Permutation-invariant qudit codes from polynomials

Yingkai Ouyang *

February 21, 2017

Abstract

A qudit code is a subspace of the state space of a fixed number of qudits. Such a code is permutation-invariant if it is unchanged under the swapping of any pair of the underlying qudits. Prior permutation-invariant codes encode a single qubit into $N$ qubits that correct $t$ arbitrary errors. We design permutation-invariant codes encoding a $d$-level system into $N$ qudits that correct $t$ arbitrary errors. The logical code-words in our permutation-invariant qudits codes are linear combinations of Dicke states, where the coefficients need not be square roots of the binomial coefficients, and the Dicke states used need to be spaced a constant weight apart. Polynomials govern the structure of the Dicke states and the coefficients in our construction. We thereby demonstrate that there is an uncountable number of such permutation-invariant codes when $N \geq (2t+1)^2(d-1) + 1$.

1 Introduction

Given the fragility of quantum information, one might hope to protect it via encoding into a quantum code. We consider quantum codes $\mathcal{C}$ that are $d$-dimensional subspaces of a finite dimensional complex vector space $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$. In physics, the tensor product structure of $\mathcal{H}$ is commonly interpreted as the set of all unnormalized $N$-qudit states, where each qudit has a dimension of exactly $d$. In the problem of quantum error correction, an arbitrary density matrix $\rho$ with support on the quantum code $\mathcal{C}$ is initialized, and a fixed quantum channel $\mathcal{N}$ which models the decoherence process acts on $\rho$. A problem in quantum error correction is then to find quantum codes for which $\mathcal{R}(\mathcal{N}(\rho))$ approximates $\rho$ well for arbitrary $\rho$ in the codespace, where $\mathcal{R}$ is an optimal recovery map that depends only on the noisy channel and the quantum code. A quantum code corrects $t$ errors, if for every noisy quantum channel with Kraus operators that corrupt at most $t$ qudits, there exists a recovery map $\mathcal{R}$ such that $\mathcal{R}(\mathcal{N}(\rho)) = \rho$ for every state $\rho$ supported on the codespace.

In this paper, we study the structure of a special family of quantum codes that are invariant under any permutation of the underlying qudits. Such codes are called permutation-invariant quantum codes, or simply permutation-invariant codes. The error correction capabilities of these codes have been studied by various authors [Rus00, PR04, Ouy14, OF16] using various quantum error correction criterion [KL97, LNCY97] with roots in operator theory. It is not yet known if techniques in classical coding theory could apply to permutation-invariant codes. In this sense, permutation-invariant quantum codes are markedly different from the oft studied quantum stabilizer codes [Got97] where techniques in classical coding theory are known to apply [CRSS98, Rai99].

Permutation-invariant codes are completely immune to noisy quantum channels encountered in a multitude of situations. Such situations include the stochastic reordering and coherent exchange of quantum packets, out-of-order delivery of classical packets [Pax97], and also the effect of the exchange interaction

*Singapore University of Technology and Design. yingkai.ouyang@sutd.edu.sg
in certain many-electron systems [Blu03, Rus00]. A quantum permutation channel, which has each of its Kraus operators a power series of a linear combination of matrices that permute the underlying qudits [OF16], models such situations. When the noisy channel is approximately equal to a permutation channel, one might also desire error correction capabilities against quantum channels with Kraus operators that only act non-trivially on a small number qudits. Since the decoherence-free-subspace [ZR97] of quantum permutation channels is the space of all permutation-invariant quantum states, permutation-invariant codes [Rus00, PR04, Ouy14, OF16] are natural candidates to encode quantum information into physical systems with dynamics well approximated by quantum permutation channels.

Previously constructed permutation-invariant codes have been restricted to systems comprised of solely qubits. For $N$-qubit systems, the symmetric subspace is spanned by Dicke states with weights from 0 to $N$. Here, a Dicke state of weight $w$ is a uniform superposition over all computation basis states with exactly $w$ excitations, and we denote it as $|D^N_w\rangle$. For example, the Dicke state on five qubits with two excitations is $|D^5_2\rangle$ and can be expressed as the superposition

$$
\frac{1}{\sqrt{10}}(|11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle \\
+ |10100\rangle + |01010\rangle + |00101\rangle + |10010\rangle + |01001\rangle).
$$

Let $g, n, N$ be integers such that $g, n \geq 2t + 1$ and $N \geq gn$. Then the logical codewords of the permutation-invariant codes that correct $t$ errors given by Ref. [Ouy14] generalizing the 9-qubit Ruskai code [Rus00] have the logical codewords

$$
|0_L\rangle = \sum_{z=0,\ldots,\lceil n/2\rceil} \sqrt{\left(\frac{n}{2z}\right)^{2-n+1}} |D^N_{2g^z}\rangle \\
|1_L\rangle = \sum_{z=0,\ldots,\lfloor (n-1)/2\rfloor} \sqrt{\left(\frac{n}{2z+1}\right)^{2-n+1}} |D^N_{g(2z+1)}\rangle.
$$

(1.1)

In [Ouy14], the logical codewords in Eq. (1.1) 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 logical codewords all of the form given by Eq. (1.1). However in this construction, the correction of only a single amplitude damping error is possible.

In this paper, we generalize the codes given by Eq. (1.1) substantially, while still retaining the ability to correct $t$ arbitrary errors. We construct permutation-invariant codes encoding a $d$-dimensional system into $N$ qudits each of dimension $q$ that correct arbitrary $t$ qudit errors using polynomials $p_0(z), \ldots, p_{q-1}(z)$ and $f(x)$. The following theorem applies for any $q \geq 2$.

Theorem 1.1. For all positive integers $t$, there is a permutation-invariant code on $N$ qudits of length $(2t + 1)^2(d - 1)$ with dimension $d$ that correct $t$ errors.

The logical codewords used in our code construction are linear combinations of Dicke states that need not have weights spaced a constant number apart, and the corresponding coefficients need not be proportional to the square root of a binomial coefficient. When the permutation-invariant codes in Theorem 1.1 are constructed over qubits, these coefficients correspond directly to the coefficients in the binomial bosonic codes [MSB+16]. The flexibility in designing the coefficients allows us to show that for all $q \geq 2$ there is an uncountable number of permutation-invariant codes that correct a fixed number of errors, provided that the length of these codes is sufficiently large, which we state in the following theorem.
Theorem 1.2. For every positive integer \( t \), there is an uncountable number of permutation-invariant codes on \( N \) qudits of length at least \((2t+1)^2(d-1)+1\) with dimension \( d \) that correct \( t \) errors.

Theorem 1.2 is interesting because previous constructs of permutation-invariant codes that can correct at least one error [Rus00, PR04, Ouy14, OF16], only give a finite number of permutation-invariant codes on \( N \) qubits for any fixed integer \( N \).

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 explain how the coefficients of the polynomial \( f(x) = \sum_{z=0}^{n} f(z)x^{z} \) and the values of the polynomials \( p_0(z), \ldots, p_{q-1}(z) \) for \( z = 0, \ldots, n \) relate to our code construction in Theorem 3.1 which constructs permutation-invariant codes encoding a single qubit and Theorem 3.5 which constructs permutation-invariant codes encoding a \( d \)-level system. Explicit examples of permutation-invariant codes that follow from these two theorems are supplied. These two theorems are also used to prove Theorem 1.1 and Theorem 1.2. In Section 4, we prove Theorem 3.1 and Theorem 3.5. In Section 5, we give some concluding remarks.

2 Preliminaries

2.1 Ordered partitions and permutation-invariant sets

Let \( \mathbb{N} = \{0, 1, \ldots, \} \) denote the set of the non-negative integers. We say that a vector \( \mathbf{n} = (n_0, \ldots, n_{q-1}) \) is an ordered partition of a positive integer \( N \) into \( q \) parts if \( n_0, \ldots, n_{q-1} \in \mathbb{N} \) and \( n_0 + \cdots + n_{q-1} = N \). 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 \( \mathcal{T}_{N,q} \).

For every \( N \)-tuple \( \mathbf{c} = (c_1, \ldots, c_N) \in \{0, \ldots, q-1\}^N \) and \( k \in \mathbb{N} \), let \( w_t(k) = |\{i : c_i = k\}| \) be the number of components of \( \mathbf{c} \) that are equal to \( k \), and let \( \tilde{w}_t(\mathbf{c}) = (w_0(\mathbf{c}), \ldots, w_{q-1}(\mathbf{c})) \). We denote the multinomial coefficient that counts the number of \( N \)-tuples \( \mathbf{c} \) in \( \{0, \ldots, q-1\}^N \) for which \( \tilde{w}_t(\mathbf{c}) = (n_0, \ldots, n_{q-1}) \) as \( \binom{N}{n} = \frac{N!}{n_0! \cdots n_{q-1}!} \). For every ordered partition \( \mathbf{n} = (n_0, \ldots, n_{q-1}) \) of \( N \) into \( q \) parts, we define the permutation-invariant set of type \( \mathbf{n} \) as \( C_n = \{ \mathbf{c} \in \{0, \ldots, q-1\}^N : \tilde{w}_t(\mathbf{c}) = \mathbf{n} \} \).

Given \( N \)-tuples \( \mathbf{x}, \mathbf{y} \in \mathbb{N}^N \), we denote the Hamming distance between \( \mathbf{x} \) and \( \mathbf{y} \) as \( d_H(\mathbf{x}, \mathbf{y}) = |\{1 \leq i \leq N : x_i \neq y_i\}| \). 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 \( C_n \) and the elements of \( C_u \) as

\[
\Delta(\mathbf{n}, \mathbf{u}) = \min\{d_H(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C_n, \mathbf{y} \in C_u \}. \tag{2.1}
\]

We denote \( \Delta(T) \) as the minimum distance between distinct permutation-invariant sets induced by \( T \subset \mathcal{T}_{N,q} \), where formally

\[
\Delta(T) = \min\{\Delta(\mathbf{n}, \mathbf{u}) : \mathbf{n}, \mathbf{u} \in T, \mathbf{n} \neq \mathbf{u} \}. \tag{2.2}
\]

2.2 Dicke states

The permutation-invariant codes of this paper are expressed as linear combinations of Dicke states, which we proceed to describe. The space of a single qudit of dimension \( q \) is \( \mathbb{C}^q \), and we let \( \{|0\rangle, \ldots, |q-1\rangle\} \) denote an orthonormal basis of \( \mathbb{C}^q \). Given any \( N \)-tuple \( \mathbf{c} = (c_1, \ldots, c_N) \in \{0, \ldots, q-1\}^N \), we denote \( |\mathbf{c}\rangle = |c_1\rangle \otimes \cdots \otimes |c_N\rangle \) as the corresponding \( N \)-qudit tensor product state. Given any ordered partition \( \mathbf{n} \in \mathcal{T}_{N,q} \), we denote the Dicke state of type \( \mathbf{n} \) and the unnormalized Dicke state of type \( \mathbf{n} \) respectively as

\[
|D_n\rangle = \sqrt{|C_n|^{-1}} \sum_{\mathbf{c} \in C_n} |\mathbf{c}\rangle = \frac{1}{\sqrt{\binom{N}{n}}} \sum_{\mathbf{c} \in C_n} |\mathbf{c}\rangle, \tag{2.3}
\]
\[ |H_n| = \sum_{c \in C_n} |c| \quad \text{(2.4)} \]

The set of Dicke states \( \{|D_n\} : n \in T_{N,q} \) 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 \( |D_n| \). 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.

### 2.3 Quantum error correction

This subsection reviews the Knill-Laflamme criterion [KL97] for a quantum code to be able to correct errors. To state this criterion precisely, we review terminology related to quantum states, density matrices and quantum channels [NC00].

For complex Euclidean space \( \mathcal{H} \), let \( L(\mathcal{H}) \) denote the set of linear operators mapping \( \mathcal{H} \) to \( \mathcal{H} \). When \( \mathcal{H} \) has a dimension of \( d \), \( L(\mathcal{H}) \) is the set of complex square matrices of size \( d \). We use \( \mathcal{D}(\mathcal{H}) \) to denote the set of density matrices on \( \mathcal{H} \), which is the set of all positive semi-definite and trace one matrices in \( L(\mathcal{H}) \). A quantum code \( \mathcal{C} \) in \( \mathcal{H} \) is a subspace of \( \mathcal{H} \). Given an orthonormal basis \( \{|\psi_i\} \) of \( \mathcal{C} \), every \( |\psi_i\rangle \) is a logical codeword of \( \mathcal{C} \). We let \( \mathcal{D}(\mathcal{C}) \subseteq \mathcal{D}(\mathcal{H}) \) denote the set of density matrices with support only on the quantum code \( \mathcal{C} \). A quantum channel \( \Phi : L(\mathcal{H}) \rightarrow L(\mathcal{H}) \) is a completely positive and trace-preserving linear map that takes density matrices \( \mathcal{H} \) to density matrices on \( \mathcal{H} \). Every such quantum channel has a non-unique Kraus representation [HK69, HK70, Kra83] \( \Phi(\rho) = \sum_{K \in \mathcal{R}_\Phi} K \rho K^\dagger \) where \( \sum_{K \in \mathcal{R}_\Phi} K^\dagger K = 1_{\mathcal{H}} \) and \( \mathcal{R} \subseteq L(\mathcal{H}) \) is a Kraus set of \( \Phi \).

The theory of quantum error correction has its roots in the Knill-Laflamme (KL) error correction conditions [KL97]. Given a quantum code \( \mathcal{C} \), the necessary and sufficient conditions for the perfect recovery of errors induced by a noisy channel \( \mathcal{N} \) on density matrices in \( \mathcal{D}(\mathcal{C}) \) using an optimal recovery channel \( \mathcal{R} \) can be stated in the following theorem.

**Theorem 2.1 (Knill-Laflamme [KL97]).** Given a complex Euclidean space \( \mathcal{H} \), let \( \mathcal{C} \subseteq \mathcal{H} \) be a \( d \)-dimensional code and \( \{|\psi_1\rangle, \ldots, |\psi_d\rangle\} \) be any orthonormal basis of \( \mathcal{C} \). Let \( \mathcal{N} \) be a quantum channel with Kraus set \( \mathcal{R}_{\mathcal{N}} \). Suppose that there exist complex numbers \( g_{A,B} \) such that the following conditions hold for all \( A,B \in \mathcal{R}_{\mathcal{N}} \).

1. **Orthogonality condition:** \( \langle \psi_a|A^\dagger B|\psi_b\rangle = 0 \) for all \( a \neq b \).
2. **Non-deformation conditions:** \( \langle \psi_a|A^\dagger B|\psi_a\rangle = g_{A,B} \) for all \( a = 1, \ldots, d \).

Then there exists a quantum channel \( \mathcal{R} \) such that for every \( \rho \in \mathcal{D}(\mathcal{C}) \), \( \mathcal{R}(\mathcal{N}(\rho)) = \rho \).

To determine if a quantum code corrects \( t \) errors, one can let the noisy channel \( \mathcal{N} \) have only Kraus operators that acts non-trivially on at most \( t \) qubits, and check if the orthogonality and non-deformation conditions of the above theorem hold. Alternatively it suffices to check if the above conditions hold when \( A \) and \( B \) are arbitrary multi-qudit Pauli operators that act non-trivially on at most \( t \) qubits.

### 3 Main result

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 $(p_0(z), \ldots, p_{q-1}(z))$ that is an ordered partition of $N$ into $q$ parts for every $z = 0, \ldots, n$.

As long as the permutation-invariant sets induced by the ordered partitions $(p_0(z), \ldots, p_{q-1}(z))$ 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 3.1.** Let $f(x) = (x - 1)^n g(x) = \sum_{z=0}^{n} f_z x^z$ be a polynomial of degree $n$, where $g(x)$ is a polynomial with real coefficients. Let $p_0(z), \ldots, p_{q-1}(z)$ be polynomials such that for all $z = 0, \ldots, n$, $p(z) = (p_0(z), \ldots, p_{q-1}(z))$ is an ordered partition of the positive integer $N$. Let

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

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

(3.1)

Suppose that $\Delta(\{ p(z) : z = 0, \ldots, n \}) \geq 2t + 1$ and that the degree of the polynomials $p_0(z), \ldots, p_{q-1}(z)$ is at most $\frac{n-1}{2}$, where $t$ is a positive integer. Then $\{ |0_L \rangle, |1_L \rangle \}$ is an orthonormal basis and spans a code that corrects $t$ errors.

Note that for the permutation-invariant codes in [Rus00, Ouy14], the logical codewords 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 3.1.

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 3.2.** With the construction of Theorem 3.1, $N = 19$ qubits are used with the polynomial $f(x) = (1+x)(x-1)^5$ and the tuple of polynomials $p(z) = (N - 1 - 3z, 1 + 3z)$ to obtain a permutation-invariant code encoding one qubit that corrects one arbitrary error. The logical codewords are

$$
|0_L \rangle = \frac{\sqrt{4} |D_{4}^{19} \rangle + \sqrt{3} |D_{3}^{19} \rangle + |D_{2}^{19} \rangle}{\sqrt{10}}, \quad |1_L \rangle = \frac{|D_{1}^{19} \rangle + \sqrt{3} |D_{3}^{19} \rangle + \sqrt{4} |D_{2}^{19} \rangle}{\sqrt{10}}.
$$

**Example 3.3.** With the construction of Theorem 3.1, $N = 108$ qutrits are used with the polynomial $f(x) = (1+x)(x-1)^5$ and the tuple of polynomials $p(z) = (N - 3z^2, 3z^2, 0)$ to obtain a permutation-invariant code encoding one qubit that corrects one arbitrary error. The logical codewords are

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

$$
|1_L \rangle = \frac{|D_{(108,0,0)} \rangle + \sqrt{3} |D_{(96,12,0)} \rangle + \sqrt{4} |D_{(33,75,0)} \rangle}{\sqrt{10}}.
$$

**Example 3.4.** With the construction of Theorem 3.5, $N = 36$ qubits are used with the polynomial $f(x) = (1 + x + x^2 + x^3 + x^4)^3$ and the tuple of polynomials $p(z) = (N - 3z, 3z)$ to obtain a permutation-invariant code encoding one qubit that corrects one arbitrary error. The logical codewords are

$$
|0_L \rangle = \frac{\sqrt{4} |D_{4}^{19} \rangle + \sqrt{3} |D_{3}^{19} \rangle + |D_{2}^{19} \rangle}{\sqrt{10}}, \quad |1_L \rangle = \frac{|D_{1}^{19} \rangle + \sqrt{3} |D_{3}^{19} \rangle + \sqrt{4} |D_{2}^{19} \rangle}{\sqrt{10}}.
$$
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 \((1 + x + \cdots + x^{d-1})^{2r+1}\) to yield a polynomial.

2. A tuple of polynomials \((p_0(z), \ldots, p_{q-1}(z))\) that is an ordered partition of \(N\) into \(q\) parts for every \(z = 0, \ldots, n\).

**Theorem 3.5.** 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 \(p_0(z), \ldots, p_{q-1}(z)\) be polynomials such that for all \(z = 0, \ldots, n\), \(p(z) = (p_0(z), \ldots, p_{q-1}(z))\) is an ordered partition of the positive integer \(N\). For \(k = 0, \ldots, d-1\), let

\[
|k_L\rangle = \sqrt{d} (f_0 + \cdots + f_n)^{-1/2} \sum_{\substack{z=0,\ldots,n \quad \left( (z-k)/d \in \mathbb{N} \right) \quad \text{Suppose that } \Delta(\{p(z) : z = 0, \ldots, n\}) \geq 2t + 1 \text{ and that the degree of the polynomials } p_0(z), \ldots, p_{q-1}(z) \text{ is at most } \frac{m-1}{t}, \text{ where } t \text{ is a positive integer. Then } \{|k_L\rangle : k = 0, \ldots, d-1\} \text{ is an orthonormal basis and spans a code that corrects } t \text{ errors.} \]

Theorem 3.5 immediately implies Theorem 1.1 which says that one can correct \(t\) errors using a permutation-invariant code that encodes a \(d\)-level system into \((2t+1)^2(d-1)\) qudits via the following example.

**Example 3.6.** Let \(N = (2t+1)^2(d-1)\), \(f(x) = (1 + x + \cdots + x^{d-1})^{2r+1} = \sum_{n=0}^{2r+1} f_n x^n\), \(p_1(z) = (2t+1)z, p_0(z) = N - p_1(z)\), and \(p_2(z), \ldots, p_{q-1}(z) = 0\). The construction of Theorem 3.5 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 logical codewords are \(\{|k_L\rangle, k = 0, \ldots, d-1\}\) where

\[
|k_L\rangle = \sqrt{d^{-m+1}} \sum_{\substack{z=0,\ldots,(2t+1)(d-1) \quad \left( (z-k)/d \in \mathbb{N} \right) \quad \text{We now give examples of permutation-invariant codes on qubits that correct a single error while encoding a 3-level system, a 4-level system and a 5-level system that are all based on Example 3.6.} \]

**Example 3.7.** Let \(N = 18\), \(f(x) = (1 + x + x^2)^3 = \sum_{z=0}^{6} f_z x^z\), \(p_1(z) = 3z, p_0(z) = N - 3z\). The construction of Theorem 3.5 yields an 18-qubit permutation invariant code that encodes a 3-level system and corrects 1 error. The logical codewords 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 3.8.** Let \(N = 27\), \(f(x) = (1 + x + x^2 + x^3)^3 = \sum_{z=0}^{9} f_z x^z\), \(p_1(z) = 3z, p_0(z) = N - 3z\). The construction of Theorem 3.5 yields a 27-qubit permutation invariant code that encodes a 4-level system and corrects
yields a 36-qubit permutation invariant code that encodes a 5-level system and corrects 1 error. The logical codewords 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 3.9. Let \( N = 36 \), \( f(x) = (1 + x + x^2 + x^3 + x^4)^3 = \sum_{i=0}^{12} f_i x^i \), \( p_1(z) = 3z \), \( p_0(z) = N - 3z \). The construction of Theorem 3.5 yields a 36-qubit permutation invariant code that encodes a 5-level system and corrects 1 error. The logical codewords 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 logical codewords of the permutation-invariant codes supplied in Examples 3.7, 3.8 and 3.9 are identical to the coefficients of the logical codewords 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 2.1. In our situation, we also need to prove that the non-defomration conditions in Theorem 2.1 hold.

Using Theorem 3.5, we prove Theorem 1.2: we prove that there is an uncountable number of permutation-invariant quantum codes of length at least \((2t + 1)(d - 1) + 1\) of dimension \(d\) that corrects \(t\) errors by explicitly constructing these codes.

**Proof of Theorem 1.2.** We consider the codes of given by Theorem 3.5, 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 \( p(z) \) such that \( \Delta\{\{p(z) : z = 0, \ldots, n\}\} \geq 2t + 1 \).

Now \( \sum_{z=0}^{n} f_z = f(1) = d^m (\cos^2 \theta + \sin^2 \theta) = d^m \). Since the logical codewords \( |k_L\rangle \) of Theorem 3.5 have a unit norm, this implies that \( \sum_{(z-k)/d \in \mathbb{N}} \sqrt{f_z} = \frac{1}{d} \sum_{z=0}^{m} f_z \) for every \( k = 0, \ldots, d - 1 \), and hence \( f_0 + f_d + f_{2d} + \cdots = d^{m-1} \). Hence the logical zero of our code can be written as

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

For distinct values of \(\theta\) and \(\phi\) 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
\[
\langle 0_\theta | 0_\theta \rangle = d^{-m} \sum_{z=d}^\infty \sqrt{f_{\theta,z} f_{\phi,z}}
\]
\[
= \sqrt{xy} + d^{-m} \sum_{z=d}^{m} \sqrt{f_{\theta,z} f_{\phi,z}}
\]
\[
\leq \sqrt{xy} + \sqrt{(1-x)(1-y)} = (\sqrt{x}, \sqrt{1-x}) \cdot (\sqrt{y}, \sqrt{1-y})
\]

Since \(0 \leq x, y \leq 1\), 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 \(0 \leq \langle 0_\theta | 0_\theta \rangle < 1\), and this completes the proof.

\[\square\]

4 Proof of Theorem 3.1 and Theorem 3.5

The proof of the Theorem 3.1 and Theorem 3.5 rely crucially on the fact that \(f(x)\) and \(p_0(z), \ldots, p_{q-1}(z)\) are polynomials. We begin by giving a summation identity that is related to the coefficients of the polynomial \(f(x)\) as given in the following lemma.

**Lemma 4.1.** 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 \(\gamma\), 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 \(k = 1, \ldots, d-1\),
\[
\sum_{z=0}^{n} f_z \omega^{zk} = f_0 + f_1 \omega^k + \cdots + f_n \omega^{kn} = 0. \tag{4.1}
\]

Moreover for every \(c = 1, \ldots, m-1\) and \(k = 1, \ldots, d-1\),
\[
\sum_{z=0}^{n} f_z \omega^{zk} \omega^c = f_1 \omega^k 1^c + \cdots + f_n \omega^{kn} n^c = 0. \tag{4.2}
\]

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

The \(j\)-th derivative of \(f(x)\) for every \(j = 1, \ldots, m-1\) is
\[
\frac{d^j}{dx^j} f(x) = \frac{d^j}{dx^j} \sum_{z=0}^{n} f_z x^z = \sum_{z=0}^{n} f_z(z)_j x^{z-j}, \tag{4.3}
\]
and there exists some polynomial \(h(x)\) such that
\[
\frac{d^j}{dx^j} f(x) = (1 + x + \cdots + x^{d-1}) h(x). \tag{4.4}
\]
Hence (4.4) implies that \(\omega^k \frac{d^j}{dx^j} f(x)\) also evaluates to zero for \(x = \omega^k\) for every \(k = 1, \ldots, d-1\). Hence
\[
0 = \omega^k j \sum_{z=0}^{n} f_z(z)_j \omega^{k(z-j)} = \sum_{z=0}^{n} f_z(z)_j \omega^{kz}. \tag{4.5}
\]
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 $z^c = \sum_{j=0}^{c} S(c, j)(z)_j$. Hence

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

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

Hence $0 = f(\omega^k) = \sum_{z=0}^{n} f_z \omega^k$ for every $k = 1, \ldots, d - 1$, and this proves (4.2).

Lemma 4.1 immediately implies the following identity.

**Lemma 4.2.** Let $m$ be a positive integer, $g(x)$ be a polynomial of degree $\gamma$, 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 $h_z = f_z(-1)^c$. 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 4.1 implies that for all $c = 0, \ldots, m - 1$, we have $\sum_{z=0}^{n} h_z (-1)^z c^z = 0$. Making the substitution $h_z = f_z(-1)^c$, we get $\sum_{z=0}^{n} f_z c^z = 0$, we prove the lemma. \qed

We emphasize that in Lemma 4.2, 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 4.2 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
   $$(1-0)^j + (4)1^j + (-5)2^j + (5)3^j + (-4)4^j + (1)5^j = 0.$$ 

The following lemma states that given that $p(z)$ is a tuple of polynomials, $\langle D_{p(z)}|P|D_{p(z)} \rangle$ is always a polynomial in $z$ for every operator $P$ in $L((C^q)^{\otimes N})$.

**Lemma 4.3.** Let $p(z) = (p_0(z), \ldots, p_{q-1}(z))$ be an ordered partition of the positive integer $N$ for all $z = 0, \ldots, q - 1$ and $p_0(z), \ldots, p_{q-1}(z)$ are polynomials of degree at most $\theta$. Then for every matrix $P \in L((C^q)^{\otimes N})$ of weight $w$, $\langle D_{p(z)}|P|D_{p(z)} \rangle$ is a polynomial of degree at most $w \theta$ in the variable $z$. 

9
Proof. Without loss of generality, the permutation-invariance of the Dicke states $|D_{p(z)}\rangle$ allows us to consider $P = E \otimes I_{w+1,...,N}$ that operates non-trivially on the first $w$ qudits, where $I_{w+1,...,N}$ 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

$$|H_{p(z)}\rangle = \sum_{a \in T_{w,q}} \sum_{b \in T_{N-w,q}} |H_a\rangle \otimes |H_b\rangle,$$

(4.6)

where $|H_a\rangle$ and $|H_b\rangle$ are unnormalized Dicke states on $w$ qudits and $N - w$ qudits respectively.

$$\langle H_{p(z)}|P|H_{p(z)}\rangle = \sum_{a,a' \in T_{w,q}} \sum_{b,b' \in T_{N-w,q}} \langle H_{a'}|E|H_a\rangle \langle H_{b'}|H_b\rangle.$$

(4.7)

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

$$\langle H_{p(z)}|P|H_{p(z)}\rangle = \sum_{a \in T_{w,q}} \sum_{b \in T_{N-w,q}} \langle H_a|E|H_a\rangle \langle H_b|H_b\rangle.$$

(4.8)

Hence

$$\langle D_{p(z)}|P|D_{p(z)}\rangle = \langle H_{p(z)}|P|H_{p(z)}\rangle \left(\begin{array}{c} N \\ p(z) \end{array}\right)^{-1},$$

$$= \sum_{p(z) - a \in T_{N-w,q}} \langle H_a|E|H_a\rangle \left(\begin{array}{c} N-w \\ p(z) - a \end{array}\right) \left(\begin{array}{c} N \\ p(z) \end{array}\right)^{-1}. $$

(4.9)

Since $\langle H_a|E|H_a\rangle$ is independent of the variable $z$, it suffices to show that every $\left(\begin{array}{c} N-w \\ p(z) - a \end{array}\right) \left(\begin{array}{c} N \\ p(z) \end{array}\right)^{-1}$ in (4.9) is a polynomial of order at most $w\theta$ in the variable $z$.

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

$$\left(\begin{array}{c} N-w \\ p(z) - a \end{array}\right) \left(\begin{array}{c} N \\ p(z) \end{array}\right)^{-1} = \frac{(N-w)!}{(p_0(z) - a_1)! \cdots (p_{q-1}(z) - a_q)! (p_0(z))! \cdots (p_{q-1}(z))!} \frac{N!}{(N)_w}.$$

(4.10)

Since each $p_j(z)$ is a polynomial of order at most $\theta$, it follows that $\left(\begin{array}{c} N-w \\ p(z) - a \end{array}\right) \left(\begin{array}{c} N \\ p(z) \end{array}\right)^{-1}$ is a polynomial of order at most $w\theta$ in the variable $z$. □

Having proved in Lemma 4.3 that the quadratic function with respect to the Dicke states of type $p(z)$ are polynomials in $z$, and the combinatorial identity given by Lemma 4.1 and Lemma 4.2, we are ready to prove Theorem 3.1 and Theorem 3.5.

Theorem 3.1 can be seen as a consequence of the Knill-Laflamme error correction criterion in Theorem 2.1 and the Lemmas 4.1 and Lemma 4.3. In its proof, the orthogonality condition of Theorem 2.1 is trivially satisfied, and the non-deformation condition of Theorem 2.1 holds because of the aforementioned lemmas.
Proof of Theorem 3.1. Let $f(x), p(z)$ and $|k_L\rangle$ be as given in Theorem 3.1 for $k = 0, 1$. Since $P \in L(\mathbb{C}^d \otimes N)$ operates non-trivially on at most $2t$ qudits and the codes $C_p(z)$ have a mutual minimum distance of at least $2t+1$, the orthogonality condition of Theorem 2.1 holds.

To show that the non-deformation conditions of Theorem 2.1 hold, it suffices to show that

$$\langle 0_L | P | 0_L \rangle = \sqrt{2} (|f_0| + \cdots + |f_n|)^{-1} \sum_{z=0,...,n} f_z \langle |D_p(z)| | P | D_p(z) \rangle, \quad (4.11)$$

and

$$\langle 1_L | P | 1_L \rangle = \sqrt{2} (|f_0| + \cdots + |f_n|)^{-1} \sum_{z=0,...,n} -f_z \langle |D_p(z)| | P | D_p(z) \rangle. \quad (4.12)$$

Now

$$\langle 0_L | P | 0_L \rangle - \langle 1_L | P | 1_L \rangle = \sqrt{2} \sum_{z=0,...,n} f_z \langle |D_p(z)| | P | D_p(z) \rangle. \quad (4.13)$$

Lemma 4.3 implies that the polynomials $\langle D_p(z)| | P | D_p(z) \rangle$ have degree no more than $2t\theta$ in the variable $z$. Hence for some constants $\alpha_c \in \mathbb{C}$

$$\sum_{z=0}^{n} f_z \langle |D_p(z)| | P | D_p(z) \rangle = \sum_{z=0}^{n} f_z \sum_{c=0}^{2t\theta} \alpha_c z^c = \sum_{c=0}^{2t\theta} \alpha_c \left( \sum_{z=0}^{n} f_z z^c \right). \quad (4.14)$$

The bracketed term above is zero because of Lemma 4.3. Hence $\langle 0_L | P | 0_L \rangle = \langle 1_L | P | 1_L \rangle$ for every $P \in L(\mathbb{C}^d \otimes N)$ that operates non-trivially on at most $2t$ qudits. This proves that the non-deformation condition of Theorem 2.1 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. }

The proof of Theorem 3.5 is similar to the proof of Theorem 3.1, which uses Theorem 2.1 with the Lemmas 4.2 and Lemma 4.3. In this proof, the orthogonality condition of Theorem 2.1 is no longer trivially satisfied and relies on the aforementioned lemmas. The non-deformation condition of Theorem 2.1 on the other hand is satisfied trivially.

Proof of Theorem 3.5. Consider the Fourier transform of the codes

$$|\tilde{k}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^j |j_L\rangle = (f_0 + \cdots + f_n)^{-1/2} \sum_{z=0}^{n} \omega^{kz} \sqrt{f_z} |D_p(z)\rangle. \quad (4.15)$$

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 2.1 holds whenever $P$ is an $N$ qudit operator that acts non-trivially on at most $2t$ qudits. Note that

$$\langle \tilde{k} | P | \tilde{j} \rangle = (f_0 + \cdots + f_n)^{-1} \sum_{z=0}^{n} \sum_{y=0}^{n} \omega^{-kz+yz} \sqrt{f_z f_y} \langle |D_p(z)| | P | D_p(y) \rangle. \quad (4.16)$$
Since $P$ affects at most $2t$ qudits, Dicke states of distinct types do not overlap under $P$. Hence

$$\langle \tilde{k} | P | \tilde{j} \rangle = (f_0 + \cdots + f_n)^{-1} \sum_{z=0}^n \omega^{(j-k)z} f_z \langle D_{p[z]} | P | D_{p[z]} \rangle. \quad (4.17)$$

Using the fact that $\langle D_{p[z]} | P | D_{p[z]} \rangle$ is a low order polynomial and the combinatorial identity in Lemma 4.1, it follows that $\langle \tilde{k} | P | \tilde{j} \rangle = 0$ whenever $j \neq k$, which is the orthogonality condition of Theorem 2.1. The non-deformation condition of Theorem 2.1 holds trivially because for every $k = 0, \ldots, d - 1$,

$$\langle \tilde{k} | P | \tilde{k} \rangle = (f_0 + \cdots + f_n)^{-1} \sum_{z=0}^n f_z \langle D_{p[z]} | P | D_{p[z]} \rangle. \quad (4.18)$$

\[\square\]

5 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].

6 Acknowledgments

Y.O acknowledges Tommaso Demarie for his comments on an earlier version of the manuscript. This research was supported by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01.

References

[Blu03] Stephen Blundell. *Magnetism in Condensed Matter*. Oxford master series in condensed matter physics, Great Clarendon Street, Oxford OX2 6DP, first edition, 2003.

[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.

[Got97] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[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.
