Constructing qubits in physical systems

2001 J. Phys. A: Math. Gen. 34 7067

(http://iopscience.iop.org/0305-4470/34/35/331)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 7067–7079 PII: S0305-4470(01)22120-9

Constructing qubits in physical systems

Lorenza Viola, Emanuel Knill and Raymond Laflamme

Los Alamos National Laboratory, MS B265, Los Alamos, NM 87545, USA

E-mail: lviola@lanl.gov, knill@lanl.gov, laflamme@lanl.gov

Received 16 February 2001
Published 24 August 2001
Online at stacks.iop.org/JPhysA/34/7067

Abstract

The notion of a qubit is ubiquitous in quantum information processing. In spite of the simple abstract definition of qubits as two-state quantum systems, identifying qubits in physical systems is often unexpectedly difficult. There is an astonishing variety of ways in which qubits can emerge from devices. What essential features are required for an implementation to properly instantiate a qubit? We give three typical examples and propose an operational characterization of qubits based on quantum observables and subsystems.

PACS numbers: 03.67.-a, 03.67.Lx, 89.70.+c
Mathematics Subject Classification: 81P68, 68Q05, 15A69

1. Introduction

Quantum bits (*qubits*) are the elementary units of information that are used to represent quantum data [1]. Thus, the idea of a qubit underlies all investigations in the rapidly growing science of quantum information—including quantum information theory, quantum communication, quantum computation, quantum complexity, and quantum game theory [2–5]. In particular, qubits are the basic building blocks for defining the standard model of quantum computation as introduced by Deutsch [6], which has so far provided the appropriate representation for identifying and understanding *efficient* ways of processing information using quantum mechanics. Its investigation resulted in feasible algorithms for factoring large integers [7] and for simulating many-particle quantum systems [8], two problems not known to be efficiently solvable with classical computers.

A qubit can be thought of as the extension of a classical bit obtained by applying the superposition principle. When quantum superposition states of many qubits are constructed in the tensor product state space that quantum mechanics prescribes for a composite system, quantum entanglement arises as an additional information resource with no classical counterpart. However, qubits share with classical bits the fundamental property of being a *fungible* information resource [9, 10]: While both classical and quantum information is intended, in fact required, to be physically realized, it is *abstractly* defined and therefore independent of the details of the underlying physical realization.

The fungibility property is essential to quantum information in two respects. First, by defining quantum information independent of the details of specific physical devices and their complex physics, it has been possible to study qubit properties at the abstract level and thus to obtain a deeper understanding of the distinctive features that qubits inherit from their intrinsic quantum-mechanical nature. Examples of fundamental results following from the basic properties of superpositions and of the randomness associated with quantum measurements include the fact that qubits in an unknown quantum state cannot be perfectly copied (no-cloning theorem [11, 12]) and they cannot be broadcast (no-broadcasting theorem [13]). On the other hand they can be reliably communicated by means of the quantum teleportation protocol [14], an extremely useful protocol with many applications [15]. Second, from a practical standpoint, the arbitrariness of the physical realization implied by fungibility allows for greater flexibility in the identification and design of quantum information processors. This is reflected in the amazing variety of representations of qubits that have appeared in recent proposals for physical realizations of quantum computers [16]. While such variety greatly increases the number of physical systems with the potential for quantum information processing, it can be intimidating when considering a new prospective system for implementing qubits. As recently observed by DiVincenzo [17], 'recognizing a qubit can be trickier than one might think'. Thus to determine the suitability of a physical system for quantum information processing we need to answer the following basic questions: What is a qubit, and how do we look for them?

In this paper, we identify essential criteria to be met by a system to contain physical embodiments of qubits. Our primary goal is to develop the intuition needed for 'distilling' qubits from physical systems, in the hope that such intuition will serve as a guide for exploring the full range of possibilities available for physical implementation. We do so by revisiting a few prototypical examples to obtain a general operational characterization of qubits. The examples are examined in detail in section 2. The first example shows how the state space of a collection of bosonic modes can be exploited for representing qubits based on the requirement of obtaining realizable control over the qubit observables. The second and third examples are essentially motivated by reconsidering the notion of what a qubit is in the light of our knowledge from quantum error-correcting methods. In particular, we analyze two situations where a qubit can be embedded into the larger state space of three physical two-state systems in a way which makes it robust against noise to first order in time and to arbitrary orders in time, respectively. As the level of abstraction required for constructing our example qubits grows, the qubit states are less easily related to states of the underlying physical degrees of freedom, and more powerful mathematical tools are required to describe the qubits. The emerging qubit criteria are summarized in section 3. Our analysis points to the crucial role played by *control resources* in determining a preferred qubit realization, and to an operator picture in terms of *quantum observables*, rather than states, as the appropriate framework for capturing the idea of a qubit in full generality.

2. The fungibility of qubits

The first proposals for quantum computers implemented qubits literally by exploiting explicit two-level systems. Examples of qubits in these proposals include the two levels corresponding to absence and presence of a photon in a mode [18], spin-1/2 nuclear spins [19], and the ground and one of the excited states of ions [20]. The proposals have in common the goal of implementing qubits at the fundamental level of a physical system. The recognition of how fragile these qubits' states are led to the development of quantum error correction, which necessarily involves maintaining the information by distributing it in a controlled way over a potentially large number of physical systems. As a result we reconsidered the notion of a qubit.

To illustrate the different facets of such a notion we determine how an entity equivalent to an abstractly defined qubit can be constructed in three prototypical situations. An abstractly defined qubit can be identified with an ideal two-state quantum system Q whose associated state space is a two-dimensional complex Hilbert space $\mathcal{H}_{\mathsf{q}} \simeq \mathbb{C}^2$. An orthonormal basis $\{|0\rangle_{\mathsf{q}}, |1\rangle_{\mathsf{q}}\}$ (computational basis) is fixed in $\mathcal{H}_{\mathsf{q}}$ and we make the identification $|0\rangle_{\mathsf{q}} \simeq (1, 0)$, $|1\rangle_{\mathsf{q}} \simeq (0, 1)$ with vectors in $\mathbb{C}^2$. Operations on states are conveniently expressed in terms of the Pauli operators $\sigma_{\mathsf{x}}, \sigma_{\mathsf{y}}, \sigma_{\mathsf{z}}$, which obey commutation and anti-commutation relationships of the form

$$[\sigma_\alpha, \sigma_\beta] = 2\mathrm{i} \sum_\gamma \varepsilon_{\alpha\beta\gamma} \sigma_\gamma \tag{1}$$

$$\{\sigma_\alpha, \sigma_\beta\} = 2\,\delta_{\alpha\beta}\,\mathbb{1} \tag{2}$$

with $\alpha, \beta, \gamma \in \{\mathsf{x}, \mathsf{y}, \mathsf{z}\}$, and $\varepsilon_{\alpha\beta\gamma}$ and $\mathbb{1}$ being the completely antisymmetric symbol and the identity on $\mathcal{H}_{\mathsf{q}}$, respectively. To simplify notations, we define $X := \sigma_{\mathsf{x}}$, $Y := \sigma_{\mathsf{y}}$, $Z := \sigma_{\mathsf{z}}$.

As we will see, the abstract state space of a qubit is not necessarily directly related to the state space of the physical systems. However, the operators are naturally embedded in the operator algebras associated with the physical observables.

2.1. The bosonic qubit

Bosonic qubits are the basic building blocks in a recent proposal for linear optics quantum computation (LOQC) [21]. The relevant physical system is a collection of $2n$ distinguishable modes which describe the elementary excitations of the quantized electromagnetic field [22]. Each mode is characterized by annihilation and creation operators $\mathbf{a}_k, \mathbf{a}_k^\dagger, k = 1, \ldots, 2n$, which satisfy bosonic commutation rules $[\mathbf{a}_k, \mathbf{a}_{k'}] = [\mathbf{a}_k^\dagger, \mathbf{a}_{k'}^\dagger] = 0$, $[\mathbf{a}_k^\dagger, \mathbf{a}_{k'}] = \delta_{kk'}$. In particular, number states of mode k are defined as eigenstates of the number operator $\mathbf{n}_k = \mathbf{a}_k^\dagger \mathbf{a}_k$ for mode k, $\mathbf{n}_k |n_k\rangle_k = n_k |n_k\rangle_k$. Number states constitute a basis for the state space of a given mode, i.e., $\mathcal{H}_k = \mathrm{span}\{|n_k\rangle_k \mid n_k = 0, 1, 2, \ldots\}$ (Fock representation). Accordingly,

$$\mathcal{S} \simeq \mathcal{H}_1 \otimes \mathcal{H}_2 \cdots \otimes \mathcal{H}_{2n} \tag{3}$$

is the overall state space in which we have to look for qubits. We use the abbreviation $|n_1\rangle_1 \ldots |n_{2n}\rangle_{2n} = |n_1 \ldots n_{2n}\rangle$ for product number states in $\mathcal{S}$.

Clearly, a variety of (inequivalent) prescriptions is conceivable for representing qubits in $\mathcal{S}$. In LOQC, an encoding based on two modes and one boson is adopted via the mapping

$$\begin{aligned} |0\rangle_{\mathsf{q}(k,k')} &\to |0\rangle_k\, |1\rangle_{k'} \\ |1\rangle_{\mathsf{q}(k,k')} &\to |1\rangle_k\, |0\rangle_{k'} \end{aligned} \tag{4}$$

for a qubit supported by modes (k, k'). This choice is motivated by the potential for easy implementations of single-qubit transformations via passive linear optical elements. It is worth pointing out that encodings similar to the above, where the degree of freedom carrying quantum information is identified with the presence of a quasi-particle in one of two modes or sites, or the presence/absence of a quasi-particle in a single mode or site, can make sense for quantum statistics other than the bosonic one. Thus, the present discussion is relevant to situations where information is stored in anyonic [23, 24] or fermionic [25, 26] qubits. A different scheme for embedding a generic finite-dimensional quantum system (or *qudit*) in the state space of bosonic degrees of freedom was recently proposed in [27].

According to (4), the state space of the bosonic qubit, $\mathcal{H}_{\mathsf{q}(k,k')} = \mathrm{span}\{|0\rangle_{\mathsf{q}(k,k')}, |1\rangle_{\mathsf{q}(k,k')}\}$, is identified with the one-excitation sector of the two-mode Hilbert space $\mathcal{H}_{(k,k')} = \mathcal{H}_k \otimes \mathcal{H}_{k'}$.

By letting $n_{k,k'}$ denote the eigenvalue of the joint number operator $\mathbf{n}_{k,k'} = \mathbf{n}_k + \mathbf{n}_{k'}$, one has formally

$$\mathcal{H}_{(k,k')} = \mathcal{H}_k \otimes \mathcal{H}_{k'} \simeq \bigoplus_{n_{k,k'}=0}^{\infty} \mathcal{H}^{(n_{k,k'})} \simeq \mathcal{H}_{\mathsf{q}(k,k')} \oplus \tilde{\mathcal{H}}_k \tag{5}$$

where $\mathcal{H}^{(n_{k,k'})}$ is the subspace of states in $\mathcal{H}_{(k,k')}$ with $n_{k,k'}$ bosons, and $\tilde{\mathcal{H}}_k = \oplus_{\{n_{k,k'}\neq 1\}} \mathcal{H}^{(n_{k,k'})}$. The state space of n bosonic qubits, which is obtained via an effective tensor-product construction of one-qubit spaces, likewise relates to the overall state space $\mathcal{S}$ in a non-trivial way. Assuming a pairing between modes of the form $(k, k') = (k, k+1)$ for the ith encoded qubit, $i = (k+1)/2 = 1, \ldots, n$, we obtain

$$\begin{aligned}(\mathcal{H}_1 \otimes \mathcal{H}_2) \otimes \cdots \otimes (\mathcal{H}_{2n-1} \otimes \mathcal{H}_{2n}) &= \mathcal{H}_{(1,2)} \otimes \mathcal{H}_{(3,4)} \otimes \cdots \otimes \mathcal{H}_{(2n-1,2n)} \\ &\simeq \bigotimes_{k=1,3,\ldots,2n-1} \left[\bigoplus_{n_{k,k+1}=0}^{\infty} \mathcal{H}^{(n_{k,k+1})} \right] \simeq \left[\mathcal{H}_{\mathsf{q}_1} \otimes \mathcal{H}_{\mathsf{q}_2} \cdots \otimes \mathcal{H}_{\mathsf{q}_n}\right] \oplus \tilde{\mathcal{H}}\end{aligned} \tag{6}$$

where for each two-mode state space $\mathcal{H}_{(k,k+1)}$ a decomposition similar to (5) has been used, $\mathcal{H}_{\mathsf{q}_i} = \mathcal{H}_{\mathsf{q}(2i-1,2i)}$, and $\tilde{\mathcal{H}}$ collects all the contributions with excitation different from one in at least one of the pairs of modes.

Several remarks on the above state space structure are in order. In the one-qubit case, the presence of the summand $\tilde{\mathcal{H}}_k$ in (5) causes the bosonic qubit to be effectively embedded into a larger state space where infinitely many 'non-qubit' levels are present. One can formally rewrite this separation so that the additional levels form part of an effective environment [28]. The formal state space of the two resulting interacting subsystems is written as

$$\mathcal{H}_{\mathsf{qe}} = (\mathcal{H}_{\mathsf{q}(k,k')} \oplus |v_{\mathsf{q}}\rangle) \otimes (\tilde{\mathcal{H}}_k \oplus |v_{\mathsf{e}}\rangle) \tag{7}$$

where $|v_{\mathsf{q}}\rangle$ and $|v_{\mathsf{e}}\rangle$ are adjoined 'vacuum' states, and we make the identification $\mathcal{H}_{\mathsf{q}(k,k')} \to \mathcal{H}_{\mathsf{q}(k,k')} \otimes |v_{\mathsf{e}}\rangle$. The idea generalizes to n qubits, in which case the role of the effective 'non-qubit' environment is assumed by $\tilde{\mathcal{H}}$ in (6).

Whenever a non-zero amplitude is found in the space $\tilde{\mathcal{H}}$, one or more qubits have 'leaked-out' from the intended logical space $\mathcal{H}_L = \otimes_i \mathcal{H}_{\mathsf{q}_i}$ so that the state no longer maps to a state of qubits. To guarantee that the state belongs to the qubits for *all* times t means restricting the overall evolution operator $\mathcal{U}(t)$ to the sub-manifold of unitary operators $U(\mathcal{H}_L) \oplus U(\tilde{\mathcal{H}}) \subset U(\mathcal{S})$. It is essential to realize that such a requirement is in general unnecessary as well as overly restrictive. While care should be taken to ensure that no leakage allows the qubits to stray away from the logical space at the beginning and at the end of every quantum gate, one should not insist on retaining a mapping into qubits at every intermediate time. In other words, qubits need only exist *stroboscopically* in time.

In the LOQC proposal, relaxing the constraint of well defined qubit states at intermediate steps is indispensable for achieving the required two-bit conditional dynamics. For example, in [21], the most basic conditional sign-flip gate c-σ_{z} on two bosonic qubits, say $\mathsf{q}_1 = \mathsf{q}(1,2)$ and $\mathsf{q}_2 = \mathsf{q}(3,4)$, is decomposed into a sequence of operations

$$\mathsf{c}\text{-}\sigma_{\mathsf{z}}^{(\mathsf{q}_1,\mathsf{q}_2)} = U_{\mathrm{BS}}^{(1,3)\dagger} U_{\mathrm{NS}_1} U_{\mathrm{NS}_3} U_{\mathrm{BS}}^{(1,3)} \in U\left(\mathcal{H}_{\mathsf{q}_1} \otimes \mathcal{H}_{\mathsf{q}_2}\right) \oplus U(\tilde{\mathcal{H}}) \tag{8}$$

where both the beam-splitter gate $U_{\mathrm{BS}}^{(1,3)}$ and the non-deterministic gate U_{NS_j} on mode $j = 1, 3$ cause a temporary departure from the one-excitation space of each qubit. This implementation is also non-deterministic, meaning that it requires post-selection, with a known success probability. In [21], the non-determinism can be removed by exploiting the quantum teleportation protocol [14, 15].

In spite of the complicated underlying state space structure, a bosonic qubit $\mathsf{q}(k,k')$ can be straightforwardly characterized in terms of its generating observables. On the $2n$-mode state space $\mathcal{S}$, define the operator

$$P_{k,k'} := \frac{1}{2\pi}\int_0^{2\pi} \mathrm{d}\varphi\, \mathrm{e}^{-\mathrm{i}(\mathbf{n}_k+\mathbf{n}_{k'}-1)\varphi} \tag{9}$$

on $\mathcal{H}_{(k,k')}$, and $\mathbb{1}$ elsewhere. $P_{k,k'}$ satisfies $P_{k,k'} = P_{k,k'}^\dagger = P_{k,k'}^2$, and

$$P_{k,k'}|n_1 n_2 \ldots n_{2n}\rangle = \delta_{n_k+n_{k'},1}\,|n_1 n_2 \ldots n_{2n}\rangle. \tag{10}$$

Hence, the restriction $\hat{P}_{k,k'}$ of $P_{k,k'}$ to $\mathcal{H}_{(k,k')}$, $\hat{P}_{k,k'} : \mathcal{H}_{(k,k')} \to \mathcal{H}_{\mathsf{q}(k,k')}$, and the product $\mathcal{P} := P_{1,2}P_{3,4}\ldots P_{2n-1,2n}$, $\mathcal{P} : \mathcal{S} \to \mathcal{H}_{\mathsf{q}_1}\otimes\cdots\otimes\mathcal{H}_{\mathsf{q}_n}$, are the projectors onto the one-qubit and the n-qubit space, respectively. Clearly, the action of $\hat{P}_{k,k'}$ is the identity operation when further restricted to the qubit space, i.e., $\hat{P}_{k,k'} =_{\mathsf{q}} \mathbb{1}_{\mathsf{q}(k,k')}$, where $=_{\mathsf{q}}$ means equality over $\mathcal{H}_{\mathsf{q}(k,k')}$. For fixed k, k', one finds that

$$\hat{P}_{k,k'}(\mathbf{n}_k+\mathbf{n}_{k'})\hat{P}_{k,k'} = \hat{P}_{k,k'}(\mathbf{n}_k+\mathbf{n}_{k'}) = (\mathbf{n}_k+\mathbf{n}_{k'})\hat{P}_{k,k'}. \tag{11}$$

From this one can readily check that the following operators act as encoded generating observables for the bosonic qubit $\mathsf{q}(k,k')$, with $k' = k+1$:

$$\begin{aligned} Z_{\mathsf{q}(k,k')} &= (\mathbf{n}_{k'} - \mathbf{n}_k)\hat{P}_{k,k'} \\ X_{\mathsf{q}(k,k')} &= (\mathbf{a}_k^\dagger \mathbf{a}_{k'} + \mathbf{a}_k \mathbf{a}_{k'}^\dagger)\hat{P}_{k,k'} \end{aligned} \tag{12}$$

and $Y_{\mathsf{q}(k,k')} = [Z_{\mathsf{q}(k,k')}, X_{\mathsf{q}(k,k')}]/2\mathrm{i} = -\mathrm{i}Z_{\mathsf{q}(k,k')}X_{\mathsf{q}(k,k')}$. These observables obey commutation/anti-commutation rules identical to (1) and (2). Evolutions generated by the Hamiltonians given in (12) can be readily constructed from the action of optical phase shifters and beam splitters respectively, which allows for an easy implementation of arbitrary one-qubit ($U(2)$) gates via passive linear optics.

The final ingredients that are required to make the bosonic qubit useful include the ability to initialize the qubit in the intended logical space $\mathcal{H}_{\mathsf{q}(k,k')}$, and the ability to read-out the qubit observables. In LOQC, the state preparation of qubit $\mathsf{q}(k,k')$ can be accomplished by using a single-photon source to prepare mode k in $|0\rangle_k$ and mode k' in $|1\rangle_{k'}$. To measure the bosonic qubit it suffices to use a photo-detector on the mode k, which destructively determines whether one or more photons were present in the mode. Further details are in [21].

2.2. The three-bit encoded qubit

Our second example comes from quantum error correction using stabilizer codes. Consider the simplest possible situation, where we wish to protect one quantum bit against single bit-flip errors by encoding it into three physical qubits. A quantum code can be specified by a two-dimensional subspace of the overall state space $\mathcal{S}$, $\mathcal{C} = \mathrm{span}\{|0_L\rangle, |1_L\rangle\} \subset \mathcal{S}$. To protect against single bit-flip errors, a repetition code $\mathcal{C}$ can be defined by the encoding

$$(c_0|0\rangle + c_1|1\rangle)\otimes|00\rangle \mapsto c_0|0_L\rangle + c_1|1_L\rangle = c_0|000\rangle + c_1|111\rangle. \tag{13}$$

It is easily checked that $\mathcal{C}$ satisfies the necessary and sufficient conditions for error-recovery with respect to the error set $\mathsf{E} = \{E_0 = \mathbb{1}, E_1 = X_1, E_2 = X_2, E_3 = X_3\}$ [3, 29]. Note that $E_a = E_a^\dagger = E_a^{-1}$ for errors in E. Let $\mathcal{V}^i$ denote the subspace spanned by $\mathsf{E}|i_L\rangle$, for $i = 0$, 1, and let us choose as orthonormal bases in the $\mathcal{V}^i$'s the result of applying the errors to the logical states (13), i.e.,

$$\begin{aligned} \mathcal{V}^0 &= \mathrm{span}\{|000\rangle, |100\rangle, |010\rangle, |001\rangle\} = \mathrm{span}\{|v_a^0\rangle\} \\ \mathcal{V}^1 &= \mathrm{span}\{|111\rangle, |011\rangle, |101\rangle, |110\rangle\} = \mathrm{span}\{|v_a^1\rangle\} \end{aligned} \tag{14}$$

with $|v_a^i\rangle = E_a|i_L\rangle$, $i = 0, 1$, $a = 0, \ldots, 3$. Then $\mathcal{S} \simeq \mathcal{V}^0 \oplus \mathcal{V}^1$ and a recovery super-operator can be explicitly constructed by defining, for each error $E_a \in \mathsf{E}$,

$$R_a = E_a \sum_{i=0,1} \left|v_a^i\right\rangle\left\langle v_a^i\right|. \tag{15}$$

The fact that the quantum operation $\mathcal{R} = \{R_a\}$ defined by $\mathcal{R} : \rho \mapsto \sum_a R_a \rho R_a^\dagger$ for density operators ρ actually restores the state of the encoded qubit after an error in E happens is due to the property that every combination $R_a X_b$ is a multiple of the identity operation on $\mathcal{C}$. Thus, the basic idea for using this code is to apply $\mathcal{R}$ after the errors happened. While this procedure successfully protects our bit of quantum information, it is conceptually dissatisfying, because it would appear that *after* the errors happened, but *before* application of $\mathcal{R}$, the information is corrupted by noise. Is there a representation that clearly separates errors and information in such a way that it is clear that the quantum information is never affected? In other words, where does the protected qubit reside both before and after errors occurred?

The basic insight is to regard the error-correcting code as an appropriate *subsystem* [30]. This is possible by establishing the mapping

$$\left|v_a^i\right\rangle \simeq |i\rangle_{\mathsf{q}} \otimes \left|v_a^0\right\rangle_{\mathcal{E}} \tag{16}$$

for the basis vectors of the $\mathcal{V}^i$'s (hence $\mathcal{S}$) introduced before. In the right-hand side of (16), the $|i\rangle_{\mathsf{q}}$ vectors, $i = 0, 1$, are taken as basis states of a two-dimensional complex space that will serve as the protected qubit state space, while the $|v_a^0\rangle_{\mathcal{E}}$ store the bit string that uniquely identifies the error syndrome. Essentially, the state $|v_a^0\rangle_{\mathcal{E}}$ is meant to fully encode the effect of the noise on the code. The correspondence (16) is a prescription for decomposing the physical coding space $\mathcal{S}$ into the tensor product of a qubit space $\mathcal{Q}$ and a syndrome space $\mathcal{E}$:

$$\mathcal{S} \simeq \mathcal{Q} \otimes \mathcal{E} \simeq \mathbb{C}^2 \otimes \mathbb{C}^4. \tag{17}$$

If we choose to represent the syndrome corresponding to E_0 (no error) by $|00\rangle_{\mathcal{E}}$, then clearly $\mathcal{C} \simeq \mathcal{Q} \otimes |00\rangle_{\mathcal{E}}$. In the representation (17), it is straightforward to visualize the errors' effect on the code. For an arbitrary encoded state $|\psi\rangle = c_0|0_L\rangle + c_1|1_L\rangle \in \mathcal{C}$, we find

$$\begin{aligned} E_a|\psi\rangle &= c_0\left|v_a^0\right\rangle + c_1\left|v_a^1\right\rangle \simeq c_0|0\rangle_{\mathsf{q}} \otimes \left|v_a^0\right\rangle_{\mathcal{E}} + c_1|1\rangle_{\mathsf{q}} \otimes \left|v_a^0\right\rangle_{\mathcal{E}} \\ &= [c_0|0\rangle_{\mathsf{q}} + c_1|1\rangle_{\mathsf{q}}] \otimes \left|v_a^0\right\rangle_{\mathcal{E}} = |\psi\rangle_{\mathcal{Q}} \otimes \left|v_a^0\right\rangle_{\mathcal{E}} \end{aligned} \tag{18}$$

where in the last equality the mapping (17) is made explicit. By construction, the vector $|v_a^0\rangle_{\mathcal{E}}$ depends on E_a alone. Thus, information in $\mathcal{Q}$ is completely unaffected by errors in E: the factor $\mathcal{Q}$ in (17) is the qubit subsystem where the protected quantum information resides.

It is worth comparing this picture with the familiar description of the error-correcting code based on the stabilizer formalism [31]. In the stabilizer language, the code $\mathcal{C}$ is characterized by its stabilizer group,

$$\mathsf{S} = \{\mathbb{1}, Z_1Z_2, Z_2Z_3, Z_1Z_3\}. \tag{19}$$

S is generated by $M_1 = Z_1Z_2$ and $M_2 = Z_2Z_3$, and the code $\mathcal{C}$ is a joint eigenspace of the two stabilizer generators. The commutation pattern between each error E_a and the stabilizer generators M_j diagnoses the error syndrome completely. In our case, it simply reads $E_0 \to 00$, $E_1 \to 10$, $E_2 \to 11$, $E_3 \to 01$, where 0, 1 encodes whether the error commutes or anti-commutes with the corresponding generator, respectively.

A basis of the state space of the three qubits can be built from joint eigenvectors of a sufficiently large (maximal) set of commuting operators. Such a set can be obtained by adding to M_1 and M_2 the operator $L = Z_1$ (for example). The corresponding joint eigenvectors may be labeled $|l, m_1, m_2\rangle$, where, for convenience, we denote by l, m_1, m_2 not the ± 1 eigenvalues

of the corresponding operators L, M_1, M_2, but the eigenvalues of the projectors onto the -1 subspace, e.g., the label $l = 0$ ($l = 1$) corresponds to a $+1$ (-1) eigenvalue of the operator L. The code $\mathcal{C}$ is then spanned by the vectors $|0, 0, 0\rangle$ and $|1, 0, 0\rangle$. The quantum number $l \in \{0, 1\}$ can be thought of as labeling a two-state degree of freedom. This also translates into a prescription for decomposing the overall coding space

$$\mathcal{S} \simeq \mathcal{Q}' \otimes \mathcal{E}' \simeq \mathbb{C}^2 \otimes \mathbb{C}^4 \tag{20}$$

via a correspondence of the form

$$|l, m_1, m_2\rangle \simeq |l\,\rangle_{\mathsf{q}'} \otimes |m_1, m_2\rangle_{\mathcal{E}'}. \tag{21}$$

Note that this prescription is not unique, as it depends on the choice of phase of the different eigenvectors. (It can be made unique by considering L and the global flip $X_1X_2X_3$ as generators for the algebra of observables for the degree of freedom carried by q'.) The difference between the representations (21) and (16) accounts for the different views of error-correcting codes that comes from the subsystem idea. The difference can be explicitly appreciated by looking at the correspondences between the states in the two factorizations. We have, for instance,

$$\begin{aligned} \left|v_0^0\right\rangle &= |000\rangle \simeq |0\rangle_{\mathsf{q}} \otimes |00\rangle_{\mathcal{E}} \simeq |0\rangle_{\mathsf{q}'} \otimes |00\rangle_{\mathcal{E}'} \\ \left|v_0^1\right\rangle &= |111\rangle \simeq |1\rangle_{\mathsf{q}} \otimes |00\rangle_{\mathcal{E}} \simeq |1\rangle_{\mathsf{q}'} \otimes |00\rangle_{\mathcal{E}'} \end{aligned} \tag{22}$$

but

$$\begin{aligned} \left|v_1^1\right\rangle &= |011\rangle \simeq |1\rangle_{\mathsf{q}} \otimes |10\rangle_{\mathcal{E}} \simeq |0\rangle_{\mathsf{q}'} \otimes |10\rangle_{\mathcal{E}'} \\ \left|v_1^0\right\rangle &= |100\rangle \simeq |0\rangle_{\mathsf{q}} \otimes |10\rangle_{\mathcal{E}} \simeq |1\rangle_{\mathsf{q}'} \otimes |10\rangle_{\mathcal{E}'} \end{aligned} \tag{23}$$

meaning that the degree of freedom q' has its values flipped by some error combination and is therefore not explicitly protected. Specifically, $E_1[c_0|0_L\rangle + c_1|1_L\rangle] \simeq [|c_0|1\rangle_{\mathsf{q}'} + c_1|0\rangle_{\mathsf{q}'}] \otimes |10\rangle_{\mathcal{E}'}$. The error can be undone by a flip of q' conditional on the state of $\mathcal{E}'$. Thus, while in this picture error detection and error recovery necessarily appear as two separate steps, the earlier factorization (16) makes sure that the need for an explicit error-correction step is removed once information is properly stored: to first order in time, the effect of the noise is only to 'heat' the ancillary degrees of freedom carried by the syndrome subsystem $\mathcal{E}$, and all that is required to recover from errors is to 'reset' the latter subsystem to the state $|00\rangle_{\mathcal{E}}$. This is exactly what the recovery quantum operation $\mathcal{R}$ accomplishes, as is clear by representing every operator R_a in (15) using the mapping (16), i.e.,

$$R_a \simeq \mathbb{1}^{(\mathcal{Q})} \otimes \left|v_0^0\right\rangle\!\left\langle v_a^0\right|^{(\mathcal{E})}. \tag{24}$$

The best method for characterizing the protected qubit living in $\mathcal{Q}$ is in terms of its observables. This is easily done by starting with the obvious observables restricted to the code subspace: $Z_{\mathcal{C}} = |0_L\rangle\langle 0_L| - |1_L\rangle\langle 1_L|$, $X_{\mathcal{C}} = |0_L\rangle\langle 1_L| + |1_L\rangle\langle 0_L|$. The Z and X observables for the subsystem associated with $\mathcal{Q}$ can then be obtained by applying the errors in the following way:

$$\begin{aligned} Z_{\mathsf{q}} &= Z_{\mathcal{C}} + E_1 Z_{\mathcal{C}} E_1 + E_2 Z_{\mathcal{C}} E_2 + E_3 Z_{\mathcal{C}} E_3 \\ X_{\mathsf{q}} &= X_{\mathcal{C}} + E_1 X_{\mathcal{C}} E_1 + E_2 X_{\mathcal{C}} E_2 + E_3 X_{\mathcal{C}} E_3. \end{aligned} \tag{25}$$

Note that the required behavior of Z_{q}, X_{q} on the subsystem $\mathcal{Q}$ follows from the property that each operator $E_a\mathcal{O}_{\mathcal{C}}E_a$ in (25), $\mathcal{O}_{\mathcal{C}} = Z_{\mathcal{C}}$ or $X_{\mathcal{C}}$, has the intended action on states of the form $E_a|i_L\rangle$, $i = 0, 1$. The relevant commutation and anti-commutation rules (1) and (2) are readily verified. In addition to belonging to the set of operators commuting with the stabilizer group (the so-called normalizer $\mathsf{N}(\mathsf{S})$ [31]), the above qubit observables have the property that they also commute with every operator that is a repeated combination of a reset operator followed

by an error, e.g., $\ldots E_{b'}R_{a'}E_bR_a$. This sheds light on the algebraic nature of our three-bit subsystem, which is characterized as a *noiseless subsystem* of the multiplicative algebra $\mathcal{A}$ constructed from recovery operators followed by errors[1]. The fact that *every* quantum error-correcting code can be pictured as a noiseless subsystem of a suitable operator algebra is established in [30].

2.3. The three spin-1/2 symmetric qubit

Consider a system S composed by three physical, distinguishable spin-1/2 particles. Suppose that the interaction with the environment B results in a particularly simple form of noise, *collective* noise, where B couples in a symmetric way to each spin [32]. A relevant example of this situation occurs when the spins couple identically to a fluctuating magnetic field. Our task is to devise a scheme for embedding in S a qubit that is protected from noise.

For collective noise, the interaction Hamiltonian H_{SB} can be written as

$$H_{SB} = \sum_{\alpha=\mathsf{x},\mathsf{y},\mathsf{z}} S_\alpha \otimes B_\alpha \tag{26}$$

where $S_\alpha = \sum_i \sigma_\alpha^{(i)}/2$, $\alpha = \mathsf{x}, \mathsf{y}, \mathsf{z}$, are the components of the total spin angular momentum and the B_α's are environment operators. Note that the operators S_α are the generators of a Lie group $SU(2)$ which corresponds to global spatial rotations of the spins, and can be identified with the familiar $SU(2)$ of angular momentum theory [33]. Suppose that the self-Hamiltonian of the spins can also be expressed in terms of the $\{S_\alpha\}$. One possibility for constructing a protected qubit is to look for a pair of simultaneous degenerate eigenstates of the S_α's [32, 34], i.e.,

$$S_\alpha|\psi_l\rangle = c_\alpha|\psi_l\rangle \quad \alpha = \mathsf{x}, \mathsf{y}, \mathsf{z}, \quad l = 1, 2. \tag{27}$$

Since the eigenvalues c_α do not depend on l, the two eigenstates cannot be distinguished by the environment. Thus, if they can be found, they define a basis of a protected qubit's state space. In our case, one finds that (27) can be only satisfied with $c_\alpha = 0$, meaning that the states $|\psi_l\rangle$ belong to the so-called $S^2 = 0$ singlet representation of $su(2)$, i.e., they are invariant under $SU(2)$ rotations. Unfortunately, no state of three spin-1/2 particles obeys this invariance condition, and a minimum number of four physical spin-1/2 particles is required for the singlet representation to occur with degeneracy at least two [32]. In spite of this impossibility to find a *subspace* of the three-spin state space $\mathcal{S}$ which is immune against noise, it turns out that we are still able to construct a *noiseless subsystem* of $\mathcal{S}$ [30, 35–37] by considering observables commuting with the S_α's. The idea, which we describe next, is to identify in $\mathcal{S}$ a protected degree of freedom.

Since the Hamiltonians S_α generate the spatial rotation group acting symmetrically on the three spins, it is natural to decompose the state space $\mathcal{S}$ of the spins according to the total angular momentum $S^2 = \sum_\alpha S_\alpha^2$:

$$\mathcal{S} = \mathcal{H}_{3/2} \oplus \mathcal{H}_{1/2} \tag{28}$$

where the subspaces $\mathcal{H}_S$ are the eigenspaces of S^2 corresponding to angular momentum $S = 3/2, 1/2$, with $S^2 = S(S+1)$. They have dimension $\dim(\mathcal{H}_{3/2}) = (2 \cdot 3/2 + 1) = 4$, $\dim(\mathcal{H}_{1/2}) = 2(2 \cdot 1/2 + 1) = 4$, respectively. Let us focus on the $S = 1/2$ component. The fact that $\mathcal{H}_{1/2}$ has dimension four implies that the two-dimensional spin-1/2 representation

[1] The multiplicative (or associative) algebra $\mathcal{J}$ generated by a linear set of operators $\mathcal{J}_1 = \mathrm{span}\{\mathbb{1}, J_1, J_2, \ldots\}$ contains all the linear complex combinations of products of operators in $\mathcal{J}_1$.

of the rotation group occurs twice, meaning that physically there are two distinct, equivalent routes for generating angular momentum[2] $S = 1/2$. A basis of states for $\mathcal{H}_{1/2}$ is constructed by considering joint S^2, S_z-eigenvectors, $\{|\lambda, s_z\rangle_{1/2} \,|\, \lambda = 0, 1;\ s_z = \pm 1/2\}$, where s_z is the S_z-eigenvalue and the quantum number λ identifies which of the distinct routes the corresponding eigenvector belongs to. Because angular momentum operators S_α are confined to act non-trivially and equivalently within each route, the S_α have an identical, diagonal action on the degree of freedom supported by the quantum number λ. This degenerate behavior of noise operators with respect to λ is exactly the two-fold degeneracy we are looking for.

A better grasp of the protected structure which is emerging in $\mathcal{H}_{1/2}$ is obtained by establishing the mapping

$$|\lambda, s_z\rangle_{1/2} \simeq |\lambda\rangle_{\mathsf{q}} \otimes |s_z\rangle_{1/2} \tag{29}$$

where now $\{|\lambda\rangle_{\mathsf{q}}\}$ is an orthonormal basis in $\mathbb{C}^2$ and $|s_z\rangle_{1/2}$ is the S_z-eigenvector with eigenvalue s_z. Under such an identification, the subspace $\mathcal{H}_{1/2}$ can be represented as

$$\mathcal{H}_{1/2} \simeq \mathcal{H}_{\mathsf{q}} \otimes \mathcal{D}_{1/2} \simeq \mathbb{C}^2 \otimes \mathbb{C}^2. \tag{30}$$

The actions of the noise operators S_α on $\mathcal{H}_{1/2}$ take a correspondingly simple form,

$$S_\alpha \simeq \mathbb{1}^{(\mathcal{H}_{\mathsf{q}})} \otimes \sigma(\alpha) \tag{31}$$

where $\sigma(\alpha)$ is a unit linear combination of Pauli operators which depends on the choice of basis states in $\mathcal{H}_{\mathsf{q}}$. These algebraic identities provide the starting point for identifying $\mathcal{H}_{1/2}$ as the state space of an effective bi-partite system, and for associating an abstract subsystem with each factor in the tensor product (30). In particular, by virtue of the identity action of noise operators in (31), the left factor $\mathcal{H}_{\mathsf{q}}$ provides a *noiseless* subsystem where a qubit can safely reside, protected from noise for (ideally) arbitrarily long times.

Because the $\mathbb{C}^2$-basis vectors $|\lambda\rangle_{\mathsf{q}}$ are left arbitrary in (29), various realizations are possible as basis states of our three-spin noiseless qubit. Two convenient choices are listed below:

$$\begin{aligned}
|\tilde{0}\rangle_{\mathsf{q}} \otimes |+1/2\rangle_{1/2} &= \frac{1}{\sqrt{2}}\,(|01\rangle - |10\rangle)|0\rangle \\
|\tilde{1}\rangle_{\mathsf{q}} \otimes |+1/2\rangle_{1/2} &= \frac{1}{\sqrt{6}}\,(2|001\rangle - |010\rangle - |100\rangle) \\
|\tilde{0}\rangle_{\mathsf{q}} \otimes |-1/2\rangle_{1/2} &= \frac{1}{\sqrt{2}}\,(|10\rangle - |01\rangle)|1\rangle \\
|\tilde{1}\rangle_{\mathsf{q}} \otimes |-1/2\rangle_{1/2} &= \frac{1}{\sqrt{6}}\,(2|110\rangle - |101\rangle - |011\rangle)
\end{aligned} \tag{32}$$

which can be easily built up from singlet/triplet states of spins 1 and 2 [38], or

$$\begin{aligned}
|0\rangle_{\mathsf{q}} \otimes |+1/2\rangle_{1/2} &= \frac{1}{\sqrt{3}}\,(|001\rangle + \omega|010\rangle + \omega^2|100\rangle) \\
|1\rangle_{\mathsf{q}} \otimes |+1/2\rangle_{1/2} &= \frac{1}{\sqrt{3}}\,(|001\rangle + \omega^2|010\rangle + \omega|100\rangle) \\
|0\rangle_{\mathsf{q}} \otimes |-1/2\rangle_{1/2} &= \frac{1}{\sqrt{3}}\,(|110\rangle + \omega|101\rangle + \omega^2|011\rangle) \\
|1\rangle_{\mathsf{q}} \otimes |-1/2\rangle_{1/2} &= \frac{1}{\sqrt{3}}\,(|110\rangle + \omega^2|101\rangle + \omega|011\rangle)
\end{aligned} \tag{33}$$

[2] In representation-theoretical terms, the appropriate decomposition of the state space is obtained as the Clebsch–Gordan sum of irreducible representations of $su(2)$ which, for our three-spin system, reads $\mathcal{S} \simeq \mathcal{D}_{3/2} \oplus \mathcal{D}_{1/2} \oplus \mathcal{D}_{1/2}$ [33].

with $\omega = \mathrm{e}^{2\pi \mathrm{i}/3}$, which connects directly with standard basis states for the two-dimensional irreducible representation $\mathbf{D}^{(1)}$ of the permutation group S_3 acting on the spins [39]. In (32) and (33), the notations $\{|\tilde{0}\rangle_{\mathsf{q}}, |\tilde{1}\rangle_{\mathsf{q}}\}$ and $\{|0\rangle_{\mathsf{q}}, |1\rangle_{\mathsf{q}}\}$ have been used to account for the different choices of the basis states $\{|\lambda\rangle_{\mathsf{q}}\}$ in $\mathcal{H}_{\mathsf{q}}$. It is important to realize that a possibly mixed state of $\mathcal{S}$ of the form $\rho = |\psi\rangle\langle\psi| \otimes \rho_{1/2}$, where $|\psi\rangle = c_0|0\rangle_{\mathsf{q}} + c_1|1\rangle_{\mathsf{q}}$ and $\rho_{1/2}$ is an arbitrary density operator on $\mathcal{D}_{1/2}$, is a pure state of the qubit living in $\mathcal{H}_{\mathsf{q}}$.

The bases given above establish an equivalence between the state spaces of a pair of two-state systems and the subspace $\mathcal{H}_{1/2}$ of the three spins' state space $\mathcal{S}$. The method can be systematized and the introduction of a different state space can be avoided by directly considering the set of physical observables available for the three spins. Observables that are not affected by the interaction operators S_α are the scalars under spatial rotations, which are given by

$$\begin{aligned} s_{12} &= \vec{\sigma}^{(1)} \cdot \vec{\sigma}^{(2)} = X_1X_2 + Y_1Y_2 + Z_1Z_2 \\ s_{23} &= \vec{\sigma}^{(2)} \cdot \vec{\sigma}^{(3)} = X_2X_3 + Y_2Y_3 + Z_2Z_3 \\ s_{31} &= \vec{\sigma}^{(3)} \cdot \vec{\sigma}^{(1)} = X_3X_1 + Y_3Y_1 + Z_3Z_1. \end{aligned} \tag{34}$$

Since these scalars commute with the interactions, their expectations are protected from noise. If we can combine them so that their expectations define states of a qubit, a noiseless qubit has been found. It is sufficient to form combinations that algebraically behave like the Pauli operators. Let $P_{\mathsf{q}} : \mathcal{S} \mapsto \mathcal{H}_{\mathsf{q}}$ denote the projector over $\mathcal{H}_{\mathsf{q}}$,

$$P_{\mathsf{q}} = \frac{\mathbb{1}}{2} - \frac{1}{6}(s_{12} + s_{23} + s_{31}) \tag{35}$$

where $\mathbb{1}$ denotes the identity operator over $\mathcal{S}$ and P_{q} satisfies $P_{\mathsf{q}} =_{\mathsf{q}} \mathbb{1}_{\mathsf{q}}$ when restricted to $\mathcal{H}_{\mathsf{q}}$. Then the following choice of observables works and corresponds to the ω-basis introduced above:

$$\begin{aligned} X_{\mathsf{q}} &= \frac{1}{6}(2s_{12} - s_{23} - s_{31})P_{\mathsf{q}} = E_{12}P_{\mathsf{q}} \\ Y_{\mathsf{q}} &= -\frac{\sqrt{3}}{6}(s_{23} - s_{31})P_{\mathsf{q}} \end{aligned} \tag{36}$$

where $E_{12} = (\mathbb{1} + \vec{\sigma}^{(1)} \cdot \vec{\sigma}^{(2)})/2$ is the unitary operator swapping the first two spins. Z_{q} is given explicitly as $Z_{\mathsf{q}} = [X_{\mathsf{q}}, Y_{\mathsf{q}}]/2\mathrm{i} = \sqrt{3}/6\,\tau_{123}$, where τ_{123} is the totally antisymmetric operator $\tau_{123} = \sum_{\alpha\beta\gamma} \varepsilon_{\alpha\beta\gamma}\sigma_\alpha^{(1)}\sigma_\beta^{(2)}\sigma_\gamma^{(3)}$, $\alpha, \beta, \gamma \in \{\mathsf{x}, \mathsf{y}, \mathsf{z}\}$. Similar expressions hold for the singlet–triplet basis (32), e.g., $X_{\mathsf{q}} = -\sqrt{3}(s_{23} - s_{31})P_{\mathsf{q}}/6$, and $Z_{\mathsf{q}} = -E_{12}P_{\mathsf{q}}$. Since the commutation and anti-commutation rules obeyed by the observables are identical to (1) and (2), the operator algebra they generate by multiplication and Hermitian conjugation is the algebra of a two-state quantum system.

An important simplification to the above discussion is worth mentioning. This occurs when not only S^2 but S_z also correspond to good (i.e., conserved) quantum numbers for the dynamics of the three physical spins. In this case, using appropriate encoded states rather than the physical three-spin states is motivated by the possibility of achieving universal control by means of purely angular momentum-preserving quantum gates. Note that three is the minimal number of physical qubits allowing for simultaneous eigenvectors of S^2, S_z with degeneracy at least equal to two. The resulting qubits are the basic ingredients in a recent proposal for universal quantum computation via exchange interactions [38]. The mathematical description of these qubits is simpler than that of the noiseless three-spin case, as the full subsystem structure (30) is not required. The relevant observation is that if no mixing between the sets

of states in $\mathcal{H}_{1/2}$ corresponding to $s_z = \pm 1/2$ occurs, a further decomposition applies within the $\mathcal{H}_{1/2}$ subspace:

$$\mathcal{H}_{1/2} \simeq \mathbb{C}^2 \otimes \mathcal{D}_{1/2} \simeq \mathbb{C}^2 \otimes \left(\mathcal{D}_{1/2}^{(+)} \oplus \mathcal{D}_{1/2}^{(-)}\right) \simeq \mathbb{C}^2 \otimes (\mathbb{C} \oplus \mathbb{C}) \simeq \mathbb{C}^2 \oplus \mathbb{C}^2. \tag{37}$$

This means that the two subspaces spanned by $\{|\lambda, +1/2\rangle_{1/2}\}$ and $\{|\lambda, -1/2\rangle_{1/2}\}$, $\lambda = 0, 1$ (the first and second pair of states in either (32) or (33)) are *individually* capable of encoding a qubit. Of course, none of these qubits will retain the robust behavior against all collective noise. Over each $\mathbb{C}^2$-summand of (37), the relevant qubit observables are still given by the combinations of scalars determined above. Note that, once a fixed angular momentum projection is chosen, say $s_z = +1/2$, states belonging to $\mathbb{C}^2 \otimes \mathcal{D}_{1/2}^{(-)}$ as well as to $\mathcal{H}_{3/2}$ behave as 'non-qubit' levels similarly to what we encountered in the case of the bosonic qubit. In particular, this results in a many-qubit state space structure analogous to (6), with a non-trivial summand $\tilde{\mathcal{H}}$ accounting for all the possible 'non-qubit' configurations.

Explicit prescriptions are mentioned in [38] for both initializing the logical qubit to the $|\tilde{0}\rangle_{\mathsf{q}}$ state, and for implementing the final qubit measurement. Initialization may be achieved by relying on the natural equilibration processes of the physical spins in the presence of a polarizing magnetic field, while measurement of the qubit in the $\{|\tilde{0}\rangle_{\mathsf{q}}, |\tilde{1}\rangle_{\mathsf{q}}\}$ basis ($s_z = +1/2$) may be accomplished by determining the singlet versus triplet state of spins 1, 2.

3. Criteria for a qubit

So what is a qubit? From the mathematical point of view, the main lesson that emerges from the above examples, and from the many others that can be analyzed along similar lines, is that the algebraic notion of a *subsystem* provides the most general framework for capturing the variety of ways in which qubits may be constructed. Subsystems, intended as factors (in the tensor product sense) of subspaces of a possibly larger state space, are the structures where we have identified qubits throughout our analysis. Because the information-carrying qubits can be far removed from the 'natural' physical systems that a device is based on, states of qubit subsystems often look complicated when expressed in a basis associated with the physical degrees of freedom, making it difficult to recognize their properties and dynamical behavior. The situation is much simpler, and the description more compact, if the qubit is realized in an *operator* sense through its *observables*.

The idea of describing quantum systems in terms of operators forming a complex associative algebra, whose Hermitian elements provide the system's observables, underlies the operator approach to quantum and quantum-statistical mechanics [40]. Similarly, the general definition of a subsystem is motivated [30] by a fundamental representation theorem for finite-dimensional associative operator algebras closed under Hermitian conjugation, stating that for any such algebra $\mathcal{A}$ a direct sum representation of the overall state space $\mathcal{S}$ exists,

$$\mathcal{S} \simeq \bigoplus_i \mathcal{C}_i \otimes \mathcal{D}_i \tag{38}$$

in such a way that $\mathcal{A}$ has identity action over each factor $\mathcal{C}_i$, $\mathcal{A} \simeq \oplus_i \mathbb{1}^{(\mathcal{C}_i)} \otimes \mathrm{End}(\mathcal{D}_i)$. Thus, if $\mathcal{A}$ is the algebra constructed from noise operators (*interaction algebra* [30]), a noiseless factor (subsystem) $\mathcal{C}_i$ is naturally characterized by an irreducible representation of the so-called *commutant* $\mathcal{A}'$, which is formed from the operators commuting with everything in $\mathcal{A}$.

Motivated by this general perspective, a necessary condition for having a qubit is that it is a subsystem whose associative operator algebra is identical with (isomorphic to) the 'right' operator algebra of a two-state quantum system, i.e., one whose generators satisfy the set of composition rules specified in (1) and (2). Notice that this requirement is stronger than the one

based on the *su*(2) commutation rules (1) alone. While the latter are crucial in determining the appropriate *Lie*-algebraic structure (thereby obtaining the correct symmetry properties) of our qubit, (1) and (2) together are necessary (and sufficient) for ensuring the correct *associative* structure of the relevant algebra. In particular, the condition $\mathcal{O}_{\mathsf{q}}^2 = \mathbb{1}_{\mathsf{q}}$ should hold for the generating observables $\mathcal{O}_{\mathsf{q}}$ to ensure that the appropriate representation in terms of an abstract spin-1/2 particle is realized.

How sensible is this definition from a physical standpoint? Looking back at our examples once more, one observes that identifying the correct algebraic structure does not guarantee by itself the ability of using the associated subsystem as a qubit. In a sense, this is only the first step toward constructing a qubit. Suppose, however, that we did actually succeed at determining a set of observables which generate the correct operator algebra, and suppose, in addition, that we have the capabilities for implementing the following manipulations:

- *Unitary control*. Apply the observables as Hamiltonians to effect universal control operations on the subsystem.
- *Initialization*. Apply suitable non-unitary control, i.e., a quantum operation, so as to leave the subsystem in a state whose expectation on the observables matches that of $|0\rangle$ for some choice of the observable $|0\rangle\langle 0|$.
- *Read-out*. Strong version: perform von Neumann projective measurements of the subsystem observables, which together with unitary control implies the ability to initialize. Weak version: perform weak ensemble measurements of the subsystem observables.

Then what we have constructed is, for all practical purposes, a qubit.

4. Summary and conclusions

We have provided an operational guideline for constructing qubits in physical systems. Our analysis emphasizes the role of operator algebras and observables as the most powerful and comprehensive language to be used for defining qubits in full generality. One obvious implication is that a qubit ends up being a much more versatile and general object than one might at first conceive of. In a broader context, it was recently argued by Steane [41] that a picture in terms of operators rather than state vectors could provide a more insightful perspective for understanding various aspects of quantum information processing, including the origin of the apparent improvements in efficiency over classical information processing. In a sense, a definition of the qubit in general operator terms can then be regarded as the first necessary step of this program.

Acknowledgments

This work was supported by the NSA and by the DOE under contract W-7405-ENG-36.

References

[1] Schumacher B 1996 *Phys. Rev.* A **54** 2614
[2] Bennett C H and DiVincenzo D P 2000 *Nature* **406** 247
[3] Preskill J 1999 Lecture Notes on Quantum Computation http://www.theory.caltech.edu/~preskill/ph229
[4] Hey A J G (ed) 1999 *Feynman and Computation* (Reading, MA: Perseus)
[5] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[6] Deutsch D 1985 *Proc. R. Soc. Lond.* A **400** 97

[7] Shor P W 1994 *Proc. 35th Ann. Symp. on the Foundations of Computer Science* (Los Alamitos CA: IEEE Computer Society Press) p 124
[8] Lloyd S 1996 *Science* **273** 1073
[9] Bennett C H 1999 *Feynman and Computation* ed A J G Hey (Reading, MA: Perseus) p 177
[10] Toffoli T 1999 *Feynman and Computation* ed A J G Hey (Reading, MA: Perseus) p 349
[11] Wooters W K and Zurek W H 1982 *Nature* **299** 802
[12] Dieks D 1982 *Phys. Lett.* A **92** 271
[13] Barnum H, Caves C M, Fuchs C A, Jozsa R and Schumacher B 1966 *Phys. Rev. Lett.* **76** 2818
[14] Bennett G C H, Brassard D, Crépeau C, Jozsa R, Peres A and Wooters W K 1993 *Phys. Rev. Lett.* **70** 1895
[15] Gottesman D and Chuang I L 1999 *Nature* **402** 390
[16] Special focus issue on Experimental Proposals for Quantum Computation 2000 *Fort. Phys.* **48** nos 9–11
[17] DiVincenzo D P 2000 *Fort. Phys.* **48** p 771
[18] Milburn G J 1989 *Phys. Rev. Lett.* **62** 1224
[19] Lloyd S 1993 *Science* **26** 143
[20] Cirac J and Zoller P 1995 *Phys. Rev. Lett.* **74** 4091
[21] Knill E, Laflamme R and Milburn G J 2001 *Nature* **409** 46
[22] Walls D F and Milburn G J 1994 *Quantum Optics* (Berlin: Springer)
[23] Kitaev A Yu 1997 *Preprint* quant-ph/9707021
[24] Lloyd S 2000 *Preprint* quant-ph/0004010
[25] Lloyd S 1998 *Unconventional Models of Computation* ed Calude C S, Casti J and Dinneen M J (Berlin: Springer)
[26] Bravyi S B and Kitaev A Yu 2000 *Preprint* quant-ph/0003137
[27] Gottesman D, Kitaev A and Preskill J 2000 *Preprint* quant-ph/0008040
[28] Tian L and Lloyd S 2000 *Phys. Rev.* A **62** 050301
[29] Knill E and Laflamme R 1997 *Phys. Rev.* A **55** 900
[30] Knill E, Laflamme R and Viola L 2000 *Phys. Rev. Lett.* A **84** 2525
[31] Gottesman D 1998 *Preprint* quant-ph/9705052 (Caltech PhD Thesis)
[32] Zanardi P and Rasetti M 1997 *Phys. Rev. Lett.* **79** 3306
[33] Cornwell J F 1984 *Group Theory in Physics* (New York: Academic)
[34] Lidar D A, Chuang I L and Whaley K B 1998 *Phys. Rev. Lett.* **81** 2594
[35] Viola L, Knill E and Lloyd S 2000 *Phys. Rev. Lett.* **85** 3520
[36] Zanardi P 1999 *Phys. Rev.* A **63** 012301
(Zanardi P *Preprint* quant-ph/9910016)
[37] De Filippo S 2000 *Phys. Rev.* A **62** 052307
[38] DiVincenzo D P, Bacon D, Kempe J, Burkard G and Whaley K B 2000 *Nature* **408** 339
[39] Peres A 1995 *Quantum Theory: Concepts and Methods* (Dordrecht: Kluwer Academic) p 132
[40] Thirring W 1981 *A Course in Mathematical Physics* vol III (Berlin: Springer)
[41] Steane A M 2000 *Preprint* quant-ph/0003084