Introduction to Quantum Error Correction

E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola and W. Zurek

December 16, 2001

Contents

1 Concepts and Examples **4**

1.1 Trivial Two-Bit Example 5

1.2 The Repetition Code 7

1.3 A Code for a Cyclic System 8

2 Principles of Noise Control **10**

2.1 Error Detection 11

2.2 From Error Detection to Error Correction 12

3 Quantum Error Correction **13**

3.1 Trivial Two-Qubit Example 13

3.2 Quantum Repetition Code 14

3.3 Quantum Code for a Cyclic System 18

3.4 Three Quantum Spin-Half Particles 19

4 Error Models **22**

4.1 The Standard Error Models for Qubits 22

4.2 Quantum Noise Analysis 24

5 From Quantum Error Detection to Error Correction **26**

5.1 Quantum Error Detection 26

5.2 Quantum Error Correction 28

6 Stabilizer Codes **30**

7 Fault Tolerant Quantum Communication and Computation **32**

7.1 Requirements for Scalable QIP 32

7.2 Realizing Fault-Tolerance 33

8 Concluding Remarks **36**

In order to exploit the anticipated advantages of quantum information processing (QIP), it needs to be physically realized. There is an abundance of proposals for building the basic devices of QIP using various media exhibiting quantum properties. Examples include nuclear spins in molecules, electron spins or charge in quantum dots, collective states of superconductors, and photons [1]. In all of these cases there are well established physical models that, under ideal conditions, allow for exact realizations of quantum information and its manipulation. However, real physical systems never behave exactly like the ideal models. The main reasons for this are that a physical system cannot be completely isolated from its environment, the parameters of the system are not known exactly, and the means for controlling the system are subject to calibration errors and random fluctuations. This gives rise to the two sources of noise in physical QIP devices: Environmental noise and control errors. Attempts to reduce the effects of these errors are confronted by the conflicting needs of being able to control and reliably measure the quantum systems, which requires strong interactions with control devices, and of having the system sufficiently well isolated to maintain coherence—the subtle relationships between the phases in a quantum superposition. The fact that quantum effects rarely persist on macroscopic scales suggests that meeting these needs requires substantial artificial intervention, assuming that it is in fact possible.

Soon after P. Shor published the efficient quantum factoring algorithm, A. Steane [2] and P. Shor [3] gave the first constructions of quantum error-correcting codes. By demonstrating that quantum states can exist in protected parts of the state space, they showed that it is possible in principle to protect against environmental noise. This initiated a series of investigations by many researchers that culminated in what are now know as "accuracy thresholds" [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]. According to these thresholds, if the effects of environmental noise and control errors are sufficiently small, then it is possible to process quantum information arbitrarily accurately with efficient resource overheads. All thresholds require that the noise satisfies locality and independence assumptions and that quantum gates can be applied in parallel. As the proven thresholds involve accuracies well out of reach of present day devices, much work remains to be done to make these results practical.

In retrospect, the advances in quantum error correction and fault tolerance were made possible by the realization that error-free computation does not mean that the state of the physical devices supporting the computation is perfect. In classical information processing this is so obvious that it is often forgotten: No

two letters “e” on a written page are physically identical, and the exact number of electrons used to store a bit in a computer memory is not stable. Nevertheless, we have no difficulty in accurately identifying the desired letter or state. The conceptual difficulty with quantum information is that by its very nature, we cannot identify it by “looking” at it. The sense in which quantum information can be accurately stored in a noisy state needs to be redefined. There are two ways in which one can understand how this works. The first is by considering the stored information to be that which can in principle be extracted by an ideal prescribed quantum decoding procedure. The second is to explicitly define “subsystems” (particle-like aspects of the quantum device) that contain the desired information. The former is naturally obtained as a generalization of the usual interpretations of classical error-correction methods, while the latter is motivated by the way in which particles emerge in quantum physics.

In this introduction we motivate and explain the “ideal decoding” and “subsystems” view of quantum error correction. We explain how quantum noise in QIP can be described and classified, and summarize the requirements that need to be satisfied for fault tolerance. In view of the capabilities of today’s quantum technology, the requirements appear daunting. But the idea of “subsystems” shows that these requirements can be met in many different, and often unexpected ways.

1 Concepts and Examples

The prototypical application of error-correction is communication, where the sender needs to send information to a receiver using a noisy “communication channel”, which is a means for transmitting a physical system from one place to another. This requires “encoding” the information to be transmitted in the physical system for the channel, and after transmission, “decoding” it. The procedure is shown in Fig. 1.

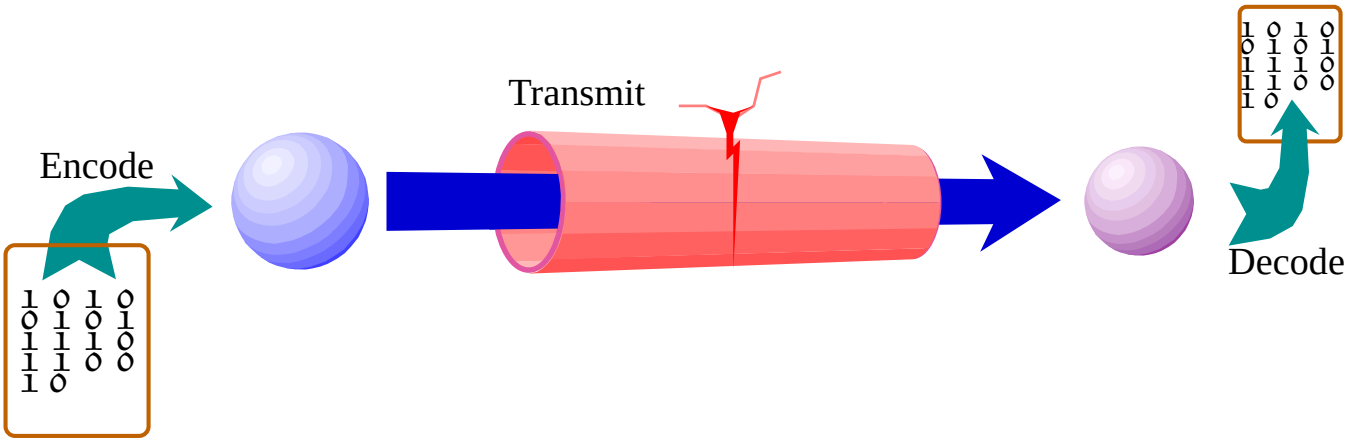


FIG. 1: A typical application of error-correction: A noisy communication channel with encoding and decoding processes for protecting against communication noise.

In computation a similar situation occurs when storing information in a memory. Here the communication channel is replaced by storage units. For fault tolerant computation, encoding and decoding procedures are largely absent because the information is normally maintained in encoded form. Instead there need to be procedures to effect computational operations on the encoded information while maintaining fault tolerance.

To illustrate the different features of error-correction for communication or storage we consider three examples. We begin by describing them for classical information, but in each case, there is a quantum analogue that will be introduced later.

1.1 Trivial Two-Bit Example

Consider a physical system consisting of two bits with state space $\{00, 01, 10, 11\}$. We use the convention that state symbols for physical systems subject to noise are in brown. States changed by noise are sometimes distinguished by using red symbols. We wish to store one bit of information. The effect of noise is to flip (apply the **not** operator to) the second bit with probability .5. The problem of protecting one bit of information is solved by storing it in the first bit, which is unaffected by this noise (Fig. 2).

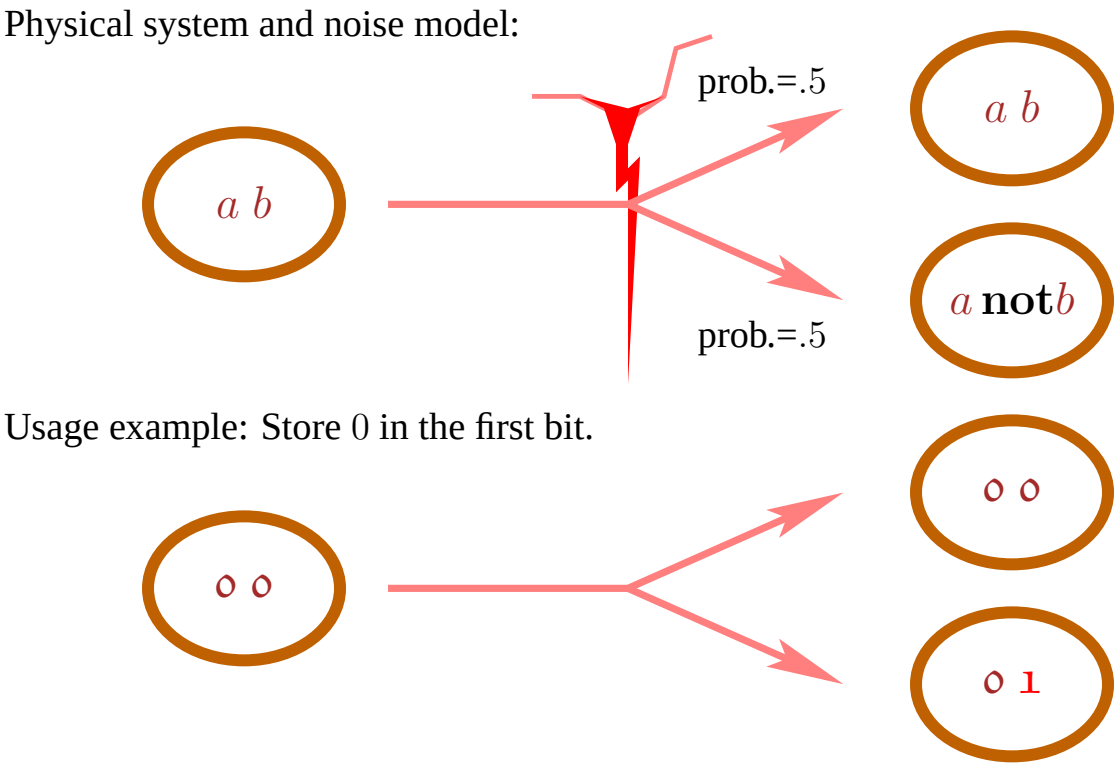


FIG. 2: A simple noise management problem. Noise only affects bit two of a two bit system. All joint states of the two bits are affected by noise. Nevertheless the value of information stored in the first bit is unchanged. This works equally well for qubits with noise acting only on the second qubit.

In terms of the process of Fig. 1, information can be encoded in the physical system by the map $0 \rightarrow 00, 1 \rightarrow 10$. Decoding consists of extracting the first of the two bits by the map:

$$\begin{aligned} 00 &\rightarrow 0 \\ 01 &\rightarrow 0 \\ 10 &\rightarrow 1 \\ 11 &\rightarrow 1 \end{aligned} \tag{1}$$

There are other combinations of encoding and decoding that work. For example, in the encoding, we could swap the meaning of 0 and 1, provided that is taken into consideration in the decoding. Thus, in terms of the behavior with respect to the noise, what is relevant is the range $\{00, 10\}$ of the encoding, not the assignment to bit values. This range is called the "code", and the states in the code are called "code words".

The example just given is typical of all ways of controlling errors. That is, there is always a way of viewing the physical system as a pair of systems, where the first carries the information to be protected and the second (hopefully) experiences the noise. Encoding consists of initializing the second system (in the example, we initialized to $\mathtt{0}$) and storing the information in the first. Decoding is accomplished by extraction of the first system. In this view, the information carrying member of the pair of systems is a "subsystem" of the full physical system. The identification of the subsystem determines the decoding.

1.2 The Repetition Code

Let the physical system consist of three bits. The effect of noise is to independently flip each bit with probability $.25$. The repetition code is obtained by duplicating the information to be protected. It is realized by the encoding $\mathtt{0} \rightarrow \mathtt{000}, \mathtt{1} \rightarrow \mathtt{111}$. The associated code is the set $\{\mathtt{000}, \mathtt{111}\}$. The information can be decoded using majority logic: If the majority of the three bits is $\mathtt{0}$, output $\mathtt{0}$, otherwise output $\mathtt{1}$. How well does this system work for protecting information against the noise? The decoding fails if two or three of the bits were flipped by the noise. The probability of a given pair of bits having flipped is $.25^2 * .75$. There are three different pairs. The probability of three bits having flipped is $.25^3$. Thus the probability of error is $3 \cdot .25^2 * .75 + .25^3 = 0.15625$. This is a significant improvement over $.25$.

To see that this example can be interpreted by viewing the physical system as a pair of subsystems, it suffices to give an identification of the physical system's states with the states of a suitable pair. The following accomplishes this goal:

$$\begin{aligned}
\mathtt{000} &\leftrightarrow \mathtt{00} \cdot \mathtt{0} \\
\mathtt{001} &\leftrightarrow \mathtt{11} \cdot \mathtt{0} \\
\mathtt{010} &\leftrightarrow \mathtt{01} \cdot \mathtt{0} \\
\mathtt{100} &\leftrightarrow \mathtt{10} \cdot \mathtt{0} \\
\mathtt{011} &\leftrightarrow \mathtt{10} \cdot \mathtt{1} \\
\mathtt{101} &\leftrightarrow \mathtt{01} \cdot \mathtt{1} \\
\mathtt{110} &\leftrightarrow \mathtt{11} \cdot \mathtt{1} \\
\mathtt{111} &\leftrightarrow \mathtt{00} \cdot \mathtt{1}
\end{aligned} \tag{2}$$

The last bit on the right-hand side of the identification is the subsystem that carries the information. The

other system consists of the first two bits on the right and is called the "syndrome" system. This is because after the noise acts with zero or one bit flips, its state (the "syndrome") identifies the error that occurred. In the identification given, the code consists of the two joint states where the syndrome system is in the state $\mathtt{oo}$.

Noise usually acts cumulatively over time. To deal with this, one can repeat the following procedure sufficiently frequently: Reset the syndrome system to $\mathtt{oo}$ using the identification given, then wait while the noise acts. Resetting can be accomplished, for example, by using the vertical shortcut of the following diagram based on the identification above:

$$\begin{array}{rcl} \mathtt{oll} & \longrightarrow & \mathtt{lo}\cdot\mathtt{l} \\ \text{reset:}\downarrow & & \downarrow \\ \mathtt{lll} & \longleftarrow & \mathtt{oo}\cdot\mathtt{l} \end{array} \tag{3}$$

A single bit flip error after a reset operation acts only on the syndrome system. For example, we can follow what happens to an encoded $\mathtt{o}$ and $\mathtt{l}$ if the second physical bit is flipped:

$$\begin{array}{ccc} \mathtt{ooo} \leftrightarrow \mathtt{oo}\cdot\mathtt{o} & & \mathtt{lll} \leftrightarrow \mathtt{oo}\cdot\mathtt{l} \\ \downarrow & & \downarrow \\ \mathtt{olo} \leftrightarrow \mathtt{ol}\cdot\mathtt{o} & & \mathtt{lol} \leftrightarrow \mathtt{ol}\cdot\mathtt{l} \end{array} \tag{4}$$

The error changes only the syndrome, and in the same way. That is, if the state of the syndrome is $\mathtt{ol}$, one can deduce that the most likely event was a flip of the middle physical bit.

1.3 A Code for a Cyclic System

Consider a physical system with seven states $0, 1, 2, 3, 4, 5, 6$. Let s_1 be the right-circular shift operator defined by $s_1(l) = l + 1$ for $0 \leq l \leq 5$ and $s_1(6) = 0$. Define $s_0 = \mathbb{1}$ (the identity operator),

$$s_k = \underbrace{s_1 \ldots s_1}_{k \text{ times}}, \tag{5}$$

and $s_{-k} = s_k^{-1}$ (left-circular shift by k). Suppose that the noise consists of applying s_k with probability qe^{-k^2}, where $q = 0.5641$ is chosen so that the probabilities sum to 1. Thus s_0 has probability 0.5641, and

s_{-1}, s_1 each have probability 0.2075. These are the main errors that we need to protect against. Continuous versions of this error model are known as "Gaussian channels".

One bit can be encoded in this physical system by the map $\mathfrak{o} \to 1, \mathfrak{1} \to 4$. To decode with protection against s_0, s_{-1} and s_1, use the mapping:

$$\begin{aligned} 0 &\to \mathfrak{o} \\ 1 &\to \mathfrak{o} \\ 2 &\to \mathfrak{o} \\ 3 &\to \mathfrak{1} \\ 4 &\to \mathfrak{1} \\ 5 &\to \mathfrak{1} \\ 6 &\to \text{fail} \end{aligned} \tag{6}$$

If 6 is encountered, we know that an error happened involving a shift of at least 2 (left or right), but there is no reasonable way of decoding it to the state of a bit. This means that the error is detected, but we cannot recover from it. Error detection can be used by the receiver of information to ask for it to be re-sent. The probability of correctly decoding with this code is at least 0.9792, the probability that the error caused a shift of at most one.

As before, a pair of syndrome and information carrying systems can be identified as being used by the decoding procedure. It suffices to correctly identify the syndromes:

$$\begin{aligned} 0 &\leftrightarrow -\mathfrak{1} \cdot \mathfrak{o} \\ 1 &\leftrightarrow \mathfrak{o} \cdot \mathfrak{o} \\ 2 &\leftrightarrow \mathfrak{1} \cdot \mathfrak{o} \\ 3 &\leftrightarrow -\mathfrak{1} \cdot \mathfrak{1} \\ 4 &\leftrightarrow \mathfrak{o} \cdot \mathfrak{1} \\ 5 &\leftrightarrow \mathfrak{1} \cdot \mathfrak{1} \end{aligned} \tag{7}$$

Resetting the syndrome system to $\mathfrak{o}$ restarts the error-correction process by putting the information in the code. A subsequent s_1 or s_{-1} error affects only the syndrome system. A new feature of this subsystem identification is that it is incomplete: Only a subset of the state space is identified. In this case, the complement can be used for error detection.

2 Principles of Noise Control

In developing an application of noise control, the first task is to establish the properties of the available physical systems. Thus it is necessary to learn:

1. The physical system to be used.
2. The available means for controlling this system.
3. The type of information to be processed.
4. The nature of the noise to be controlled.

With this information the approach used to construct the three examples of the previous section involves the following:

1. Determine a code, that is a subspace of the physical system that can represent the information to be processed.
2. Identify a pair of syndrome and information carrying subsystem for part of the state space such that the code corresponds to a "base" state of the syndrome system, and the primary sources of noise act only on the syndrome. The rest of the state space can be used for error detection.
3. Analyze the error behavior of the code and subsystem.

The task of identifying a combination of a good code and subsystems (or decoding) are interrelated. Answers to the following questions are at the foundation of the theory of error-correction: What properties does a code have to satisfy so that it can be used to protect well against a given error process? How does one obtain the decoding or subsystem identification that achieves this protection? In many cases, the answers can be based on choosing a fixed set of error operators that well represents the most likely errors, and then determining whether these error operators can be protected against without any loss of information. The answers in this case can be cast in terms of the idea of "detected" errors. This idea works equally well for classical and quantum information. We introduce it using classical information concepts.

2.1 Error Detection

Error detection was used in the cyclic system example to reject a state that could not be properly decoded. Noise control methods based on error detection alone work as follows: The encoded information is transmitted. The receiver checks whether the state is still in the code, that is, whether it could have been obtained by encoding. If not, the result is rejected. The sender can be informed of the failure so that the information can be retransmitted. Given a set of error operators that need to be protected against, the scheme is successful if for each error operator, either the information is unchanged, or the error is detected. Thus we can say that an operator E is "detectable" by a code if for each state x in the code, either $Ex = x$ or Ex is not in the code. See Fig. 3

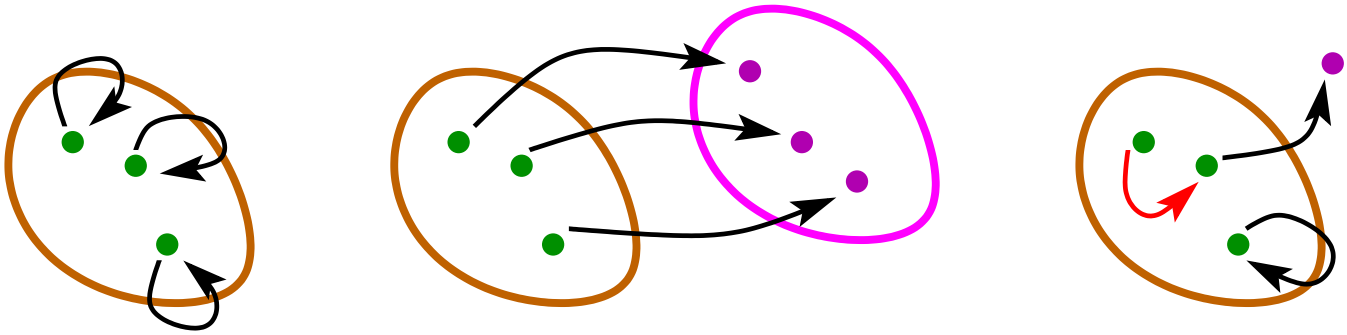


FIG. 3: Pictorial representation of typical detectable and undetectable errors for a code. The code is represented by the brown oval containing three green code words. The error operator is shown as arrows. The left two are typical detectable operators. The right one is not detectable, and the red arrow is the problem effect.

An equivalent condition for detectability, which has a natural generalization to the case of quantum information, is that for all $x \neq y$ in the code, $Ex \neq y$.

The code in the first example consists of $00, 10$. Every operator that affects only the second bit is therefore detectable. This includes all the operators in the noise model. In the second example, the code consists of $000, 111$. The identity operator has no effect and is therefore detectable. Any single or double bit flip is detectable, since the states in the code are changed to states outside the code. The error that flips all bits is not detectable, since it preserves the code but changes the states in the code. In the cyclic example, shifts by $-2, -1, 0, 1, 2$ are detectable but not shifts by 3.

2.2 From Error Detection to Error Correction

Given a code C and a set of error operators $\mathcal{E} = \{\mathbb{1} = E_0, E_1, E_2, \ldots\}$ is it possible to determine whether a decoding procedure or subsystem exists such that errors in $\mathcal{E}$ do not affect the encoded information? As explained below, the answer is yes and the solution is to check that for all $x \neq y$ in the code and all i, j, it is true that $E_i x \neq E_j y$. If this condition holds, we say that $\mathcal{E}$ is correctable by C. Observe that the notion of correctability requires a set of errors and, unlike detectability, cannot be applied to individual errors.

To see that the condition for correctability is necessary, suppose that for some $x \neq y$ in the code and i, j, we have $z = E_i x = E_j y$. If, after an unknown error in $\mathcal{E}$ happened, the state z is obtained, then it is not possible to determine whether the original codeword was x or y, because we cannot tell whether E_i or E_j occurred.

To see that the condition is sufficient, we assume it and construct a decoding method. Suppose that the state z is obtained. There can be one and only one x in the code for which some $E_{i(z)} \in \mathcal{E}$ satisfies that $E_{i(z)} x = z$. Thus x must be the original code word and we can write $x = x(z)$. Note that it is possible for two errors to have the same effect on some code words. A subsystem identification for this decoding is given by $z \leftrightarrow i(z) \cdot x(z)$, where the syndrome system consists of error operator indices, and the information carrying system consists of the code words. It is instructive to check that this subsystem construction, when applied to the examples, does give a version of the error-correcting subsystems given earlier. The subsystem identification constructed is not necessarily onto the state space of the subsystem pair. That is, for different x, the set of $i(z)$ such that $x(z) = x$ can vary and need not be all of the error indices. As we will show, this situation does not arise in the case of quantum information.

To relate the condition for correctability of an error set to detectability of errors, assume that each E_i is invertible. (This is satisfied by our examples, but not by noise operators like "reset bit two to 0".) In this case, the correctability condition is equivalent to the statement that all products $E_j^{-1} E_i$ are detectable. To see the equivalence, first suppose that some $E_j^{-1} E_i$ is not detectable. Then there are $x \neq y$ in the code such that $E_j^{-1} E_i x = y$. Consequently $E_i x = E_j y$ and the error set is not correctable. This argument can be reversed to show that correctability of $\mathcal{E}$ is equivalent to detectability of all $E_j^{-1} E_i$.

If the assumption that the errors are invertible does not hold, the relationship between detectability and correctability becomes more complicated, requiring a generalization of the inverse operation. This is

easier to do in the quantum setting.

3 Quantum Error Correction

The principles of noise control apply to the quantum setting as readily as they apply to the classical setting. The main difference is that the physical system to be used has to behave quantum mechanically and the type of information to be processed is quantum. The question of how classical information can be protected using quantum physical systems is also interesting but will not be discussed here. We illustrate the principles by considering quantum versions of the three examples of Sect. 1 and then add a uniquely quantum example with potentially practical applications in (for example) quantum dot technologies. For an explanation of the basic quantum information concepts and conventions, see [16].

3.1 Trivial Two-Qubit Example

A quantum version of the two bit example from the previous section consists of two physical qubits, where the noise randomly applies the identity or one of the Pauli operators to the second qubit. The Pauli operators are defined by

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{8}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{9}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{10}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{11}$$

Explicitly, the noise has the effect

$$|\psi\rangle_{12} \rightarrow \begin{cases} \mathbb{1}|\psi\rangle_{12} & \text{Prob. } .25 \\ {\sigma_x}^{(2)}|\psi\rangle_{12} & \text{Prob. } .25 \\ {\sigma_y}^{(2)}|\psi\rangle_{12} & \text{Prob. } .25 \\ {\sigma_z}^{(2)}|\psi\rangle_{12} & \text{Prob. } .25 \end{cases} \tag{12}$$

This is called "completely depolarizing" noise on qubit 2. Obviously a one-qubit state can be stored in the first physical qubit without being affected by the noise. An encoding operation that implements this observation is

$$|\psi\rangle \rightarrow |\psi\rangle_1 |0\rangle_2, \tag{13}$$

which realizes an ideal qubit as a two-dimensional subspace of the physical qubits. This subspace is the "quantum code" for this encoding. To decode one can discard physical qubit 2 and return qubit 1, which is considered to be a natural subsystem of the physical system. In this case, the identification of a syndrome and information carrying subsystem pair is the obvious one.

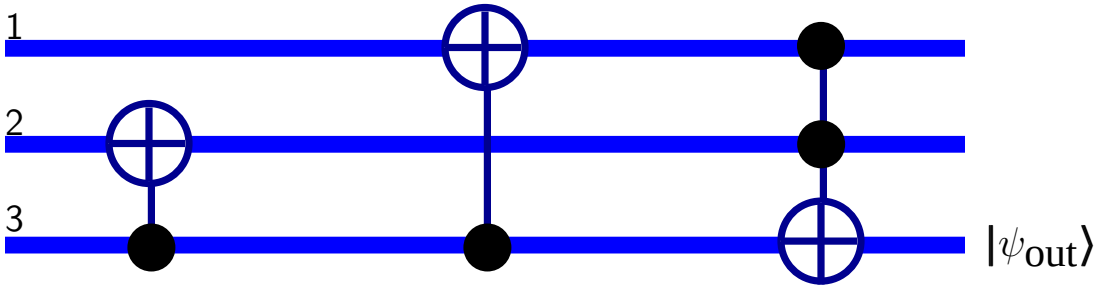
3.2 Quantum Repetition Code

The repetition code can be used to protect quantum information in the presence of a restricted noise model. Let the physical system consist of three qubits. Noise acts by applying independently, to each qubit, the flip operator σ_x with probability $.25$. The classical code can be made into a quantum code by using the superposition principle. Encoding one qubit is accomplished by

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle. \tag{14}$$

The associated quantum code is the two-dimensional subspace spanned by the encoded states.

As in the classical case, decoding is accomplished by majority logic. However, it must be implemented carefully to avoid destroying quantum coherence in the stored information. One way to do that is to use only unitary operations to transfer the stored information to the output qubit. A quantum network that does this is shown in Fig. 4.



$\|000\rangle$	$\|000\rangle$	$\|000\rangle$	$\|00\rangle\|0\rangle$
$\|001\rangle$	$\|011\rangle$	$\|111\rangle$	$\|11\rangle\|0\rangle$
$\|010\rangle$	$\|010\rangle$	$\|010\rangle$	$\|01\rangle\|0\rangle$
$\|100\rangle$	$\|100\rangle$	$\|100\rangle$	$\|10\rangle\|0\rangle$
$\|111\rangle$	$\|101\rangle$	$\|001\rangle$	$\|00\rangle\|1\rangle$
$\|110\rangle$	$\|110\rangle$	$\|110\rangle$	$\|11\rangle\|1\rangle$
$\|101\rangle$	$\|111\rangle$	$\|011\rangle$	$\|01\rangle\|1\rangle$
$\|011\rangle$	$\|001\rangle$	$\|101\rangle$	$\|10\rangle\|1\rangle$

FIG. 4: Quantum network for majority logic decoding into the output qubit 3. The effect of the network on the basis states is shown, with the top half showing the states with majority 0. The decoded qubit is separated in the last step. The quantum network conventions are as explained in [16].

As shown, the decoding network establishes an identification between the three physical qubits and a pair of systems consisting of the information carrying qubit and the two complementary, syndrome qubits. On the left-hand side of the correspondence, the information carrying qubit is not identifiable with any one (or two) of the physical qubits. Nevertheless it exists there via the identification.

A network for encoding is obtained by reversing the decoding network and initializing qubits $2, 3$ in $|00\rangle$. This makes the Toffoli gate unnecessary. The complete system with a typical error is shown in Fig. 5.

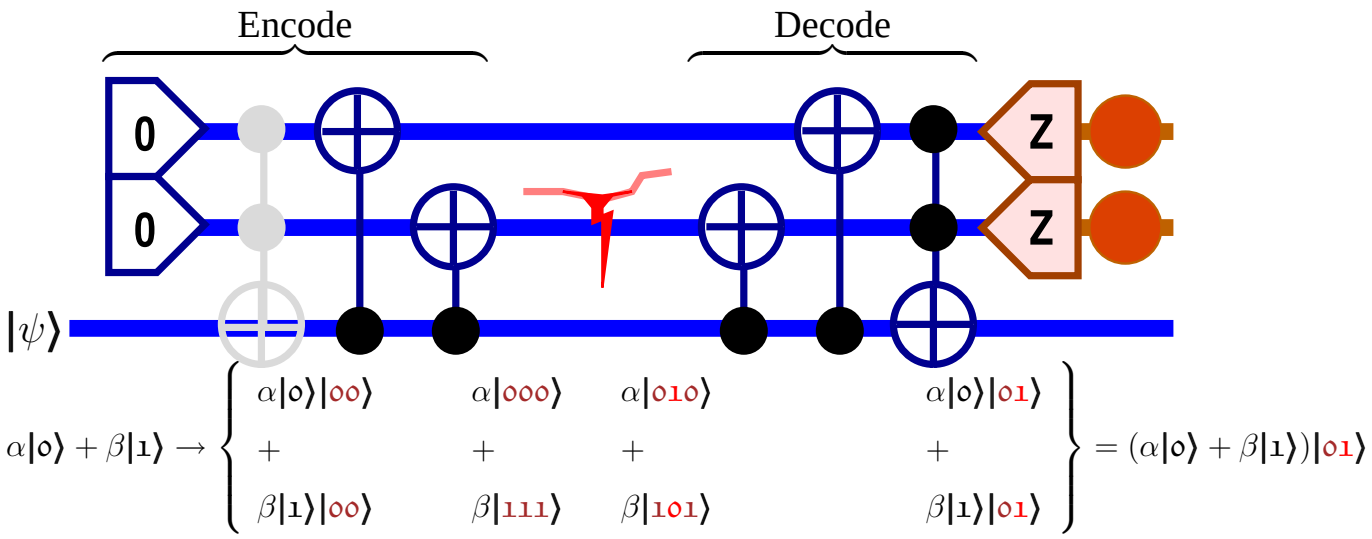


FIG. 5: Network for the repetition code system. The effect for a particular error is shown. Which error occurred can be determined from the state of the syndrome qubits (top two) at the end. This state is called the (error) syndrome. The encoding is shown as the reverse of the decoding with a prepared syndrome system. The encoding Toffoli gate has no effect in this case and can be omitted.

As in the classical case, the identification of a syndrome and information carrying subsystem is a crucial property of the error-correcting system. If the noise is happening repeatedly, we can in principle protect against it without explicitly decoding and then re-encoding, which would cause a temporary loss of protection. Instead one can find a means for directly resetting the syndrome subsystem to $|00\rangle$ (thus returning the information to the code) before the noise happens again. From this point of view, the correctable noise has no effect on the encoded information because it acts only on the syndrome subsystem—given that the latter is initially in the state $|00\rangle$. This preparation and resetting procedure is what ensures that information remains protected.

Part of the task of designing error-correcting systems is to determine how well the system performs. An important performance measure is the probability of error. In quantum systems, this is intuitively interpreted as the maximum probability with which we can see a result different from the expected one in any measurement. Specifically, to determine the error, one compares the output $|\psi_o\rangle$ of the system to the input $|\psi\rangle$. An upper bound is obtained by writing the output as a combination of the input state and an "error" state. For quantum information, combinations are linear combinations (i.e. superpositions). Thus

$|\psi_o\rangle = \gamma|\psi\rangle + |e\rangle$ (see Fig. 6).The probability of error is bounded by $\epsilon = ||e\rangle|^2$ (the "error estimate"). In general, there are many different ways of writing the output as a combination of an acceptable state and an error term. One attempts to choose the combination that minimizes the error estimate. This choice yields the number ϵ, for which $1 - \epsilon$ is called the "fidelity". A fidelity of 1 means that the output is the same (up to a phase factor) as the input.

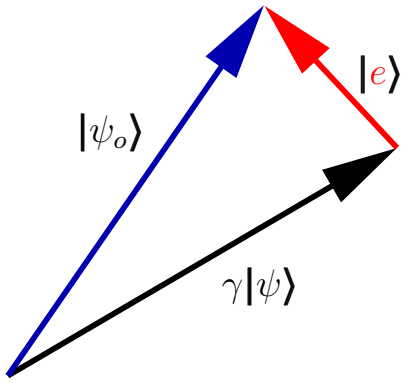


FIG. 6: Representation of an error estimate. Any decomposition of the output state $|\psi_o\rangle$ into a "good" state $\gamma|\psi\rangle$ and an (unnormalized) error term $|e\rangle$ gives an estimate $\epsilon = ||e\rangle|^2$. For pure states, the optimum estimate is obtained when the error term is orthogonal to the input state. For mixtures, one can use any representation of the state as a probabilistic combination of pure states and calculate the probabilistic sum of the pure state errors to obtain an error estimate.

To illustrate error analysis, we calculate the error for the repetition code example with the initial states $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

$$|0\rangle \xrightarrow{\text{encode}} |000\rangle \tag{15}$$

$$\longrightarrow \begin{cases} .75^3: & |000\rangle, \\ .25 * .75^2: & |100\rangle, \\ .25 * .75^2: & |010\rangle, \\ .25 * .75^2: & |001\rangle, \\ .25^2 * .75: & |110\rangle, \\ .25^2 * .75: & |101\rangle, \\ .25^2 * .75: & |011\rangle, \\ .25^3: & |111\rangle \end{cases} \tag{16}$$

$$\xrightarrow{\text{decode}} \begin{cases} .4219: & |00\rangle \cdot |0\rangle, \\ .1406: & |10\rangle \cdot |0\rangle, \\ .1406: & |01\rangle \cdot |0\rangle, \\ .1406: & |11\rangle \cdot |0\rangle, \\ .0469: & |11\rangle \cdot |1\rangle, \\ .0469: & |01\rangle \cdot |1\rangle, \\ .0469: & |10\rangle \cdot |1\rangle, \\ .0156: & |00\rangle \cdot |1\rangle \end{cases} \tag{17}$$

The final state is a mixture consisting of four correctly decoded components and four incorrectly decoded ones. The latter's information is orthogonal to the encoded information, and its probability amplitude is 0.1563, a significant improvement over 0.25. The second state behaves quite differently:

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{\text{encode}} \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{18}$$

$$\longrightarrow \begin{cases} \vdots & \\ .25^2 * .75: & \frac{1}{\sqrt{2}}\left(|110\rangle + |001\rangle\right), \\ \vdots & \end{cases} \tag{19}$$

$$\xrightarrow{\text{decode}} \begin{cases} \vdots & \\ .0469: & \frac{1}{\sqrt{2}}|11\rangle \cdot \left(|1\rangle + |0\rangle\right), \\ \vdots & \end{cases} \tag{20}$$

Not all error events have been shown, but in each case it can be seen that the state is decoded correctly, so the error is 0. This shows that the error probability can depend significantly on the initial state. To remove this dependence and give a state independent error quantity, one can use either the "average" or the "entanglement" error. See Sect. 4.2.

3.3 Quantum Code for a Cyclic System

The shift operators introduced earlier act as permutations of the seven states of the cyclic system. They can therefore be extended to unitary operators on a seven-state cyclic quantum system with logical basis $|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle$. The error model introduced earlier makes sense here without modification

as does the encoding. The decoding or subsystem identification now takes the six-dimensional subspace spanned by $|0\rangle, \ldots |5\rangle$ to a pair consisting of a three-state system with basis $|-1\rangle, |0\rangle, |1\rangle$ and a qubit. The identification of Eq. 7 extends linearly to a unitary subsystem identification. The procedure for decoding is modified by first making a measurement to determine whether the state is in the six-dimensional subspace or not. If it is, the identification is used to extract the qubit. Here is an outline of what happens in using this code for the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{\text{encode}} \frac{1}{\sqrt{2}}(|1\rangle + |4\rangle) \tag{21}$$

$$\longrightarrow \begin{cases} \vdots & \\ .05641e^{-4}: & \frac{1}{\sqrt{2}}(|3\rangle + |6\rangle), \\ \vdots & \end{cases} \tag{22}$$

$$\xrightarrow{\text{detect}} \begin{cases} & \vdots \\ .001: & \begin{cases} .5: & \text{fail} \\ .5: & |3\rangle \end{cases} \vdots \end{cases} \tag{23}$$

$$\xrightarrow{\text{decode}} \begin{cases} \vdots & \\ .0005: & \text{fail} \\ .0005: & |-1\rangle \cdot |1\rangle \\ \vdots & \end{cases} \tag{24}$$

$$= \begin{cases} \vdots & \\ .0005: & \text{fail} \\ .0005: & |-1\rangle \cdot \left(\frac{1}{2}(|0\rangle + |1\rangle) + \frac{1}{2}(-|0\rangle + |1\rangle)\right) \\ \vdots & \end{cases} \tag{25}$$

A "good" state was separated from the output in the case that is shown. The leftover error term has probability amplitude $.0005 * ((1/2)^2 + (1/2)^2) = .00025$, which contributes to the total error (not shown).

3.4 Three Quantum Spin-Half Particles

Quantum physics provides a rich source of systems with many and often not obvious opportunities for representing and protecting quantum information. Sometimes it is possible to encode information in such

a way that it is protected from noise indefinitely, without having to reset the syndrome subsystem. The prototypical example where the idea of subsystems leads to a means for encoding a qubit without error, is that consisting of three spin-half particles that experience identical random fluctuations in a "magnetic" field. A spin-half particle's state space is spanned by two states $|\uparrow\rangle$ and $|\downarrow\rangle$. Intuitively, these states correspond to the spin pointing up or down in some (fixed) reference frame. A magnetic field pointing in some direction causes a spin to precess around the axis defined by the field. In terms of the quantum spin-half particle, the effect of a field with strength given by the 3-vector $\vec{u} = (u_x, u_y, u_z)$ is to apply the Hamiltonian

$$\vec{u} \cdot \vec{\sigma} = u_x \sigma_x + u_y \sigma_y + u_z \sigma_z, \tag{26}$$

where we made the identifications $|\uparrow\rangle \leftrightarrow |0\rangle$ and $|\downarrow\rangle \leftrightarrow |1\rangle$ in choosing the basis for the Pauli matrices. In the Bloch-sphere representation [16, 17], this Hamiltonian causes a rotation around the axis defined by $\vec{u}$.

Consider three spin-half particles with noise consisting of randomly applied identical rotations on the three particles due to a field fluctuating randomly in direction and strength. This type of noise is called "collective", because it does not distinguish between the particles. As we are interested in protecting one qubit of quantum information indefinitely without intervention, the exact probability distribution does not matter. The noise Hamiltonian is of the form $\vec{u} \cdot (\vec{\sigma}^{(1)} + \vec{\sigma}^{(2)} + \vec{\sigma}^{(3)})$ with $\vec{u}$ random in time. Physicists familiar with the rules for spin addition recognize that the state space of the three spin-half particles can be viewed as consisting of a four-dimensional subspace behaving like a spin-$3/2$ particle, and two orthogonal subspaces behaving like a spin-half particle. With subsystems in mind, one can recognize the last two subspaces as being associated with two states of a complementary two-state particle. Thus, the subspace orthogonal to the spin-$3/2$ state space can be thought of as a pair of subsystems, of which the first behaves like a spin-half particle with respect to the magnetic field, and the second is untouched by the magnetic field. This is where we place the quantum information. Fig. 7 shows one way to visualize the partitioning of the state space into the spin-$3/2$ and the spin-half subspaces.

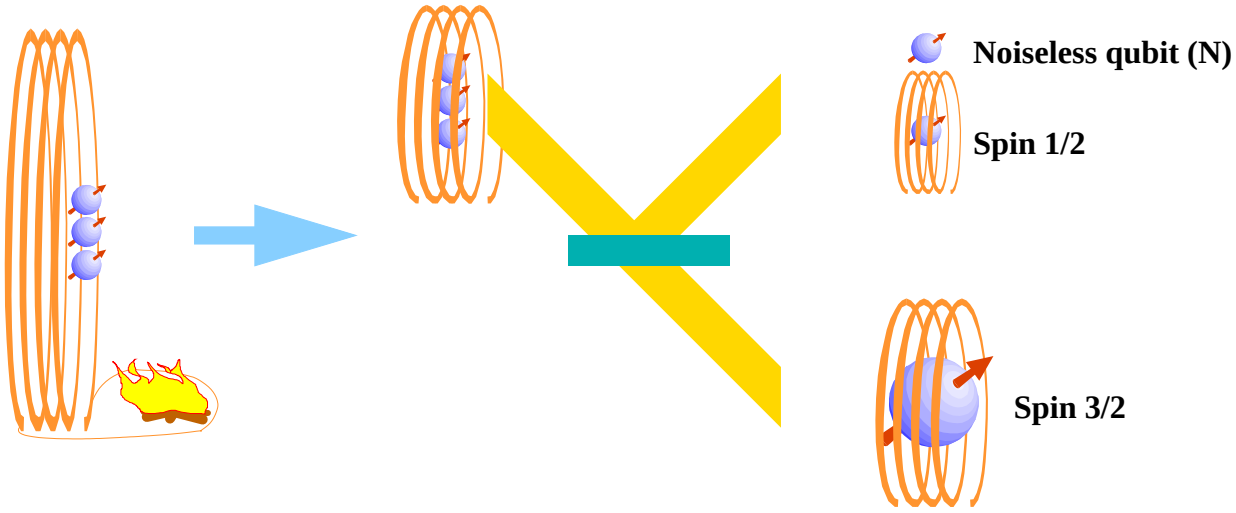


FIG. 7: One noiseless qubit from three spin-half particles The state space of three spin-half particles splits into a spin $3/2$ subspace and a spin $1/2$ subspace. The splitting can be visualized by a beam splitter or Stern-Gerlach experiment separating by total spin. The spin $1/2$ subspace is, with respect to the collective noise, equivalent to two particles, a spin-half particle experiencing the noise and a noise-less qubit.

An explicit identification of the subsystem pair is given by

$$\begin{aligned}
(|\downarrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle 3 + e^{-i2\pi/3}|\uparrow\rangle_1|\downarrow\rangle_2|\uparrow\rangle_3 + e^{i2\pi/3}|\uparrow\rangle_1|\uparrow\rangle_2|\downarrow\rangle_3)/\sqrt{3} &\leftrightarrow |\uparrow\rangle \cdot |0\rangle \\
(|\downarrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle 3 + e^{i2\pi/3}|\uparrow\rangle_1|\downarrow\rangle_2|\uparrow\rangle_3 + e^{-i2\pi/3}|\uparrow\rangle_1|\uparrow\rangle_2|\downarrow\rangle_3)/\sqrt{3} &\leftrightarrow |\uparrow\rangle \cdot |1\rangle \\
(|\uparrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle 3 + e^{-i2\pi/3}|\downarrow\rangle_1|\uparrow\rangle_2|\downarrow\rangle_3 + e^{i2\pi/3}|\downarrow\rangle_1|\downarrow\rangle_2|\uparrow\rangle_3)/\sqrt{3} &\leftrightarrow |\downarrow\rangle \cdot |0\rangle \\
(|\uparrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle 3 + e^{i2\pi/3}|\downarrow\rangle_1|\uparrow\rangle_2|\downarrow\rangle_3 + e^{-i2\pi/3}|\downarrow\rangle_1|\downarrow\rangle_2|\uparrow\rangle_3)/\sqrt{3} &\leftrightarrow |\downarrow\rangle \cdot |1\rangle
\end{aligned} \tag{27}$$

That ${\sigma_z}^{(1)} + {\sigma_z}^{(2)} + {\sigma_z}^{(3)}$ only affects the syndrome (spin-half) system is readily seen. It can be checked that the other sums of Pauli operators that can occur in the noise also affect only the syndrome system. This is why the information carrying subsystem is called “noise-less” for this situation.

The case of the three spin-half particles with collective noise is another example of error-correcting (in this case noise-less) subsystems where part of the state space serves only for error-detection. In this case, the noise cannot remove amplitude from the subspace, so if we detect error, we know that the noise model was inadequate, or we introduced errors in manipulating the state of the whole system.

4 Error Models

We have seen several models of physical systems and errors in the examples of the previous sections. Most physical systems under consideration for QIP consist of particles (or degrees of freedom) that are spatially localized, and this is reflected in the error models that are usually investigated. Because we also expect the physically realized qubits to be localized, the standard error models deal with quantum errors that act more or less independently on different qubits. Logically realized qubits, like those implemented by means of error-correcting subsystems, may have more complicated residual error behavior.

4.1 The Standard Error Models for Qubits

The standard physical systems for QIP are represented by a collection of qubits. The simplest error model for one qubit that is symmetric under qubit rotations is "independent depolarizing errors". This error model has the effect of depolarizing each qubit independently with probability p (see Eq. 12). It is considered to be the quantum analogue of the classical independent bit flip error model.

The assumption of depolarizing noise is not obviously physically reasonable. Examples abound where one or another type of noise dominates. However, given the ability to control individual qubits and independence of the noise affecting different qubits, it is possible to enforce the depolarizing error model (see below). As a result, error-control methods for depolarizing noise apply to all independent noise models. However, it is worth remembering that given detailed knowledge of the noise, a special purpose error-control method can be better than one designed for depolarizing noise.

There are several different ways of thinking about a given noise process affecting a qubit. For most situations of interest (in particular if the initial state of the system is pure), such processes can be thought of as the effect of coupling to an initially independent environment for some time. Because of this, the noise map can always be represented by

$$|\psi\rangle_S \rightarrow U^{(ES)}|0\rangle_E|\psi\rangle_S, \tag{28}$$

where $U^{(ES)}$ is a unitary operator acting jointly on the system and the environment E. Choosing an arbitrary

orthonormal basis for the environment, this can be rewritten in the form:

$$|\psi\rangle_{\mathsf{S}} \rightarrow \sum_e |e\rangle_{\mathsf{E}} \left({}^{\mathsf{E}}\langle e|U^{(\mathsf{ES})}|0\rangle_{\mathsf{E}}\right)|\psi\rangle_{\mathsf{S}} \tag{29}$$

$$= \sum_e |e\rangle_{\mathsf{E}} A_e{}^{(\mathsf{S})}|\psi\rangle_{\mathsf{S}}, \tag{30}$$

where the last step defines $A_e{}^{(\mathsf{S})} = {}^{\mathsf{E}}\langle e|U^{(\mathsf{ES})}|0\rangle_{\mathsf{E}}$. The expression $\sum_e |e\rangle_{\mathsf{E}} A_e{}^{(\mathsf{S})}$ is called an "environment labeled operator sum". The unitarity condition implies that $\sum_e A_e^\dagger A_e = \mathbb{1}$ (with system labels omitted). The basis $|e\rangle$ in the above representation of the noise need not represent any physically meaningful choice of basis of a real environment. (Exception: If the environment is physically accessible, one may measure it to extract information helpful in recovering $|\psi\rangle_{\mathsf{S}}$.) For purposes of noise analysis, the $|e\rangle$ are formal states that "label" the noise operators A_e. One can use the expression even when the $|e\rangle$ are not normalized or orthogonal, provided one makes the appropriate changes in the unitarity condition, should it be needed.

Note that the state after the noise acted is correlated with the environment. This means that after removing ("tracing out over") the environment, the state of the qubit is usually mixed. Instead of introducing an artificial environment, the noise can also be given using the density operator formalism for mixed states. In this case, defining $\rho = |\psi\rangle_{\mathsf{S}}{}^{\mathsf{S}}\langle\psi|$, the effect is given by

$$\rho \rightarrow \sum_e A_e \rho A_e^\dagger. \tag{31}$$

This is the "operator sum" formalism for general quantum operations [18].

Here is how to actively convert an arbitrary noise model into one that consists of randomly applying Pauli operators according to some distribution. Before the noise acts, apply a random Pauli operator σ_u ($u = 0, x, y, z$, $\sigma_0 = \mathbb{1}$). After the noise acts apply its inverse, $\sigma_u^\dagger = \sigma_u$, then "forget" which operator was applied. Using environment labeling, the sequence of actions can be written as follows:

$$|\psi\rangle \rightarrow \frac{1}{2}\sum_u |u\rangle_{\mathsf{C}} \sigma_u |\psi\rangle \tag{32}$$

$$\rightarrow \sum_e |e\rangle_{\mathsf{E}} \frac{1}{2}\sum_u |u\rangle_{\mathsf{C}} A_e \sigma_u |\psi\rangle \tag{33}$$

$$\rightarrow \sum_e |e\rangle_{\mathsf{E}} \frac{1}{2}\sum_u |u\rangle_{\mathsf{C}} \sigma_u^\dagger A_e \sigma_u |\psi\rangle, \tag{34}$$

where C is the system carrying the memory of which Pauli matrix was applied, and system S labels have been omitted. Using the operator sum formalism, the last expression becomes:

$$\rho \to \sum_e \sum_u \frac{1}{4} \left(\sigma_u^\dagger A_e \sigma_u\right) \rho \left(\sigma_u^\dagger A_e^\dagger \sigma_u\right). \tag{35}$$

The expression simplifies by writing $A_e = \sum_u \alpha_{ue}\sigma_u$, using the fact that the Pauli operators are a linear basis for the space of operators. Using the fact that σ_u anticommutes with σ_v if $0 \neq u \neq v \neq 0$, one can see that

$$\frac{1}{4}\sum_u \left(\sigma_u^\dagger A_e \sigma_u\right) \rho \left(\sigma_u^\dagger A_e^\dagger \sigma_u\right) = \sum_v |\alpha_{ve}|^2 \sigma_v \rho \sigma_v^\dagger. \tag{36}$$

As a result, the noise can now be thought of as acting with σ_v with probability $p_v = \sum_e |\alpha_{ve}|^2$. To convert the noise model to a standard depolarizing one, one can strengthen the above procedure by applying a random member of the group generated by the 90° rotations around the x, y and z axes (the "normalizer" of the Pauli group).

The above arguments explain why the depolarizing error model is so useful in the case where noise acts independently on different qubits. However, in most physical situations, the independence assumptions are not satisfied. For example, errors from common internal couplings between qubits are generally pairwise correlated (to first order). In addition, the operations required to manipulate the qubits and to control the encoded information act on pairs at a time, which tends to spread even single qubit noise. Still, in all these cases, the primary noise processes are local. This means that there usually exists an environment labeled sum expression for the error process in which the amplitudes associated with errors acting simultaneously on k qubits decrease exponentially with k. For example, this is the case for errors induced by a global field as in the example of the three spin-half particles in Sec. 3.4. In such cases, error-control methods that handle all or most errors involving sufficiently few qubits are still applicable.

4.2 Quantum Noise Analysis

One of the most important consequences of the subsystems interpretation of quantum information in a physical system is that quantum information can be error-free even though noise has severely changed the physical system. Almost trivially, any noise operator acting only on the syndrome subsystems has no effect on the quantum information. The goal of error control is to actively intervene and maintain the syndrome

subsystem in states where the dominant noise operators continue to have little effect on the information of interest. As discussed in Sec. 7, scalability tends to require that the intervention can "dump" noisy (or "hot") systems and replace them by prepared (or "cold") ones, thus acting a bit like a refrigerator's heat pump. An important issue in analyzing such a system is to estimate the probability of error that does affect the quantum information of interest. A simple example of how that can be done was discussed for the quantum repetition code. The same ideas can be applied in general. For example, given an error expansion for the final state of the form $\sum_e |e\rangle_{\mathsf{E}} A_e{}^{(\mathsf{S})} |\psi\rangle_{\mathsf{S}}$, we can consider the set of "good" e's those for which $A_e{}^{(\mathsf{S})}$ acts only on the syndrome subsystem. The remaining e's form the set of "bad" ones, $\mathcal{B}$. The error probability can then be estimated from above by

$$p_e \leq \left| \sum_{e \in \mathcal{B}} |e\rangle_{\mathsf{E}} A_e{}^{(\mathsf{S})} |\psi\rangle_{\mathsf{S}} \right|^2 \tag{37}$$

$$\leq \left(\sum_{e \in \mathcal{B}} ||e\rangle_{\mathsf{E}}|| A_e{}^{(\mathsf{S})}|_1 \right)^2 , \tag{38}$$

where $|A|_1 = \max_\phi \langle\phi|A|\phi\rangle$ (maximum over unit states). The second inequality usually leads to a gross overestimate but often suffices for obtaining good results for scalable systems. Since the error-expansion is not unique, a goal of the representation of the noise acting on the system is to use "good" operators to the largest extent possible. The flexibility of these error-expansions makes them very useful for analyzing noise models in conjunction with error-control methods. Exact expressions for p_e can be obtained in principle by calculating the density matrix ρ of the state of the subsystem containing the desired quantum information by "tracing out" over the syndrome subsystems. The matrix ρ can then be compared to the intended state. If the intended state is pure, given by $|\phi\rangle$, the probability of error is given by $1 - \langle\phi|\rho|\phi\rangle$.

For communication protocols, the goal is to be able to reliably transmit information through a noisy channel. In this case, we are interested in the relationships between the output and the input states. There are several ways in which one can quantify the error of the complete process from input to ouput state. One way is to identify the overall error with the average error over all possible input states in the code (uniform distribution). An elegant way appropriate for quantum information processing is to use the "entanglement fidelity" [19]. Entanglement fidelity measures the error when the input is maximally entangled with an identical "reference" system. In this process, the reference system is imagined to be untouched, so that the

state of the reference system together with the output state can be compared to the original entangled state. For a one-qubit code, the reference system is a qubit labeled R. An initial, maximally entangled state is

$$|B\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_R |0\rangle_S + |1\rangle_R |1\rangle_S \right). \tag{39}$$

Qubit S is transmitted using an error-correcting subsystem and then recovered at the end. The reference qubit is assumed to be perfectly isolated and not affected by any noise. The final state $\rho^{(RS)}$ is compared to $|B\rangle$, with the entanglement fidelity given by $f_e = \langle B|\rho^{(RS)}|B\rangle$. The entanglement error is $\epsilon_e = 1 - f_e$. It turns out that this definition does not depend on the choice of maximally entangled state. Happily, the entanglement error and the average error ϵ_a are related by a linear expression:

$$\epsilon_a = \frac{2}{3}\epsilon_e. \tag{40}$$

For k-qubit codes, the constant $\frac{2}{3}$ is replaced by $2^k/(2^k+1)$. Experimental measurements of these fidelities does not require the reference system. There are simple averaging formulas to express them in terms of the fidelities for transmitting each of a sufficiently expressive set of pure states. An example of the experimental determination of the entanglement fidelity is in [20].

5 From Quantum Error Detection to Error Correction

In the independent depolarizing noise model with error probability $p \ll 2/3$, the most likely errors are those which affect a small number of qubits. That is, if we define the "weight" of a product of Pauli operators to be the number of qubits affected, the dominant errors are those of small weight. As a result, good error-correcting codes are considered to be those for which all (or a set of most) errors of weight $< d$ can be corrected. It is desirable that d have high "rate", which means that it is a large fraction of the total number of qubits, n (the "length" of the code). Combinatorially, good codes are characterized by having high minimum distance, a concept that can be defined using ideas of error-detection.

5.1 Quantum Error Detection

Let C be a quantum code, that is a subspace of the state space of a quantum system. Let P be the operator that projects onto C, and $P^\perp = \mathbb{1} - P$ the projector onto the orthogonal complement. Then the pair $P, P^\perp$

is associated with an ideal projective measurement to determine whether a state is in the code or not. If the given state is $|\psi\rangle$, then the result of the measurement is $P|\psi\rangle$ with probability $|P|\psi\rangle|^2$ and $P^\perp|\psi\rangle$ otherwise. As in the classical case, an error-detection scheme consists of preparing the desired logical state $|\psi_i\rangle \in C$, transmitting it through a quantum channel (say), then measuring whether the state is still in the code and rejecting the state if it is not. We therefore say that C detects error operator E if for every state $|\psi_i\rangle \in C$, $PE|\psi_i\rangle = \lambda_E|\psi_i\rangle$. That is, if the state is accepted after E acted, then it has not changed except for an overall scale. The condition given is equivalent to

$$PEP = \lambda_E P \tag{41}$$

and also, for all $|\psi\rangle, |\phi\rangle \in C$,

$$\langle\psi|E|\phi\rangle = \lambda_E\langle\psi|\phi\rangle. \tag{42}$$

A third equivalent condition is obtained by taking the second definition of classical detectability and replacing $\neq$ by "orthogonal to": For all $|\phi\rangle, |\psi\rangle$ in the code with $|\phi\rangle$ orthogonal to $|\psi\rangle$, $E|\phi\rangle$ is orthogonal to $|\psi\rangle$.

For a given code C, the set of detectable errors is closed under linear combinations. That is, if E_1 and E_2 are both detectable, then so is $\alpha E_1 + \alpha E_2$. This useful property implies that to check detectability, one only has to consider the elements of a linear basis for the space of errors of interest.

Consider n qubits with depolarizing errors. For an error-detecting code to be robust, it is necessary to detect as many of the small weight errors as possible. This motivates the definition of "minimum distance": The code C has minimum distance d if the smallest weight product of Pauli operators E for which C does not detect E is d. The notion comes from classical codes for bits, where a set of code words C' has minimum distance d if the smallest number of flips required to change one code word in C' into another one in C' is d. For example, the repetition code for three bits has minimum distance 3. Note that the minimum distance for the quantum repetition code is one: Applying ${\sigma_z}^{(1)}$ preserves the code and changes the sign of $|1_L\rangle$ but not of $|0_L\rangle$. The notion of minimum distance can be generalized for noise models with specified "first order" noise operators [21]. In the case of depolarizing noise, the first order noise operators are single qubit Pauli matrices, which are the errors of weight one.

5.2 Quantum Error Correction

Let $\mathcal{E}$ be the set of errors that we wish to be able to correct. When can the code C be enhanced with a decoding procedure so that all errors in $\mathcal{E}$ are corrected? As will be explained, the necessary and sufficient condition is that errors in the set $\mathcal{E}^\dagger\mathcal{E} = \{E_1^\dagger E_2 : E_i \in \mathcal{E}\}$ are detectable. Using the conditions for detectability and writing $\mathcal{E} = \{E_0 = \mathbb{1}, E_1, \ldots\}$, this is equivalent to

$$PE_i^\dagger E_j P = \lambda_{ij} P \tag{43}$$

The condition is preserved under a linear change of basis for $\mathcal{E}$. That is, if A is any invertible matrix with coefficients a_{ij}, we can define new error operators $D_k = \sum_i E_i a_{ik}$. For the D_k, the left-hand side of Eq. 43 is

$$\begin{aligned} PD_k^\dagger D_l P &= P\left(\sum_{ij} \bar{a}_{ik} E_i^\dagger E_j a_{jl}\right) P \\ &= \sum_{ij} \bar{a}_{ik} a_{jl} \lambda_{ij} P \\ &= \left(A^\dagger \Lambda A\right)_{kl} P, \end{aligned} \tag{44}$$

where Λ is the matrix formed from the λ_{ij}. Using the fact that Λ is a positive semidefinite matrix (i.e. for all x, $x^\dagger \Lambda x \geq 0$ and $\Lambda^\dagger = \Lambda$), we can choose A such that $A^\dagger \Lambda A$ is of the form $\begin{pmatrix} \mathbb{1} & 0 \\ 0 & 0 \end{pmatrix}$. An important consequence of this (or of the linearity of quantum mechanical operations), is that the set of errors correctable by a particular code and decoding procedure is linearly closed. Thus, if E and D are corrected by the procedure, then so is $\alpha E + \beta D$.

Before explaining the condition for correctability, we consider the situation of n qubits, where it leads to a useful relationship between minimum distance and correctability of low weight errors: If a code on n qubits has minimum distance at least $2e + 1$, then the set of errors of weight at most e is correctable. This follows by observing that the weight of $E_1^\dagger E_2$ is at most the sum of the weights of the E_i. As a result of this observation, the problem of finding good ways of correcting all errors up to a maximum weight reduces to that of constructing codes with sufficiently high minimum distance. Thus questions like "what is the maximum dimension of a code of minimum distance d on n qubits?" are of great interest. As in the case of classical coding theory this problem appears to be very difficult in general. Answers are known for

small n [6] and there are asymptotic bounds [22]. Of course, for achieving low error probabilities, it is not necessary to correct all errors of weight $\leq e$, just almost all such errors. For example, the concatenated codes used for fault tolerant quantum computation achieve this goal (see Sec. 7).

We explain the necessary and sufficient condition for correctability of an error set by using the subsystems interpretation of the decoding procedure. For simplicity, assume that $\mathbb{1} \in \mathcal{E}$. First suppose that we have a decoding procedure that recovers the encoded information after any of the errors in $\mathcal{E}$ happened. Every physically realizable decoding procedure can be implemented by first adding "ancilla" quantum systems to form a total system labeled t, then performing a unitary map U resulting in a pair of systems s, q, where s corresponds to the syndrome system, and q is a quantum system with the same dimension as the code that carries the quantum information of interest after decoding. Denote the state space of the physical system containing C as $\mathcal{H}$, and the state spaces of system x by $\mathcal{H}_{\mathsf{x}}$. We have the relationships:

$$\mathcal{H}_{\mathsf{q}} \overset{V}{\leftrightarrow} C \subseteq \mathcal{H} \subseteq \mathcal{H}_{\mathsf{t}} \overset{U}{\leftrightarrow} \mathcal{H}_{\mathsf{s}} \otimes \mathcal{H}_{\mathsf{q}}, \tag{45}$$

where V is the unitary operator that encodes from $\mathcal{H}_{\mathsf{q}}$. For states we write $|\psi\rangle = |\psi\rangle_{\mathsf{q}} \overset{V}{\leftrightarrow} |\psi\rangle_{\mathsf{L}} \in C$. Because $\mathbb{1}$ is a correctable error, it must be the case that $|\psi\rangle_{\mathsf{L}} \overset{U}{\leftrightarrow} |0\rangle_{\mathsf{s}}|\psi\rangle$ for some $|0\rangle_{\mathsf{s}}$. To see this, use linearity of the maps. In general:

$$\begin{aligned} |\psi\rangle_{\mathsf{L}} &\rightarrow E_i|\psi\rangle_{\mathsf{L}} \\ &\overset{V}{\leftrightarrow} |i\rangle_{\mathsf{s}}|\psi\rangle \end{aligned} \tag{46}$$

The $|i\rangle_{\mathsf{s}}$ need not be normalized or orthogonal. Let S be the subspace spanned by the $|i\rangle_{\mathsf{s}}$. Then U induces an identification of $S \otimes \mathcal{H}_q$ with a subspace $\bar{C} \subseteq \mathcal{H}$. This is the desired subsystem identification. We can see how the errors act in this identification:

$$\begin{array}{ccc} |\psi\rangle_{\mathsf{L}} & \leftrightarrow & |0\rangle_{\mathsf{s}}|\psi\rangle \\ \downarrow & & \\ E_i|\psi\rangle_{\mathsf{L}} & \leftrightarrow & |i\rangle_{\mathsf{s}}|\psi\rangle \end{array} \tag{47}$$

This means that for all $|\psi\rangle, |\phi\rangle$,

$${}_{\mathsf{L}}\langle\psi|E_j^\dagger E_i|\phi\rangle_{\mathsf{L}} = {}_{\mathsf{s}}\langle j|i\rangle_{\mathsf{s}}\langle\psi|\phi\rangle, \tag{48}$$

that is, all errors in $\mathcal{E}^\dagger\mathcal{E}$ are detectable.

Now suppose that all errors in $\mathcal{E}^\dagger\mathcal{E}$ are detectable and choose a basis for the errors so that $\lambda_{ij} = \delta_{ij}\lambda_i$ with $\lambda_i = 1$ for $i < s$ and $\lambda_i = 0$ otherwise. Define a subsystem identification by

$$|i\rangle_{\mathsf{s}}|\psi\rangle \xrightarrow{U} E_i|\psi\rangle_{\mathsf{L}}, \tag{49}$$

for $0 \leq i < s$. By assumption and construction, ${}_{\mathsf{L}}\langle\psi|E_j^\dagger E_i|\psi\rangle_{\mathsf{L}} = \delta_{ij}$. This implies that U is unitary (after linear extension), so this is a proper identification. For $i \geq s$, $E_i|\psi\rangle_{\mathsf{L}} = 0$, which implies that for states in the code, these errors have probability 0. Therefore the identification can be used to successfully protect against $\mathcal{E}$. Note that the range of U need not be all of $\mathcal{H}$.

6 Stabilizer Codes

Most useful quantum codes are based on "stabilizer" constructions [4, 5]. A stabilizer code of length n for k qubits (abbreviated as an "$[[n, k]]$ code"), is a 2^k-dimensional subspace of the state space of n qubits that is characterized by the set of products of Pauli operators that leave each state in the code invariant. A simple example of a stabilizer code is the quantum repetition code introduced in Sec. 3.2. The code states $\alpha|000\rangle + \beta|111\rangle$ are exactly the states that are unchanged after applying ${\sigma_z}^{(1)}{\sigma_z}^{(2)}$ and ${\sigma_z}^{(1)}{\sigma_z}^{(3)}$.

To simplify the notation, we write $I = \mathbb{1}, X = \sigma_x, Y = \sigma_y, Z = \sigma_z$. A product of Pauli operators can then be written as $ZIXI = {\sigma_z}^{(1)}{\sigma_x}^{(3)}$ (as an example of length 4) with the ordering determining which qubit is being acted on by the operators in the product.

Stabilizer codes are nice because it is easy to determine which Pauli-product errors are detectable and because there is a way of interpreting them as special types of classical "linear" codes. The latter makes it possible to use well-established techniques from the theory of classical error-correcting codes to construct good quantum codes. The crucial properties can be seen by working out the quantum repetition code example using the stabilizer formalism. A stabilizer of the code is $S = \{ZZI, ZIZ\}$. Let $\bar{S}$ be the set of Pauli products that are expressible (up to a phase) as products of elements of S. Thus $\bar{S} = \{III, ZZI, ZIZ, IZZ\}$. $\bar{S}$ consists of all Pauli products that stabilize the code. The crucial property of S is that its operators commute, that is, for $A, B \in S$, $AB = BA$. According to results from linear algebra, this implies that the state space $\mathcal{H}$ can be decomposed into orthogonal subspaces $\mathcal{H}_\lambda$ such that for $A \in S$, $|\psi\rangle \in \mathcal{H}_\lambda$, $A|\psi\rangle = \lambda(A)|\psi\rangle$. The $\mathcal{H}_\lambda$ are the common eigenspaces of S. The stabilizer

code associated with S is the subspace $\mathcal{H}_\lambda$ with $\lambda(A) = 1$. The subspaces for other $\lambda(A)$ have equivalent properties and are often included in the set of stabilizer codes. For the repetition code, this subspace is spanned by the logical basis $|000\rangle$ and $|111\rangle$. From the point of view of stabilizers, there are two ways in which a Pauli product B can be detectable. The first is if $B \in \bar{S}$, since in this case B acts as the identity on the code. The other is if B anticommutes with (at least) one member (say A) of S. To see this, let $|\psi\rangle$ be in the code. Then $A\,(B|\psi\rangle) = (AB)\,|\psi\rangle = -\,(BA)\,|\psi\rangle = -B\,(A|\psi\rangle) = -B|\psi\rangle$. Thus $B|\psi\rangle$ belongs to $\mathcal{H}_\lambda$ with $\lambda(A) = -1$. Since this subspace is orthogonal to the code, B is detectable. We define the set of Pauli products that commute with all members of S as $\bar{S}^\perp$. Thus, B is detectable if either $B \notin \bar{S}^\perp$ or $B \in \bar{S}$. Note that $\bar{S} \subseteq \bar{S}^\perp$.

To construct a stabilizer code that can correct all errors of weight at most one (a "quantum one-error-correcting code"), it suffices to find S with the minimum weight of non-identity members of $\bar{S}^\perp$ being at least three. In this case we say that $\bar{S}^\perp$ has minimum distance three. As an example, we can exhibit a stabilizer for the famous length-five one-error-correcting code for one qubit [23, 24]:

$$S = \{XZZXI, IXZZX, XIXZZ, ZXIXZ\}. \tag{50}$$

As a general rule, it is desirable to exhibit the stabilizer minimally, which means that no member is the product of some of the other members. In this case, the number of qubits encoded is $n - |S|$, where n is the lenght of the code.

The correspondence between stabilizer codes and classical binary codes is obtained by replacing the symbols I, X, Y, Z in a Pauli product by $00, 01, 10, 11$, respectively. Thus, the members of the stabilizer can be thought of as binary vectors of length $2n$. We use arithmetic modulo two for sums, inner products and application of a binary matrix. Because the numbers modulo two ($\mathbb{Z}_2$) form a mathematical "field", the basic properties of vectors spaces and linear algebra apply to binary vectors and matrices. Thus, the stabilizer is minimal in the sense introduced above if the corresponding binary vectors are independent over $\mathbb{Z}_2$. Given two binary (column) vectors x, y of length two associated with Pauli products, the property of anticommuting is equivalent to $x^T B y = 1$, where B is the block diagonal $2n \times 2n$ matrix with 2×2 blocks given by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This means that $\bar{S}^\perp$ can be identified with the set of vectors x such that $x^T B y = 0$ for all binary vectors y associated with the members of S. It turns out that the inner product

$< x, y >= x^T By$ arises in the study of codes over the four-element mathematical field $GF(4)$, which can be represented by the vectors $00, 01, 10, 11$ with addition modulo 2 and a new multiplication operation. This relationship led to the construction of many good stabilizer codes [6].

7 Fault Tolerant Quantum Communication and Computation

One of the most important results of the work in quantum error-correction is the accuracy threshold theorem.

Theorem 1 *Assume the requirements for scalable quantum information processing (see below). If the error per gate (including "no-op") is less than a threshold, then it is possible to efficiently quantum compute arbitrarily accurately.*

7.1 Requirements for Scalable QIP

The value of the threshold accuracy (or error) depends strongly on which set of requirements is used, in particular, the error model that is assumed. The requirements are closely related to the basic requirements for constructing a quantum information processor [25] but have to include explicit assumptions on the noise model and on the temporal and spatial aspects of the available quantum control.

Scalable physical systems: Access to physical systems able to support qubits or other basic units of quantum information. The system must be scalable by adding more systems supporting additional, independent qubits. That is, the state spaces of the qubits must grow as required by the definition of qubits.

State preparation: The ability to prepare any qubit in the standard initial state $|0\rangle$. Any preexisiting content is assumed to be lost, as would happen if, for example the qubit is first discarded and then replaced by a prepared one. The condition can be weakened: It is sufficient that a large fraction of the qubits can be prepared in this way.

Measurement: The ability to measure any qubit in the logical basis. Again, it is sufficient to have have a sufficiently large fraction of the qubits be measurable. For solving computational problems with deterministic answers, the standard projective measurement can be replaced by noisy, weak measurement [27].

Quantum control: The ability to implement a universal set of unitary quantum gates acting on a small number (usually at most two at a time) qubits. For most accuracy thresholds, it is necessary to be able to apply the quantum control in parallel to any number of disjoint pairs of qubits. This parallelism requirement can be weakened if a nearly noise-less quantum memory is available. The requirement that two-qubit gates can be applied to any pair of qubits is unrealistic given the constraints of three-dimensional space. Work on how to deal with this problem is ongoing [11]. The universality assumption can be substantially weakened by replacing some or all unitary quantum gates with the ability to prepare special states or by having additional measurement capabilities. See, for example [28] and the references therein.

Noise: Error per gate and "no-op" must be below a threshold and satisfy independence and locality properties (see Sec. 4). For the most pessimistic such error models, the error threshold is above $\sim 10^{-6}$. For the independent depolarizing noise model, it is believed to be better than 10^{-4} [29]. There are some special error models where the threshold is substantially higher. For example, in the independent "erasure" error-model, where error events are always detected, the threshold is above $.01$, and for an error model where each error is an unintentional measurement in the standard basis of a qubit, the threshold is above $.5$ [30]. Another case where the threshold is well above $.01$ is if the goal is only to transmit it through noisy quantum channels [31].

7.2 Realizing Fault-Tolerance

The accuracy threshold theorems have been proven by giving explicit instructions for building a scalable quantum information processor and analyzing its robustness against the assumed error model. There are now well established, if not optimal, ways of obtaining scalability. They are based on the following techniques: 1. Concatenation of good, relatively short error-correcting codes. Concatenation means recursively encoding qubits several times. 2. Instructions for implementing operations directly on encoded, information carrying subsystems while minimizing the spread of errors in the operations themselves. 3. Ways in which to "correct" errors that have occurred. This ensures that an error event at any one location and time is with high probability soon shunted to discarded qubits. Again, it is necessary to ensure that the needed operations do not themselves cause errors to spread excessively. 4. Robust state preparation and measurement.

The techniques for realizing scalable computation are based on the following simple idea. Suppose that the error rate per operation for some way of realizing qubits is p. We can use these qubits and a quantum error-correcting code to encode logical qubits for which the storage error rate is reduced. For example, if a one-error correcting code is used, the error rate per storage interval for the logical qubits is expected to be $\leq cp^2$ for some constant c. Suppose that we can show how to implement encoded operations, preparations, measurement and error-correction methods such that this inequality is now valid for each basic encoded step, perhaps for a larger constant C. Suppose furthermore that the errors for the encoded information still satisfy the assumed noise model. The newly defined logical qubits then have an error rate of $\leq Cp^2$, which is less than p for $p < 1/C$. We can use the newly realized qubits as a foundation for making further logical qubits. This results in multiple levels of encoding. In the next level (level 2), the error rate is $\leq C^3p^4$, and after k iterations it is $\leq C^{2^k-1}p^{2^k}$, a doubly exponentially decreasing function of k. This procedure is called "concatenation" (Fig. 8). Since the complexity, in particular the number of physical qubits needed for each final logical qubit, grows at most exponentially in h, the procedure is considered efficient. In practice, this simple idea is still dauntingly complex, but there is hope that for realistic errors in physical systems and by cleverly trading off different variations of these techniques, much of the theoretical complexity can be avoided [32].

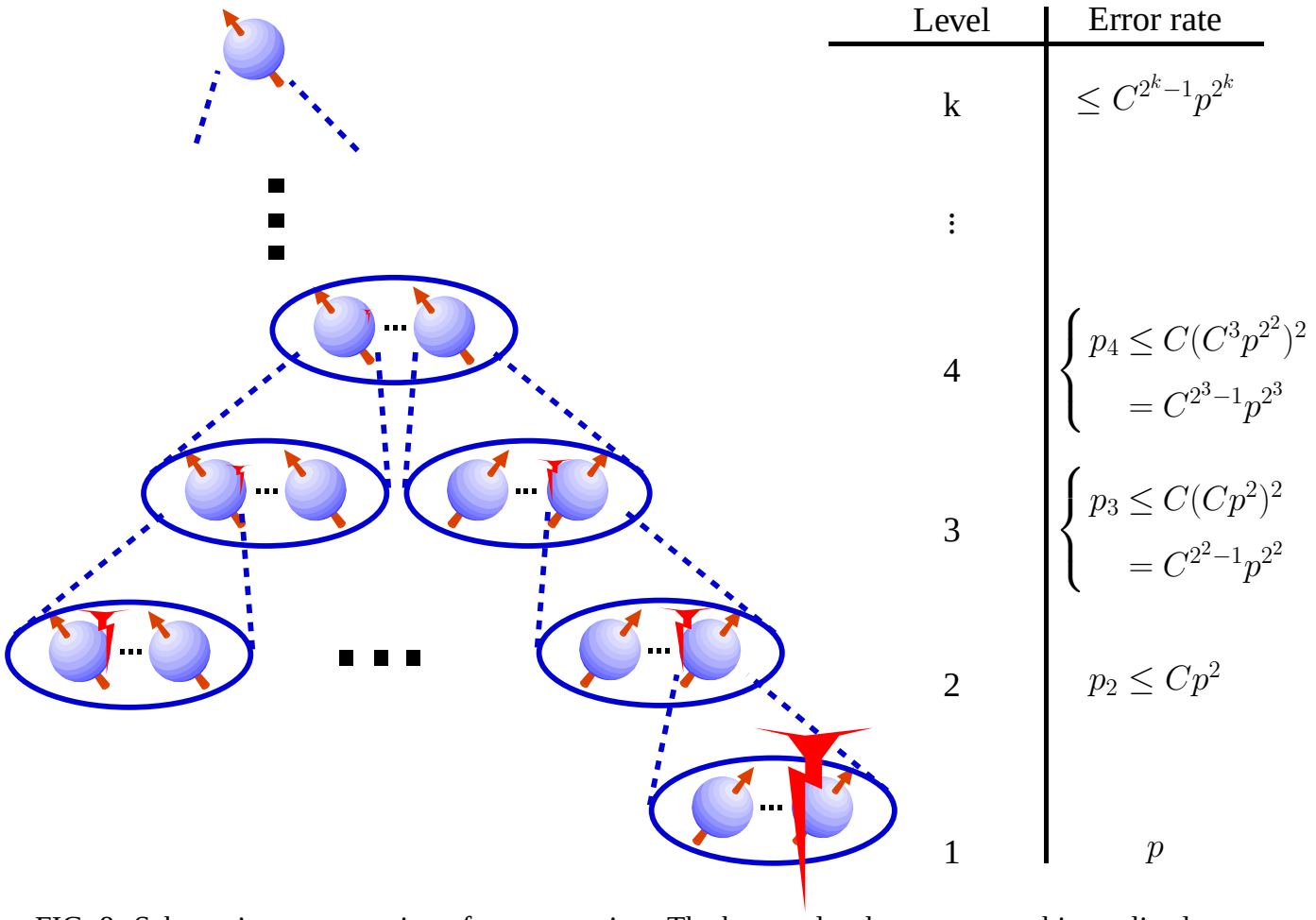


FIG. 8: Schematic representation of concatenation. The bottom level represents qubits realized more-or-less directly in a physical system. Each next level represents logical qubits defined by means of error-correcting subsystems in terms of the previous level's qubits. More efficient subsystems might represent multiple qubits in one code block rather than the one qubit per code block shown here.

Many important developments and ideas of quantum information were ultimately needed to realize encoded operations, preparations, measurements and error-correction techniques that behave well with respect to concatenation. Stabilizer codes provide a particularly nice setting for implementing many of these techniques. One reason is that good stabilizer codes are readily constructed. Another is that they enable encoding operations in a way that avoids spreading errors between qubits of a single codeword [14]. In addition, there are many tricks based on teleportation that can be used to maintain the syndrome systems in acceptably low-error states and to implement general operations systematically [33]. To learn more about all of these techniques, see the textbook by Nielsen and Chuang [34] and the works of Gottesman [14] and

Preskill [15].

8 Concluding Remarks

The advancements in quantum error-correction and fault-tolerant quantum information processing have shown that in principle scalable quantum computation is achievable. This is a crucial result that suggests that experimental efforts for quantum information processing will eventually lead to more than a few small scale applications of quantum information to communication and problems with few qubits. However, the general techniques for achieving scalability that are known are difficult to realize. Existing technologies are far from achieving sufficient accuracy for just two qubits, at least in terms of the demands of the usual accuracy threshold theorems. There is hope that more optimistic thresholds can be shown to apply by taking into consideration the specific constraints of a physical device, better understanding the dominant sources of errors, and exploiting tailor-made ways of embedding quantum information into subsystems. Current work in this area is focused on finding such methods of quantum noise control. These methods include approaches to noise control not covered in this introduction, for example, techniques for actively turning off the error-inducing environmental interactions [35, 36] and modifications to controlling quantum systems that eliminate systematic and calibration errors [37, 38]. Further work is also needed to improve the thresholds for the more pessimistic error models and for developing more efficient schemes for achieving scalability.

Addresses:

E. Knill:	Los Alamos National Laboratory,	knill@lanl.gov
R. Laflamme:	University of Waterloo and Perimeter Institute,	laflamme@iqc.ca
A. Ashikhmin:	Lucent,	aea@research.bell-labs.c
H. Barnum:	Los Alamos National Laboratory,	barnum@lanl.gov
L. Viola:	Los Alamos National Laboratory,	lviola@lanl.gov
W. Zurek:	Los Alamos National Laboratory,	whz@lanl.gov

References

[1] Special focus issue: Experimental proposals for quantum computation. *Fort. Phys.*, 48:767–1138, 2000.

[2] A. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. Lond. A*, 452:2551–2577, 1996.

[3] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:2493–2496, 1995.

[4] D. Gottesman. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. A*, 78:405–408, 1997.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over gf(4). *IEEE Trans. Inf. Theory*, 44:1369–1387, 1998.

[7] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Symposium on the Foundations of Computer Science (FOCS)*, pages 56–65, Los Alamitos, California, 1996. IEEE press.

[8] A. Yu. Kitaev. Quantum error correction with imperfect gates. In O. Hirota et al., editor, *Quantum Communication and Computing and Measurement*, New York, 1997. Plenum.

[9] E. Knill and R. Laflamme. Concatenated quantum codes. Technical Report LAUR-96-2808, Los Alamos National Laboratory, `knill@lanl.gov`, 1996. quant-ph/9608012.

[10] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)*, pages 176–188, New York, New York, 1996. ACM Press.

[11] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. quant-ph/9906129, 1999.

[12] E. Knill, R. Laflamme, and W. Zurek. Resilient quantum computation: Error models and thresholds. *Proc. R. Soc. Lond. A*, 454:365–384, 1998.

[13] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279:342–345, 1998.

[14] D. Gottesman. A theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127–137, 1998.

[15] J. Preskill. Reliable quantum computers. *Proc. R. Soc. Lond. A*, 454:385–410, 1998.

[16] E. Knill and R. Laflamme. Introduction to quantum information processing. Technical Report LAUR-01-4761, Los Alamos National Laboratory, 2001. To appear in LA Science.

[17] R. Laflamme, E. Knill, D. Cory, C. Negrevergne, S. Sinha, and R. Martinez. Introduction to NMR quantum information processing. Technical Report LAUR-02-6132, Los Alamos National Laboratory, 2001. To appear in LA Science.

[18] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Lecture Notes in Physics, Vol. 190. Springer-Verlag, Berlin, 1983.

[19] B. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54:2614–2628, 1996.

[20] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne. Implementation of the five qubit error correction benchmark. *Phys. Rev. Lett.*, 86:5811–5814, 2001.

[21] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.

[22] A. Ashikhmin and S. Litsyn. Upper bounds on the size of quantum codes. *IEEE Trans. Inf. Theory*, 45:1206–1216, 1999.

[23] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error-correcting codes. *Phys. Rev. A*, 54:3824–3851, 1996.

[24] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek. Perfect quantum error-correcting code. *Phys. Rev. Lett.*, 77:198, 1996.

[25] D.P. DiVincenzo. The physical implementation of quantum computation. *Fort. Phys.*, 48:771–783, 2000.

[26] L. Viola, E. Knill, and R. Laflamme. Constructing qubits in physical systems. *J. Phys. A*, 34(LAUR-00-5877):7067–7080, 2001.

[27] E. Knill. A note on linear optics gates by post-selection. Technical Report LAUR-01-5973, Los Alamos National Laboratory, 2001. quant-ph/0110144.

[28] M. A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the $|0\rangle$ state. quant-ph/0108020, 2001.

[29] D. Gottesman and J. Preskill. Unpublished analysis of the accuracy threshold., 1999.

[30] E. Knill, R. Laflamme, and G. Milburn. Thresholds for linear optics quantum computation. Technical Report LAUR-00-3477, Los Alamos National Laboratory, 2000. quant-ph/0006120.

[31] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters for communication. quant-ph/9803056, 1998.

[32] A. Steane. Efficient fault-tolerant quantum computing. *Nature*, 399:124–126, 1999.

[33] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390–393, 1999.

[34] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2001.

[35] L. Viola and S. Lloyd. Dynamical suppression of decoherence in two-state quantum systems. *Phys. Rev. A*, 58:2733–2744, 1998.

[36] L. Viola, E. Knill, and S. Lloyd. Dynamical decoupling of open quantum systems. *Phys. Rev. Lett.*, 82:2417–2421, 1999.

[37] M. H. Levitt. Symmetrical composite pulse sequences for NMR population-inversion 1. compensation for radiofrequency field inhomogeneity. *J. Mag. Res.*, 48:234–264, 1982.

[38] H. K. Cummins and J. A. Jones. Use of composite rotations to correct systematic errors in NMR quantum computation. quant-ph/9911072, 1999.