This is a repository copy of *Permutation-invariant qudit codes from polynomials*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/198722/

Version: Accepted Version

Permutation-invariant qudit codes from polynomials

Yingkai Ouyang [*]

Singapore University of Technology and Design,
8 Somapah Road, Singapore 487372.
Centre for Quantum Technologies, National University of Singapore
3 Science Drive 2, Singapore 117543.

September 3, 2018

Abstract

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 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.

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 ψ_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 [HK69, HK70, Kra83]. 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 Φ.

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 ρ supported on $\mathscr{C}$,

$$\mathscr{R}(\mathscr{N}(\rho)) = \rho, \tag{1.1}$$

we say that perfect quantum error correction is possible using the quantum code $\mathscr{C}$ with respect to the channel $\mathscr{N}$.

The necessary and sufficient conditions for perfect quantum error correction was originally proved by Knill and Laflamme [KL97]. We now rephrase this foundational result in quantum error correction using the language of linear algebra.

Theorem 1.1 (Knill-Laflamme [KL97])**.** *Let $\mathscr{H}$ be a complex Euclidean space, and let $\mathscr{C}$ be a d-dimensional subspace of $\mathscr{H}$ with orthonormal basis vectors $\psi_1, \ldots, \psi_d$. Let $\mathscr{N}$ be a quantum channel with Kraus operators A_i. Suppose that for all i, j there exist complex numbers $g_{i,j}$ such that the following conditions hold.*

1. *Orthogonality conditions: $\psi_a^* A_i^* A_j \psi_b = 0$ for all $a \neq b$.*

2. *Non-deformation conditions: $\psi_a^* A_i^* A_j \psi_a = g_{i,j}$ for all $a = 1, \ldots, d$.*

Then for every density operator ρ supported on $\mathscr{C}$, there exists a quantum channel $\mathscr{R}$ such that $\mathscr{R}(\mathscr{N}(\rho)) = \rho$. Moreover, $\mathscr{R}(\rho) = \sum_i R_i \rho R_i^*$ where $R_i = PU_i^*$ where $P = \sum_a \psi_a \psi_a^*$ is the projector onto $\mathscr{C}$, and U_i is the unitary in the polar decomposition of $A_i P = U_i \sqrt{P A_i^* A_i P}$.

Because of the tensor product structure of $\mathscr{H} = (\mathbb{C}_q)^{\otimes N}$, any linear operator $A \in L(\mathscr{H})$ admits the decomposition $A = \sum_j A_{j,1} \otimes \cdots \otimes A_{j,N}$. Let $I_q \in L(\mathbb{C}^q)$ denote a size q identity matrix. Then, using the decomposition of A, we can calculate the weight of A, which we define as

$$\mathrm{wt}(A) = N - \max_{S \subseteq \{1,\ldots,N\}} \{|S| : A_{j,k} = I_q\}.$$

The weight of A is the number of qudits on which A acts non-trivially. When the weight of every Kraus operator of a quantum channel is zero, the quantum channel is the identity channel. We say that a quantum channel introduces t errors if (1) the quantum channel can have Kraus operators with maximum weight t and (2) the quantum channel cannot have Kraus operators with maximum weight strictly less than t. The quantum code $\mathscr{C}$ corrects t errors if perfect quantum error correction is possible for the quantum code $\mathscr{C}$ with respect to all quantum channels that introduce up to t errors. The distance of a quantum code $\mathscr{C}$ with

basis vectors $\psi_1, \ldots, \psi_d$ is the smallest integer D, such that for every linear operator $A \in L(\mathcal{H})$ with weight strictly less than D, we have (i) $\psi_a^* A \psi_b = 0$ for all $a \neq b$ and (ii) $\psi_1^* A \psi_1 = \cdots = \psi_d^* A \psi_d$. To show that a quantum code corrects t errors, it suffices to show that the quantum code has a distance of at least $2t + 1$.

In this paper, we are interested in quantum codes that not only correct t errors, but are also invariant under the permutation of any of the underlying subsystems. To make precise this notion of permutation-invariance, note that $\mathcal{H} = (\mathbb{C}^q)^{\otimes N}$ has a tensor product structure, and its standard basis vectors are

$$\mathbf{e}_{a_1} \otimes \cdots \otimes \mathbf{e}_{a_N},$$

where $a_j = 1, \ldots, q$ for all $j = 1, \ldots, N$. and $\mathbf{e}_1, \ldots, \mathbf{e}_q$ are standard basis column vectors of $\mathbb{C}^q$. Consider a representation $\varphi : S_N \to L(\mathcal{H})$ of the symmetric group S_N such that for all $P \in S_N$,

$$\varphi(P)(\mathbf{e}_{a_1} \otimes \cdots \otimes \mathbf{e}_{a_N}) = \mathbf{e}_{P(a_1)} \otimes \cdots \otimes \mathbf{e}_{P(a_N)}. \tag{1.2}$$

A quantum code $\mathscr{C}$ is permutation-invariant if for every $P \in S_N$ and every $\psi \in \mathscr{C}$,

$$\varphi(P)\psi = \psi. \tag{1.3}$$

The stabilizer of a quantum code $\mathscr{C}$ is the maximal subset $S \subseteq L(\mathcal{H})$ such that for all $\sigma \in S$ and $\psi \in \mathscr{C}$, we have $\sigma\psi = \psi$. Additive quantum codes are the quantum codes for which their stabilizer is abelian. Since S_N is non-abelian for $N \geq 3$, permutation-invariant quantum codes are necessarily non-additive codes for $N \geq 3$. The theory of additive quantum codes has benefited much from its one-to-one correspondence to theory of finite fields [CRSS98, Rai99], but such a direct connection is unlikely to exist in the case of non-additive quantum codes such as permutation-invariant quantum codes.

In this paper, we give an algebraic construction of new families of of d-dimensional permutation-invariant codes on at least $(2t + 1)^2(d - 1)$ qudits that can also correct t errors, for any $q \geq 2$. Our codes are also non-additive and non-binary quantum codes, and their construction relies on a real polynomial $f(x)$ with multiple roots at the roots of unity, and a sequence of $q - 1$ real polynomials $p_1(z), \ldots, p_q(z)$ that satisfy some combinatorial constraints. When $N > (2t + 1)^2(d - 1)$, we prove constructively that an uncountable number of such codes exist.

The physical motivation of permutation-invariant codes arises from the complete immunity of quantum information stored in such codes from numerous physical processes that arise for example in many electron systems [Ouy14, Rus00]. Such physical processes can be described with *quantum permutation channels*, where every Kraus operator of such channels is a power series of a linear combination of $\varphi(P)$ for $P \in S_N$ [OF16]. When the quantum channel afflicting the physical system can be written as the composition of a quantum permutation channel with a quantum channel that introduces t errors, the effective quantum channel is just a quantum channel that introduces t errors. It is in this case that permutation-invariant codes [Rus00, PR04, Ouy14, OF16] are the most natural candidates to encode quantum information.

The outline of this rest of this paper is as follows. In Section 2, we introduce terminology related to ordered partitions, permutation-invariant sets, Dicke states, and quantum error correction. In Section 3, we introduce a few lemmas that relate generating functions to some combinatorial identities. In Section 4, we prove that the trace of a particular rank one projector on the symmetric subspace with a linear operator can be interpreted as a polynomial. In Section 5, we explain how the coefficients of the polynomial $f(x) = \sum_{z=0}^n f_z x^z$ and the values of the polynomials $p_1(z), \ldots, p_q(z)$ for $z = 0, \ldots, n$ relate to our code construction in Theorem 5.1 which constructs permutation-invariant codes encoding a single qubit and Theorem 5.2 which constructs permutation-invariant codes encoding a d-level system. Explicit examples of permutation-invariant codes that follow from these two theorems are supplied in Section 6. In Section 5 we also prove that there is an uncountable number of permutation-invariant quantum codes that correct t errors whenever $N > (2t + 1)^2(d - 1)$ in Theorem 6.7. In Section 7, we make comparisons of our code construction with prior permutation-invariant quantum codes. In Section 8, we give some concluding remarks.

3

2 Preliminaries

2.1 The Dirac bra-ket notation

Let $\mathscr{H}$ be a finite dimension complex Euclidean space. Every vector $\phi \in \mathscr{H}$ can be written in the Dirac bra-ket notation as $|\phi\rangle$, which is called a *ket*. The adjoint of ϕ is denoted in the Dirac bra-ket notation is $\langle\phi|$, and is called a *bra*. In this paper, in accordance with existing convention in quantum information theory, we use the Dirac bra-ket notation to denote the basis vectors of our permutation-invariant code, and also the basis vectors of the permutation-invariant space of $(\mathbb{C}^q)^{\otimes N}$.

2.2 Ordered partitions and permutation-invariant sets

Let $\mathbb{N} = \{0, 1, \dots, \}$ denote the set of the non-negative integers. We say that a vector $\mathbf{n} = (n_1, \dots, n_q)$ is an *ordered partition* of a positive integer N into q parts if $n_1, \dots, n_q \in \mathbb{N}$ and $n_1 + \cdots + n_q = N$. Here, n_i counts the number of i's that appears in the integer partition of N. We denote the set of ordered partitions of N into q parts as $T_{N,q}$.

For every N-tuple $\mathbf{c} = (c_1, \dots, c_N) \in \{1, \dots, q\}^N$ and $k \in \mathbb{N}$, let $\mathrm{wt}_k(\mathbf{c}) = |\{i : c_i = k\}|$ count the number of components of $\mathbf{c}$ that are equal to k, and let $\vec{\mathrm{wt}}_q(\mathbf{c}) = (\mathrm{wt}_1(\mathbf{c}), \dots, \mathrm{wt}_q(\mathbf{c}))$. We denote the multinomial coefficient that counts the number of N-tuples $\mathbf{c}$ in $\{1, \dots, q\}^N$ for which $\vec{\mathrm{wt}}_q(\mathbf{c}) = (n_1, \dots, n_q)$ as

$$\binom{N}{\mathbf{n}} = \frac{N!}{n_1! \dots n_q!}.$$

For every ordered partition $\mathbf{n}$ of N into q parts, we define the permutation-invariant set of type $\mathbf{n}$ as

$$C_{\mathbf{n}} = \{\mathbf{c} \in \{1, \dots, q\}^N : \vec{\mathrm{wt}}_q(\mathbf{c}) = \mathbf{n})\}.$$

Given N-tuples $\mathbf{x}, \mathbf{y} \in \mathbb{N}^N$, we denote the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ as

$$d_H(\mathbf{x}, \mathbf{y}) = |\{1 \le i \le N : x_i \ne y_i\}|.$$

Given that $\mathbf{n}$ and $\mathbf{u}$ are ordered partitions of N into q parts, we correspondingly denote the minimum Hamming distance between the elements of $C_{\mathbf{n}}$ and the elements of $C_{\mathbf{u}}$ as

$$\Delta(\mathbf{n}, \mathbf{u}) = \min\{d_H(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C_{\mathbf{n}}, \mathbf{y} \in C_{\mathbf{u}}\}. \tag{2.1}$$

For all subsets T of all ordered partitions $T \subset T_{N,q}$, we denote

$$\Delta(T) = \min\{\Delta(\mathbf{n}, \mathbf{u}) : \mathbf{n}, \mathbf{u} \in T, \mathbf{n} \ne \mathbf{u}\} \tag{2.2}$$

as the minimum distance between the distinct permutation-invariant sets induced by T.

2.3 Dicke states

The permutation-invariant codes of this paper are expressed as linear combinations of Dicke states, which we proceed to describe. Given any ordered partition $\mathbf{n} \in T_{N,q}$, we use the Dirac bra-ket notation to denote the Dicke state of type $\mathbf{n}$ and the unnormalized Dicke state of type $\mathbf{n}$ respectively as

$$
\begin{aligned}
|D_{\mathbf{n}}\rangle &= \sqrt{|C_{\mathbf{n}}|^{-1}} \sum_{\mathbf{c}=(c_1,\dots,c_N)\in C_{\mathbf{n}}} \mathbf{e}_{c_1} \otimes \cdots \otimes \mathbf{e}_{c_N} \\
&= \frac{1}{\sqrt{\binom{N}{\mathbf{n}}}} \sum_{\mathbf{c}=(c_1,\dots,c_N)\in C_{\mathbf{n}}} \mathbf{e}_{c_1} \otimes \cdots \otimes \mathbf{e}_{c_N},
\end{aligned}
\tag{2.3}
$$

and

$$|H_{\mathbf{n}}\rangle = \sum_{\mathbf{c}=(c_1,\dots,c_N)\in C_{\mathbf{n}}} \mathbf{e}_{c_1} \otimes \cdots \otimes \mathbf{e}_{c_N}. \tag{2.4}$$

The set of Dicke states $\{|D_{\mathbf{n}}\rangle : \mathbf{n} \in T_{N,q}\}$ is an orthonormal basis of the symmetric subspace of N qudits. This means that any permutation-invariant quantum state is a linear combination of these Dicke states $|D_{\mathbf{n}}\rangle$. When each qudit has a dimension of q, the dimension of the symmetric subspace of N qudits is $\binom{N+q-1}{q-1}$, which is the number of ways to assign q colors to N unordered balls.

3   The generating function $f(x)$

We give a summation identity that is related to the coefficients of the polynomial $f(x) = \sum_{z=0}^{n} f_z x^z$ by interpreting $f(x)$ as an appropriate generating function in the following lemma.

Lemma 3.1. *Let $\omega = e^{2\pi i/d}$ where d is a positive integer and $d \geq 2$. Let m be a positive integer, $g(x)$ be a polynomial of degree γ, and $n = \gamma + m(d-1)$. Let $f(x) = (1+x+\cdots+x^{d-1})^m g(x) = \sum_{z=0}^{n} f_z x^z$. Then for every $k = 1,\dots,d-1$,*

$$\sum_{z=0}^{n} f_z \omega^{kz} = f_0 + f_1 \omega^k + \cdots + f_n \omega^{kn} = 0. \tag{3.1}$$

Moreover for every $c = 1,\dots,m-1$ and $k = 1,\dots,d-1$,

$$\sum_{z=0}^{n} f_z \omega^{kz} z^c = f_1 \omega^k 1^c + \cdots + f_n \omega^{kn} n^c = 0. \tag{3.2}$$

Proof. Since the polynomial $(1+x+\cdots+x^{d-1})$ is equal to zero for every $x = \omega,\dots,\omega^{d-1}$, the polynomial $f(x)$ also evaluates to zero for every $x = \omega,\dots,\omega^{d-1}$.

Let $(z)_j = \Pi_{k=1}^{j}(z-k+1)$ denote a falling factorial where z is any real number and j is any non-negative integer. The j-th derivative of $f(x)$ for every $j = 1,\dots,m-1$ is

$$\frac{d^j}{dx^j} f(x) = \frac{d^j}{dx^j} \sum_{z=0}^{n} f_z x^z = \sum_{z=0}^{n} f_z (z)_j x^{z-j}, \tag{3.3}$$

and there exists some polynomial $h(x)$ such that

$$\frac{d^j}{dx^j} f(x) = (1+x+\cdots+x^{d-1})h(x). \tag{3.4}$$

Hence (3.4) implies that $\omega^{kj} \frac{d^j}{dx^j} f(x)$ also evaluates to zero for $x = \omega^k$ for every $k = 1,\dots,d-1$. Hence

$$0 = \omega^{kj} \sum_{z=0}^{n} f_z (z)_j \omega^{k(z-j)} = \sum_{z=0}^{n} f_z (z)_j \omega^{kz}. \tag{3.5}$$

For every positive integer c and j, let $S(c,j)$ denote the Stirling number of the second kind [vLW01] which counts the number of ways to partition the integer c into exactly j parts. The monomial z^c is a linear combination of the falling factorials $(z)_j$ given by $z^c = \sum_{j=0}^{c} S(c,j)(z)_j$, where $(z)_0 = 1$. Hence

$$\sum_{z=0}^{n} f_z z^c \omega^{kz} = \sum_{z=0}^{n} f_z \sum_{j=0}^{c} S(c,j)(z)_j \omega^{kz}$$

$$= \sum_{j=0}^{c} S(c,j) \sum_{z=0}^{n} f_z (z)_j \omega^{kz}.$$

Hence $0 = f(\omega^k) = \sum_{z=0}^{n} f_z \omega^{kz}$ for every $k = 1,\dots,d-1$, and this proves (3.2). □

5

Lmma 3.1 immediately implies the following identity.

Lemma 3.2. *Let m be a positive integer, $g(x)$ be a polynomial of degree γ, and $n = \gamma + m(d-1)$. Let $f(x) = (1-x)^m g(x) = \sum_{z=0}^n f_z x^z$. Then $f_0 + \cdots + f_n = 0$, and for every $c = 1, \ldots, m-1$, we also have*

$$\sum_{z=0}^n f_z z^c = f_1 1^c + \cdots + f_n n^c = 0.$$

Proof. Let $h(x) = f(-x)$ and $h_z = f_z(-1)^z$. Then

$$f(-x) = (1+x)^m g(-x) = \sum_{z=0}^n f_z x^z (-1)^z = \sum_{z=0}^n h_z x^z = h(x).$$

Since $h(x) = (1+x)^m g(-x)$ and $g(-x)$ is just a polynomial in x, Lemma 3.1 implies that for all $c = 0, \ldots, m-1$, we have $\sum_{z=0}^n h_z(-1)^z z^c = 0$. Making the substitution $h_z = f_z(-1)^z$, we get $\sum_{z=0}^n f_z z^c = 0$, we prove the lemma. $\qquad\square$

We emphasize that in Lemma 3.2, the coefficient f_z multiplies with a monomial in z instead of an exponential in z and hence the summation is not a power series. We give some examples of polynomials $f(x)$ for which Lemma 3.2 applies.

1. When $f(x) = (x-1)^5$, we have $f_5 = 1, f_4 = -5, f_3 = 10, f_2 = -10, f_1 = 5, f_0 = -1$. For every $j \in \{0,1,2,3,4\}$ we have

$$(-1)0^j + (5)1^j + (-10)2^j + (10)3^j + (-5)4^j + (1)5^j = 0.$$

2. When $f(x) = (1+x)(x-1)^5$, we have $f_6 = 1, f_5 = -4, f_4 = 5, f_3 = 0, f_2 = -5, f_1 = 4, f_0 = -1$. It is easy to verify that for every $j \in \{0,1,2,3,4\}$ we have

$$(-1)0^j + (4)1^j + (-5)2^j + (5)4^j + (-4)5^j + (1)6^j = 0.$$

4 From Dicke states to polynomials

Here we prove that the trace of a particular rank one projector on the symmetric subspace with a linear operator can be interpreted as a polynomial. In particular, given that $\mathbf{p}(z)$ is a tuple of polynomials, $\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(z)}\rangle$ is always a polynomial in z for every operator P in $L((\mathbb{C}^q)^{\otimes N})$.

Lemma 4.1. *Let $\mathbf{p}(z) = (p_1(z), \ldots, p_q(z))$ be an ordered partition of the positive integer N for all $z = 0, \ldots, q-1$ and $p_1(z), \ldots, p_q(z)$ are polynomials of degree at most θ. Then for every matrix $P \in L((\mathbb{C}^q)^{\otimes N})$ of weight w, $\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(z)}\rangle$ is a polynomial of degree at most $w\theta$ in the variable z.*

Proof. Without loss of generality, the permutation-invariance of the Dicke states $|D_{\mathbf{p}(z)}\rangle$ allows us to consider $P = E \otimes I_{w+1,\ldots,N}$ that operates non-trivially on the first w qudits, where $I_{w+1,\ldots,N}$ is an identity matrix on the last $N-w$ qudits. Recall that $T_{N,q}$ denotes the set of all ordered partitions of N into q parts. From the Vandermonde decomposition we have

$$|H_{\mathbf{p}(z)}\rangle = \sum_{\substack{\mathbf{a} \in T_{w,q} \\ \mathbf{b} \in T_{N-w,q} \\ \mathbf{a}+\mathbf{b}=\mathbf{p}(z)}} |H_{\mathbf{a}}\rangle \otimes |H_{\mathbf{b}}\rangle, \tag{4.1}$$

6

where $|H_\mathbf{a}\rangle$ and $|H_\mathbf{b}\rangle$ are unnormalized Dicke states on w qudits and $N - w$ qudits respectively.

$$\langle H_{\mathbf{p}(z)}|P|H_{\mathbf{p}(z)}\rangle = \sum_{\substack{\mathbf{a},\mathbf{a}'\in T_{w,q} \\ \mathbf{b},\mathbf{b}'\in T_{N-w,q} \\ \mathbf{a}+\mathbf{b}=\mathbf{p}(z) \\ \mathbf{a}'+\mathbf{b}'=\mathbf{p}(z)}} \langle H_{\mathbf{a}'}|E|H_\mathbf{a}\rangle\langle H_{\mathbf{b}'}|H_\mathbf{b}\rangle. \tag{4.2}$$

Since $\langle H_{\mathbf{b}'}|H_\mathbf{b}\rangle = 0$ whenever $\mathbf{b} \neq \mathbf{b}'$, the above can be rewritten as

$$\langle H_{\mathbf{p}(z)}|P|H_{\mathbf{p}(z)}\rangle = \sum_{\substack{\mathbf{a}\in T_{w,q} \\ \mathbf{b}\in T_{N-w,q} \\ \mathbf{a}+\mathbf{b}=\mathbf{p}(z)}} \langle H_\mathbf{a}|E|H_\mathbf{a}\rangle\langle H_\mathbf{b}|H_\mathbf{b}\rangle. \tag{4.3}$$

Hence

$$\begin{aligned}
\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(z)}\rangle &= \langle H_{\mathbf{p}(z)}|P|H_{\mathbf{p}(z)}\rangle \binom{N}{\mathbf{p}(z)}^{-1} \\
&= \sum_{\substack{\mathbf{a}\in T_{w,q} \\ \mathbf{p}(z)-\mathbf{a}\in T_{N-w,q}}} \langle H_\mathbf{a}|E|H_\mathbf{a}\rangle \binom{N-w}{\mathbf{p}(z)-\mathbf{a}}\binom{N}{\mathbf{p}(z)}^{-1}.
\end{aligned} \tag{4.4}$$

Since $\langle H_\mathbf{a}|E|H_\mathbf{a}\rangle$ is independent of the variable z, it suffices to show that every $\binom{N-w}{\mathbf{p}(z)-\mathbf{a}}\binom{N}{\mathbf{p}(z)}^{-1}$ in (4.4) is a polynomial of order at most $w\theta$ in the variable z.

For every $\mathbf{a} \in T_{w,q}$ and $\mathbf{p}(z) \in T_{N,q}$ such that $\mathbf{p}(z) - \mathbf{a} \in T_{N-w,q}$, we have

$$\begin{aligned}
\binom{N-w}{\mathbf{p}(z)-\mathbf{a}}\binom{N}{\mathbf{p}(z)}^{-1} &= \frac{(N-w)!}{(p_1(z)-a_1)!\dots(p_q(z)-a_q)!}\frac{(p_1(z))!\dots(p_q(z))!}{N!} \\
&= \frac{(p_1(z))_{a_1}\dots(p_q(z))_{a_q}}{(N)_w}.
\end{aligned} \tag{4.5}$$

Since each $p_j(z)$ is a polynomial of order at most θ, it follows that $\binom{N-w}{\mathbf{p}(z)-\mathbf{a}}\binom{N}{\mathbf{p}(z)}^{-1}$ is a polynomial of order at most $w\theta$ in the variable z. $\qquad\square$

5 Polynomial constructions of permutation-invariant codes

We provide two separate constructions of permutation-invariant codes that correct t errors. In the first construction, we restrict our attention to permutation-invariant codes that encode a single qubit into N qudits, with each qudit a q-level system. The construction relies only on the properties of the following polynomials.

1. A degree n polynomial $f(x)$ with real coefficients that has a root at $x = 1$ with multiplicity at least $2t + 1$.

2. A tuple of polynomials $(p_1(z),\dots,p_q(z))$ that is an ordered partition of N into q parts for every $z = 0,\dots,n$.

As long as the permutation-invariant sets induced by the ordered partitions $(p_1(z),\dots,p_q(z))$ are separated by a minimum distance of at least $2t + 1$, we can construct permutation-invariant codes on N qudits using these polynomials as given in the following theorem.

Theorem 5.1. *Let $f(x) = (x-1)^m g(x) = \sum_{z=0}^n f_z x^z$ be a polynomial of degree n, where $g(x)$ is a polynomial with real coefficients. Let $p_1(z), \ldots, p_q(z)$ be polynomials such that for all $z = 0, \ldots, n$, $\mathbf{p}(z) = (p_1(z), \ldots, p_q(z))$ is an ordered partition of the positive integer N. Let the logical zero and the logical one be given respectively by the states*

$$|0_L\rangle = \sqrt{2}(|f_0| + \cdots + |f_n|)^{-1/2} \sum_{\substack{z=0,\ldots,n \\ f_z > 0}} \sqrt{f_z} |D_{\mathbf{p}(z)}\rangle,$$

$$|1_L\rangle = \sqrt{2}(|f_0| + \cdots + |f_n|)^{-1/2} \sum_{\substack{z=0,\ldots,n \\ f_z < 0}} \sqrt{-f_z} |D_{\mathbf{p}(z)}\rangle. \tag{5.1}$$

Suppose that $\Delta(\{\mathbf{p}(z) : z = 0, \ldots, n\}) \geq 2t + 1$ and that the degree of the polynomials $p_1(z), \ldots, p_q(z)$ is at most $\frac{m-1}{2t}$, where t is a positive integer. Then $\{|0_L\rangle, |1_L\rangle\}$ is an orthonormal basis and spans a code that corrects t errrors.

Theorem 5.1 can be seen as a consequence of the Knill-Laflamme error correction criterion in Theorem 1.1 and the Lemmas 3.1 and Lemma 4.1. In its proof, the orthogonality condition of Theorem 1.1 is trivially satisfied, and the non-deformation condition of Theorem 1.1 holds because of the aforementioned lemmas.

Proof of Theorem 5.1. Since $P \in L((\mathbb{C}^q)^{\otimes N})$ operates non-trivially on at most $2t$ qudits and the codes $C_{\mathbf{p}(z)}$ have a mutual minimum distance of at least $2t + 1$, the orthogonality condition of Theorem 1.1 holds.

To show that the non-deformation conditions of Theorem 1.1 hold, it suffices to show that

$$\langle 0_L | P | 0_L \rangle = \sqrt{2}(|f_0| + \cdots + |f_n|)^{-1} \sum_{\substack{z=0,\ldots,n \\ f_z > 0}} f_z \langle |D_{\mathbf{p}(z)} | P | D_{\mathbf{p}(z)} \rangle, \tag{5.2}$$

and

$$\langle 1_L | P | 1_L \rangle = \sqrt{2}(|f_0| + \cdots + |f_n|)^{-1} \sum_{\substack{z=0,\ldots,n \\ f_z < 0}} -f_z \langle |D_{\mathbf{p}(z)} | P | D_{\mathbf{p}(z)} \rangle. \tag{5.3}$$

Now

$$\langle 0_L | P | 0_L \rangle - \langle 1_L | P | 1_L \rangle = \sqrt{2} \sum_{z=0,\ldots,n} f_z \langle D_{\mathbf{p}(z)} | P | D_{\mathbf{p}(z)} \rangle. \tag{5.4}$$

Lemma 4.1 implies that the polynomials $\langle D_{\mathbf{p}(z)} | P | D_{\mathbf{p}(z)} \rangle$ have degree no more than $2t\theta$ in the variable z. Hence for some constants $\alpha_c \in \mathbb{C}$

$$\sum_{z=0}^n f_z \langle D_{\mathbf{p}(z)} | P | D_{\mathbf{p}(z)} \rangle = \sum_{z=0}^n f_z \sum_{c=0}^{2t\theta} \alpha_c z^c$$

$$= \sum_{c=0}^{2t\theta} \alpha_c \left(\sum_{z=0}^n f_z z^c \right). \tag{5.5}$$

The bracketed term above is zero because of Lemma 4.1. Hence $\langle 0_L | P | 0_L \rangle = \langle 1_L | P | 1_L \rangle$ for every $P \in L((\mathbb{C}^q)^{\otimes N})$ that operates non-trivially on at most $2t$ qudits. This proves that the non-deformation condition of Theorem 1.1 holds.

Taking P to be the identity operator then implies that $\langle 0_L | 0_L \rangle = \langle 1_L | 1_L \rangle$ which proves that $|0_L\rangle$ and $|1_L\rangle$ both have unit norm. Since $|0_L\rangle$ and $|1_L\rangle$ are trivially orthogonal, $\{|0_L\rangle, |1_L\rangle\}$ is an orthonormal basis. $\square$

In the second construction, we construct permutation-invariant codes that encode a d-level system into N qudits. We rely on the properties of the following polynomials.

1. A degree n polynomial $f(x)$ with non-negative coefficients that divides $(1+x+\cdots+x^{d-1})^{2t+1}$ to yield a polynomial.

2. A tuple of polynomials $(p_1(z),\ldots,p_q(z))$ that is an ordered partition of N into q parts for every $z = 0,\ldots,n$.

Theorem 5.2. *Let $f(x) = (1+x+\cdots+x^{d-1})^m g(x)$ be a polynomial of degree n such that $f(x)$ has non-negative coefficients. Let $p_1(z),\ldots,p_q(z)$ be polynomials such that for all $z = 0,\ldots,n$, $\mathbf{p}(z) = (p_1(z),\ldots,p_q(z))$ is an ordered partition of the positive integer N. For $k = 0,\ldots,d-1$, let*

$$|k_L\rangle = \sqrt{d}(f_0+\cdots+f_n)^{-1/2} \sum_{\substack{z=0,\ldots,n \\ (z-k)/d\in\mathbb{N}}} \sqrt{f_z}|D_{\mathbf{p}(z)}\rangle. \tag{5.6}$$

Suppose that $\Delta(\{\mathbf{p}(z) : z = 0,\ldots,n\}) \geq 2t+1$ and that the degree of the polynomials $p_1(z),\ldots,p_q(z)$ is at most $\frac{m-1}{2t}$, where t is a positive integer. Then $\{|k_L\rangle : k = 0,\ldots,d-1\}$ is an orthonormal basis and spans a code that corrects t errrors.

The proof of Theorem 5.2 is similar to the proof of Theorem 5.1, which uses Theorem 1.1 with the Lemmas 3.2 and Lemma 4.1. In this proof, the orthogonality condition of Theorem 1.1 is no longer trivially satisfied and relies on the aforementioned lemmas. The non-deformation condition of Theorem 1.1 on the other hand is satisfied trivially.

Proof of Theorem 5.2. Using the Dirac bra-ket notation, we denote the discrete Fourier transform of the vectors $|k_L\rangle$ as

$$|\tilde{k}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^j|j_L\rangle = (f_0+\cdots+f_n)^{-1/2}\sum_{z=0}^{n}\omega^{kz}\sqrt{f_z}|D_{\mathbf{p}(z)}\rangle. \tag{5.7}$$

To show that $\{|k_L\rangle : k = 0,\ldots,d-1\}$ is an orthonormal basis, it suffices to prove that $\{|\tilde{k}\rangle : k = 0,\ldots,d-1\}$ is an orthonormal basis since the Fourier transform is a unitary transformation. Clearly $|\tilde{k}\rangle$ has unit norm for all $k = 0,\ldots,d-1$. Hence it remains to demonstrate that $|\tilde{j}\rangle$ and $|\tilde{k}\rangle$ are orthogonal for distinct j and k. It suffices then to show that the more general orthogonality condition $\langle\tilde{k}|P|\tilde{j}\rangle = 0$ of Theorem 1.1 holds whenever P is an N qudit operator that acts non-trivially on at most $2t$ qudits. Note that

$$\langle\tilde{k}|P|\tilde{j}\rangle = (f_0+\cdots+f_n)^{-1}\sum_{z=0}^{n}\sum_{y=0}^{n}\omega^{-kz+jy}\sqrt{f_z f_y}\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(y)}\rangle. \tag{5.8}$$

Since P has a weight of at most $2t$, Dicke states of distinct types do not overlap under P, and

$$\langle\tilde{k}|P|\tilde{j}\rangle = (f_0+\cdots+f_n)^{-1}\sum_{z=0}^{n}\omega^{(j-k)z}f_z\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(z)}\rangle. \tag{5.9}$$

Since $\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(z)}\rangle$ is a low order polynomial, the combinatorial identity in Lemma 3.1 implies that $\langle\tilde{k}|P|\tilde{j}\rangle = 0$ whenever $j \neq k$, which is the orthogonality condition of Theorem 1.1. The non-deformation condition of Theorem 1.1 holds trivially because for every $k = 0,\ldots,d-1$,

$$\langle\tilde{k}|P|\tilde{k}\rangle = (f_0+\cdots+f_n)^{-1}\sum_{z=0}^{n}f_z\langle D_{\mathbf{p}(z)}|P|D_{\mathbf{p}(z)}\rangle. \tag{5.10}$$

$\square$

6 Examples of permutation-invariant codes

We now supply a few examples of permutation-invariant codes where the weight distribution for the Dicke states for the permutation-invariant code is linearly shifted, and the square of the amplitudes do not follow the binomial distribution.

Example 6.1. With the construction of Theorem 5.1, $N = 19$ qubits are used with the polynomial $f(x) = (1+x)(x-1)^5$ and the tuple of polynomials $\mathbf{p}(z) = (N-1-3z, 1+3z)$ to obtain a permutation-invariant code encoding one qubit that corrects one arbitrary error. The orthonormal basis vectors are

$$|0_L\rangle = \frac{\sqrt{4}|D_{(15,4)}\rangle + \sqrt{5}|D_{(6,13)}\rangle + |D_{(0,19)}\rangle}{\sqrt{10}}, \quad |1_L\rangle = \frac{|D_{(18,1)}\rangle + \sqrt{5}|D_{(12,7)}\rangle + \sqrt{4}|D_{(3,16)}\rangle}{\sqrt{10}}.$$

Example 6.2. With the construction of Theorem 5.1, $N = 108$ qutrits are used with the polynomial $f(x) = (1+x)(x-1)^5$ and the tuple of polynomials $\mathbf{p}(z) = (N-3z^2, 3z^2, 0)$ to obtain a permutation-invariant code encoding one qubit that corrects one arbitrary error. The orthonormal basis vectors are

$$|0_L\rangle = \frac{\sqrt{4}|D_{(105,3,0)}\rangle + \sqrt{5}|D_{(60,48,0)}\rangle + |D_{(0,108,0)}\rangle}{\sqrt{10}}$$

$$|1_L\rangle = \frac{|D_{(108,0,0)}\rangle + \sqrt{5}|D_{(96,12,0)}\rangle + \sqrt{4}|D_{(33,75,0)}]\rangle}{\sqrt{10}}.$$

Example 6.3. Let $N = (2t+1)^2(d-1)$, $f(x) = (1+x+\cdots+x^{d-1})^{2t+1} = \sum_{z=0}^{(2t+1)(d-1)} f_z x^z$, $p_1(z) = (2t+1)z$, $p_2(z) = N - p_1(z)$, and $p_3(z), \ldots, p_q(z) = 0$. The construction of Theorem 5.2 yields an N-qudit permutation invariant code that encodes a d-level system into $(2t+1)^2(d-1)$ qudits and can correct t errors. The orthonormal basis vectors are $\{|k_L\rangle, k = 0, \ldots, d-1\}$ where

$$|k_L\rangle = \sqrt{d^{-m+1}} \sum_{\substack{z=0,\ldots,(2t+1)(d-1) \\ (z-k)/d\in\mathbb{N}}} \sqrt{f_z}|D_{\mathbf{p}(z)}\rangle.$$

We now give examples of permutation-invariant codes on qubits that correct a single error while encoding a 3-level system, a 4-level system and a 5-level system that are all based on Example 6.3.

Example 6.4. Let $N = 18$, $f(x) = (1+x+x^2)^3 = \sum_{z=0}^6 f_z x^z$, $p_1(z) = 3z, p_2(z) = N - 3z$. The construction of Theorem 5.2 yields an 18-qubit permutation invariant code that encodes a 3-level system and corrects 1 error. The orthonormal basis vectors are

$$|0_L\rangle = \frac{|D_{(18,0)}\rangle + \sqrt{7}|D_{(9,9)}\rangle + |D_{(0,18)}\rangle}{3},$$

$$|1_L\rangle = \frac{\sqrt{3}|D_{(15,3)}\rangle + \sqrt{6}|D_{(6,12)}\rangle}{3},$$

$$|2_L\rangle = \frac{\sqrt{6}|D_{(12,6)}\rangle + \sqrt{3}|D_{(3,15)}\rangle}{3}.$$

Example 6.5. Let $N = 27$, $f(x) = (1+x+x^2+x^3)^3 = \sum_{z=0}^9 f_z x^z$, $p_1(z) = 3z, p_2(z) = N - 3z$. The construction of Theorem 5.2 yields a 27-qubit permutation invariant code that encodes a 4-level system and corrects

1 error. The orthonormal basis vectors are

$$|0_L\rangle = \frac{|D_{(27,0)}\rangle + \sqrt{12}|D_{(15,12)}\rangle + \sqrt{3}|D_{(3,24)}\rangle}{4},$$

$$|1_L\rangle = \frac{\sqrt{3}|D_{(24,3)}\rangle + \sqrt{12}|D_{(12,15)}\rangle + |D_{(0,27)}\rangle}{4},$$

$$|2_L\rangle = \frac{\sqrt{6}|D_{(21,6)}\rangle + \sqrt{10}|D_{(9,18)}\rangle}{4},$$

$$|3_L\rangle = \frac{\sqrt{10}|D_{(18,9)}\rangle + \sqrt{6}|D_{(6,21)}\rangle}{4}.$$

Example 6.6. Let $N = 36$, $f(x) = (1 + x + x^2 + x^3 + x^4)^3 = \sum_{z=0}^{12} f_z x^z$, $p_1(z) = 3z, p_2(z) = N - 3z$. The construction of Theorem 5.2 yields a 36-qubit permutation invariant code that encodes a 5-level system and corrects 1 error. The orthonormal basis vectors are

$$|0_L\rangle = \frac{|D_{(36,0)}\rangle + \sqrt{18}|D_{(21,15)}\rangle + \sqrt{6}|D_{(6,30)}\rangle}{5},$$

$$|1_L\rangle = \frac{\sqrt{3}|D_{(33,3)}\rangle + \sqrt{19}|D_{(18,18)}\rangle + \sqrt{3}|D_{(3,33)}\rangle}{5},$$

$$|2_L\rangle = \frac{\sqrt{6}|D_{(30,6)}\rangle + \sqrt{18}|D_{(15,21)}\rangle + |D_{(0,36)}\rangle}{5},$$

$$|3_L\rangle = \frac{\sqrt{10}|D_{(27,9)}\rangle + \sqrt{15}|D_{(12,24)}\rangle}{5},$$

$$|4_L\rangle = \frac{\sqrt{15}|D_{(24,12)}\rangle + \sqrt{10}|D_{(9,27)}\rangle}{5}.$$

At this point, we remark that the coefficients in the orthonormal basis vectors of the permutation-invariant codes supplied in Examples 6.4, 6.5 and 6.6 are identical to the coefficients of the orthonormal basis vectors of the binomial bosonic codes in [MSB$^+$16]. Since the error model considered for the binomial bosonic codes is more restricted than the error model we consider, to prove that the binomial bosonic codes work, one only needs to demonstrate the orthogonality property of the Knill-Laflamme error correction criterion in Theorem 1.1. In our situation, we also need to prove that the non-deformation conditions in Theorem 1.1 hold.

We now present a result that is in the same spirit as the result on permutation-invariant quantum codes in Ref. [PR04], where an uncountable number of codes correcting a single error on 9 qubits was demonstrated, and we essentially rely on the construction of permutation-invariant quantum codes from Theorem 5.2.

Theorem 6.7. *Let t and d be positive integers with $d \geq 2$, and let N be an integer such that $N \geq (2t+1)^2(d-1)$. Then there is a permutation-invariant code on $N = (2t+1)^2(d-1)$ qudits with dimension d that correct t errors. Furthermore if $N > (2t+1)^2(d-1)$, there is an uncountable number of permutation-invariant codes on N qudits with dimension d that correct t errors.*

Proof. The first result follows directly from Example 6.3. It remains to prove the second result. We consider the codes of given by Theorem 5.2, with $f(x) = f_\theta(x)$ where

$$f_\theta(x) = (1 + x + \cdots + x^{d-1})^m(\cos^2\theta + x\sin^2\theta),$$

for $0 \leq \theta \leq \pi/2$, and any choice of the q-tuple of polynomials $\mathbf{p}(z)$ such that $\Delta(\{\mathbf{p}(z) : z = 0, \ldots, n\}) \geq 2t + 1$.

Now $\sum_{z=0}^{n} f_z = f(1) = d^m(\cos^2\theta + \sin^2\theta) = d^m$. Since the orthonormal basis vectors $|k_L\rangle$ of Theorem 5.2 have a unit norm, this implies that $\sum_{\substack{z=0,\dots,n \\ (z-k)/d\in\mathbb{N}}} \sqrt{f_z} = \frac{1}{d}\sum_{z=0}^{n} f_z$ for every $k = 0,\dots d-1$, and hence $f_0 + f_d + f_{2d} + \cdots = d^{m-1}$. Hence the logical zero of our code can be written as

$$|0_\theta\rangle = \sqrt{d^{-m+1}} \sum_{\substack{z=0,\dots,m(d-1) \\ z/d\in\mathbb{N}}} \sqrt{f_{\theta,z}}|D_{\mathbf{p}(z)}\rangle,$$

and the subscript in $|0_\theta\rangle$ makes explicit the dependence of the logical zero with the parameter θ, and $f_\theta(x) = \sum_{z=0}^{m(d-1)} f_{\theta,z}x^z$. For all values of θ and ϕ in $[0,\pi/2]$, $|0_\theta\rangle$ is orthogonal to $|k_L\rangle$ for all $k = 1,\dots,d-1$. Hence it suffices to show that $0 \le \langle 0_\theta|0_\phi\rangle < 1$ for all distinct values of θ and ϕ in $[0,\pi/2]$.

For distinct values of θ and ϕ in $[0,\pi/2]$, the values $x = \frac{\cos^2\theta}{d^{m-1}}$ and $y = \frac{\cos^2\phi}{d^{m-1}}$ are distinct. Note that

$$\langle 0_\theta|0_\phi\rangle = d^{-m+1}\sum_{z|d} \sqrt{f_{\theta,z}f_{\phi,z}}$$
$$= \sqrt{xy} + d^{-m+1}\sum_{z|d,z\ge d} \sqrt{f_{\theta,z}f_{\phi,z}}$$
$$\le \sqrt{xy} + \sqrt{(1-x)(1-y)} = (\sqrt{x},\sqrt{1-x})\cdot(\sqrt{y},\sqrt{1-y})$$

Since $0 \le x,y \le 1$, the above dot product is non-negative. The vectors $(\sqrt{x},\sqrt{1-x})$ and $(\sqrt{y},\sqrt{1-y})$ both have unit norm, and hence the Cauchy-Schwarz inequality implies that their dot product is at most one. Furthermore, the Cauchy-Schwarz inequality for the dot product between $(\sqrt{x},\sqrt{1-x})$ and $(\sqrt{y},\sqrt{1-y})$ is a strict inequality since x and y are distinct. Hence $0 \le \langle 0_\theta|0_\phi\rangle < 1$, and this completes the proof. $\square$

7 Comparison with previous permutation-invariant codes

Previously constructed permutation-invariant codes have been restricted to systems comprised of solely qubits, with Hilbert space $(\mathbb{C}^2)^{\otimes N}$. Let g,n,N be integers such that $g,n \ge 2t+1$ and $N \ge gn$. Then the orthonormal basis vectors of the permutation-invariant codes that correct t errors given by Ref. [Ouy14] generalizing the 9-qubit Ruskai code [Rus00] have the orthonormal basis vectors

$$|0_L\rangle = \sum_{z=0,\dots,\lfloor n/2\rfloor} \sqrt{\binom{n}{2z}2^{-n+1}}|D_{(2gz,N-2gz)}\rangle$$
$$|1_L\rangle = \sum_{z=0,\dots,\lfloor n-1/2\rfloor} \sqrt{\binom{n}{2z+1}2^{-n+1}}|D_{(g(2z+1),N-g(2z+1))}\rangle. \tag{7.1}$$

In [Ouy14], the orthonormal basis vectors in Eq. (7.1) are superpositions over Dicke states with amplitudes proportional to the square root of a binomial coefficient, where these Dicke states have weights spaced a constant number apart. In [OF16], the authors proved the possibility of encoding more than a single qubit into a permutation invariant code with orthonormal basis vectors all of the form given by Eq. (7.1). However in this construction, the correction of only a single amplitude damping error is possible.

8 Concluding remarks

In this paper, we construct permutation-invariant codes from certain polynomials, and thereby generalize the construction of the permutation-invariant codes that rely on a binomial distribution [Ouy14, Rus00] to

those that rely on more general distributions. From previous constructions of permutation-invariant codes, there is only a finite number of permutation-invariant-quantum codes of a fixed length; here we show an uncountable number of permutation-invariant codes on N qudits that correct t errors and encode a d-level system exist, given that N is sufficiently large. It seems likely that the results in this paper can be combined with the technique of pasting permutation-invariant codes [OF16] to construct other permutation-invariant codes with modest error correction capabilities. However it remains a open problem to generalize the seven qubit permutation-invariant codes of Pollatsek and Ruskai [PR04].

Note that for the permutation-invariant codes in [Rus00, Ouy14], the orthonormal basis vectors necessarily have amplitudes that are proportional to the square root of the binomial distribution, and the weights of the Dicke states are spaced an equal distance apart. These two properties need not hold in the permutation-invariant codes of Theorem 5.1.

9   Acknowledgments

References

[CRSS98]   A Robert Calderbank, Eric M Rains, PM Shor, and Neil JA Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.

[HK69]   K E. Hellwig and K Kraus. Pure operations and measurements. *Communications in Mathematical Physics*, 11(3):214–220, 1969.

[HK70]   K E. Hellwig and K Kraus. Operations and measurements. II. *Communications in Mathematical Physics*, 16(2):142–147, 1970.

[KL97]   Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, February 1997.

[Kra83]   Karl Kraus. *Lecture Notes in Physics 190 : States, Effects, and Operations Fundamental Notions of Quantum Theory*. Springer Berlin / Heidelberg, first edition, 1983.

[MSB$^+$16]   Marios H. Michael, Matti Silveri, R. T. Brierley, Victor V. Albert, Juha Salmilehto, Liang Jiang, and S. M. Girvin. New class of quantum error-correcting codes for a bosonic mode. *Phys. Rev. X*, 6:031006, Jul 2016.

[OF16]   Yingkai Ouyang and Joseph Fitzsimons. Permutation-invariant codes encoding more than one qubit. *Phys. Rev. A*, 93:042340, Apr 2016.

[Ouy14]   Yingkai Ouyang. Permutation-invariant quantum codes. *Phys. Rev. A*, 90(6):062317, 2014.

[PR04]   Harriet Pollatsek and Mary Beth Ruskai. Permutationally invariant codes for quantum error correction. *Linear Algebra and its Applications*, 392(0):255–288, 2004.

[Rai99]   E M Rains. Nonbinary quantum codes. *IEEE Transactions on Information Theory*, 45(6):1827–1832, September 1999.

[Rus00]   Mary Beth Ruskai. Pauli Exchange Errors in Quantum Computation. *Phys. Rev. Lett.*, 85(1):194–197, July 2000.

[vLW01]   Jacobus Hendricus van Lint and Richard Michael Wilson. *A course in combinatorics*. Cambridge university press, 2001.