Linear Algebra and its Applications 532 (2017) 43–59

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

# Permutation-invariant qudit codes from polynomials

Yingkai Ouyang [a,b,*]

[a] *Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372, Singapore*
[b] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*

A R T I C L E   I N F O

*Article history:*
Received 8 March 2017
Accepted 21 June 2017
Available online 27 June 2017
Submitted by C.-K. Li

*MSC:*
primary 81P70, 94B25
secondary 05A10, 94B60

*Keywords:*
Quantum coding
Combinatorial codes

A B S T R A C T

A permutation-invariant quantum code on $N$ qudits is any subspace stabilized by the matrix representation of the symmetric group $S_N$ as permutation matrices that permute the underlying $N$ subsystems. When each subsystem is a complex Euclidean space of dimension $q \geq 2$, any permutation-invariant code is a subspace of the symmetric subspace of $(\mathbb{C}^q)^N$. We give an algebraic construction of new families of $d$-dimensional permutation-invariant codes on at least $(2t+1)^2(d-1)$ qudits that can also correct $t$ errors for $d \geq 2$. The construction of our codes relies on a real polynomial with multiple roots at the roots of unity, and a sequence of $q-1$ real polynomials that satisfy some combinatorial constraints. When $N > (2t+1)^2(d-1)$, we prove constructively that an uncountable number of such codes exist.



* Correspondence to: Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372, Singapore.
*E-mail address:* yingkai_ouyang@sutd.edu.sg.

http://dx.doi.org/10.1016/j.laa.2017.06.031

## 1. Introduction

The theory of quantum information and linear algebra is intimately related. The fundamental entities in quantum information theory are quantum states and quantum processes, and they both can be defined in the language of linear algebra. States on physical systems can be represented either as vectors of unit norm or positive semidefinite linear operators of unit trace on a complex Hilbert space, while quantum processes are linear maps from quantum states to quantum states. In this paper, we only need to consider $N$-qudit quantum states with Hilbert space $\mathscr{H} = (\mathbb{C}^q)^{\otimes N}$ with $q \geq 2$, and quantum processes that map $N$-qudit states to $N$-qudit states, where the Hilbert space of a single qudit is $\mathbb{C}^q$. Here, $N$ is the number of qudits in the physical system that we consider. When $q = 2$ and $q = 3$, we say that there are $N$ qubits and $N$ qutrits in the physical system respectively.

In quantum information theory, a quantum state is either a pure state or a probabilistic ensemble of pure states known as a mixed state, with an associated complex Hilbert space $\mathscr{H}$. A pure state is a vector in $\mathscr{H}$ with unit norm; a mixed state is a positive semidefinite operator with unit trace in $L(\mathscr{H})$. In the spectral decomposition of a mixed state $\rho = \sum_i p_i \psi_i \psi_i^*$, its eigenvectors of unit norm $\psi_i$ and eigenvalues $p_i$ correspond to the underlying pure states and their associated probabilities respectively. A quantum state represented as a linear operator is known as a density operator, and we denote the set of all density operators on $\mathscr{H}$ as $\mathfrak{D}(\mathscr{H})$. The set $\mathfrak{D}(\mathscr{H})$ is isomorphic to the set of all positive semi-definite operators in $L(\mathscr{H})$ with unit trace, and this allows one to have a purely linear algebraic interpretation of any quantum state.

In this paper, we represent a quantum process with a quantum channel, which maps a density operator to a density operator. The theory of quantum channels is well-studied, and the characterization of quantum channels as a completely positive and trace-preserving maps dates back to the work of Choi and others. Namely, a linear map $\Phi : L(\mathscr{H}) \to L(\mathscr{H})$ is a quantum channel if and only if it is completely positive and trace-preserving (CPT). It is often convenient to utilize the non-unique Kraus representation of a quantum channel [2,3,5]. Namely, for any quantum channel $\Phi : L(\mathscr{H}) \to L(\mathscr{H})$, there exist linear operators $A_i \in L(\mathscr{H})$ such that for every $\rho \in L(\mathscr{H})$,

$$\Phi(\rho) = \sum_i A_i \rho A_i^*$$

and $\sum_i A_i^* A_i$ is the identity operator on $\mathscr{H}$. The linear operators $A_i$ are known as Kraus operators of $\Phi$.

The theory of quantum error correction is a subfield of quantum information theory where the robustness of certain families of quantum states under certain families of quantum processes is studied. The fundamental object in quantum error correction is the quantum code $\mathscr{C}$, which is a $d$-dimensional subspace of $\mathscr{H}$. A possible goal in quantum error correction can be to find quantum codes $\mathscr{C}$ for a fixed quantum channel $\mathscr{N}$. When there exists a quantum channel $\mathscr{R}$ such that for every density operator $\rho$ supported on $\mathscr{C}$,