Permutation-invariant codes encoding more than one qubit

Yingkai Ouyang*
Singapore University of Technology and Design, 8 Somapah Road, Singapore

Joseph Fitzsimons
Singapore University of Technology and Design, 8 Somapah Road, Singapore
and Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore

(Received 9 December 2015; published 26 April 2016)

A permutation-invariant code on m qubits is a subspace of the symmetric subspace of the m qubits. We derive permutation-invariant codes that can encode an increasing amount of quantum information while suppressing leading-order spontaneous decay errors. To prove the result, we use elementary number theory with prior theory on permutation-invariant codes and quantum error correction.

DOI: 10.1103/PhysRevA.93.042340

I. INTRODUCTION

The promise offered by the fields of quantum cryptography [1,2] and quantum computation [3] has fueled recent interest in quantum technologies. To implement such technologies, one needs a way to reliably transmit quantum information, which is inherently fragile and often decoheres because of unwanted physical interactions. If a decoherence-free subspace (DFS) [4] of such interactions were to exist, encoding within it would guarantee the integrity of the quantum information. Indeed, in the case of the spurious exchange couplings [5], the corresponding DFS is just the symmetric subspace of the underlying qubits. In practice, only approximate DFSs are accessible because of small unpredictable perturbations to the dominant physical interaction [6], and using approximate DFSs necessitates a small amount of error correction. When the approximate DFS is the symmetric subspace, permutation-invariant codes can be used to negate the aforementioned errors [7–9]. However, as far as we know, all previous permutation-invariant codes encode only one logical qubit [7–9]. One may then wonder if there exist permutation-invariant codes that can encode strictly more quantum information than a single qubit while retaining some capability to be error corrected.

The first example of a permutation-invariant code which encodes one qubit into 9 qubits while being able to correct any single qubit error was given by Ruskai over a decade ago [7]. A few years later, Ruskai and Pollatshek found 7-qubit permutation-invariant codes encoding a single qubit which correct arbitrary single-qubit errors [8]. Recently permutation-invariant codes encoding a single qubit into $(2t+1)^2$ qubits that correct arbitrary t-qubit errors have been found [9]. Here, we extend the theory of permutation-invariant codes. Our permutation-invariant code $\mathcal{C}$ has as its basis vectors the logical 1 of D distinct permutation invariant codes given by Ref. [9], where each such code encodes only a single qubit. Surprisingly, this simple construction can yield a permutation-invariant code encoding more than a single qubit while correcting spontaneous decay errors to leading order.

Permutation-invariant codes are particularly useful in correcting errors induced by *quantum permutation channels with spontaneous decay errors*, with Kraus decomposition $\mathcal{N}(\rho) = \mathcal{A}(\mathcal{P}(\rho)) = \sum_{\alpha,\beta} A_\beta P_\alpha \rho P_\alpha^\dagger A_\beta$, where $\mathcal{P}$ and $\mathcal{A}$ are quantum channels satisfying the completeness relation $\sum_\alpha P_\alpha^\dagger P_\alpha = \sum_\beta A_\beta^\dagger A_\beta = \mathbb{1}$ and $\mathbb{1}$ is the identity operator on m qubits. The channel $\mathcal{P}$ has each of its Kraus operators P_α proportional to $e^{i\theta_\alpha \hat{a}_\alpha}$, where θ_α is the infinitesimal parameter and the infinitesimal generator $\hat{a}_\alpha$ is any linear combination of exchange operators. By a judicious choice of θ_α and $\hat{a}_\alpha$, the channel $\mathcal{P}$ can model the stochastic reordering and coherent exchange of quantum packets as well as out-of-order delivery of classical packets [10]. The channel $\mathcal{A}$, on the other hand, models spontaneous decay errors, otherwise also known as amplitude damping errors, where an excited state in each qubit independently relaxes to the ground state with probability γ. Our permutation-invariant code is inherently robust against the effects of channel $\mathcal{P}$ and can suppress all errors of order γ introduced by channel $\mathcal{A}$, and is hence approximately robust against the composite noisy permutation channel $\mathcal{N}$.

II. MAIN RESULT

We quantify the error-correction capabilities of our permutation-invariant codes $\mathcal{C}$ with code projector Π beginning from the approximate quantum error-correction criterion of Leung *et al.* [11]. Since the Kraus operators P_α of the permutation channel leave the code space of any permutation-invariant code unchanged, it suffices only to consider the effects of the amplitude-damping channel $\mathcal{A}$. The optimal entanglement fidelity between an adversarially chosen state ρ in the permutation-invariant code space and error-corrected noisy counterpart is just

$$1 - \epsilon = \sup_{\mathcal{R}} \inf_{\rho} \mathcal{F}_e(\rho, \mathcal{R} \circ \mathcal{A}), \qquad (1)$$

where ϵ is the *worst case error* [9] that we need to suppress. Lower bounds for the above quantity can be found using various techniques from the theory of optimal recovery channels [9,12–17], but we restrict our attention to the simpler (but suboptimal) approach of Refs. [9,11]. Suppose that we can find a truncated Kraus set Ω [18] of the channel $\mathcal{A}$ such that for every distinct pair of $A, B \in \Omega$, the spaces $A\mathcal{C}$ and $B\mathcal{C}$ are pairwise orthogonal. Then the truncated recovery map of Leung *et al.* $\mathcal{R}_{\Omega,\mathcal{C}}(\mu) := \sum_{A\in\Omega} \Pi U_A^\dagger \mu U_A \Pi$ is a valid quantum operation, where U_A is the unitary in the polar decomposition of $A\Pi = U_A\sqrt{\Pi A^\dagger A \Pi}$. Since $\mathcal{R}_{\Omega,\mathcal{C}}$ is now

*yingkai_ouyang@sutd.edu.sg

a special instance of a recovery channel in Eq. (1), we trivially get $\epsilon \leqslant 1 - \inf_\rho \mathcal{F}_e(\rho, \mathcal{R}_{\Omega,\mathcal{C}} \circ \mathcal{A})$. As explained in Ref. [9], the analysis of Leung *et al.* [11] allows one to show that

$$\mathcal{F}_e(\rho, \mathcal{R}_{\Omega,\mathcal{C}} \circ \mathcal{A}) \geqslant \sum_{A\in\Omega} \lambda_A, \tag{2}$$

where $\lambda_A = \min_{\substack{|\psi\rangle \in \mathcal{C} \\ \langle\psi|\psi\rangle = 1}} \langle\psi|A^\dagger A|\psi\rangle$ quantifies the worst-case deformation of each corrupted code space $A\mathcal{C}$.

The symmetric subspace of m qubits is central to the study of permutation-invariant codes, and has a convenient choice of basis vectors, namely the *Dicke states* [9,19–21]. A Dicke state of weight w, denoted as $|\mathrm{D}^m_w\rangle$, is a normalized permutation-invariant state on m qubits with a single excitation on w qubits. Our code $\mathcal{C}$ is the span of the logical states $|d_L\rangle$ for $d = 1,\dots,D$, and these states can be written as superposition over Dicke states, with amplitudes proportional to the square root of the binomial distribution. Namely for positive integers n_d and g_d,

$$|d_L\rangle = \sum_{j\in\mathcal{I}_d} \sqrt{\frac{\binom{n_d}{j}}{2^{n_d-1}}}\,|\mathrm{D}^m_{g_d j}\rangle, \tag{3}$$

and the set $\mathcal{I}_d$ comprises the odd integers from 1 to $2\lfloor\frac{n_d-1}{2}\rfloor + 1$. The states $|d_L\rangle, A|d_L\rangle$ can be made to be pairwise orthogonal via a judicious choice of constraints on the positive integer parameters $n_1,\dots,n_D$, $g_1,\dots,g_D$, and m.

We elucidate the case for $D \geqslant 3$ since permutation-invariant codes encoding only one qubit [9] are already known. Here, we require $n_1,\dots,n_D$ to be pairwise coprime integers with $n_1 \leqslant \dots \leqslant n_D$, and define their product to be $N = n_1 \dots n_D$. The length of our code is a polynomial in N, given by $m = N^q$ for any integer $q \geqslant 3$. Moreover, we set $g_d = N/n_d$ so that for distinct d and d', the greatest common divisor of g_d and $g_{d'}$ is precisely $\gcd(g_d,g_{d'}) = N/(n_d n_{d'}) > 1$, so that g_d and $g_{d'}$ are not coprime. Furthermore, we require that $g_d \geqslant 3$, $n_d \geqslant 4$.

The reason for requiring g_d and $g_{d'}$ to not be coprime is that it allows the inner products $\langle d_L|d'_L\rangle$ and $\langle d_L|A^\dagger B|d'_L\rangle$ to be identically zero for distinct d and d' and for any operators A,B acting nontrivially on strictly less than $\frac{\min_d g_d}{2}$ qubits when N is even. To see this, we analyze the linear Diophantine equation

$$x_{d,d'} g_d = y_{d,d'} g_{d'} + s, \tag{4}$$

with $s = 0,\pm 1$. This linear Diophantine equation has a solution $(x_{d,d'}, y_{d,d'})$ if and only if s is a multiple of $\gcd(g_d,g_{d'})$, where $\gcd(a,b)$ denotes the greatest common divisor between integers a and b which is the largest positive integer that divides both a and b. Having $\gcd(g_d,g_{d'}) > 1$ ensures that Eq. (4) has no solution for nonzero s such that $|s| < \gcd(g_d,g_{d'})$. When $s = 0$, integer solutions $(x_{d,d'}, y_{d,d'})$ where $0 < x_{d,d'} g_d = y_{d,d'} g_{d'} < N$ do not exist. To see this, note that the minimum positive solutions of Eq. (4) are precisely $x_{d,d'} = \frac{g_{d'}}{\gcd(g_d,g_{d'})}$ and $y_{d,d'} = \frac{g_d}{\gcd(g_d,g_{d'})}$, and hence we must require that $\frac{g_d g_{d'}}{\gcd(g_d,g_{d'})} < N$ be an invalid inequality. But our construction gives $\frac{g_d g_{d'}}{\gcd(g_d,g_{d'})} = \frac{g_d g_{d'} n_d n_{d'}}{N} = N$. This immediately implies several orthogonality conditions on the states given by Eq. (3) for large n_1.

We use a sequence of large consecutive primes and an even number to construct our sequence of coprimes. We let $n_1 = p_k$, where p_k denotes the kth prime, and let $n_2 = n_1 + 1$. We also let $n_j = p_{k+j-2}$ for all $j = 3,\dots,D$, which gives us our D coprime integers. The length of our code is $m = [(p_k + 1)(p_k \dots p_{k+D-2})]^q$. In the special case when $D = 3$, we can use the existence of twin primes n_1 and n_3 a bounded distance apart [22] (at most 600 apart [23]), and let $n_2 = n_1 + 1$, which yields $m = [n_1 n_3 (n_1 + 1)]^q$.

The oft-used Kraus operators for an amplitude-damping channel on a single qubit are $A_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|$ and $A_1 = \sqrt{\gamma}|0\rangle\langle 1|$ respectively, with γ modeling the probability for a transition from the excited $|1\rangle$ state to the ground state $|0\rangle$. On m qubits, the Kraus operators of the amplitude-damping channel have a tensor product structure, given by $A_{x_1} \otimes \dots \otimes A_{x_m}$, where $x_1,\dots,x_m = 0,1$. We focus our attention on the Kraus operators $K_0 = A_0^{\otimes m}$, and F_j which applies A_1 on the jth qubit and applies A_0 everywhere else for $j = 1,\dots,m$. The choice of Kraus operators for a quantum channel is not unique, and we can equivalently consider a subset of the Kraus operators in a Fourier basis. Namely, for $\ell = 1,\dots,m$, we define $K_\ell = \frac{1}{\sqrt{m}} \sum_{j=1}^m \omega^{(\ell-1)(j-1)} F_j$, where $\omega = e^{2\pi i/m}$. We choose the set of Kraus operators that we wish to correct to be $\Omega = \{K_0, K_1, \dots, K_m\}$.

Now the spaces $A\mathcal{C}$ and $B\mathcal{C}$ are orthogonal for distinct $A,B \in \Omega$. Note that for $\ell,\ell' = 1,\dots,m$,

$$\begin{aligned}
&\langle d_L|K_\ell^\dagger K_{\ell'}|d_L\rangle \\
&\quad= \frac{1}{m}\sum_{j=1}^m\sum_{j'=1}^m \omega^{-(\ell-1)(j-1)+(\ell'-1)(j'-1)}\langle d_L|F_j^\dagger F_{j'}|d_L\rangle \\
&\quad= \sum_{j=1}^m \omega^{(\ell'-\ell)(j-1)}\langle d_L|F_j^\dagger F_j|d_L\rangle \\
&\qquad+ \frac{1}{m}\sum_{d=1}^{m-1}\sum_{j=1}^m \omega^{-(\ell-1)(j-1)+(\ell'-1)(j-1+d)}\langle d_L|F_j^\dagger F_{j+d}|d_L\rangle,
\end{aligned} \tag{5}$$

where the addition in the subscript is performed modulo m. Using the invariance of $\langle d_L|F_j^\dagger F_j|d_L\rangle$ and $\langle d_L|F_j^\dagger F_{j'}|d_L\rangle$ for distinct $j,j' = 1,\dots,m$ along with the identity

$$\sum_{d=1}^{m-1}\sum_{j=1}^m \omega^{-(\ell-1)(j-1)+(\ell'-1)(j-1+d)} = (m\delta_{\ell',1} - 1)m\delta_{\ell,\ell'},$$

one can simplify (5) to get

$$\begin{aligned}
&\langle d_L|K_\ell^\dagger K_{\ell'}|d_L\rangle \\
&\quad= \delta_{\ell,\ell'}(\langle d_L|F_1^\dagger F_1|d_L\rangle + (m\delta_{\ell,1} - 1)\langle d_L|F_1^\dagger F_m|d_L\rangle),
\end{aligned} \tag{6}$$

which completes the proof of the orthogonality of $A\mathcal{C}$ and $B\mathcal{C}$ for distinct $A,B \in \Omega$.

Now we have

$$\begin{aligned}
\langle d_L|K_0^\dagger K_0|d_L\rangle &= \sum_{t\in\mathcal{I}_d} \frac{\binom{n_d}{t}}{2^{n_d-1}}(1-\gamma)^{g_d t}, \\
\langle d_L|F_1^\dagger F_1|d_L\rangle &= \gamma\sum_{t\in\mathcal{I}_d} \frac{\binom{n_d}{t}}{2^{n_d-1}}(1-\gamma)^{g_d t-1}\frac{g_d t}{m}, \\
\langle d_L|F_1^\dagger F_m|d_L\rangle &= \gamma\sum_{t\in\mathcal{I}_d} \frac{\binom{n_d}{t}}{2^{n_d-1}}(1-\gamma)^{g_d t-1}\frac{g_d t(m-g_d t)}{m(m-1)}.
\end{aligned} \tag{7}$$

Using the Taylor series $(1-\gamma)^{g_d t} = 1 - g_d t\gamma + \frac{g_d t(g_d t-1)}{2}\gamma^2 + O(\gamma^3)$ and $(1-\gamma)^{g_d t-1} = 1-(g_d t-1)\gamma + O(\gamma^2)$ with the binomial identities $\sum_{t=0}^{n_d} t\binom{n_d}{t} = 2^{n_d-1}n_d$, $\sum_{t=0}^{n_d} t^2\binom{n_d}{t} = 2^{n_d-2}n_d(n_d+1)$, and $\sum_{t=0}^{n_d} t^3\binom{n_d}{t} = 2^{n_d-3}n_d^2(n_d+3)$ [9,24], we get

$$\begin{aligned}
\langle d_L|K_0^\dagger K_0|d_L\rangle &= 1 - \frac{N}{2}\gamma \\
&\quad + \left(\frac{N^2+Ng_d}{8} - \frac{N}{4}\right)\gamma^2 + O(\gamma^3),\\
\langle d_L|F_1^\dagger F_1|d_L\rangle &= \frac{N}{2m}\gamma - \left(\frac{N^2+Ng_d}{4m} - \frac{N}{2m}\right)\gamma^2 \\
&\quad + O(\gamma^3),\\
\langle d_L|F_1^\dagger F_m|d_L\rangle &= \frac{\left(\frac{N}{2} - \frac{N^2+Ng_d}{4m}\right)}{m-1}\gamma \\
&\quad + \frac{N^3+3N^2g_d}{8m(m-1)}\gamma^2 \\
&\quad - \frac{(N^2+Ng_d)\left(1+\frac{1}{m}\right)-2N}{4(m-1)}\gamma^2 \\
&\quad + O(\gamma^3).
\end{aligned} \tag{8}$$

Now for all $|\psi\rangle \in \mathcal{C}$ where $\langle\psi|\psi\rangle = 1$, we can write $|\psi\rangle = \sum_{d=1}^{D} a_d|d_L\rangle$ such that $\sum_{d=1}^{D}|a_d|^2 = 1 + O(2^{-n_1})$.[1] Hence for all $A \in \Omega$, $\langle\psi|A^\dagger A|\psi\rangle = \sum_{d=1}^{D}|a_d|^2\langle d_L|A^\dagger A|d_L\rangle$, which implies that $\lambda_A \geqslant \min_{d=1,\dots,D}\langle d_L|A^\dagger A|d_L\rangle[1+O(2^{-n_1})]$. This implies that

$$1-\epsilon \geqslant 1 - \frac{Ng_1}{4m}\gamma - \frac{cN^2}{8}\gamma^2 + O(\gamma^3) + O(2^{-n_1}), \tag{9}$$

where

$$c = 1 + \frac{2g_D - g_1}{N} - \frac{2}{N} + \frac{3g_1}{m} + \frac{4g_1}{N}. \tag{10}$$

Since $m = N^q$, $1-\epsilon \geqslant 1 - \frac{1}{4N^{q-2}}\gamma - \frac{cN^2}{8}\gamma^2 + O(\gamma^3) + O(2^{-n_1})$ and for fixed N and large q, the asymptotic error is second order in γ with $\epsilon \sim \frac{c'N^2}{8}\gamma^2 + O(\gamma^3) + O(2^{-n_1})$, where $c' = 1 + \frac{2g_D-g_1}{N} - \frac{2}{N} + \frac{4g_1}{N}$.

III. CONCLUSION

In summary, we have generalized the construction of permutation-invariant codes to enable the encoding of multiple qubits while suppressing leading-order spontaneous decay errors. These permutation-invariant codes might allow for the construction of new schemes in physical systems, such as improved quantum communication along isotropic Heisenberg spin chains [25–28]. Symmetry of error-correction codes have also recently been exploited to symmetrize prover strategies in the context of interactive proofs [29,30], and so the extremely high symmetry of the codes studied here may also have theoretical implications.

ACKNOWLEDGMENTS

This research was supported by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01. Y.O. also acknowledges support from the Ministry of Education, Singapore.

[1]The term $O(2^{-n_1})$ arises because of the slight nonorthogonality of the states $|d_L\rangle$.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 2nd ed. (Cambridge University Press, Cambridge, UK, 2000).

[4] P. Zanardi and M. Rasetti, Noiseless Quantum Codes, Phys. Rev. Lett. **79**, 3306 (1997).

[5] S. Blundell, *Magnetism in Condensed Matter*, Oxford Master Series in Condensed Matter Physics (Oxford University Press, Oxford, 2003).

[6] D. A. Lidar, D. Bacon, and K. B. Whaley, Concatenating Decoherence-Free Subspaces with Quantum Error Correcting Codes, Phys. Rev. Lett. **82**, 4556 (1999).

[7] M. B. Ruskai, Pauli Exchange Errors in Quantum Computation, Phys. Rev. Lett. **85**, 194 (2000).

[8] H. Pollatsek and M. B. Ruskai, Permutationally invariant codes for quantum error correction, Lin. Algebra Appl. **392**, 255 (2004).

[9] Y. Ouyang, Permutation-invariant quantum codes, Phys. Rev. A **90**, 062317 (2014).

[10] V. Paxson, End-to-end internet packet dynamics, SIGCOMM Comput. Commun. Rev. **27**, 139 (1997).

[11] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, Approximate quantum error correction can lead to better codes, Phys. Rev. A **56**, 2567 (1997).

[12] H. Barnum and E. Knill, Reversing quantum dynamics with near-optimal quantum and classical fidelity, J. Math. Phys. **43**, 2097 (2002).

[13] A. S. Fletcher, P. W. Shor, and M. Z. Win, Channel-adapted quantum error correction for the amplitude damping channel, IEEE Trans. Inf. Theory **54**, 5705 (2008).

[14] N. Yamamoto, Exact solution for the max-min quantum error recovery problem, in *Proceedings of the 48th IEEE Conference on Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference, CDC/CCC 2009* (IEEE, Shanghai, 2009), pp. 1433–1438.

[15] J. Tyson, Two-sided bounds on minimum-error quantum measurement, on the reversibility of quantum dynamics, and on maximum overlap using directional iterates, J. Math. Phys. **51**, 92204 (2010).

[16] C. Bény and O. Oreshkov, General Conditions for Approximate Quantum Error Correction and Near-Optimal Recovery Channels, Phys. Rev. Lett. **104**, 120501 (2010).
[17] C. Bény and O. Oreshkov, Approximate simulation of quantum channels, Phys. Rev. A **84**, 022333 (2011).
[18] Y. Ouyang and W. H. Ng, Truncated quantum channel representations for coupled harmonic oscillators, J. Phys. A **46**, 205301 (2013).
[19] M. Bergmann and O. Gühne, Entanglement criteria for Dicke states, J. Phys. A **46**, 385304 (2013).
[20] T. Moroder, P. Hyllus, G. Tóth, C. Schwemmer, A. Niggebaum, S. Gaile, O. Gühne, and H. Weinfurter, Permutationally invariant state reconstruction, New J. Phys. **14**, 105001 (2012).
[21] G. Tóth and O. Gühne, Entanglement and Permutational Symmetry, Phys. Rev. Lett. **102**, 170503 (2009).
[22] Y. Zhang, Bounded gaps between primes, Ann. Math. **179**, 1121 (2014).
[23] J. Maynard, Small gaps between primes, arXiv:1311.4600 (unpublished).
[24] A. Prudnikov, Y. A. Brychkov, and O. Marichev, *Integrals and Series, Vol. 1: Elementary Functions* (Taylor & Francis, London, 1986).
[25] D. Burgarth and S. Bose, Conclusive and arbitrarily perfect quantum-state transfer using parallel spin-chain channels, Phys. Rev. A **71**, 052315 (2005).
[26] D. Burgarth, V. Giovannetti, and S. Bose, Efficient and perfect state transfer in quantum chains, J. Phys. A **38**, 6793 (2005).
[27] D. Burgarth and S. Bose, Perfect quantum state transfer with randomly coupled quantum chains, New J. Phys. **7**, 135 (2005).
[28] K. Shizume, K. Jacobs, D. Burgarth, and S. Bose, Quantum communication via a continuously monitored dual spin chain, Phys. Rev. A **75**, 062328 (2007).
[29] J. Fitzsimons and T. Vidick, A multiprover interactive proof system for the local Hamiltonian problem, in *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science* (ACM, New York, 2015), pp. 103–112.
[30] Z. Ji, Classical verification of quantum proofs, arXiv:1505.07432 (unpublished).