneously contain parts corresponding to different classical states. A complex quantum machine could thus process an exponentially large number of classical calculations in one run. Problems like factoring would be tractable with quantum parallelization.
- Complex quantum systems lose their coherence much more quickly than simple ones. Decoherence destroys quantum parallelism, generating errors. Despite the "no-cloning" theorem, quantum error correction is possible, massaging errors and entropy out of systems and prolonging their unitary life.
- Some individual quantum gates have been made. Roughly 2000 (plus many more for error correction), coherent as they interact, would be needed to factor a 400 bit number. This is a big challenge for the future.

- There has been a lot of excitement in the media about NMR quantum computing. However, the idea that we will soon be quantum computing with our coffee is probably mostly froth. Nevertheless, research in this this practical area, along with that on ion traps, atomic beams, photons, quantum dots and superconductors, is at a very interesting stage.

- Research is on-going into uses for processors containing just a handful of qubits, as these will be the first to emerge. Coherently manipulating entanglement in these systems is the goal—this may have applications to frequency standards and in quantum simulations, as well as being of tremendous fundamental importance. Of course, the search is also still on for other useful quantum algorithms, additional to Shor's, which would run on bigger machines.

- In addition to the practical interest in QIT, the fields of quantum information and computing provide a new arena for testing and understanding fundamental questions in quantum mechanics. For example, they have helped stimulate experimentalists to master the mapping out of actual quantum states of light, atoms and molecules, and encouraged theorists to delve deeper into quantum entanglement and separability.

- Quantum information technology seems unlikely to displace large areas of existing IT and more likely to emerge alongside it, defining new applications and markets. Given the might of the current industry, the short term payback will therefore almost certainly come from evolutionary quantum-assisted developments. However, given the successes at the basic research level over the last few years, it seems clear that future research efforts should be spread across the whole spectrum, rather than simply being focussed on evolutionary short term goals.

References

[1] K. K. Likharev, *Physics World*, vol. **10**, no. 5, 39 (May 1997).

[2] A. Barenco, *Contemporary Physics* **37**, 375 (1996).

[3] A. K. Ekert and R. Jozsa, *Rev. Mod. Phys.* **68**, 733 (1996).

[4] T. P. Spiller, *Proceedings of the IEEE*, vol. **84**, no. 12, 1719 (1996).

[5] http://vesta.physics.ucla.edu/ smolin/index.html
http://eve.physics.ox.ac.uk/QChome.html
http://feynman.stanford.edu/qcomp/
http://www.iro.umontreal.ca/labs/theorique/index_en.html
http://xxx.lanl.gov/archive/quant-ph

[6] R. Rivest, A. Shamir and L. Adleman, "On Digital Signatures and Public Key Cryptosystems," *MIT Laboratory for Computer Science Technical Report*, MIT/LCS/TR-212 (January 1979).

[7] A. Einstein, B. Podolsky and N. Rosen, *Physical Review* **47**, 777 (1935).

[8] J. S. Bell, *Physics* **. 1**, 195 (1964); *Rev. Mod. Phys.* **38**, 447 (1966).

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).

[10] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett* **69**, 2881 (1992).

[11] B. Schumacher, *Phys. Rev.* A **51**, 2738 (1995).

[12] J. von Neumann, *Mathematical foundations of quantum mechanics*, Ch. 5 (Princeton University Press, 1955).

[13] R. Landauer, *Phys. Lett.* A **217**, 188 (1996).

[14] A. Peres, *Phys. Rev.* A **32**, 3266 (1985).

[15] U. Weiss, *Quantum dissipative systems*, Series in Modern Condensed Matter Physics Vol. 2, (World Scientific Press, 1993). (This book also contains a large list of very useful references.)

[16] H. Carmichael, *An open systems approach to quantum optics*, Lecture Notes in Physics m18, (Springer-Verlag Press, 1993).

[17] M. Sargent III, M. O. Scully and W. E. Lamb, Jr., *Laser Physics*, Ch. 16 (Addison-Wesley Press, 1974).

[18] N. Gisin and I. C. Percival, *J. Phys.* A **25**, 5677 (1992).

[19] M. B. Plenio and P. L. Knight, "The quantum jump approach to dissipative dynamics in quantum optics," eprint quant-ph/9702007, to appear in *Rev. Mod. Phys.*.

[20] W. K. Wootters and W. H. Zurek, *Nature*, **299**, 802 (1982).

[21] D. Dieks, *Phys. Lett.* A **92**, 271 (1982).

[22] C. H. Bennett, F. Bessette, G. Brassard, L. Savail and J. Smolin, *J. Cryptology* **5**, 3 (1992).

[23] C. H. Bennett, International Business Machines Corporation, "Interferometric quantum cryptographic key distribution system," United States Patent Number 5,307,410 (April 26, 1994).

[24] A. Muller, H. Zbinden and N. Gisin, *Europhys. Lett.* **33**, 335 (1996).

[25] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller and W. Tittel, "Interferometry with Faraday mirrors for quantum cryptography," eprint quant-ph/9703024, to appear in *Electronics Letters*, 1997.

[26] J. D. Franson and B. C. Jacobs, "Quantum cryptography without optical fibers," in QELS '96, paper presented at the Quantum Electronics and Laser Science Conference, Vol.10 1996 Technical Digest Series, Conference Edition (IEEE Cat. No. 96CH35902).

[27] B. C. Jacobs and J. D. Franson, "Feasibility of global systems for quantum cryptography," preprint, 1996, submitted to Electronics Letters.

[28] P. W. Shor, *Phys. Rev.* A **52**, 2493 (1995).

[29] A. R. Calderbank and P. W. Shor, *Phys. Rev* A **54**, 1098 (1996).

[30] A. M. Steane, *Proc. R. Soc. Lond.* A **452**, 2551 (1996).

[31] A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996).

[32] P. W. Shor, "Fault-tolerant quantum computation," in *Proc. 37th Symp. on Foundations of Computer Science* (IEEE Computer Society Press, 1996).

[33] A. M. Steane, "Active stabilisation, quantum computation and quantum state synthesis," eprint quant-ph/9611027, University of Oxford preprint 1996, submitted to *Phys. Rev. Lett.*.

[34] P. W. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring," in *Proc. 35th IEEE Symp. on Foundations of Computer Science*, ed. S. Goldwasser (IEEE Computer Society Press, 1994).

[35] S. Lloyd, *Science* **273**, 1073 (1996).

[36] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annual ACM Symposium on the Theory of Computing (STOC)* (1996); *Phys. Rev. Lett.* **79**, 325 (1997).

[37] L. K. Grover, "A fast quantum mechanical algorithm for estimating the median," eprint quant-ph/9607024.

[38] S. F Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio and J. I. Cirac, "On the improvement of frequency standards with quantum entanglement," eprint quant-ph/9707014.

[39] N. A. Gershenfeld and I. L. Chuang, *Science* **275**, 350 (1997).

[40] D. G. Cory, A. F. Fahmy and T. F. Havel, *Proceedings of the National Academy of Sciences* **94**, 1634 (1997); D. G. Cory, M. D. Price, A. F. Fahmy and T. F. Havel, *Physica* D (in press), eprint quant-ph/9709001.

[41] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland, *Phys. Rev. Lett.* **75**, 4714 (1995).

[42] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi and H. J. Kimble, *Phys. Rev. Lett.* **75**, 4710 (1995).

[43] R. Laflamme, E. Knill, W. H. Zurek, P. Catasti and S. V. S. Mariappan, "NMR GHZ," eprint quant-ph/9709025.

[44] D. M. Greenberger, M. Horne and A. Zeilinger in *Bell's theorem, quantum mechanics and conceptions of the universe*, ed. M. Kafatos (Kluwer Press, 1989).