PHYSICAL REVIEW A

ATOMIC, MOLECULAR, AND OPTICAL PHYSICS

THIRD SERIES, VOLUME 56, NUMBER 1 JULY 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.

Five quantum register error correction code for higher spin systems

H. F. Chau*
Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong

(Received 18 February 1997)

I construct a quantum error correction code (QECC) in higher spin systems using the idea of multiplicative group character. Each N-state quantum particle is encoded as five N-state quantum registers. By doing so, this code can correct any quantum error arising from any one of the five quantum registers. This code generalizes the well-known five qubit perfect code in spin-1/2 systems and is shown to be optimal for higher spin systems. I also report a simple algorithm for encoding. The importance of multiplicative group character in constructing QECCs will be addressed. [S1050-2947(97)50707-4]

PACS number(s): 03.65.Bz, 02.10.Lh, 89.70.+c, 89.80.+h

The power of a quantum computer is perhaps best illustrated by the powerful Shor quantum polynomial time factorization algorithm [1]. However, the real power of a quantum computer may be much more limited because it is extremely vulnerable to disturbance [2]. Nevertheless, Shor pointed out later that the effect of quantum decoherence can be compensated for if we introduce redundancy in the quantum state in a suitable way. We first encode the quantum state into a larger Hilbert space H. Then we measure the wave function in a suitable subspace C of H. And finally we apply a unitary transformation to the orthogonal complement of C according to our 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). Since then, many QECCs have been discovered (see, for example, Refs. [4–10]) and various theories on the QECC have also been developed (see, for example, Refs. [7–14]). In particular, the necessary and sufficient condition for a QECC is [12–14]

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

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 deal with decoherence of individual spin-$\frac{1}{2}$ particles with the environment. Besides, the information loss to the environment is assumed to be unrecoverable. More recently, Duan and Guo considered the decoherence of spin-$\frac{1}{2}$ particles with the same environment. Based on a specific model of the environment in thermal equilibrium, they found a new coding scheme [15]. Another investigation concentrates on the mutual decoherence between the quantum spins inside the quantum computer. Chau pointed out that the ability to correct quantum errors among various registers inside a quantum computer is equivalent to the ability to correct the quantum error of a single quantum higher spin particle [10]. Thus, it is interesting to construct QECCs for quantum registers with higher spin.

The QECC for particles with spin higher than $\frac{1}{2}$ was found by Chau using group-theoretical methods. He encodes each quantum particle as nine quantum registers. And by doing so, his code can correct any quantum error involving exactly one quantum register [10]. Nonetheless, his code is not perfect.[1] So, it is natural to ask if it is possible to construct more economical codes for higher spin systems.

*Electronic address: hfchau@hkusua.hku.hk

[1] See Ref. [4] for a precise definition of a perfect code.

An affirmative answer is provided in this paper. I report a way to encode each quantum particle as five quantum registers, which can correct an error in at most one of the five registers. I also show that this code is optimal in the sense that no QECC with codeword length less than five can correct a general one quantum register error. For spin-$\frac{1}{2}$ particles, this code is equivalent to the perfect codes discovered by Laflamme *et al.* [4] and Bennett *et al.* [14] up to unitary transformations. As you will see in the derivation, the success of this five-register code relies heavily on the sum rule of the multiplicative group character of the finite additive group $\mathbb{Z}_N$.

The (multiplicative) group character of the finite additive group $\mathbb{Z}_N$ is a map $\chi{:}\mathbb{Z}_N\rightarrow\mathbb{C}$ satisfying [16]

$$\chi(a+b)=\chi(a)\chi(b) \tag{2}$$

for all $a,b\in\mathbb{Z}_N$. Then χ satisfies the sum rule [16]

$$\sum_{m\in\mathbb{Z}_N}\chi(m)=\begin{cases}N & \text{if } \chi \text{ is the trivial character,}\\ 0 & \text{otherwise.}\end{cases} \tag{3}$$

More concretely, the above sum rule can be written as

$$\sum_{m=0}^{N-1}\omega_N^{mk}=\begin{cases}N & \text{if } k=0 \bmod N,\\ 0 & \text{for } k=1,2,\ldots,N-1 \bmod N,\end{cases} \tag{4}$$

where ω_N is a primitive Nth root of unity.

To see how we use Eq. (4) to construct our five quantum register code, let us begin by denoting the N mutually orthogonal eigenstates in each quantum register by $|0\rangle,|1\rangle,\ldots,|N-1\rangle$. Then, I claim that the following encoding scheme can correct any quantum error occurring in at most one of the quantum registers

$$\begin{aligned}|k\rangle\mapsto{}&\frac{1}{N^{3/2}}\sum_{p,q,r=0}^{N-1}\omega_N^{k(p+q+r)+pr}|p+q+k\rangle\otimes|p+r\rangle\\ &\otimes|q+r\rangle\otimes|p\rangle\otimes|q\rangle\equiv\frac{1}{N^{3/2}}\sum_{p,q,r=0}^{N-1}\omega_N^{k(p+q+r)+pr}\\ &\times|p+q+k,p+r,q+r,p,q\rangle\end{aligned} \tag{5}$$

for $k=0,1,\ldots,N-1$, where all the additions in the state kets and in the sum are modulo N.

Let me denote the one-bit quantum error E_α occurring at the ith quantum register by the symbol $E_{i,\alpha}$. To prove the above claim, it suffices to show that Eq. (1) holds for any quantum errors $A=E_{i,\alpha}$ and $B=E_{j,\beta}$ for $1\leqslant i\leqslant j\leqslant 5$.

First, I consider the case when $(i,j)=(1,4)$ as a warm up. We have

$$\begin{aligned}&\langle k_{\text{encode}}|E^\dagger_{1,\alpha}E_{4,\beta}|k'_{\text{encode}}\rangle\\ &\quad=\frac{1}{N^3}\sum_{p,q,r,p',q',r'=0}^{N-1}\omega_N^{k'(p'+q'+r')+p'r'-k(p+q+r)-pr}\\ &\qquad\times\langle p+q+k|E^\dagger_\alpha|p'+q'+k'\rangle\langle p+r|p'+r'\rangle\\ &\qquad\times\langle q+r|q'+r'\rangle\langle p|E_\beta|p'\rangle\langle q|q'\rangle\end{aligned}$$

$$\begin{aligned}&=\frac{1}{N^3}\sum_{p,q,r,p',q',r'=0}^{N-1}\omega_N^{k'(p'+q'+r')+p'r'-k(p+q+r)-pr}\\ &\quad\times\delta_{q+r,q'+r'}\delta_{q,q'}\delta_{p+r,p'+r'}\\ &\quad\times\langle p+q+k|E^\dagger_\alpha|p'+q'+k'\rangle\langle p|E_\beta|p'\rangle\\ &=\frac{1}{N^3}\sum_{p,q,r=0}^{N-1}\omega_N^{(k'-k)(p+q+r)}\\ &\quad\times\langle p+q+k|E^\dagger_\alpha|p+q+k'\rangle\langle p|E_\beta|p\rangle\\ &=\delta_{k,k'}\frac{1}{N^2}\sum_{p,q=0}^{N-1}\langle p+q|E^\dagger_\alpha|p+q\rangle\langle p|E_\beta|p\rangle\\ &\equiv\delta_{k,k'}\Lambda_{1,\alpha;4,\beta},\end{aligned} \tag{6}$$

where $\Lambda_{1,\alpha;4,\beta}$ is independent of k. Thus, Eq. (1) holds when $(i,j)=(1,4)$. Using the same trick, it is easy to verify that Eq. (1) holds when $(i,j)=(1,1)$, (2,2), (3,3), (4,4), (5,5), (1,5), and (3,5).

Now, I proceed to the more difficult case when $(i,j)=(1,2)$. We have

$$\begin{aligned}&\langle k_{\text{encode}}|E^\dagger_{1,\alpha}E_{2,\beta}|k'_{\text{encode}}\rangle\\ &\quad=\frac{1}{N^3}\sum_{p,q,r,p',q',r'=0}^{N-1}\omega_N^{k'(p'+q'+r')+p'r'-k(p+q+r)-pr}\\ &\qquad\times\delta_{p,p'}\delta_{q,q'}\delta_{q+r,q'+r'}\langle p+q+k|E^\dagger_\alpha|p'+q'+k'\rangle\\ &\qquad\times\langle p+r|E_\beta|p'+r'\rangle\\ &\quad=\frac{1}{N^3}\sum_{p,q,r=0}^{N-1}\omega_N^{(k'-k)(p+q+r)}\langle p+q+k|E^\dagger_\alpha|p+q+k'\rangle\\ &\qquad\times\langle p+r|E_\beta|p+r\rangle.\end{aligned} \tag{7}$$

By relabeling $x=p+q$, $y=p+r$, and $z=r$, Eq. (7) can be rewritten as

$$\begin{aligned}\langle k_{\text{encode}}|E^\dagger_{1,\alpha}E_{2,\beta}|k'_{\text{encode}}\rangle&=\frac{1}{N^3}\sum_{x,y,z=0}^{N-1}\omega_N^{(k'-k)(x+z)}\\ &\quad\times\langle x+k|E^\dagger_\alpha|x+k'\rangle\langle y|E_\beta|y\rangle\\ &=\delta_{k,k'}\frac{1}{N^2}\sum_{x,y=0}^{N-1}\langle x|E^\dagger_\alpha|x\rangle\langle y|E_\beta|y\rangle\\ &\equiv\delta_{k,k'}\Lambda_{1,\alpha;2,\beta},\end{aligned} \tag{8}$$

where $\Lambda_{1,\alpha;2,\beta}$ is independent of k. Thus, Eq. (1) holds when $(i,j)=(1,2)$. In a similar way, one can show that Eq. (1) is also true for $(i,j)=(1,3)$.

Now, I move on to the case when $(i,j)=(2,3)$. By direct computation, we obtain

$$\begin{aligned}&\langle k_{\text{encode}}|E^\dagger_{2,\alpha}E_{3,\beta}|k'_{\text{encode}}\rangle\\ &\quad=\frac{1}{N^3}\sum_{p,q,r,p',q',r'=0}^{N-1}\omega_N^{k'(p'+q'+r')+p'r'-k(p+q+r)-pr}\end{aligned}$$

$$\times\delta_{p,p'}\delta_{q,q'}\delta_{p+q+k,p'+q'+k'}\langle p+r|E_\alpha^\dagger|p'+r'\rangle$$
$$\times\langle q+r|E_\beta|q'+r'\rangle$$
$$=\delta_{k,k'}\frac{1}{N^3}\sum_{p,q,r,r'=0}^{N-1}\omega_N^{(r'-r)(k+p)}\langle p+r|E_\alpha^\dagger|p+r'\rangle$$
$$\times\langle q+r|E_\beta|q+r'\rangle. \tag{9}$$

By relabeling $x=r'-r$, $y=p+r$, $z=q+r$, and $u=p$, Eq. (9) can be written as

$$\langle k_{\text{encode}}|E_{2,\alpha}^\dagger E_{3,\beta}|k'_{\text{encode}}\rangle$$
$$=\delta_{k,k'}\frac{1}{N^3}\sum_{u,x,y,z=0}^{N-1}\omega_N^{x(u+k)}\langle y|E_\alpha^\dagger|y+x\rangle\langle z|E_\beta|z+x\rangle$$
$$=\delta_{k,k'}\frac{1}{N^2}\sum_{x,y,z=0}^{N-1}\langle y|E_\alpha^\dagger|y+x\rangle\langle z|E_\beta|z+x\rangle$$
$$\equiv\delta_{k,k'}\Lambda_{2,\alpha;3,\beta}, \tag{10}$$

where $\Lambda_{2,\alpha;3,\beta}$ is independent of k. Hence, Eq. (1) is also satisfied when $(i,j)=(2,3)$. Using similar methods, it can be shown that Eq. (1) holds if $(i,j)=(2,4)$, (2,5), and (3,4).

Finally, I consider the case when $(i,j)=(4,5)$. By direct computation, we find that

$$\langle k_{\text{encode}}|E_{4,\alpha}^\dagger E_{5,\beta}|k'_{\text{encode}}\rangle$$
$$=\frac{1}{N^3}\sum_{p,q,r,p',q',r'=0}^{N-1}\omega_N^{k'(p'+q'+r')+p'r'-k(p+q+r)-pr}$$
$$\times\delta_{p+r,p'+r'}\delta_{q+r,q'+r'}\delta_{p+q+k,p'+q'+k'}\langle p|E_\alpha^\dagger|p'\rangle$$
$$\times\langle q|E_\beta|q'\rangle$$
$$=\frac{1}{N^3}\sum_{p,q,r,p',q',r'=0}^{N-1}\omega_N^{k'(p'+q'+r')+p'r'-k(p+q+r)-pr}$$
$$\times\delta_{2p+k,2p'+k'}\delta_{2q+k,2q'+k'}\delta_{2r-k,2r'-k'}\langle p|E_\alpha^\dagger|p'\rangle$$
$$\times\langle q|E_\beta|q'\rangle. \tag{11}$$

Let us analyze the situation by considering the following two subcases:

Subcase (a): If $k-k'$ is odd and N is even, then it is impossible to find $p,p'\in\mathbb{Z}_N$ such that $2p+k=2p'+k'\,\text{mod}N$. Hence, the existence of the $\delta_{2p+k,2p'+k'}$ term in Eq. (11) implies that $\langle k_{\text{encode}}|E_{4,\alpha}^\dagger E_{5,\beta}|k'_{\text{encode}}\rangle=0$.

Subcase (b): if either $k-k'$ is even or N is odd, then it is possible to find $p,p'\in\mathbb{Z}_N$ such that $2p+k=2p'+k'\,\text{mod}N$. That is to say, it make sense to regard $(k'-k)/2$ as an integer in $\mathbb{Z}_N$. Then Eq. (11) becomes

$$\langle k_{\text{encode}}|E_{4,\alpha}^\dagger E_{5,\beta}|k'_{\text{encode}}\rangle$$
$$=\frac{1}{N^3}\sum_{p,q,r=0}^{N-1}\omega_N^{[(k'-k)/2][3p+2q+r-(3k'-k)/2]}$$
$$\times\left\langle p|E_\alpha^\dagger|p-\frac{k'-k}{2}\right\rangle\left\langle q|E_\beta|q-\frac{k'-k}{2}\right\rangle$$
$$=\delta_{k,k'}\frac{1}{N^2}\sum_{p,q=0}^{N-1}\langle p|E_\alpha^\dagger|p\rangle\langle q|E_\beta|q\rangle$$
$$\equiv\delta_{k,k'}\Lambda_{4,\alpha;5,\beta}, \tag{12}$$

where $\Lambda_{4,\alpha;5,\beta}$ is independent of k. Therefore, the encoding scheme in Eq. (5) satisfies Eq. (1) for any (i,j) with $1\leqslant i,j\leqslant 5$; and, hence, this scheme is able to correct any quantum error arising at any one of the quantum registers as promised.

The key idea used in this five-register code is (i) the multiplicative group character sum rule in Eq. (3), (ii) the relabeling of some variables in the summation, and (iii) the strong correlation between the five quantum registers.[2] Since the sum rule in Eq. (3) plays a very important role in both the five and the nine quantum register codes [10], it will be interesting to rewrite other existing QECCs for spin-$\frac{1}{2}$ particles in a form similar to that of Eq. (5). This may provide a way to generalize these codes to higher spin systems.

Back to the case when $N=2$. The above encoding scheme above can be explicitly written as

$$|0\rangle\mapsto\frac{1}{\sqrt{8}}[|00000\rangle+|01100\rangle+|10101\rangle+|11001\rangle+|11010\rangle$$
$$-|10110\rangle+|01111\rangle-|00011\rangle] \tag{13a}$$

and

$$|1\rangle\mapsto\frac{1}{\sqrt{8}}[|10000\rangle-|11100\rangle-|00101\rangle+|01001\rangle-|01010\rangle$$
$$-|00110\rangle+|11111\rangle+|10011\rangle]. \tag{13b}$$

This scheme can be transformed to the perfect code obtained by Laflamme *et al.* [4] (and hence also Bennett *et al.*'s [14]) by a simple unitary transformation: first permute the five quantum registers by $P(13524)$, then add an extra phase of π to the encoding state whenever $p+r+k$ is even. That is to say, Laflamme *et al.*'s perfect code can be written as

$$|k\rangle\mapsto\frac{1}{\sqrt{8}}\sum_{p,q,r}(-1)^{(p+1)(r+1)+k(p+q+r+1)}|p+q+1\rangle$$
$$\otimes|p\rangle\otimes|p+r\rangle\otimes|q\rangle\otimes|q+r\rangle, \tag{14}$$

for $k=0,1$.

Now, I give a simple encoding algorithm for this code. Using a series of quantum binary conditional-NOT gates, we may ''copy'' the state $|k,0,0,0,0\rangle$ to $|k,0,k,k,k\rangle$ efficiently. Next, we apply quantum discrete Fourier transforms similar to that used in Shor's algorithm [1,17,18] separately to the third, fourth, and fifth quantum registers. Then, we add an additional phase of ω_N^{pr} to the system using a Toffoli-like gate [19,20]. We then use a series of quantum binary conditional-NOT gates to ''copy'' the fourth register to the second one. Finally, by suitably adding the quantum registers

[2] In other words, the high entanglement entropy in this code.

together using reversible quantum logic gates, we obtain the quantum code as required. The entire encoding procedure can be summarized below:

$$
\begin{aligned}
|k,0,0,0,0\rangle &\mapsto |k,0,k,k,k\rangle \\
&\mapsto \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{k(p+q+r)} |k,0,r,p,q\rangle \\
&\mapsto \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{k(p+q+r)+pr} |k,0,p,q,r\rangle \\
&\mapsto \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{k(p+q+r)+pr} |k,p,r,p,q\rangle \\
&\mapsto \frac{1}{N^{3/2}} \sum_{p,q,r=0}^{N-1} \omega_N^{k(p+q+r)+pr} \\
&\quad \times |p+q+k,p+r,q+r,p,q\rangle. \qquad (15)
\end{aligned}
$$

Finally, I present a proof of the optimality of the above QECC. More precisely, I will show that it is not possible to correct a general quantum error involving exactly one quantum register by encoding each quantum particle by four (or less) quantum registers. Following Sec. V B in Ref. [12] (see also Ref. [21]), I suppose that a single error correcting quantum code with codeword length four exists. Then one can always write

$$
|i_{\text{encode}}\rangle = \sum_{p,q,r,s=0}^{N-1} \alpha_{pqrs}^{(i)} |p,q,r,s\rangle \qquad (16)
$$

for $i=0,1,\ldots,N-1$. Define the reduced density matrices

$$
\rho_{p'q';pq}^{(i)} = \sum_{r,s=0}^{N-1} (\alpha_{p'q'rs}^{(i)})^* \alpha_{pqrs}^{(i)} \qquad (17)
$$

for all i, and

$$
(E_{(i_0,j_0)})_{ij} = \begin{cases} 1 & \text{if } i=i_0 \text{ and } j=j_0, \\ 0 & \text{otherwise.} \end{cases} \qquad (18)
$$

Now we consider the error operators $E_{3,(i_0,j_0)}$ and $E_{4,(i_0,j_0)}$, which act on the third and fourth register, respectively. Suppose $|i_{\text{encode}}\rangle \neq |j_{\text{encode}}\rangle$; then from Eqs. (1), (16), and (17), one arrives at

$$
\rho^{(i)} \rho^{(j)} = 0 \qquad (19)
$$

for all $i \neq j$. Similarly, we consider the actions of $E_{1,(i_0,j_0)}$ and $E_{2,(i_0,j_0)}$ on the encoded registers. Putting $i=j$ in Eq. (1), one arrives at

$$
\rho^{(i)} = \rho^{(j)} \qquad (20)
$$

for all i,j. From Eqs. (19) and (20), one concludes that all the (Hermitian) reduced density matrices $\rho^{(i)}$ are nilpotent. However, this is possible only if $\rho^{(i)}=0$ and hence $\alpha_{pqrs}^{(i)}=0$ for all $i,p,q,r,s=0,1,\ldots,N-1$. This contradicts the assumption that $\sum_{p,q,r,s=0}^{N-1} \alpha_{pqrs}^{(i)} |p,q,r,s\rangle$ encodes the quantum state $|i\rangle$. Thus, the codeword length must be at least five. Consequently, the five quantum register code reported here is optimal.

I would like to thank E. Knill and R. Laflamme for pointing out a mistake in the earlier version of this manuscript, and M. Grassl for pointing out the use of Ref. [12] to prove the optimality of this code. In addition, valuable discussions with M. Ben-Or are gratefully acknowledged.

[1] P. W. Shor, in *Proceedings 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 **54**, 4741 (1996).

[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, Phys. Rev. Lett. **78**, 405 (1997).

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

[10] H. F. Chau, Phys. Rev. A **55**, 839 (1997).

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

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

[13] E. Knill (unpublished).

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

[15] L.-M. Duan and G.-C. Guo (unpublished).

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

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

[18] P. Hoyer (unpublished).

[19] H. F. Chau and F. Wilczek, Phys. Rev. Lett. **75**, 748 (1995).

[20] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).

[21] M. Grassl (private communication).