PHYSICAL REVIEW A

ATOMIC, MOLECULAR, AND OPTICAL PHYSICS

THIRD SERIES, VOLUME 55, NUMBER 2 **FEBRUARY 1997**

RAPID COMMUNICATIONS

The Rapid Communications section is intended for the accelerated publication of important new results. Since manuscripts submitted to this section are given priority treatment both in the editorial office and in production, authors should explain in their submittal letter why the work justifies this special handling. A Rapid Communication should be no longer than 4 printed pages and must be accompanied by an abstract. Page proofs are sent to authors.

Correcting quantum errors in higher spin systems

H. F. Chau*

Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong

(Received 16 October 1996)

I consider the theory of the quantum error correcting code (QECC), where each quantum particle has more than two possible eigenstates. In this higher spin system, I report an explicit QECC that is related to the symmetry group $\mathbb{Z}_2^{\otimes(N-1)}\otimes S_N$. This QECC, which generalizes Shor's simple majority vote code [Phys. Rev. A **52**, 2493 (1995)], is able to correct errors arising from exactly one quantum particle. I also provide a simple encoding algorithm. [S1050-2947(97)50302-7]

PACS number(s): 03.65.Bz, 02.20.Df, 89.70.+c, 89.80.+h

Quantum computers are powerful enough to efficiently factorize composite numbers [1]. Nevertheless, quantum computers are extremely vulnerable to disturbance [2]. Decoherence between the quantum computer and the environment, together with decoherence between different parts of a quantum computer may seriously affect the output of a computation.

By encoding the quantum state into a larger Hilbert space H, it is possible to reduce the decoherence error with the environment. By first measuring the wave function in a suitable subspace C of H and then by applying a unitary transformation to the orthogonal complement of C according to the measurement result, it is possible to correct quantum errors due to decoherence with the environment [3]. This kind of scheme is now called the quantum error correction code (QECC). The first QECC was discovered by Shor. Using the idea of simple majority vote, he encodes each quantum bit (qubit) by nine qubits. His code is able to correct one qubit of error [3]. Since then, many QECCs have been discovered (see, for example, Refs. [4–9]) and various theories on QECC have also been developed (see, for example, Refs. [7–13]). In particular, the necessary and sufficient condition for a QECC is [11–13]

$$\langle i_{\text{encode}}|A^{\dagger}B|j_{\text{encode}}\rangle=\lambda_{A,B}\delta_{ij}\,, \tag{1}$$

where $|i_{\text{encode}}\rangle$ denotes the encoded quantum state $|i\rangle$ using the QECC, A,B are the possible errors that can be handled by the QECC, and $\lambda_{A,B}$ is a complex constant independent of $|i_{\text{encode}}\rangle$ and $|j_{\text{encode}}\rangle$.

Early QECCs concentrate on the decoherence of a quantum computer with the environment. Individual quantum registers in a quantum computer are assumed to be placed far apart from each other so that decoherence among them can be ignored. Nonetheless, this assumption is not true in general. To understand why, let me first summarize the simplest possible spin-$\frac{1}{2}$-particle-based quantum computer model: A single spin-$\frac{1}{2}$ particle (A) is used as a messenger. It shuttles around other spin-$\frac{1}{2}$ particles (B) and interacts with them from time to time. Although decoherence between particles (B) may be neglected, decoherence between (A) and (B) can be serious (compare with a similar ''gearbox quantum computer'' proposal by DiVincenzo [14]).

Therefore, it is natural to construct a QECC that corrects this kind of ''internal'' decoherence error among different quantum registers. This can be achieved by constructing a QECC that may correct errors involving multiple spins (see, for example, Refs. [5,6,8,10]). Alternatively, we may map this problem to that of correcting a single quantum error in a system with higher spin. Suppose the messenger (A) has to interact with a specific spin-$\frac{1}{2}$ register (C) in (B). We may regard the combination of (A) and (C) as a single quantum particle with spin $\frac{3}{2}$. If we encode this spin-$\frac{3}{2}$ state by a QECC and correct the quantum error immediately after the interaction process, decoherence between (A),(C) and the environment can be greatly suppressed. The advantage of

*Electronic address: hfchau@hkusua.hku.hk

this method is that, in general, fewer quantum registers are required. The reason is simple: resources are concentrated on correcting errors in (A) and (C), while extra resources are needed for a general multiple quantum error correcting code in order to take care of the less frequent decoherence error within (B).

Another reason to consider the QECC for a higher spin system is that the quantum registers used may consist of more than two possible states. For example, the two-bit quantum logic gate experimentally studied by Monroe *et al.* uses extra states for preparation and measurement [15]. Error correction may be required to prevent the quantum register from going to the unwanted states during the computation.

In this paper, I consider the QECC for particles with spin higher than $\frac{1}{2}$. I study a special kind of QECC that is related to the symmetry group $\mathbb{Z}_2^{\otimes(N-1)}\otimes S_N$, where N is the number of states of each spin. An explicit example of a QECC that is able to correct one quantum register[1] of error is given. My code reduces to the simple majority vote code proposed by Shor [3] when $N=2$.

I denote the N mutually orthogonal eigenstates in each quantum register by $|0\rangle,|1\rangle,\ldots,|N-1\rangle$. Any quantum error involving exactly one quantum register can be described by an operator E acting on that quantum register. Clearly we can represent E by a nonzero $N\times N$ complex matrix. That is to say, $E\in\mathcal{A}\equiv\mathbb{C}^{N\times N}\setminus\{0\}$. Further properties of the quantum error operator can be found elsewhere [16]. It is easy to check that for any $E\in\mathcal{A}$, we can find complex numbers α, β_i, γ_{mn} and δ_{mn}, not all zero, such that

$$E=\alpha I_N+\sum_{i=1}^{N-1}\beta_i R_i+\sum_{m\neq n}(\gamma_{mn}P_{mn}+\delta_{mn}Q_{mn}), \tag{2}$$

where the sum in the third term runs from $m,n=0$ to $N-1$, I_N is the $N\times N$ identity matrix, and R_i, P_{mn}, Q_{mn} are given by

$$(R_i)_{xy}=\begin{cases}1 & \text{if } x=y \text{ and } x\neq i\\ -1 & \text{if } x=y=i\\ 0 & \text{otherwise,}\end{cases} \tag{3a}$$

$$(P_{mn})_{xy}=\begin{cases}1 & \text{if } x=y \text{ and } x\neq m,n\\ 1 & \text{if } x=m,y=n \text{ or } x=n,y=m\\ 0 & \text{otherwise,}\end{cases} \tag{3b}$$

and

$$(Q_{mn})_{xy}=\begin{cases}1 & \text{if } x=y \text{ and } x\neq m,n\\ 1 & \text{if } x=m,y=n\\ -1 & \text{if } x=n,y=m\\ 0 & \text{otherwise,}\end{cases} \tag{3c}$$

respectively. Physically, R_i adds a phase shift of π to the part of the state ket whenever the quantum register is in the state $|i\rangle$. The action of P_{mn} interchanges $|m\rangle$ with $|n\rangle$ while leaving the other quantum states unchanged. Similarly, Q_{mn} maps $|m\rangle$ to $|n\rangle$ and $|n\rangle$ to $-|m\rangle$ while leaving the other quantum states unchanged. Therefore, R_i and P_{mn} model the effect of phase error and spin flip, respectively, and Q_{mn} models the effect of combined phase and spin flip error. Note that I_N, R_i, P_{mn}, and Q_{mn} are Hamiltonian operators, and hence are physical observables. Besides, they form a linearly independent set.

From Eq. (2), it is easy to show that a QECC can handle one quantum register of error if and only if it can handle errors arising from the actions of R_i, P_{mn}, and Q_{mn}. Using the group-theoretic method of the QECC developed by Calderbank *et al.* [8], I consider the finite group G generated by the elements R_i, P_{mn} and Q_{mn}. Since $P_{mn}=P_{0m}\circ P_{0n}\circ P_{0m}$, $Q_{mn}=P_{0m}\circ Q_{0n}\circ P_{0m}$, and $Q_{0n}=R_n\circ P_{0n}$, the group G is given by

$$G=\langle R_1,R_2,\ldots,R_{N-1},P_{01},P_{02},\ldots,P_{0\,N-1}\rangle. \tag{4}$$

Thus, G is isomorphic to $\mathbb{Z}_2^{\otimes(N-1)}\otimes S_N$. According to Knill [12], this choice of error bases is ''nice'' but not ''very nice'' in general.

Equation (4) implies that the ability to correct the $2(N-1)$ kinds of quantum errors R_n and P_{1n} $(n=1,2,\ldots,N-1)$ is a necessary condition for correcting any quantum errors involving one quantum register. Here, I show that this condition is also sufficient. As shown by Gottesman [9], we may paste the QECC as follows: Suppose C_1 and C_2 are two QECCs correcting errors E_1 and E_2, respectively. Let us consider the situation in which both errors occur in the same set of quantum registers. One can first encode the quantum register using code C_1, and then further encode the resultant quantum registers by the code C_2. The resultant quantum code can correct errors in the form $E_2\circ E_1$. Thus, by pasting QECCs that correct the quantum errors R_n and P_{1n} $(n=1,2,\ldots,N-1)$ in a suitable way, one obtains a QECC for quantum errors given by the group G, and hence this code corrects quantum errors involving exactly one quantum register.

Since the coding scheme

$$|i\rangle\mapsto|iii\rangle \tag{5}$$

can correct quantum errors P_{mn}, and the coding scheme

$$|1\rangle\mapsto\frac{1}{\sqrt{8}}(|1\rangle+|i\rangle)\otimes(|1\rangle+|i\rangle)\otimes(|1\rangle+|i\rangle),$$

$$|i\rangle\mapsto\frac{1}{\sqrt{8}}(|1\rangle-|i\rangle)\otimes(|1\rangle-|i\rangle)\otimes(|1\rangle-|i\rangle),$$

$$|j\rangle\mapsto|jjj\rangle \tag{6}$$

can correct the quantum error R_i. One may paste these codes together to obtain the required QECC that can correct errors involving one quantum register. Nevertheless, this construction is not practical since it involves too many quantum registers.

Here, I report a more economical code. Suppose ω_N is a primitive Nth root of unity, then

[1]Note that the state of each quantum register spans an N-dimensional Hilbert space. When $N>2$, it is not appropriate to call it a qubit because the quantum register holds more information than one qubit.

$$\sum_{m=0}^{N-1} \omega_N^{mk} = \begin{cases} 0 & \text{for } k=1,2,\ldots,N-1 \\ N & \text{if } k=N. \end{cases} \tag{7}$$

Consequently, state kets $|0\rangle+\omega_N^k|1\rangle+\omega_N^{2k}|2\rangle+\ldots+\omega_N^{(N-1)k}|N-1\rangle$ are mutually orthogonal to each other for $k=0,1,\ldots,N-1$. Besides, one can verify that the encoding

$$|m\rangle \mapsto \frac{1}{N^{3/2}}\left[\sum_{k=0}^{N-1} \omega_N^{km}|k\rangle\right]\otimes\left[\sum_{k=0}^{N-1} \omega_N^{km}|k\rangle\right]\otimes\left[\sum_{k=0}^{N-1} \omega_N^{km}|k\rangle\right]$$
$$= \frac{1}{N^{3/2}}\sum_{k,p,q=0}^{N-1} \omega_N^{(k+p+q)m}|kpq\rangle \tag{8}$$

can correct phase quantum errors R_i $(i=1,2,\ldots,N-1)$.

Since R_i commutes with P_{mn}, by pasting the two codes in Eqs. (5) and (8) together, we obtain a QECC that handles errors in G (see Ref. [9]). I explicitly write down this code below:

$$|m\rangle \mapsto \frac{1}{N^{3/2}}\left[\sum_{k=0}^{N-1} \omega_N^{km}|kkk\rangle\right]\otimes\left[\sum_{k=0}^{N-1} \omega_N^{km}|kkk\rangle\right]$$
$$\otimes\left[\sum_{k=0}^{N-1} \omega_N^{km}|kkk\rangle\right]$$
$$= \frac{1}{N^{3/2}}\sum_{k,p,q=0}^{N-1} \omega_N^{(k+p+q)m}|kkkpppqqq\rangle \tag{9}$$

for all $m=0,1,2,\ldots,N-1$. Note that this code encodes each quantum register by nine of them, and it is able to correct any quantum errors arising from exactly one quantum register. When $N=2$, it reduces to the simple majority code by Shor [3].

The above QECC is closely related to the (multiplicative) group character χ of the finite additive group $\mathbb{Z}_N$. Note that $\chi:\mathbb{Z}_N\to\mathbb{C}$ is a map satisfying [17]

$$\chi(a+b)=\chi(a)\chi(b) \tag{10}$$

for all $a,b\in\mathbb{Z}_N$. If we identify each eigenstate $|m\rangle$ with $m\in\mathbb{Z}_N$, then Eq. (7) is a direct consequence of the sum rule [17]

$$\sum_{m\in\mathbb{Z}_N}\chi(m)=\begin{cases} N & \text{if } \chi \text{ is the trivial character} \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

The above sum rule ensures that the encoded states $|m_{\text{encode}}\rangle$ given by Eq. (8) are mutually orthogonal.

Now, I provide a simple encoding algorithm for this code. Using a series of quantum binary conditional-NOT gates, we may ''copy'' the quantum state $|m00000000\rangle$ to $|m00m00m00\rangle$ efficiently. Then, we may apply a quantum discrete Fourier transform similar to that used in Shor's factorization algorithm [1,18] separately to the first, fourth, and seventh quantum registers in order to produce the required encoding scheme. That is to say, for each $|m\rangle$ in the first, fourth, and the seventh quantum registers, we apply a unitary transformation, mapping it to the state

$$|m\rangle \mapsto \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \omega_N^{km}|k\rangle. \tag{12}$$

Using the same idea as in Shor's algorithm, the above transformation can be achieved efficiently. To obtain the required encoding, we finally ''copy'' the first quantum register into the second and third, the fourth into the fifth and sixth, and the seventh into the eighth and ninth. The entire process can be summarized below:

$$|m00000000\rangle \mapsto |m00m00m00\rangle$$
$$\mapsto \frac{1}{N^{3/2}}\sum_{k,p,q=0}^{N-1} \omega_N^{(k+p+q)m}|k00p00q00\rangle$$
$$\mapsto \frac{1}{N^{3/2}}\sum_{k,p,q=0}^{N-1} \omega_N^{(k+p+q)m}|kkkpppqqq\rangle. \tag{13}$$

In order to have enough room in the encoded Hilbert space for the QECC, the condition

$$[1+(N^2-1)n]N \leqslant N^n \tag{14}$$

must be satisfied, in which n is the number of quantum register. Moreover, the code is said to be perfect if the equality in Eq. (14) holds [4]. Nonetheless, Eq. (9) is not a perfect code, and more efficient QECCs may exist. It will be interesting to find them out.

[1] P. W. Shor, in *Proceeding of the 35th Annual Symposium on the Foundation of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.

[2] R. Landauer, in *Proceedings of PHYSCOMP94*, edited by D. Matzke (IEEE Computer Society, Los Alamitos, CA, 1994), p. 54.

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

[4] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

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

[6] A. M. Steane, Phys. Rev. A (to be published).

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

[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane (unpublished).

[9] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[10] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).

[11] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[12] E. Knill (unpublished).

[13] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[14] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[15] C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995).

[16] B. Schumacher (unpublished).

[17] K. Ireland, and M. Rosen, *A Classical Introduction To Modern Number Theory*, 2nd ed. (Springer, New York, 1990), Chap. 8.

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