Generalized Young Symmetrizers for the Analysis of Control Systems on Tensor Spaces

Domenico D’Alessandro Jonas T. Hartwig

Abstract

We describe a method to analyze and decompose the dynamics of a control system on a Lie group subject to symmetries. The method is based on the concept of generalized Young symmetrizers of representation theory. It naturally applies to the situation where the system evolves on a tensor product space and there exists a finite group of symmetries for the dynamics which interchanges the various factors. This is the case for quantum mechanical multipartite systems, such as spin networks, where each factor of the tensor product represents the state of one of the component systems. We present several examples of applications and indicate directions for future research.

Keywords: Systems on Lie groups; Symmetries; Applications of Representation Theory to Control; Control of Quantum Mechanical Systems.

1 Introduction

In geometric control theory, one often considers systems of the form
\begin{equation}
\dot{X} = AX + \sum_{j=1}^{m} B_j u_j X, \quad X(0) = 1,
\end{equation}
where \(X\) varies in a (matrix) Lie group and \(A\) and \(B_j\)'s belong to the corresponding Lie algebra, with \(u_j\) the controls, and 1 is the identity of the group. It is a well known fact [18] that the set of available states for (1) is the connected Lie group \(e^L\), containing the identity 1, corresponding to the Lie algebra \(L\) generated by \(A\) and \(B_j\), assuming that \(e^L\) is compact. Therefore system (1) is called controllable if \(e^L\) is some ‘natural’ Lie group where the system should evolve such as the special orthogonal group \(SO(N)\) or the unitary group \(U(N)\). If the system of interest has the form
\begin{equation}
\dot{\psi} = A\psi + \sum_{j=1}^{m} B_j u_j \psi, \quad \psi(0) = \psi_0,
\end{equation}
where \(\psi\) belongs to a vector space \(\tilde{V}\), real or complex, the reachable set for \(\psi\), is \(\{X\psi_0 \mid X \in e^L\}\) and \(X\) belongs to a representation [12] of \(e^L\) on \(\tilde{V}\).

This fact has had many applications. In particular, for controlled quantum mechanical systems [7], the equation (2) or (1) is the Schrödinger equation (subject to a semiclassical control field \(\vec{u}(t) := (u_1, ..., u_m)\)). In this case, the matrices \(A\) and \(B_j\) in (1), (2) belong to the Lie algebra \(u(N)\) of skew-Hermitian \(N \times N\) matrices, so that \(L\) is a Lie subalgebra of \(u(N)\). The matrix \(X\) in (1) is called the (quantum mechanical) evolution operator and \(\psi\) is the state of the quantum system belonging to a Hilbert space which we shall assume finite dimensional. In this case (operator) controllability is said to be verified if \(e^L\) is the full unitary (\(U(N)\)) or special unitary (\(SU(N)\)) Lie group.

Although controllability is the generic situation, often, in reality, symmetries in the dynamics cause the dynamical Lie algebra \(L\), generated by \(A\) and \(B_j\)'s, to be a proper Lie subalgebra of the natural Lie algebra associated to the system (for example \(u(N)\)). The problem therefore arises to analyze the structure of this Lie algebra and to
understand how this impacts the dynamics of the systems (2), (1). In the quantum mechanical case, more structure can be assumed since, in general, \( L \subseteq u(N) \). This implies (see, e.g., [8]) that \( L \) is a reductive Lie algebra [17], i.e., the direct sum of an Abelian Lie algebra \( A \) and a semisimple Lie algebra \( S \), i.e., \( L = A \oplus S \), with \( [A, S] = 0 \). Moreover, the Lie group corresponding to the semisimple part, \( S, e^S \), which is a subgroup of \( U(N) \), is always compact, so that \( e^L \) can be considered compact except for an Abelian part which commutes with all of it. Computational algorithms [8, 9] exist that, from a basis of \( L \subseteq u(N) \), compute a basis of \( A \). Computing a basis of \( A \) corresponding to the semisimple part, \( S \), can be written as \( S = S_1 \oplus S_2 \oplus \cdots \oplus S_r \), where \( S_j \) are the simple ideals, and \( [S_j, S_k] = \delta_{j,k} S_j \). This effectively provides a decomposition of the dynamics of (1), (2) in every case, which can be calculated with a computer algorithm. However, especially for higher dimensional systems, with this procedure, we often lose insight on the structure of the Lie algebra and how the inherent symmetries of the problems are taken into account in such a decomposition. Moreover the decomposition of the action of the Lie group \( e^L \) on the Hilbert space \( \tilde{V} \) does not come naturally as a consequence of this approach. In applications to multipartite quantum systems the underlying quantum system vector space \( \tilde{V} \) is the tensor product \( \tilde{V} := V^{\otimes n} \), and the dimensions of the matrices \( A \) and \( B_j \) in (1), (2) grow exponentially with \( n \) as \( \dim(V)^n \). In this paper we describe an approach based on ideas of representation theory to decompose the dynamical Lie algebra and therefore the dynamics of (1), (2) as well as those of (2). This approach naturally takes into account the symmetries of the problem and gives as a result the decomposition of the dynamics on the state space.

**Definition 1.1.** A group of matrices \( G \) is said to be a group of symmetries for system (1)-(2), if any element of \( G \) commutes with all matrices \( A \) and \( B_j \)'s in (1)-(2).

This definition is stronger than the concept of symmetries often given in an optimal control context (see, e.g., [3], [22]) where one assumes that for every \( \Pi \in G, \Pi A \Pi^{-1} = A \) and \( \Pi B_j \Pi^{-1} \in \text{span} \{B_1, \ldots, B_m\} \). In fact in the second case controllability is often verified while in the first case it is not. Although extensions are of clear interest, we shall assume that \( G \) is a finite group. We remark that since \( A \) and all \( B_j \) are assumed to commute with all elements in \( G \), it follows (from the Jacobi identity) that the dynamical Lie algebra generated by them also commutes with all of \( G \).

Most of our treatment will concern \( L \subseteq u(d^n) \) where \( d \) is the dimension of the Hilbert basis \( V \). In these cases, it is of interest to characterize the largest subalgebra of \( u(d^n) \) which commutes with \( G, u^G(d^n) \). The dynamical Lie algebra \( L \) is a, not necessarily proper, subalgebra of \( u^G(d^n) \). To describe \( u^G(d^n) \), take a (orthogonal) basis of \( i u(d) \), \( E := \{Q_1, \ldots, Q_{d^2}\} \), so that a basis of \( u(d^n) \) is given by the \( d^2 \) tensor products \( i F_1 \otimes F_2 \otimes \cdots \otimes F_n \), with the \( F_j \) in \( E \). Consider the action of \( G \) on \( u(d^n) \), \( E \rightarrow XEX^{-1}, X \in G \), and \( E \in u(d^n) \). For this action, \( u^G(d^n) \) is the span of fixed points. We have the following.

**Proposition 1.2.** There is a one to one correspondence between elements of an orthogonal basis of \( u^G(d^n) \) and the orbits of \( iu(d^n) \) under the above action of \( G \). Such a correspondence is given by

\[
O \leftrightarrow i \sum_{E_j \in O} E_j,
\]

where \( O \) is an orbit and the sum extends over all \( E_j \) in the orbit \( O \).

Therefore a basis for \( u^G(d^n) \) can be found by studying the orbits of the set of all words of length \( n \) from an alphabet \( E \) under the action of the group \( G \). The dimension of \( u^G(d^n) \) is equal to the number of orbits. This can be calculated in general using the Burnside’s orbit counting theorem (see, e.g., [22]),

\[
\#\text{orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}^g|,
\]

where \( \text{Fix}^g \) denotes the set of elements fixed by \( g \).

**Proof.** (Proof of Proposition 1.2) Collect the elements of the standard basis of \( iu(d^n) \) in sets of elements belonging to the same orbit. Elements in different sets are linearly independent. Moreover write \( E \in u^G(d^n) \) as \( E = i \sum_{O \in \mathcal{O}} E_O \) where \( \mathcal{O} \) is the set of orbits and \( E_O \) is a linear combination of elements in the orbit \( O \). Since \( XEX^{-1} = E \) and each orbit is invariant, we have

\[
XEX^{-1} = i \sum_{O \in \mathcal{O}} XE_O X^{-1} = E = i \sum_{O \in \mathcal{O}} E_O,
\]
which implies that for every orbit $O$, and every $X \in G$, $XE_OX^{-1} = E_O$. Write $E_O = \sum_j \alpha_j E_j$ where $E_j$ are the elements in the orbit $O$ and for some coefficients $\alpha_j$. Fix $j$ and $k$ and an $X \in G$ so that $X$ maps $E_j$ to $E_k$. Such an $X$ always exists because, by definition, the action of $G$ is transitive on its orbits. Moreover, the map associated with $X$ is a bijection from the orbit to itself. By imposing $XE_OX^{-1} = E_O$ we find that $\alpha_j = \alpha_k$. Since this is valid for arbitrary $j$ and $k$, we find that $E_O$ must be proportional to the right hand side of (3).

Example 1.3. (Completely Symmetric Spin Networks) Consider a network of $n$ identical spin $\frac{1}{2}$ particles under the control action of a common magnetic field and exhibiting (identical) Ising interaction with each other [6]. Since every spin interacts with every other spin in the same way, we call such networks completely symmetric. The state space is $V^\otimes n$ where $V = \mathbb{C}^2$ with the standard inner product $\langle \phi|\psi \rangle := \phi^\dagger \psi$. Schrödinger equation for the dynamics is given by (2) with $A = -iH_{zz}$ and $\sum B_j u_j := -iH_x u_x - iH_y u_y$, where the quantum mechanical Hamiltonians, $H_{zz}$, $H_x$ and $H_y$, acting on $V^\otimes n$ are given by

$$H_x = \sum x \otimes \cdots \otimes x \otimes 1 \otimes \cdots \otimes 1,$$  
\hspace{1cm} (5)

$$H_y = \sum y \otimes \cdots \otimes y \otimes 1 \otimes \cdots \otimes 1,$$  
\hspace{1cm} (6)

$$H_{zz} = \sum z \otimes \cdots \otimes z \otimes 1 \otimes \cdots \otimes 1 \otimes \sigma_z \otimes 1 \otimes \cdots \otimes 1,$$  
\hspace{1cm} (7)

$u_x$ and $u_y$ represent $x$ and $y$ components of the external (semi-classical) control magnetic field and $\sigma_{x,y,z}$ are the standard Pauli matrices defined as

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (8)$$

In (5), (6) the sum is taken over all the identical spins, while in (7) it is taken over all the $\binom{n}{2}$ combinations of spins, that is, every pair of spin is assumed to interact with each other in the same (Ising) way. The group of all permutations on $n$ objects, i.e., the symmetric group $S_n$, acts as a group of symmetries for this system by permuting the tensor factors:

$$\Pi(v_1 \otimes \cdots \otimes v_n) = v_{\Pi(1)} \otimes \cdots \otimes v_{\Pi(n)}, \quad \forall \Pi \in S_n \quad (9)$$

The three Hamiltonians commute with the action of the symmetric group $S_n$. Therefore the dynamical Lie algebra $\mathcal{L}$ is a subalgebra of $u^{S_n}(2^n)$. The dimension of $u^{S_n}(2^n)$ which, from Proposition [2] is equal to the number of orbits of the permutation group over words with 4 symbols of length $n$, was calculated in [4] to be $\binom{n+3}{n+3}$. In fact, it was shown in [3], that the dynamical Lie algebra $\mathcal{L}$ in this case is exactly equal to $u^{S_n}(2^n) \cap su(2^n)$, i.e., $u^{S_n}(2^n)$ with the restriction that the trace is equal to 0.

Models of this type often represent crystals of identical equidistant particles, so as to have the same interaction with each other. Therefore the low dimensional cases are particularly interesting from a physical standpoint and in [3] the cases $n = 2$ and $n = 3$ where treated in detail by decomposing the dynamical Lie algebra and its action on invariant subspaces of $V^\otimes n$ and giving constructive control algorithms. In applications to quantum information however, the cases with large value of $n$ are important as one would like to know how the dynamics behave as $n$ gets large assuming that one is able to artificially synthesize such a symmetric spin network in the laboratory. In this paper, as a result of our method, we will show how to decompose the dynamical Lie algebra and the dynamics for this system for every $n$. The calculations for the case $n = 4$ will be presented in detail.

Example 1.4. (Circularly Symmetric Spin Networks) Consider again a network of identical spin $\frac{1}{2}$ particles interacting via Ising $z$-$z$ interaction but with nearest neighbor interaction only. The Hamiltonians modeling the interaction with the external magnetic (control) field in the $x$ and $y$ direction are again given by (5) and (6), but the Hamiltonian modeling the interaction between the particles, $H_{zz}$ in (7), has to be replaced by

$$H_{zz}^{NN} = \sigma_z \otimes \sigma_z \otimes 1 \otimes \cdots \otimes 1 \otimes \sigma_z \otimes 1 \otimes \cdots \otimes 1 \otimes 1 \otimes 1 \otimes \cdots \otimes 1 \otimes 1 \otimes \sigma_z \otimes \sigma_z + \sigma_z \otimes 1 \otimes \cdots \otimes 1 \otimes \sigma_z. \quad (10)$$

The relevant group of symmetries here is the Abelian subgroup $C_n$ of $S_n$ generated by the circular shift $\{1, 2, ..., n\} \rightarrow \{n, 1, 2, ..., n-1\}$, i.e., the permutation $Z := (123 \cdots n)\hspace{1cm} (11)$

The dynamical Lie algebra $\mathcal{L}$ is a subalgebra of $u^{C_n}(2^n)$,
interesting to note that, contrary to what happened in Example 1.3, the dynamical Lie algebra \( l_u \) whose dimension again can be computed as the number of orbits using Proposition 4. In particular the dimension of \( \mathfrak{u}^C_n(2^n) \) is derived in Appendix A and it is given by

\[
\dim \mathfrak{u}^C_n(2^n) = \frac{1}{n} \sum_{m \mid n} 4^m \phi(m),
\]

(11)

where \( \sum_{m \mid n} \) means we sum over all positive integers \( m \) which divide \( n \), and \( \phi(m) \) is Euler’s totient function (see, e.g., [1]) defined as the number of positive integers \( k \) less than or equal to \( m \) which are relatively prime to \( m \). It is interesting to note that, contrary to what happened in Example 1.3, the dynamical Lie algebra \( l_u \) in this case may be a proper subalgebra of \( \mathfrak{u}^C_n(2^n) \) (modulo the requirement of zero trace). Consider the case \( n = 3 \). From formula (11) since \( \phi(1) = 1 \) and \( \phi(3) = 2 \), we have

\[
\dim \mathfrak{u}^C_3(2^3) = \frac{1}{3} (4^1 \times 1 + 4^1 \times 2) = 24,
\]

Therefore \( \mathfrak{u}^C_n(2^n) \) is, in the case \( n = 3 \), a proper superalgebra of \( \mathfrak{u}^{S_n}(2^n) \), which has dimension \( \binom{n+3}{n} = 20 \). However, for \( n = 3 \), the dynamical Lie algebra generated by \( H_{zz} \) in (11) and (13) (15) is the same as the one generated by (13) (15) since the Hamiltonian \( H_{\mathbb{C}^N}^{S_k} \) in (10) coincides with the Hamiltonian \( H_{zz} \) in (7) in the case \( n = 3 \). So the dynamical Lie algebra is \( \mathcal{L} = \mathfrak{u}^{S_n}(2^n) \cap \mathfrak{su}(2^n) \) in this case because of the result of [4]. This has dimension 19 while \( \mathfrak{u}^{S_n}(2^n) \cap \mathfrak{su}(2^n) \) has dimension 23.

In this paper we shall present a method to analyze and decompose the dynamics of systems with symmetries, such as the ones of Examples 1.3 and 1.4 which divide \( \mathfrak{u} \). We shall describe the application to the previous two examples. In particular the application to the systems of Example 1.3 extends the results of [4] to the case of arbitrary number of spins. Central to our method is the concept of Young symmetrizers. These are operators on \( V^{\otimes n} \) belonging to the group algebra associated with \( G \) (see definition in the next section) which decompose the vector space \( V^{\otimes n} \) into invariant subspaces. Each subspace gives a representation of the associated dynamical Lie algebra \( \mathcal{L} \). Moreover, certain representations are isomorphic to each other and the structure of the Lie algebra \( \mathcal{L} \) in this favorite basis is naturally displayed.

The paper is organized as follows: In Section 2 we give some background notions from representation theory including the definition and properties of generalized Young symmetrizers (GYS). This will help us state the problem to be solved in a more formal way. In Section 3 we describe the dynamical analysis of control systems on tensor spaces and discuss how Young symmetrizers are obtained in two special cases. For Abelian groups and for the case of the full symmetric group \( S_n \). In Section 4 we use the method and calculate the generalized Young symmetrizers for the Examples 1.3 and 1.4 thus, in particular, extending the results of [4]. Computations for the case of Example 1.3 with \( n = 4 \) are described in detail as an illustration. In Section 5 we summarize the content of the paper, compare it with the results in the literature on this topic and indicate directions for future research.

2 Background and Statement of the Problem

2.1 Representation theory and statement of the problem

What we call dynamical Lie algebra \( \mathcal{L} \) is, in fact, a representation of an ‘abstract’ Lie algebra \( \hat{\mathcal{L}} \) on a vector space \( \hat{\mathcal{V}} \subseteq \mathbb{C}^N \) (over \( \mathbb{R} \) or \( \mathbb{C} \)), i.e., a Lie algebra homomorphism \( \rho : \hat{\mathcal{L}} \to \mathfrak{gl}(\hat{\mathcal{V}}) \), where \( \mathfrak{gl}(\hat{\mathcal{V}}) \) is the Lie algebra of matrices on \( \hat{\mathcal{V}} \), with the standard commutator \( [A, B] := AB - BA \). A Lie algebra homomorphism is a linear map \( \rho \) which preserves the Lie bracket, i.e., \( \rho([A, B]) = [\rho(A), \rho(B)] \) where \( [\cdot, \cdot]_1 \) is the Lie bracket in \( \hat{\mathcal{L}} \). A representation of a (finite) group \( G \) on a vector space \( \mathcal{V} \subseteq \mathbb{C}^N \) (over \( \mathbb{R} \) or \( \mathbb{C} \)) is a group homomorphism \( \rho_G : G \to GL(\mathcal{V}) \) where \( GL(\mathcal{V}) \) is the group of invertible \( N \times N \) linear operator (matrices) on \( \mathcal{V} \). A group homomorphism is a map which preserves the group operations. An analogous definition can be given and will be used for representations of algebras, as linear maps from an algebra with image in the algebra of \( N \times N \) matrices, which preserve the algebra structure. Given a representation \( \rho \) of a group, Lie algebra or algebra) on a vector space \( \mathcal{V} \), the action of the representation on \( \mathcal{V}, \mathcal{V} \to \rho(g)\mathcal{V} \), where \( g \) is an element of the group, Lie algebra or algebra, is often denoted by \( g\mathcal{V} \), when the representation is clear from the context.

In the following, our focus will be on representations of Lie algebras and in particular of the dynamical Lie algebras \( \mathcal{L} \) and of \( \mathfrak{u}^G(N) \) (Lie algebra of elements of \( u(N) \) invariant under \( G \)). We shall not distinguish in notation
between the Lie algebra and its representation, and use the standard notation of denoting with a superscript, i.e., as \( \mathcal{A}^G \) the subalgebra of \( \mathcal{A} \) invariant under the action of \( G \). Here it is assumed that \( G \) also has a representation, \( \rho_G \), and it acts on \( \mathcal{A} \) as \( A \to \rho_G(\Pi)A\rho_G^{-1}(\Pi) \) for \( \Pi \in G \) and \( A \in \rho(\mathcal{A}) \). The vector space \( \tilde{V} \) is often referred to as the ‘representation’ and we shall follow such a terminology as well. A representation of a Lie algebra is said to be skew-Hermitian if its image belongs to \( u(N) \).

**Definition 2.1.** A representation \( (\rho, V) \) of a Lie algebra \( \mathcal{L} \) or a group \( G \) or an algebra \( \mathcal{A} \) \( \tilde{V} \) is called decomposable, if there exists a decomposition \( \tilde{V} := \tilde{V}_1 \oplus \tilde{V}_2 \) where \( \tilde{V}_1 \) and \( \tilde{V}_2 \) are invariant subspaces of \( \tilde{V} \). If this is not possible, the representation is called indecomposable. It is called reducible if there exists a proper nonzero subspace of \( \tilde{V} \) which is invariant under the representation, irreducible if this is not possible.

It is clear that if a representation is irreducible, it is also indecomposable. However the converse is not always true. It is true for the two main cases of interest here: representations of finite groups and skew-Hermitian representations of Lie algebras, both on complex vector spaces. The fact that this is true for finite groups follows from Maschke’s theorem (see, e.g., Theorem 1.2 in [24]) while for skew-Hermitian Lie algebra representations, we simply notice that if \( \tilde{V}_1 \) is invariant in \( \tilde{V} \), then \( \tilde{V}_1^\perp \) is also invariant so that reducibility implies decomposability. This also implies that for these two cases (skew-Hermitian Lie algebra representations and finite group representations) every representation can be decomposed into a finite number of irreducible representation and it is therefore completely reducible.

In view of these notions the problem to be solved in this paper is as follows:

**Problem:**

*Given a skew-Hermitian representation of a (dynamical) Lie algebra \( \mathcal{L} \) with a symmetry finite group \( G \), on a finite dimensional Hilbert space \( \tilde{V} \), find a decomposition of \( \tilde{V} := \oplus \tilde{V}_j \) where the \( \tilde{V}_j \)'s are orthogonal to each other and each of them is an irreducible representation of \( \mathcal{L} \). Determine the nature of each representation \( \tilde{V}_j \).*

The orthogonal bases of the \( \tilde{V}_j \)'s give a change of coordinates which puts the matrices in \( \mathcal{L} \) and therefore the equations (1), (2) in block diagonal form. The control problem then becomes a problem of control in parallel on each of these subspaces. Such a decomposition in block diagonal form does not come natural with the method of [8]. Our treatment will actually solve a slightly weaker problem than the one above stated. For a given finite group \( G \) we shall be concerned with finding a decomposition into irreducible decompositions (and the associated change of basis) for \( u^G(N) \), the largest Lie algebra in \( u(N) \) which is invariant under \( G \). \( \mathcal{L} \) is in general a subalgebra of \( u^G(N) \) which can be strictly proper even if we mod out the requirement that the matrices have zero trace, as we have have seen in Example 1.4. However, the change of coordinates which puts \( u^G(N) \) in block diagonal form also puts \( \mathcal{L} \) in block diagonal form and the block corresponding to \( \tilde{L} \) form a subalgebra of the block corresponding to \( u^G(N) \).

Representations of a group \( G \) are usually defined up to isomorphism and are considered equivalent when they are isomorphic. To describe the concept of isomorphism we need to define the concept of a \( G \)-map between representations \( (\rho_V, \tilde{V}) \) and \( (\rho_W, \tilde{W}) \). This is a linear map \( T : \tilde{V} \to \tilde{W} \) such that \( T\rho_V(g) = \rho_W(g)T \) for every \( g \in G \). Often this formula is written as \( Tg = gT \) without explicit reference to the representation. The space of \( G \)-maps from \( \tilde{V} \) to \( \tilde{W} \) is denoted by \( \text{Hom}_G(\tilde{V}, \tilde{W}) \). If there exists an element in \( \text{Hom}_G(\tilde{V}, \tilde{W}) \) which is also an isomorphism the two representations \( (\rho_V, \tilde{V}) \) and \( (\rho_W, \tilde{W}) \) are said to be isomorphic.

### 2.2 Dual representations and self-duality

From a representation \( (\rho, \tilde{V}) \), one can construct various other representations. In particular consider the representation of a (finite) group \( G \), where \( \rho(g) \) acts on \( \tilde{V} \) on the left. The dual representation \( (\rho^*, \tilde{V}^*) \) is the representation on \( \tilde{V}^* \), the dual of \( \tilde{V} \), defined by \( \rho^*(g)\phi := \phi(\rho(g^{-1})) \). Recall that \( \tilde{V}^* \) is the space of \( \mathbb{C} \)-linear maps from \( \tilde{V} \) to \( \mathbb{C} \) and the map on the right hand side is the composition of the action of \( \rho(g^{-1}) \) with \( \phi \) on \( \tilde{V} \). In this definition, the action on \( \tilde{V}^* \) is a left action, just like the action on \( \tilde{V} \) since \( \rho^*(g_1 g_2)\phi := \phi(\rho((g_1 g_2)^{-1})) = \phi(g_2^{-1} g_1^{-1}) = \phi(g_2^{-1})\rho(g_1^{-1}) = \rho^*(g_1)\rho^*(g_2)\phi \). This definition preserves the action of \( \tilde{V}^* \) on \( \tilde{V} \) in that for every \( \phi \in \tilde{V}^* \) and \( \tilde{v} \in \tilde{V} \) we have

\[
[\rho^*(g)\phi](\rho(g)\tilde{v}) := \phi(\rho(g^{-1})\rho(g)\tilde{v}) = \phi(\tilde{v}).
\]
A representation is called self dual if it is isomorphic to its dual representation. In particular, if the vector space \( \tilde{V} \) has an inner product \( \langle \cdot | \cdot \rangle \), this canonically (i.e., independently of the basis) defines an isomorphism between \( \tilde{V} \) and \( \tilde{V}^* \) which associates to \( \tilde{v} \in \tilde{V} \), the operator \( \langle \tilde{v} | \cdot \rangle \) in \( \tilde{V}^* \). Then the isomorphism of representations means \( \rho^*(g) \langle \tilde{v} | \cdot \rangle = \langle \rho(g) \tilde{v} | \cdot \rangle \), while by definition we have
\[
\rho^*(g) \langle \tilde{v} | \cdot \rangle = \langle \tilde{v} | \rho(g^{-1}) \cdot \rangle = \langle [\rho(g^{-1})]^{-1} \tilde{v} | \cdot \rangle.
\]
Therefore the canonical isomorphism gives an isomorphism of representations if and only if \( [\rho(g^{-1})]^{-1} = \rho(g) \), i.e., the image of the representation \( \rho \) is unitary. We remark that, for a finite group \( G \), which is the case we are considering here, it is always possible to choose the inner product so that the representation \( \rho \) has unitary image. This is a consequence of Weyl unitary trick (see, e.g., [13]). Given \( (\rho, \tilde{V}) \), replace the inner product \( \langle \cdot | \cdot \rangle \) on \( \tilde{V} \) with the inner product \( \langle \cdot | \cdot \rangle_G \) defined as
\[
\langle \tilde{v} | \tilde{w} \rangle_G := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g) \tilde{v} | \rho(g) \tilde{w} \rangle.
\]
With the inner product \( \langle \cdot | \cdot \rangle_G \), for a fixed \( h \in G \), and any \( \tilde{v} \) and \( \tilde{w} \) in \( \tilde{V} \), we have
\[
\langle \tilde{v} | \rho(h) \tilde{w} \rangle_G := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g) \tilde{v} | \rho(g) \rho(h) \tilde{w} \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g) \tilde{v} | \rho(gh) \tilde{w} \rangle = \frac{1}{|G|} \sum_{m \in G} \langle \rho(m) \rho(h^{-1}) \tilde{v} | \rho(m) \tilde{w} \rangle := \langle \rho(h^{-1}) \tilde{v} | \tilde{w} \rangle_G,
\]
and therefore \( \rho(h^{-1}) = (\rho(h))^t \). Therefore if we take the canonical isomorphism \( \tilde{V} \to \tilde{V}^* \) induced by such inner product \( \langle \cdot | \cdot \rangle_G \), the representation \( (\rho, \tilde{V}) \) is isomorphic to its dual.

A completely similar treatment can be done in the case where the representation \( \rho \) acts on the right of \( \tilde{V} \), that is, it is a right action \( \tilde{v} \to \tilde{v} \rho(g) \). In this case, the dual representation \( \rho^* \) on \( \tilde{V}^* \) is also defined as a right representation, and with, for \( \phi \in \tilde{V}^* \), \( \phi \rho^*(g) := \phi \rho(g) \) where, in the right hand side, we have composition of two maps. Often one omits the symbol \( \rho \) or \( \rho^* \) and indicate \( g \in G \) on the left or on the right according to whether we mean a left or right representation while Greek letters such as \( \tilde{v} \) denote elements in \( \tilde{V}^* \) and vectors \( \tilde{v} \in \tilde{V} \). Using this convention we can express the relation between left and right representation as \( g^{-1} \phi := \phi g \) and \( g^{-1} \tilde{v} = \tilde{v} g \). So the above definitions of the left and right representations on \( \tilde{V}^* \) can be written as \( g \phi(\tilde{v}) := \phi(g \tilde{v}) \) and \( (\phi g)(\tilde{v}) = \phi(g \tilde{v}) \).

As above, we can always consider (using Weyl unitary trick) an inner product in \( \tilde{V} \) for which the representation of \( G \) is unitary. With this inner product \( \langle \cdot | \cdot \rangle_G \), the canonical map \( \tilde{V} \to \tilde{V}^* \) which associates to \( \tilde{v} \), the linear operator \( \langle \tilde{v} | \cdot \rangle \) is a right \( G \)-isomorphism, since \( \forall \tilde{v} \in \tilde{V} \),
\[
\langle \tilde{v} g | \tilde{w} \rangle_G = \langle g^{-1} \tilde{v} g \tilde{w} \rangle_G = \langle \tilde{v} (g^{-1})^t \tilde{w} \rangle_G = \langle \tilde{v} | g \tilde{w} \rangle_G = (\langle \tilde{v} | \cdot \rangle g) \tilde{w}.
\]
Therefore \( \tilde{V} \) and \( \tilde{V}^* \) are dual to each other whether we consider them both as left or right representations. We record this fact for future use.

**Proposition 2.2.** Every left or right representation of a finite group is self dual.

### 2.3 Group algebra and the regular representation

Given a finite group \( G \), the group algebra \( \mathbb{C}[G] := \bigoplus_{n \in G} \mathbb{C} \) is the complex vector space with basis \( G \) equipped with multiplication given by bilinearly extending the group operation. For example, for \( G = S_3 \)
\[
(12) \cdot (\lambda \cdot (1) + \mu \cdot (13)) = \lambda \cdot (12) + \mu \cdot (12) \cdot (13) = \lambda \cdot (12) + \mu \cdot (132),
\]
for \( \lambda, \mu \in \mathbb{C} \) (here we used the convention of multiplying permutations from right to left, as compositions of transformations). If \( G \) has a linear action on a complex vector space \( \tilde{V} \) (such as \( \tilde{V} := V^{\otimes n} \)) then the group algebra \( \mathbb{C}[G] \) also has an action on \( \tilde{V} \) which is the natural extension of the action of the group \( G \). If we take \( \tilde{V} = \mathbb{C}[G] \) the action of \( G \) on \( \tilde{V} \) gives a representation of \( G \) called the regular representation. The regular representation is in general not irreducible and it also contains, as irreducible components, all the irreducible representations of the finite
group $G$ with a multiplicity (up to isomorphism) equal to the dimension of the representation (see, e.g., [12]). That is, we have

$$\mathbb{C}[G] = \bigoplus_j (\tilde{V}_j)^{\oplus \dim \tilde{V}_j},$$

which in particular implies that $\sum_j (\dim \tilde{V}_j)^2 = \dim \mathbb{C}[G] = |G|$, the number of elements in the group $G$. For example, the group $S_3$ has three irreducible representations: 1) the trivial representation where $S_3$ acts trivially on the one-dimensional vector space $\tilde{V} = \mathbb{C}$ as $\rho_\mathbb{C}(g) \tilde{v} = \tilde{v}$ for every $\tilde{v} \in \tilde{V}$, $g \in S_3$ and it is irreducible since $\tilde{V}$ is one-dimensional; 2) the alternating (or sign) representation where $S_3$ acts on $\tilde{V} = \mathbb{C}$ as $\rho_\mathbb{C}(g) \tilde{v} = \text{sign}(g) \tilde{v}$ which is also irreducible since it is one dimensional. 3) the standard representation where $S_3$ acts on the two-dimensional vector space $\tilde{V} \subset \mathbb{C}^3$, spanned by linear combination of three vectors $x_1 \tilde{e}_1 + x_2 \tilde{e}_2 + x_3 \tilde{e}_3$, with $x_1 + x_2 + x_3 = 0$, as $(\rho_\mathbb{C}(\Pi))x_1 \tilde{e}_1 + x_2 \tilde{e}_2 + x_3 \tilde{e}_3 = x_1 \tilde{e}_{\Pi(1)} + x_2 \tilde{e}_{\Pi(2)} + x_3 \tilde{e}_{\Pi(3)}$ for the permutation $\Pi$. One can check that there is no one-dimensional subspace invariant under all operators $\rho_\mathbb{C}(g)$, hence the representation is irreducible. The standard representation appears two times in the regular representation (up to isomorphism) while the trivial and alternating representation are both one dimensional giving a total dimension of 6.

2.4 Generalized Young Symmetrizers (GYS) and the decomposition of the regular representation

Definition 2.3. (Generalized Young Symmetrizers (GYS)) Given a finite group $G$, a complete set of Generalized Young Symmetrizers is a set of elements $\{P_j\}$, $j = 1, \ldots, m$, of the associated group algebra $\mathbb{C}[G]$ satisfying the following properties:

1. (Completeness)

$$1 = \sum_j P_j$$

where 1 is the identity of the group.

2. (Orthogonality)

$$P_j P_k = \delta_{j,k} P_j, \quad \forall j, k;$$

where $\delta_{j,k}$ is the Kronecker delta.

3. (Primitivity) For every $g \in G$

$$P_j g P_j = \lambda_g P_j,$$

for every $P_j$ with $\lambda_g$ a scalar that depends on $g$.

Generalized Young symmetrizers are called a complete set of primitive orthogonal idempotent in ring theory. Their significance in representation theory is that they generate ideals in the group algebra $\mathbb{C}[G]$ which correspond to irreducible sub-representations of the regular representation of $G$. In particular given a set of GYS’s we can write $\mathbb{C}[G]$ as

$$\mathbb{C}[G] = \mathbb{C}[G]1 = \mathbb{C}[G](\sum_j P_j) = C_1 + C_2 + \cdots + C_m,$$

where $C_j := \mathbb{C}[G]P_j$, $j = 1, \ldots, m$ is a left ideal of $\mathbb{C}[G]$ and in particular an invariant subspace of for $G$ in $\mathbb{C}[G]$, i.e., a sub-representation of the regular representation. Let $x \in C_j \cap C_k$, with $j \neq k$. Then there exist $A_j$ and $A_k$ in $\mathbb{C}[G]$ so that $x = A_j P_j = A_k P_k$. Multiplying $A_j P_j = A_k P_k$ on the right by $P_j$ and using (13) we obtain $x = A_j P_j = 0$. Therefore the sum in (16) is a direct sum of sub-representations, i.e., $\mathbb{C}[G] = \bigoplus_{j=1}^m C_j$. According to Theorem III.3 of the Appendix III of [25], condition (15) is necessary and sufficient so that the ideal $C_j$ is minimal which means that it does not properly contain any other ideal. This is usually expressed by saying that the idempotent $P_j$ is primitive and in terms of representations means that the representation associated with $C_j$ is irreducible. We refer to the Appendix III of [25] for further discussion and properties on the decomposition of the regular representation.

Primitive, orthogonal idempotent are called Young Symmetrizers in the context of the symmetric group $S_n$ and therefore we use here the terminology ‘Generalized Young Symmetrizers’ to refer to the case of a general finite group. In the case of the symmetric group, Young symmetrizers are obtained from Young tableaux as summarized in many textbooks such as [12], [13], and [25]. We shall review the main points in subsection 3.1.
For our purposes, it is important to see elements in the group algebra \( \mathbb{C}[G] \), in particular when \( G \) is a subgroup of \( S_n \), as operators on a vector space \( \tilde{V} \), which is, for instance, the case when \( \tilde{V} = V^\otimes n \) and the action of \( G \) permutes the elements in \( V^\otimes n \). We can view, in particular the idempotents \( \{ P_j \} \) as operators on \( \tilde{V} (= V^\otimes n) \). If \( \tilde{V} \) has a (natural) inner product we can also require that the GYS are Hermitian with respect to this inner product, i.e.,

\[
P_j = P_j^\dagger, \quad j = 1, 2, ..., m.
\]

In fact, without reference to the inner product on \( \tilde{V} \), an involution, \( \dagger \), on the group algebra can be defined as \((\sum_{g \in G} \lambda_g g)^\dagger := \sum_{g \in G} \lambda_g g^{-1}\) and this definition for a unitary representation on \( \tilde{V} \) coincides with the fact that the matrices corresponding to the \( P_j \) are Hermitian. The Hermiticity property will be useful in our treatment and we shall use the results of \([2] \) and \([16] \) which showed how to modify the standard procedure to obtain Young Symmetrizers in order to obtain Hermitian Young Symmetrizers, for the case of the symmetric group. To the best of our knowledge there is no general procedure to obtain a complete set of GYS for a general finite group, nor there is a general practical procedure to obtain a set of Hermitian GYS once a set of GYS is known. We shall discuss this more in the next sections.

2.5 The general duality representation theorem

Most of the treatment above deals with representations of a finite group \( G \) and the decomposition of its regular representation into irreducible components. However, given a Lie algebra \( \mathcal{R} \) (e.g., \( u(2^n) \)) and its subalgebra \( \mathcal{R}^G \) (e.g., \( u^G(2^n) \)), consisting of all the elements of \( \mathcal{R} \) which commute with \( G \), and a representation of \( \mathcal{R}^G \) on a vector space \( V \) (e.g., \( V^\otimes n \)) we are interested, not in the irreducible sub-representations of \( \mathcal{R}^G \) but in a decomposition of the representation of \( \mathcal{R}^G \) into its irreducible components. The general duality representation theorem (cf., \([13] \) section 4.1, 4.2 and \([21] \)) provides the link between these two decompositions. Notice that when we say that \( \mathcal{R}^G \) is the set of elements of \( \mathcal{R} \) that commute with \( G \) we assume that we have a representation of \( G \) on \( \tilde{V} \) (e.g., \( V^\otimes n \)), i.e., we see elements of \( G \) and therefore \( \mathbb{C}[G] \) as linear operators on \( \tilde{V} \) (as it was described at the end of the previous subsection) which commute with the linear operators corresponding to \( \mathcal{R}^G \).

Before stating the theorem we state one more property of the GYS in the following proposition. To every GYS \( P_j \), is associated an irreducible sub-representation, given by \( C_j := \mathbb{C}[G]P_j \) and according to \([12] \) there are \( \dim(C_j) \) sub-representations isomorphic to \( C_j \) in the regular representation, each of them corresponding to a GYS \( P_k \). A test to check whether two sub-representations are isomorphic is provided by the following (Theorem III.4 in \([25] \))

**Proposition 2.4.** Two GYS \( P_j \) and \( P_k \) give isomorphic representations if and only if there exists a \( g \in G \) such that \( P_j g P_k \neq 0 \).

Since for every irreducible representation corresponding to \( \mathbb{C}[G]P_j := C_j \) there is an equivalence class of irreducible representations, we denote by \( [j] \) the equivalence class of irreducible representations isomorphic to \( C_j \), and by \( \hat{G} \) the set of all equivalence classes of irreducible representations. Then we have the following (cf. Theorem 4.5 in \([21] \) and Theorem 4.2.1 in \([13] \))

**Theorem 1.** (General duality representation theorem) Assume that the Lie algebra \( \mathcal{R} \) defines an irreducible representation \( \phi \) on \( \tilde{V} \) and that the representation \( \rho \) of \( G \) on \( \tilde{V} \) is such that \( \forall g \in G, \rho(g)\phi(R)\rho^{-1}(g) = \phi(R) \) for each \( R \in \mathcal{R} \) and \( g \in G \). Consider the irreducible representations \( C_j \) of \( G \) contained in the regular representation. Then we have,

\[
\tilde{V} \cong \bigoplus_{[j] \in \hat{G}} \text{Hom}_G(C_j, \tilde{V}) \otimes C_j,
\]

where the sum is independent of the choice of the representative \( j \in [j] \). Each \( \text{Hom}_G(C_j, \tilde{V}) \) is an irreducible representation of \( \mathcal{R}^G \). Furthermore \( \text{Hom}_G(C_j, \tilde{V}) \) and \( \text{Hom}_G(C_k, \tilde{V}) \) are isomorphic if and only if \( [j] = [k] \).

We remark that some of the spaces \( \text{Hom}_G(C_j, \tilde{V}) \) may be zero. The action of \( \mathcal{R}^G \) on \( \text{Hom}_G(C_j, \tilde{V}) \) maps \( T \in \text{Hom}_G(C_j, \tilde{V}) \) to \( rT \) for \( r \in \mathcal{R}^G \). Notice that \( rT \) is indeed in \( \text{Hom}_G(C_j, \tilde{V}) \) since, for \( g \in G \), \( rTg = rgT = grT \). In formula \([13] \) the dimension of the spaces \( C_j \) indicates the multiplicity with which the irreducible representation \( \text{Hom}_G(C_j, \tilde{V}) \) enters the representation \( \tilde{V} \). Therefore formula \([13] \) can also be written as

\[
\tilde{V} \cong \bigoplus_{[j] \in \hat{G}} (\text{Hom}_G(C_j, \tilde{V}))^{\oplus \dim(C_j)}.
\]
Consider the matrix representations of the restrictions of $\mathcal{R}^G$ to $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$ and $\text{Hom}_G(\mathcal{C}_k, \tilde{V})$, with $j, k \in [j]$. In particular let $\Phi$ be the isomorphism of the theorem and let $\{T^j_1, \ldots, T^j_m\}$ a basis of $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$ so that $\{\Phi(T^j_1), \ldots, \Phi(T^j_m)\}$ is a basis of $\text{Hom}_G(\mathcal{C}_h, \tilde{V})$. If $r$ is an element of $\mathcal{R}^G$, we have, for $l = 1, \ldots, m$, $rT^j_l = \sum_{s=1}^m a^j_{ls}T^j_s$ for some coefficients $a^j_{ls}$, and $\Phi rT^j_l = \sum_{s=1}^m a^j_{ls}\Phi(T^j_s) = r\Phi(T^j_l)$, so that the coefficients (and therefore the matrix representations) coincide in the given bases.

The proof of Theorem \ref{thm:main} was given in Theorem 4.5 of \cite{14} and Theorem 4.2.1 of \cite{13} for the case where $\mathcal{R}$ is an algebra. We give a sketch of this proof in Appendix B explaining why the proof extends the our case where $\mathcal{R}$ is a Lie algebra.

### 3 Method of decomposition of dynamics

Theorem \ref{thm:main} solves the problem of relating the representation of the finite group $G$ to the representations of a Lie algebra of operators commuting with $G$. This theorem is however still too abstract to be applied in practice in the decomposition of dynamics on a vector space $\tilde{V}$. We need to do two things: First, we need to characterize the space $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$; Then we need to describe how the space $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$ sits in $\tilde{V}$ in the decomposition \cite{13}. The concept of $\text{GY}$s will be central to this task.

In order to describe $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$, we have to recall some more notions on dual representations and tensor products. Consider, in general, two representations $V$ and $W$ of the same group $G$. These are also representations of the group algebra $\mathbb{C}[G]$ and in this context, they take the name of modules. We have already described how to obtain the dual representation for $V$, which we denote by $V^*$, in which $G$ (and therefore $\mathbb{C}[G]$) has a left or right action. Seen as a representation of the algebra $\mathbb{C}[G]$, $V^*$ is a left or right module. Extending what we have said for group actions, to emphasize the fact that a space $M$ is a right (left) module for an algebra $A$, the action on $\mu \in M$ is denoted by right (left) multiplication, i.e., as $\mu a$ ($a \mu$) for $a \in A$. For a general algebra $A$, consider now a left $A$-module $L$ and a right $A$-module $R$. Then one defines the tensor product over the algebra $A$, $R \otimes_A L$ as

$$R \otimes_A L := R \otimes L/N, \quad N := \text{span}\{\mu a \otimes \bar{w} - \mu \otimes aw' | \bar{w} \in L, \mu \in R, a \in A\}. \quad (19)$$

Notice in particular that, with this definition, for every $a \in A$,

$$[\mu a \otimes \bar{w}] = [\mu \otimes aw], \quad (20)$$

where $[\cdot]$ denotes the equivalence class in the quotient $R \otimes L/N$. The following proposition will be used in our characterization of $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$. Its proof is postponed to Appendix C. The algebra $A$ of interest for us will be the group algebra $\mathbb{C}[G]$. Let $\mathcal{R}^G$ be a (Lie) algebra acting on a vector space $W$ and commuting with the action of a finite group $G$. Then $\mathcal{R}^G$ acts on $V^* \otimes_{\mathbb{C}[G]} W$ by $(1 \otimes r)(\phi \otimes \bar{w}) = [\phi \otimes r\bar{w}]$. This linear action is well defined because it does not depend on the representative chosen in $V^* \otimes W$ since

$$(1 \otimes r)(\phi a \otimes \bar{w} - \phi \otimes aw') = \phi a \otimes r\bar{w} - \phi \otimes raw' = \phi a \otimes r\bar{w} - \phi \otimes ar\bar{w};$$

for $a \in \mathbb{C}[G]$. Also recall that $\mathcal{R}^G$ acts on $\text{Hom}_G(V, W)$ as well transforming $T \in \text{Hom}_G(V, W)$ to $rT = r \circ T \in \text{Hom}_G(V, W)$ with $r \in \mathcal{R}^G$. Therefore both $V^* \otimes_{\mathbb{C}[G]} W$ and $\text{Hom}_G(V, W)$ are (left) $\mathcal{R}^G$-modules.

**Proposition 3.1.** As $\mathcal{R}^G$-modules $V^* \otimes_{\mathbb{C}[G]} W$ and $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$ are isomorphic.

Applying the proposition to $\text{Hom}_G(\mathcal{C}_j, \tilde{V})$ of Theorem \ref{thm:main} we obtain

$$\text{Hom}_G(\mathcal{C}_j, \tilde{V}) \simeq C^*_j \otimes_{\mathbb{C}[G]} \tilde{V} = \mathbb{C}[G]P_j^* \otimes_{\mathbb{C}[G]} \tilde{V} \simeq \mathbb{C}[G]P_j \otimes_{\mathbb{C}[G]} \tilde{V} = \mathbb{C}[G] \otimes_{\mathbb{C}[G]} P_j \tilde{V} \simeq 1 \otimes P_j \tilde{V} \simeq P_j \tilde{V}. \quad (21)$$

In the first equality we used the proposition. In the second one we used the definition of $\mathcal{C}_j$. In the third one, we used the self duality of $\mathcal{C}_j$. The fourth one follows from the observation \cite{20} applied for $\mu \in \mathbb{C}[G]$, $\bar{w} \in \tilde{V}$ and $a = P_j$. The fifth one follows from the general isomorphism $A \otimes_A W \simeq 1 \otimes W$, for a general algebra $A$ given by $[a \otimes \bar{w}] \rightarrow 1 \otimes aw'$, for $a \in A$ and $\bar{w} \in W$ (cf. \cite{20}). Note also that these are $\mathcal{R}^G$-isomorphisms. For the first isomorphism, this follows from Proposition \ref{prop:iso}. That the map $\mathbb{C}[G]P_j \otimes_{\mathbb{C}[G]} \tilde{V} \rightarrow \mathbb{C}[G] \otimes_{\mathbb{C}[G]} P_j \tilde{V}$ is an $\mathcal{R}^G$-isomorphism follows from the fact that $\mathcal{R}^G$ only acts on the second factor, and that $gr = rg$ for every $r \in \mathcal{R}^G$ and $g \in G$ so that $P_j r = r P_j$. That the remaining maps are $\mathcal{R}^G$-isomorphisms follows from the fact that $\mathcal{R}^G$ only acts on the second tensor factor.
Plugging (21) into (18) we obtain, for a complete set of GYS \{P_j\},

\[ \tilde{V} = \bigoplus_{j=1}^{m} (\text{Im}(P_j)), \]

where \text{Im}(P_j) are the images of \(P_j\) as a linear operator on \(\tilde{V}\). Such images are invariant under the action of \(R^G\). If, moreover, the GYS have the Hermiticity property (17), because of the orthogonality in (14), the bases of the subspaces \text{Im}(P_j) provide the change of basis to put the matrices in \(R^G\) in block diagonal form.

We now want to understand more in detail the nature of the action of \(R^G\) on each single subspace \text{Im}(P_j). Recall that we have said in our discussion following Theorem 1 that in appropriate bases these actions on \text{Im}(P_j) and \text{Im}(P_k) coincide if \(P_j\) and \(P_k\) correspond to isomorphic representations of \(G\). With a view to the applications that will follow, we shall assume that the Lie algebra \(R\) of Theorem 1 is \(u(\dim(\tilde{V}))\), so that \(R^G = u^G(\dim(\tilde{V}))\). The space of all complex linear transformations on \(\tilde{V}\), \(\text{End}_C(\tilde{V})\), is the complexification of \(R := u(\dim(\tilde{V}))\) and \(\text{End}_G(\tilde{V})\) (the subspace of linear transformations \(A\) such that \(\rho(g)A = A\rho(g)\) for all \(g \in G\)) is the complexification of \(R^G := u^G(\dim(\tilde{V}))\).

By \(C\)-linearly extending the action of \(R^G\) on \(P_j\tilde{V}\) to an action of \(\text{End}_G(\tilde{V})\), we see that \(P_j\tilde{V}\) is an irreducible representation of \(\text{End}_G(\tilde{V})\). By (18), we obtain a description of the endomorphism algebra:

\[ \text{End}_G(\tilde{V}) \simeq \bigoplus_{[j] \in G} \left\{ \begin{bmatrix} A & \cdots \\ \vdots & \ddots & \ddots \\ \end{bmatrix} \mid A \in \text{End}_C(P_j\tilde{V}) \right\} \]

where for each \([j]\) in the direct sum there are \(\dim \text{Hom}_G(G_j, \tilde{V})\) identical blocks \(A\) in the block matrix.

Therefore we get

**Theorem 2.** Assume \(R = u(\dim \tilde{V})\). Then

\[ R^G = R \cap \text{End}_G(\tilde{V}) = \bigoplus_{[j] \in G} \left\{ \begin{bmatrix} A & \cdots \\ \vdots & \ddots & \ddots \\ \end{bmatrix} \mid A \in \dim(\tilde{V}) \right\} \]

In particular, the restriction of \(R^G\) to each irreducible sub-representation \(\text{Im}P_j\) is the full \(u(\dim P_j\tilde{V})\).

### 3.1 Determination of the GYS

The above method assumes that we are able to obtain, for a given group of symmetries \(G\), the corresponding (Hermitian) GYS in the associated group algebra \(\mathbb{C}[G]\). To the best of our knowledge, there is no general method to achieve this and it has to be done on a case by case basis. We now discuss two cases where this can be achieved. In these cases, we assume that the space \(\tilde{V}\) is the tensor product of a number \(n\) of identical vector spaces \(V\), i.e., \(\tilde{V} = V^\otimes n\) and \(G\) is a subgroup of the symmetric group \(S_n\). We remark that in principle this is not a restriction since from Caley’s theorem every finite group is isomorphic to a subgroup of \(S_n\) [15]. We will indicate here two situations where it is possible to obtain Hermitian GYS: The case of the *full* symmetric group \(G = S_n\) and the case of an *Abelian* group \(G \subseteq S_n\).

#### 3.1.1 GYS for the symmetric group \(G := S_n\)

The construction of the GYS is classic in the case where \(G = S_n\) (see, e.g., [26]). Conjugacy classes within \(S_n\) are determined by the cycle type of a permutation, i.e., the number of cycles of a certain length. For example for \(n = 9\), the permutation \((123)(546)(78)(9)\) has cycle type: 2 for cycles of length 3, 1 for length 2 and 1 for length 1. Cycle types also correspond to partitions of \(n\), i.e., sets of positive integer numbers \(\lambda := \{\lambda_1, \ldots, \lambda_k\}\) with \(\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1\), with \(\lambda_1 + \lambda_2 + \cdots + \lambda_k = n\). For example, the cycle type of \((123)(546)(78)(9)\) corresponds to the partition of \(n = 9\), \((3, 3, 2, 1)\) meaning that the permutations (in the given conjugacy classes) have a cycle of length 3 another cycle of length 3, a cycle of length 2 and a cycle of length 1. Partitions are encoded by Young diagrams which are diagrams composed of boxes in rows of non-decreasing lengths corresponding to the numbers in the partitions. For example, the partition of 9, \((3, 3, 2, 1)\) is encoded in the Young diagram.
It is a known fact in the theory of representation of finite groups that the number of irreducible representations of a finite group $G$ is equal to the number of conjugacy classes in $G$. Therefore, in the case of the symmetric group, $S_n$, the number of the irreducible representations is equal to the number of Young diagrams. In fact, for $S_n$, there is a stronger correspondence between Young diagrams and irreducible sub-representations of the regular representation. If $\lambda$ is a partition of $n$, a standard Young tableau of shape $\lambda$ is obtained from the corresponding Young diagram by distributing the numbers $1, 2, \ldots, n$ over the boxes in such a way that each row and column forms a strictly increasing sequence. For example,

$$ T : \begin{array}{cccc}
1 & 2 & 5 & 7 \\
3 & 6 & 7 & 8 \\
4 & 8 & 9 & \\
\end{array} $$

is a standard Young tableaux of shape $\lambda := (3, 3, 2, 1)$. The set of all standard Young tableaux of shape $\lambda$ is denoted by $\text{SYT}(\lambda)$. Then there is a correspondence between irreducible sub-representations of the regular representation, corresponding to the partition $\lambda$ (which are all isomorphic), and elements in $\text{SYT}(\lambda)$. In particular, if the number of rows corresponding to the shape of $\lambda$ is strictly greater than the dimension of $V$, then there is no representation. In these cases, $\text{Hom}_G(C_j, V^\otimes n) \simeq P_j V^\otimes n = 0$ in formula (21) is zero. However if the number of rows of the Young diagram corresponding to $\lambda$ is less than or equal to $\dim(V)$, there is a one to one correspondence between elements in $\text{SYT}(\lambda)$ and (isomorphic) irreducible sub-representations of the regular representation of $G$, determined by the corresponding Young symmetrizer. The Young symmetrizer $P_T$ corresponding to a standard Young tableau $T$ in $\text{SYT}(\lambda)$ is obtained as follows: Let $R_T$ be the subgroup of $S_n$ consisting of all permutations $\Pi$ which preserves the rows of $T$. Similarly, let $C_T$ be the subgroup of $S_n$ of all permutations preserving the columns of $T$. For example:

$$ T : \begin{array}{ccc}
1 & 2 & 5 \\
3 & 6 & 7 \\
4 & 8 & 9 \\
\end{array} \quad R_T = S_{\{1,2,5,7\}} \times S_{\{3,6\}} \times S_{\{4,9\}} \quad C_T = S_{\{1,3,4,8\}} \times S_{\{2,6,9\}} $$

we omitted the singleton symmetric groups such as $S_{\{5\}}$ because they are the trivial group. Here, for instance, $S_{\{1,2,5,7\}}$ is the subgroup of permutations over the elements $\{1, 2, 5, 7\}$.

The row symmetrizer $r_T$, column anti-symmetrizer $c_T$ are elements of $\mathbb{C}[S_n]$ defined as follows:

$$ r_T = \sum_{\sigma \in R_T} \sigma \quad c_T = \sum_{\sigma \in C_T} (\text{sgn}\sigma)\sigma $$

The Young symmetrizer associated with $T$, $P'_T$, is defined as

$$ P'_T := r_T \cdot c_T. $$

Let us consider, for example $n = 3$ and the standard Young tableau

$$ T = \begin{array}{cc}
1 & 2 \\
3 & \end{array} $$

Then $R_T = S_{\{1,2\}}$ and $C_T = S_{\{1,3\}}$ and

$$ r_T = 1 + (12), \quad c_T = 1 - (13), $$

$$ P'_T := r_T \cdot c_T = (1 + (12))(1 - (13)) = 1 - (13) + (12) - (12)(13) = 1 - (13) + (12) - (132). $$

Young symmetrizers defined this way satisfy, after being divided by a normalization factor, the completeness property [13] and the primitivity property [13]. Therefore they give irreducible sub-representations of the regular
representation. They satisfy the orthogonality property (13), in general, only for small values of $n$ ($n \leq 4$). The recent paper [16], motivated by applications in quantum chromodynamics, shows how to modify the procedure above so that the resulting Young symmetrizers also satisfy properties (14) and (17). The procedure of [16] has been then modified in [2] to make it significantly more efficient, in particular for large values of $n$. We shall use the original algorithm of [16] which is a recursive algorithm and we shall call the modified Hermitian Young Symmetrizers of [16] the KS-Young symmetrizers. For a Young Tableau $T$ corresponding to a partition of $n$ let \( \text{Pre}(T) \) be the Young tableau obtained from $T$ by removing the box containing the highest number and therefore corresponding to a partition of $n - 1$. For example for the tableau $T$ in (24)

\[
\begin{array}{cccc}
1 & 2 & 5 \\
3 & 6 & 7 \\
4 & 8 \\
\end{array}
\]

(26)

The KS-Young symmetrizer $P_T$ associated with a tableau $T$ coincides with the standard Young symmetrizer $P'_T$, if $n \leq 2$. If $n > 2$, it is obtained recursively as

\[
P_T = (P_{\text{Pre}(T)} \otimes 1)P'_T(P_{\text{Pre}(T)} \otimes 1).
\]

(27)

This definition satisfies the requirements (13), (14), (15) and (17) [16]. More information can be obtained from the Young tableau $T$ even without calculating the corresponding KS-Young symmetrizer $P_T$. For instance, the dimension of $\Im(P_T)$ is equal to (cf. Lemma 3 in [16])

\[
\dim(\Im(P_T)) = \prod_{l=1}^{r} \prod_{k=1}^{\lambda_l} (N - l + k) \text{Hook}(T).
\]

(28)

Here $N = \dim(V)$, $\text{Hook}(T)$ is the Hook length of the Young diagram associated with $T$. It is calculated by considering, for each box of the Young diagram the number of boxes directly to the right + the number of boxes directly below + 1 and then taking the product of all the numbers obtained. For example the Hook length of the Young tableau in (24) is 2160. $\lambda_l$ is the length of the $l$-th row in the diagram with $r$ the number of rows. Notice that it follows from formula (28) that if the number of rows of the tableau is greater than the dimension $N$ of the vector space $V$, then $\dim(\Im(P_T)) = 0$.

3.1.2 GYS for finite Abelian groups

Let $G$ be a finite Abelian group. In this case, it is known that every finite-dimensional irreducible representation of $G$ is one-dimensional. In the following we shall use some concepts concerning the character $\chi$ of a representation $\rho$. This is a function $G \rightarrow \mathbb{C}$ defined as $\chi(g) = \text{Tr}\rho(g)$, for $g \in G$. Characters corresponding to irreducible (and therefore one dimensional) representations are called irreducible characters. There is a one to one correspondence between irreducible characters and irreducible representations. Every irreducible character is a group homomorphism $\chi : G \rightarrow \mathbb{C}^\times$, whose image is contained in the unit circle $S^1$ in the complex plane $\mathbb{C}^\times$. Recall that from formula (12) (with $\dim(V_j) = 1$) there are $|G|$ different irreducible representations and therefore $|G|$ different characters. To each such character $\chi$ we associate an element $P_\chi$ of the group algebra $\mathbb{C}[G]$ as follows:

\[
P_\chi := \frac{1}{|G|} \sum_{g \in G} \chi(g)g
\]

(29)

**Proposition 3.2.** The set $\{P_\chi\}$ where $\chi$ ranges over the set of all possible irreducible characters, forms a complete set of Hermitian GYS for the group $G$, i.e., it satisfies properties (13)-(15) and (17).

**Proof.** Consider the following calculation.
\[ P_{\chi}P_{\chi'} = \frac{1}{|G|^2} \sum_{g, g' \in G} \chi(g) \chi'(g')gg' \]
\[ = \frac{1}{|G|^2} \sum_{h \in H} \left( \sum_{g, g' \in G} \chi(g) \chi'(g') \right) h \]
\[ = \frac{1}{|G|^2} \sum_{h \in H} \left( \sum_{g \in G} \chi(g) \chi'(g^{-1}h) \right) h \]
\[ = \frac{1}{|G|} \sum_{h \in H} (\chi * \chi')(h)h \]

where \( \chi * \chi' \) denotes the convolution, defined by
\[ (\chi * \chi')(h) = \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi'(g^{-1}h) \]

From Theorem 2.13 in [14], \( \chi * \chi' = \delta_{\chi, \chi'} \). Thus we get the orthogonality relation [14], that is,
\[ P_{\chi}P_{\chi'} = \delta_{\chi, \chi'} P_{\chi} \]
as desired.

To see that \( P_{\chi} \) is Hermitian, we calculate
\[ P_{\chi}^\dagger = \sum_{g \in G} \overline{\chi(g)} g^{-1} = \sum_{g \in G} \chi(g^{-1}) g^{-1} = \sum_{h \in G} \chi(h) h = P_{\chi}. \]

In the last equality, we used the substitution \( h = g^{-1} \). In the second equality, we used the fact that \( \chi(g) \chi(g^{-1}) = \chi(gg^{-1}) = 1 \) so that \( \chi(g^{-1}) = \frac{1}{\overline{\chi(g)}} \), and since \( \chi \) has image in the unit circle in the complex plane, we have \( \chi(g^{-1}) = \overline{\chi(g)} \).

Next, we have
\[ \sum_{\chi} P_{\chi} = \frac{1}{|G|} \sum_{\chi} \sum_{g \in G} \chi(g) g = \frac{1}{|G|} \sum_{g \in G} \left( \sum_{\chi} \chi(g) \right) g \]

(30)

The function of \( g \), \( \frac{1}{|G|} \sum_{\chi} \chi \) is equal to 0 if \( g \neq 1 \) and it is equal to 1 if \( g = 1 \). This follows from an application of (for instance) Corollary 1.21 in [24] Using this, the right hand side of (30) equals 1.

Lastly, we need to show that \( P_{\chi}gP_{\chi} = \lambda g P_{\chi} \), i.e., property (15). In fact, we have, since the group \( G \) is Abelian,
\[ P_{\chi}gP_{\chi} = P_{\chi}P_{\chi}g = P_{\chi}g = \frac{1}{|G|} \sum_{h \in G} \chi(h) hg = \frac{1}{|G|} \sum_{m \in G} \chi(mg^{-1}) m = \]
\[ \frac{1}{|G|} \sum_{m \in G} \chi(m) \chi(g^{-1}m) = \chi(g^{-1}) \left( \frac{1}{|G|} \sum_{m \in G} \chi(m) m \right) = \chi(g^{-1}) P_{\chi}, \]
as desired. \[ \square \]

4 Examples: spin networks subject to symmetries

We now apply the above described method to the analysis of the dynamics for the two examples described in the introduction, i.e., the completely symmetric spin networks of Example [13] and the circularly symmetric spin networks of Example [14]. We start with the latter.

\[ ^3 \text{Applied with } \chi_i(1) = \dim(V_i) = 1 \]

\[ ^4 \text{This is applied with } h = 1 \text{ and recalling that for an Abelian group each element is a conjugacy class by itself, so that the size of each conjugacy class is } 1. \]
4.1 Circularly symmetric spin networks (Example 1.4)

In the case of the circularly symmetric spin networks described in Example 1.4, the symmetry group is the subgroup $C_n$ of $S_n$, generated by the permutation $Z := (123 \cdots n)$, i.e., $C_n := \{Z^0 = 1, Z, Z^2, \ldots, Z^{n-1}\}$. Since $C_n$ is an Abelian group, every finite-dimensional irreducible representation is 1-dimensional. There are exactly $n$ not equivalent such representations which we denote by: $\rho_0, \rho_1, \ldots, \rho_{n-1}$. They are given by

$$\rho_k : C_n \rightarrow GL(1, \mathbb{C}) = \mathbb{C}^\times$$

$$\rho_k(Z^j) = e^{kj}$$

where $e := e^{2\pi i/n}$ is the $n$-th root of the identity. The character associated to the representation $\rho_k$, $k = 0, 1, 2, \ldots, n - 1$ is $\chi_k(Z^j) := \text{Tr} \rho_k(Z^j) = e^{kj}$. Using Proposition 3.2, a complete set of GYS is then given by the following $n$ elements of the group algebra $\mathbb{C}[C_n]$:

$$P_k = \frac{1}{n} \sum_{j=0}^{n-1} \chi_k(Z^j)Z^j = \frac{1}{n} \sum_{j=0}^{n-1} e^{kj}Z^j, \quad k = 0, 1, \ldots, n - 1. \quad (33)$$

4.1.1 States and decomposition of the dynamical Lie algebra

We now want to decompose the Lie algebra $\mathfrak{u}^G(2^n)$, which has dimension given in formula (11), using the GYS’s. From this we deduce the decomposition of the dynamical Lie algebra $\mathcal{L}$ for the system of $n$ interacting spin with circular symmetry. Recall that we have shown in Example 1.4 that $\mathcal{L} \subset \mathfrak{u}^G(2^n)$, in general.

Let $V = \mathbb{C}^2$ modeling the state of spin $\frac{1}{2}$ systems. States in $V^{\otimes n}$ are labeled by binary words $\underline{a} = a_1a_2\ldots a_n \in \{0, 1\}^n$ as follows:

$$|\underline{a}\rangle = \bar{a}_1 \otimes \bar{a}_2 \otimes \cdots \otimes \bar{a}_n,$$

where $\bar{0} = (\frac{1}{2}, -\frac{1}{2})$, $\bar{1} = (\frac{1}{2}, \frac{1}{2})$.

We now use the GYS method to obtain the decomposition of $u^G(2^n)$ and the change of coordinates to achieve a block diagonal form for it. According to the method, we have to describe $\mathfrak{Im}(P_k)$, for a complete set of GYS’s $\{P_k\}$. We notice that the space of states $|\underline{a}\rangle$ where $\underline{a}$ is a word of period $T$ necessarily dividing $n$ is invariant under $C_n$ and, therefore, under any element of the group algebra $\mathbb{C}[C_n]$ such as the GYS’s $\{P_k\}$. The period $T$ is the smallest positive integer such that $Z^T(\underline{a}) = \underline{a}$. We denote the subspace of $V^{\otimes n}$ of all $T$-periodic states as $V_T^{\otimes n}$, and we have

$$(P_k V^{\otimes n}) = \bigoplus_{T|n} (P_k V_T^{\otimes n}). \quad (35)$$

Consider a general vector $|\underline{a}\rangle$ in the standard basis of $V^{\otimes n}$ and belonging to $V_T^{\otimes n}$. With a GYS, $P_k$, defined in (33), we have

$$P_k(|\underline{a}\rangle) = \frac{1}{n} \sum_{i=0}^{n-1} e^{ki} \cdot |a_1 + ia_2 + i \cdots a_{n+i}\rangle \quad (36)$$

where the indices of $a_j$ are considered modulo $n$. Since the word $a_1a_2\cdots a_n$ is periodic of period $T$, that is, $a_1a_2T \cdots a_{n+T} = a_1a_2 \cdots a_n$, or $Z^T(\underline{a}) = \underline{a}$ in the right hand side of (36), we can divide the summation variable $i$ by $T$ to get

$$i = Tq + r, \quad 0 \leq r < T, \quad 0 \leq q < \frac{n}{T}. \quad (37)$$

Thus

$$P_k(|\underline{a}\rangle) = \frac{1}{n} \sum_{r=0}^{T-1} \left( \sum_{q=0}^{\frac{n}{T}-1} e^{kTq+kr} \cdot |a_1 + r, a_2 + r \cdots a_{n+r}\rangle \right) = \frac{1}{n} \sum_{r=0}^{T-1} e^{kr} \left( \sum_{q=0}^{\frac{n}{T}-1} e^{kTq} \cdot |a_1 + r, a_2 + r \cdots a_{n+r}\rangle \right) \quad (38)$$

The quantity in parenthesis can be computed as a geometric series to give

$$\sum_{q=0}^{\frac{n}{T}-1} e^{kTq} = \begin{cases} \frac{1}{e^{kT} - 1}, & \text{if } e^{kT} = 1, \\ \frac{e^{kTn/T - 1}}{e^{kT} - 1}, & \text{otherwise}, \end{cases} \quad (39)$$
since $\varepsilon^n = 1$, as by definition $\varepsilon := e^{i\frac{2\pi}{p}}$. Using this we get

$$P_k(\langle w \rangle) = \begin{cases} \frac{1}{T} \sum_{r=0}^{T-1} \varepsilon^{kr} \cdot |a_1 + a_2 + \cdots + a_{n+r}|, & \text{if } \varepsilon^{kT} = 1, \\ 0, & \text{otherwise.} \end{cases}$$

(40)

Then $P_k(\langle w \rangle)$ is nonzero if and only if $\varepsilon^{kT} = 1$, which happens if and only $n/T$ divides $k$.

**Example 4.1.** Consider for instance $n = 4$, so that $V^{\otimes n}$ is 16-dimensional. In general the possible values of period (dividing $n = 4$) are $T = 1$, $T = 2$, and $T = 4$. Let us calculate $\text{Im}(P_0)$. All $T = 1$, $T = 2$, and $T = 4$ are such that $n/T = 4/T$, divide $k = 0$. We have one state for each orbit of $C_4$, which gives 6 states $\frac{1}{4} \sum_{j=0}^3 Z^j|0000\rangle$, $\frac{1}{4} \sum_{j=0}^3 Z^j|1111\rangle$, $\frac{1}{4} \sum_{j=0}^3 Z^j|1000\rangle$, $\frac{1}{4} \sum_{j=0}^3 Z^j|1100\rangle$, $\frac{1}{4} \sum_{j=0}^3 Z^j|1010\rangle$, and $\frac{1}{4} \sum_{j=0}^3 Z^j|0111\rangle$, which span $\text{Im}P_0$. For $k = 1$ the only possibility is $T = 4$, so that $n/T = 1$. We have the three states: $\frac{1}{4} \sum_{j=0}^3 e^j Z^j|1000\rangle$, $\frac{1}{4} \sum_{j=0}^3 e^j Z^j|0111\rangle$, $\frac{1}{4} \sum_{j=0}^3 e^j Z^j|1100\rangle$. For $k = 3$ the only possibility is also $T = 4$, and we also have three states: $\frac{1}{4} \sum_{j=0}^3 e^{2j} Z^j|1000\rangle$, $\frac{1}{4} \sum_{j=0}^3 e^{2j} Z^j|0111\rangle$, and $\frac{1}{4} \sum_{j=0}^3 e^{2j} Z^j|1100\rangle$. For $T = 2$, we have one state $\frac{1}{4} \sum_{j=0}^3 e^{2j} Z^j|1100\rangle$. Therefore we have $\text{dim}(\text{Im}P_0) = 6$, $\text{dim}(\text{Im}P_1) = 3$, $\text{dim}(\text{Im}P_2) = 4$, $\text{dim}(\text{Im}P_3) = 3$, so that $u^{-C_4}(2^4) = u(6) + u(3) + u(4) + u(3)$, since all the irreducible representations associated to the GYS, $P_k$, are inequivalent and from Theorem 2 the dimension of $u^{-C_4}(2^4)$ which is equal to $6^2+3^2+4^2+3^2=70$ can also be calculated using formula (11), which gives $\frac{1}{4}(4^2 + 4^2 + 2 	imes 2^2) = 70$.

We now want to calculate in general the dimension of $\text{Im}(P_k)$, which we define by $m_k := \text{dim}(\text{Im}(P_k))$, so that

$$u^{-C_n}(2^n) = u(m_0) + u(m_1) + \cdots + u(m_{n-1}).$$

(41)

Consider the set $X_k$ of binary words $a$ of length $n$ and with a period $T$ such that $n/T$ divides $k$. Since the cyclic group $C_n$ preserves the period, $X_k$ is invariant under $C_n$. The cyclic group $C_n$ acts on $X_k$ by cyclic permutations of the letters. Moreover, as we have seen above, $P_k$ is non zero only on the vector subspace of $V^{\otimes n}$ spanned by the vectors corresponding to the words in $X_k$. Similarly to what done in Proposition 1.2, there is a one to one correspondence between the orbits of $C_n$ in $X_k$ and elements in a basis of $\text{Im}(P_k)$ given, using (40), by

$$[(a_1 a_2 \cdots a_n)] \in X_k/C_n \leftrightarrow \frac{1}{T} \sum_{r=0}^{T-1} \varepsilon^{kr} \cdot |a_1 + a_2 + \cdots + a_{n+r}|,$$

(42)

which is independent of the representative chosen for $[(a_1 a_2 \cdots a_n)]$. In particular $m_k = \text{dim}(P_k) = |X_k/C_n|$. Using this we obtain in Appendix A

$$m_k = \frac{1}{n} \sum_{m|\gcd(n,k)} w(n,k,m) \cdot \phi(m)$$

(43)

where $w(n,k,m)$ is the number of binary words $a$ of length $n$ and period $T$, $m$ divides $n/T$ and $n/T$ divides $k$. Here again, as in formula (11), $\phi(m)$ denotes the Euler’s totient function computed at $m$.

### 4.1.2 The case where $n$ is a prime number

Suppose $n = p$ where $p$ is a prime number. If $k = 0$ there are two terms in the sum, the one corresponding to $m = 1$ and the one corresponding to $m = p$. For $m = 1$ we can take words of period $T = 1$ and $T = p$ which represent all possible $2^p$ words. So we have a term $2^p \phi(1) = 2^p$ in the sum. For $m = p$ we can only take words of period $T = 1$, since words of period $p$ are such that $n/T = 1$ and $m = p$ does not divide $1$. There are only 2 of such words (000· · · 0) and (111· · · 1). So we have a term $2\phi(p) = 2(p-1)$ in the sum. Therefore, we have

$$m_0 = \frac{1}{p} (2^p + 2(p-1)) = 2 + \frac{(2^p - 2)}{p}.$$ 

Notice that for any integer $a$ and prime number $p$, the quantity $a^p - a$ is divisible by $p$, by Fermat’s Little Theorem (see, e.g., [13]). If $k > 0$ then, independently of the value of $k$, the only possible period in the sum is $T = p$
and the only possible value of $m$ is $m = 1$. So there is only one term in the sum corresponding to all words except the two of period $T = 1$. We obtain

$$m_k = m_0 - 2 = \frac{1}{p}(2^p - 2), \quad 1 \leq k < p.$$  \hfill (44)

Consequently,

$$u^{C_p}(2^n) = \begin{bmatrix} u((2^p - 2)/p) & & & & u((2^p - 2)/p) \\ & u((2^p - 2)/p) & & & \\ & & \ddots & & \\ & & & u((2^p - 2)/p) & \\ & & & & u((2^p - 2)/p) \end{bmatrix}$$  \hfill (45)

The dimension is equal to

$$\dim u^{C_p}(2^n) = \frac{(2^p + 2p - 2)^2 + (p - 1)(2^p - 2)^2}{p^2} = 4 + (4^p - 4)/p$$  \hfill (46)

after simplification. This also agrees with the formula (11) for $n = p$ a prime number.

### 4.1.3 The dynamical Lie algebra for a circularly symmetric spin network

As we have discussed in Example 1.4, the dynamical Lie algebra $L$ associated with a circularly symmetric network of spin $\frac{1}{2}$ particles may in general be a proper subalgebra of $u^{C_n}(2^n)$. Nevertheless the change of coordinates which we have obtained in this section places $L$ in a block diagonal form from which it is easier to understand its structure. We illustrate this for the case $n = 3$.

Since $n = 3$ is a prime number, we can use the simplified formula (10) for $m_0 = \dim(\text{Im}(P_0))$, $m_1 = \dim(\text{Im}(P_1))$, $m_2 = \dim(\text{Im}(P_2))$, and we get $m_0 = 4$, $m_1 = 2$, $m_2 = 2$. From formula (40) we obtain a formula for an orthogonal basis of $\text{Im}(P_0)$ which, after normalization, are given by

$$\varphi_0 := |000\rangle;$$
$$\varphi_1 := |111\rangle;$$
$$\varphi_2 := \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle);$$
$$\varphi_3 := \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle).$$ \hfill (47)

We also obtain a formula for an orthonormal basis of $\text{Im}(P_1)$ ($\epsilon := e^{i2\pi/3}$)

$$\psi_1 := \frac{1}{\sqrt{3}}(|100\rangle + \epsilon|010\rangle + \epsilon^2|001\rangle);$$
$$\psi_2 := \frac{1}{\sqrt{3}}(|011\rangle + \epsilon|101\rangle + \epsilon^2|110\rangle).$$ \hfill (48)

and a formula for an orthonormal basis of $\text{Im}(P_2)$,

$$\eta_1 := \frac{1}{\sqrt{3}}(|100\rangle + \epsilon^2|010\rangle + \epsilon|001\rangle);$$
$$\eta_2 := \frac{1}{\sqrt{3}}(|011\rangle + \epsilon^2|101\rangle + \epsilon|110\rangle).$$ \hfill (49)

By calculating the action of $-iH_{zz}^{NN}$, $-iH_x$ and $-iH_y$ in (5), (10), (10) on the above basis, using the fact that $1 + \epsilon + \epsilon^2 = 0$, we obtain, the expression of these operators in the new basis, which is, $-i\hat{H}_{zz}^{NN} = \text{diag}(-3i, -3i, i, i, i, i, i, i, i, i)$,
and

\[
-i\hat{H}_x := \begin{bmatrix}
0 & 0 & -i\sqrt{3} & 0 \\
0 & 0 & 0 & -i\sqrt{3} \\
-i\sqrt{3} & 0 & 0 & -2i \\
0 & -\sqrt{3}i & -2i & 0
\end{bmatrix},
\quad
-i\hat{H}_y := \begin{bmatrix}
0 & 0 & \sqrt{3} & 0 \\
0 & 0 & 0 & -\sqrt{3} \\
-\sqrt{3} & 0 & 0 & 2 \\
0 & \sqrt{3} & -2 & 0
\end{bmatrix}.
\]

The upper left blocks generates any possible \(4 \times 4\) skew-Hermitian block, while the \(2 \times 2\) blocks are required to be equal, something which is not true for general matrices in \(u(C^3(2^j))\) (cf. equation (15)). Therefore the dimension of the dynamical Lie algebra is \(4^2 + 2^2 - 1 = 20 - 1\), where the \(-1\) is due to the fact that the trace has to be equal to zero. In fact such Lie algebra coincides with the one we would have obtained had we considered the full symmetric group \(S_3\) as the symmetry group of this model. From this decomposition we can infer further properties concerning the 'subspace controllability' of the system under consideration. We know that the subsystems identified by the vectors \(\{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}, \{\psi_1, \psi_2\}, \{\eta_1, \eta_2\}\) are all state controllable and the system whose state is spanned by \(\{\varphi_0, \varphi_1, \varphi_2, \varphi_3, \psi_1, \psi_2\}\) or \(\{\varphi_0, \varphi_1, \varphi_2, \varphi_3, \eta_1, \eta_2\}\) are also state controllable. However, the full system is not state controllable. For example, the sub-system with state spanned by \(\{\psi_1, \psi_2, \eta_1, \eta_2\}\) is not controllable. With the given decomposition at hand, we can then set up control problems on the single invariant subspaces. For example, the space spanned by \(\{\psi_1, \psi_2\}\) can be used to mimic a quantum bit in quantum computation implementation. The redundancy in the states makes them more robust as compared to the implementation with a single physical spin. 

### 4.2 Completely symmetric spin networks (Example [1.3])

The GYS and the associated change of coordinates for the case of completely symmetric networks of Example 1.3 can be calculated with the method of Young tableau described in subsection 3.1.1. Here we calculate the explicit change of coordinates for the case of completely symmetric networks of Example 1.3.

The image of the permutation group of the symbols \(\{a_1, a_2, ..., a_r\}\) is the permutation group of the symbols \(\{a_1, a_2, ..., a_r\}\). We also denote by \(V_j, j = 0, 1, 2, 3, 4\), the subspaces of \(V^{\otimes 4}\) spanned by states with \(j\) 1’s, so that, for instance, \(V_0 = \text{span}\{0000\}\).

#### 4.2.1 Young diagram corresponding to the partition (4)

There is only one Standard Young Tableaux (SYT) corresponding to such a partition given by

\[
\begin{array}{cccc}
1 & 2 & 3 & 4
\end{array}
\]

The corresponding KS-Young Symmetrizer \(P^{\text{KS}}\) coincides with the standard Young symmetrizer \(P^S\). (This can be shown by induction to be true for every KS-symmetrizer corresponding to partition \((n)\) for every \(n\).)

The image of \(P^{\text{KS}}\) is spanned by the symmetric orthogonal states (for simplicity we omit the normalization factor).

\[
\varphi_0 = |0000\rangle, \\
\varphi_1 = |1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle, \\
\varphi_2 = |1100\rangle + |0110\rangle + |0011\rangle + |0101\rangle + |0101\rangle + |1011\rangle, \\
\varphi_3 = |1111\rangle + |1010\rangle + |1001\rangle + |1101\rangle + |1101\rangle,
\]

\[
\varphi_4 = |1111\rangle.
\]
4.2.2 Young diagram corresponding to partition (3, 1)

There are three SYT's corresponding to a partition (3, 1). They are

\[
\begin{array}{ccc}
1 & 2 & 3 \\
4 & & \\
\end{array},
\begin{array}{ccc}
1 & 2 & 4 \\
3 & & \\
\end{array},
\begin{array}{ccc}
1 & 3 & 1 \\
2 & & \\
\end{array}
\]

Using the recursive method of [16] described in subsection 3.1.1 we compute the KS-Young symmetrizers and the corresponding bases.

- For \( P_{12} \) we get, up to a multiplicative constant,

\[
P_{12} P'_{12} P'_{12} = P' P' P' = S_{1,2,3}A_{1,4}S_{1,2,3},
\]

which applied to \( V_0 \) and \( V_4 \) gives zero, while applied to \( V_{1,2,3} \) gives the span of \( \psi_{1,2,3} \) with (again we omit normalization factors)

\[
\psi_1 = |1000⟩ + |0100⟩ + |0010⟩ - 3|0001⟩
\]

\[
\psi_2 = |1100⟩ + |1010⟩ + |0110⟩ - |1001⟩ - |0101⟩ - |0011⟩
\]

\[
\psi_3 = |0111⟩ + |1011⟩ + |1101⟩ - 3|1110⟩.
\]

Notice that \( \psi_3 \) is obtained from \( \psi_1 \) by exchanging the 1's and the 0's.

- For \( P_{13} \) we get, up to a multiplicative constant,

\[
P_{13} P'_{13} P'_{13} = P' P' P' = S_{1,2,3}A_{1,3}S_{1,2,3} = S_{1,2,3}A_{1,3}S_{1,2,3} = S_{1,2,3}A_{1,3}S_{1,2,3}.
\]

which applied to \( V_0 \) and \( V_4 \) gives zero, while applied to \( V_{1,2,3} \) gives the span of \( \chi_{1,2,3} \) with (again we omit normalization factors)

\[
\chi_1 = |1000⟩ + |0100⟩ - 2|0010⟩
\]

\[
\chi_2 = 2|1100⟩ - 2|0011⟩ + |1001⟩ + |0110⟩ - |1010⟩ - |0110⟩
\]

\[
\chi_3 = |0111⟩ + |1011⟩ - 2|1101⟩.
\]

- For \( P_{23} \) we get, up to a multiplicative constant,

\[
P_{23} P'_{23} P'_{23} = P' P' P' = A_{1,2}S_{1,3}A_{1,2}S_{1,3} = A_{1,2}S_{1,3}A_{1,2}S_{1,3}.
\]

which applied to \( V_0 \) and \( V_4 \) gives zero, while applied to \( V_{1,2,3} \) gives the span of \( \eta_{1,2,3} \) with (again we omit normalization factors)

\[
\eta_1 = |1000⟩ - |0100⟩,
\]

\[
\eta_2 = |1010⟩ + |1001⟩ - |0110⟩ - |0101⟩.
\]

\[
\eta_3 = |0111⟩ - |1011⟩.
\]
### 4.2.3 Young diagram corresponding to partition (2, 2)

There are two SYT’s corresponding to a partition (2, 2). They are

\[
\begin{array}{cc}
1 & 2 \\
3 & 4
\end{array} \quad \begin{array}{cc}
1 & 3 \\
2 & 4
\end{array}
\]

Using the algorithm in [16] we compute the KS-Young symmetrizers and the corresponding bases.

- For \( P \) we get, up to a multiplicative constant,

\[
P = P' P' P' P' = P' P' P' P' P' P' P' P' P' P' P' P' P' P' =
\]

\[
S_{1,2} A_{1,3} S_{1,2} S_{3,4} A_{1,3} A_{2,4} S_{1,2} A_{1,3} S_{1,2},
\]

which applied to \( V_{0,1,3,4} \) gives zero, while applied to \( V_2 \) gives the span of

\[
\mu_2 = 2|1100\rangle + |20011\rangle – |0110\rangle – |1010\rangle – |0101\rangle – |0101\rangle
\]

- For \( P \) we get, up to a multiplicative constant,

\[
P = P' P' P' P' = P' P' P' P' P' P' P' P' P' P' P' P' P' P' =
\]

\[
A_{1,2} S_{1,3} A_{1,2} S_{1,3} S_{2,4} A_{1,2} A_{3,4} A_{1,2} S_{3,4} A_{1,2} = A_{1,2} S_{1,3} A_{1,2} S_{1,3} S_{2,4} A_{3,4} A_{1,2} S_{1,3} A_{1,2},
\]

which applied to \( V_{0,1,3,4} \) gives zero, while applied to \( V_2 \) gives the span of

\[
\nu_2 = |1010\rangle + |0101\rangle – |0110\rangle – |1010\rangle.
\]

### 4.2.4 Structure of the dynamical Lie algebra \( \mathcal{L} \)

According to the theory developed in this paper the above change of coordinates transforms the \( u^{S_n}(2^4) \) into a block diagonal form with one copy of \( u(5) \) acting on \( \text{span}\{\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_4\} \), the so called symmetric states, three copies of \( u(3) \) acting respectively on \( \text{span}\{\psi_1, \psi_2, \psi_3\} \), \( \text{span}\{\chi_1, \chi_2, \chi_3\} \), or \( \text{span}\{\eta_1, \eta_2, \eta_3\} \) and two copies of \( u(1) \) acting, respectively, on \( \text{span}\{\nu_1\} \) or \( \{\nu_2\} \). Therefore in the given coordinates matrices in \( \mathcal{L} = su^{S_n}(2^4) \) (recall that from the results of [4] the dynamical Lie algebra \( \mathcal{L} \) is equal to \( u^{S_n}(2^n) \) except for the requirement that the matrices have zero trace) have the form (cf. Theorem[2])

\[
\begin{pmatrix}
A_5 & 0 & 0 & 0 & 0 & 0 \\
0 & B_3 & 0 & 0 & 0 & 0 \\
0 & 0 & B_3 & 0 & 0 & 0 \\
0 & 0 & 0 & C_1 & 0 & 0 \\
0 & 0 & 0 & 0 & C_1 & 0
\end{pmatrix}
\]

where \( A_5 \) is an arbitrary matrix in \( u(5) \), \( B_3 \) is an arbitrary matrix in \( u(3) \) and \( C_1 \) is an arbitrary number in \( u(1) \) (i.e., a purely imaginary number), with \( Tr(A_5) + 3Tr(B_3) + 2C_1 = 0 \). Therefore, according to Theorem[2] the system is state controllable on each of the invariant subspaces, and in particular on the space \( \text{span}\{\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_4\} \) of symmetric states, a fact that is true for every \( n \). Similarly to what it has been done for Example[17] in the previous subsection, we can calculate the matrices of the restrictions of \( -iH_z \), \( -iH_x \) and \( -iH_y \) to the various invariant subspaces and consider control theoretic problems in each subspace.
5 Concluding Remarks

We have laid the theoretical foundations of the decomposition of the dynamics of control systems with symmetries based on ideas of representation theory. The main application we have in mind are multi-partite quantum systems where the state space is naturally described on a tensor space with the symmetry group being made up of permutations between the different subsystems. However, the approach can be used to decompose a state space which has a structure different from the one of a tensor space, when subject to a finite set of symmetries. The representation theory approach naturally allows us to identify invariant subspaces of the dynamics on which we can set up independent control problems. According to Theorem 2 on each of these subsystems the dynamics is controllable.

Central to our treatment is the concept of a set of Generalized Young Symmetrizers (GYS’s), that is a complete set of primitive idempotent of the group algebra \( \mathbb{C}[G] \) associated with the finite group of symmetries \( G \) of the system. Their knowledge leads to a decomposition of the group algebra \( \mathbb{C}[G] \) into the irreducible representations of \( G \). They can also be seen as linear operators on the state space of the system \( \hat{V} \), and through a duality theorem (Theorem 1) they give the decomposition (22) of the dynamics into its invariant subspaces. There are two cases in which we are able to obtain the GYS’s explicitly. One of them is when the group of symmetries is the full group \( S_n \) of permutations of \( n \) objects. In this case, one uses the classical construction with Young diagrams and Young tableau (see, e.g., [25]) with the modification given in [16] [2] which is used to make the GYS’s Hermitian. In the Abelian case, we have given an explicit formula (29) for the GYS in terms of the characters associated with the representations. We remark that in the Abelian case, by considering the elements of the group of symmetries \( G \) as operators on the state space \( \hat{V} \), we could have simultaneously diagonalized the operators in \( G \). In the given basis, we can find elements of the group algebra \( \mathbb{C}[G] \) of the form \( \text{diag}(\lambda, \lambda, ..., \lambda, 0, 0, ..., 0) \), \( \text{diag}(0, 0, ..., 0, \mu, \mu, ..., \mu, 0, 0, ..., 0) \), \( \text{diag}(0, 0, ..., \nu, \nu, ..., \nu) \). In this basis, imposing that the Lie algebra commutes with \( G \) we obtain the block diagonal structure for the matrices in the Lie algebra of matrices commuting with \( G \). With formula (22) we have cast the case of Abelian groups in the general method of generalized Young symmetrizers and gave a systematic way to find such GYS. In fact, the projection operator \( P_\chi \) in (29) is a projection onto a common eigenspace of the elements \( h \) in the group \( G \) since, using (24) it is easily seen that, for every \( \hat{v} \in \hat{V} \), \( \hbar P_\chi \hat{v} = \chi(h^{-1})P_\chi \hat{v} \).

We have applied the GYS approach to two types of quantum spin networks, under global control, and we have described the structure of the dynamical Lie algebra for spins which have a next neighborhood interaction in a circular configuration and spin which are pairwise interacting. The results for the latter type of systems are a direct generalization, to any number \( n \) of spin, of the results in [4] which were restricted to the case of \( n \leq 3 \). We have presented the calculations for the case of \( n = 4 \) in detail in the previous section.

There has recently been a large amount of literature on the analysis and decomposition of the dynamics of systems on Lie groups that are not controllable, especially in the context of quantum control systems. In general, lack of controllability may be due to the presence of a group of symmetries but may also occur without any symmetry. This means that the Lie algebra generated by the matrices \( A \), and \( B_j \) in (1) fail to generate some ‘natural’ Lie algebra which, in the case of quantum systems is \( u(N) \), \( su(N) \) or \( sp(N/2) \) if we are only interested in controllability of the state (rather than the possibility to reach any desired unitary operator). The paper [8] and the book [9] present general algorithms to obtain the decomposition of the dynamical Lie algebra in the uncontrollable case. The paper [8] does not assume symmetries and does not use representation theory. The starting point of the algorithms is a basis of the dynamical Lie algebra from which one calculates bases of the simple ideals and the centralizer of the dynamical Lie algebra. This approach is very general but it does not naturally take into account the action of the dynamical Lie algebra on the underlying vector space. Moreover, although the algorithms can always be used for a specific systems they do not naturally give insights for classes of systems, as does the method described here, and computations might be difficult if the dimensions grows exponentially with the number of subsystems as in the case of spin networks. The paper [28] presents a comprehensive study of the various possible subalgebras of the dynamical Lie algebra under symmetries for spin networks, and, more in general, of symmetries in quantum systems controllability. Controllability of spin networks subject to symmetries were considered in the papers [26], [27], where several results were given on the subspace controllability of certain networks and on how this is related to the network configuration.

We hope that this paper will stimulate a unified approach to the analysis of controlled dynamics under symmetry based on the concept of Young symmetrizer and using techniques of representation theory. For this to happen, several mathematical problems will have to be resolved. More general methods to find GYS’s have to be found which somehow bridge the gap between the two cases discussed here, the Abelian case and the case of the fully...
symmetric group $S_n$. It will be important also to see how this method applies to different classes of spin networks, with possibly spin-spin interactions different from the Ising interaction we have considered in our examples. A technique to identify the (maximal) group of symmetries from the topology of the network will also be important to achieve, since in this paper we have assumed the group of symmetries $G$ given. Finally, it is a very important and intriguing question how non-controllable quantum systems can be used for quantum computation. In general, the dynamical Lie algebra describes the type of operations that can be performed with a given experimental set-up. Dimension formulas such as the one in (11) describe how the computational power increases with the number $n$ of subsystems. Some of these subsystems on which we have state controllability can be used to implement quantum computation in a robust fashion exploiting physical redundancy. Moreover, some of the invariant subspaces are important from a quantum information perspective. For example the states (47) include the famous GHZ-states [11] and W-states [10], and this was the main motivation for the paper [4].

Acknowledgement

Domenico D’Alessandro was partially supported by the NSF under Grant ECCS 1710558. The authors would like to thank Dr. F. Albertini for helpful discussions on the topic of this paper.

References

[1] M. Abramowitz and I.A. Stegun, Handbook of Mathematical Functions, New York: Dover Publications.
[2] J. Alcock-Zeilinger and H. Weigert, Compact Hermitian Young projection operators, J. Math. Phys. 58(5), October 2016.
[3] F. Albertini and D. D’Alessandro, On symmetries in time optimal control, sub-Riemannian geometries and the K-P problem, Journal of Dynamical and Control Systems, (2018), Vol. 23, n.1.
[4] F. Albertini and D. D’Alessandro, Controllability of Symmetric Spin Networks arXiv:1803.06689v1 [quant-ph], Journal of Mathematical Physics, to appear.
[5] T. M. Apostol, Introduction to Analytic Number Theory, Undergraduate texts in Mathematics, New York-Heidelberg: Springer Verlag, 1976.
[6] J. Chen, H. Zhou, C. Duan, and X. Peng, Preparing GHZ and W states on a long-range Ising spin model by global control, Physical Review A (2017)
[7] D. D’Alessandro, Introduction to Quantum Control and Dynamics, CRC Press, Boca Raton FL, August 2007.
[8] D. D’Alessandro, Constructive decomposition of the controllability Lie algebra for Quantum systems, IEEE Transactions on Automatic Control June 2010, 1416-1421.
[9] W. A. de Graaf, Lie Algebras; Theory and Algorithms. Amsterdam, The Netherlands: North Holland, 2000.
[10] W. Dür, G. Vidal and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A, 62, 062314 (2000)
[11] D. M. Greenberger, M. A. Horne and A. Zeilinger, Going beyond Bell’s theorem, in Bell’s Theorem, Quantum Theory and the Conceptions of the Universe, pp. 73-76, Kluwer Academics, Dordrecht, The Netherlands, (1989).
[12] W. Fulton and J. Harris, Representation Theory; A First Course, Graduate Texts in Mathematics, No. 129, Springer, New York 2004.
[13] R. Goodman, N.R. Wallach, Symmetry, Representations and Invariants, Springer Graduate Texts in Mathematics, 2009.
[14] I. M. Isaacs, Character Theory of Finite Groups, Dover, New York, 1976.
Appendix A: Proofs of Formula (11) and of Formula (43)

5.1 Proof of Formula (11)

Proof. By Proposition 1.2 we have
\[ \dim u_{C_n}(2^n) = \#\text{orbits} \]  
(56)

where \( \#\text{orbits} \) is the number of orbits with respect to the action of \( C_n \) on the set of all words of length \( n \) in the four symbols \( 1, \sigma_x, \sigma_y, \sigma_z \).

Recall Burnside counting theorem which applied to our case gives:
\[ \#\text{orbits} = \frac{1}{|C_n|} \sum_{g \in C_n} |\text{Fix}_g| \]  
(57)

The cyclic group \( C_n = \langle Z \rangle \) has a unique subgroup \( H_m \) of order \( m \) for every positive divisor \( m \) of \( n \), namely \( H_m = \langle Z^{n/m} \rangle \). Since every element \( g \) of \( C_n \) generates some subgroup, we can partition \( C_n \) into subsets corresponding to which subgroup they generate. Then we get
\[ \#\text{orbits} = \frac{1}{n} \sum_{m|n} \sum_{g \in C_n \atop (g) = H_m} |\text{Fix}_g| \]  
(58)

\footnote{We use the standard convention in group theory denoting by \( \langle F_1, F_2, ..., F_s \rangle \) the group generated by the set \( \{F_1, F_2, ..., F_s\} \).}
where \( \sum_{m|n} \) means we sum over all positive integers \( m \) which divide \( n \). Next we use the fact that a word is fixed by \( g \) if and only if it is fixed by the cyclic subgroup \( \langle g \rangle \). Thus we get from (58)

\[
\#\text{orbits} = \frac{1}{n} \sum_{m|m} \sum_{g \in C_m \cap \langle g \rangle = H_m} |\text{Fix}_{H_m}^g| \tag{59}
\]

Now recall that any cyclic group has many possible generators. In particular if \( g \) generates a group \( G \) of order \( m \), \( g^n \) generates \( G \) if and only if \( \gcd(a,m) = 1 \). Applying this to \( G = H_m \), which is cyclic of order \( m \), \((Z^\#)^\circ \) generates \( H_m \) if and only if \( \gcd(a,m) = 1 \). The Euler’s totient function \( \phi(m) \) counts the number of positive integers \( a \) less than or equal to \( m \) having greatest common divisor 1 with \( m \). Therefore \( H_m \) has \( \phi(m) \) generators. This means that we can rewrite (59) as follows:

\[
\#\text{orbits} = \frac{1}{n} \sum_{m|m} |\text{Fix}_{H_m}^g| \cdot \phi(m) \tag{60}
\]

If \( m \) is a positive integer that divides \( n \) then the number of words of length \( n \) in 4 letters that are fixed by \( H_m \) (equivalently, by \( Z^{n/m} \)) is \( 4^{n/m} \) because such words are uniquely determined by the first \( n/m \) positions, which can be arbitrarily chosen. This gives us the formula we wanted to show

\[
\#\text{orbits} = \dim u^{C_n}(2^n) = \frac{1}{n} \sum_{m|m} 4^{n/m} \phi(m). \tag{61}
\]

\( \square \)

Formula (61) can be written using Dirichlet convolution (see, e.g., [5]),

\[
f \ast g = \sum_{m|m} f(n/m)g(m), \tag{62}
\]

which is defined for any two complex-valued functions \( f \) and \( g \) defined on the set of divisors of \( n \). We have that

\[
\dim u^{C_n}(2^n) = f \ast \phi, \quad f(m) = \frac{1}{n} 4^m. \tag{63}
\]

### 5.2 Proof of Formula (43)

With the same steps as in the proof of the previous formula applied to \( X_k \) rather than the whole set of words we arrive at (cf., formula (60))

\[
|X_k/C_n| = \frac{1}{n} \sum_{m|m} |\text{Fix}_{H_m}^g| \cdot \phi(m), \tag{64}
\]

where now the set fixed by \( H_m \), \( \text{Fix}_{H_m}^g \) is considered in \( X_k \) rather than in the space of all \( 2^n \) binary words. Recall that \( H_m \) is the subgroup generated by \( Z^{n/m} \). A word \( \underline{a} \) in \( X_k \) is fixed by \( H_m \) if and only if \( Z^{n/m}(\underline{a}) = \underline{a} \). This in turn holds if and only \( n/m \) is a multiple of the period \( T \) of \( \underline{a} \). Therefore the words in \( \text{Fix}_{H_m}^g \) have period \( T \) such that \( n/T \) divides \( k \) and \( m \) divides \( n/T \). Their number by definition is \( w(n,m,k) \). Moreover in the sum (64) \( m \) has to divide \( n/T \) and therefore \( n \), and \( n/T \) has to divide \( k \), so that \( m \) also has to divide \( k \). Therefore the nonzero terms are obtained for \( m \) at most equal to the greatest common divisor of \( n \) and \( k \), i.e., \( \gcd(n,k) \) which gives formula (43).

### Appendix B: Proof of Theorem 1 (Sketch)

We shall mostly follow [21] which however follows [13]. The first step is to define classes of \( G \)-equivalent irreducible representations \( [j] \) on \( \hat{V} \). Since \( G \) is finite and \( \hat{V} \) is a representation of \( G \), it can be decomposed into its irreducible components. By collecting equivalent irreducible components, we define \( \hat{V}_{[j]} := \bigoplus_{j \in [j]} \hat{V}_j \) and we have the so-called isotypical decomposition (cf. Proposition 3.9 in [21]), i.e.,

\[
\hat{V} = \bigoplus_{[j] \in \hat{G}} \hat{V}_{[j]}, \tag{65}
\]
where $\hat{G}$ denotes the (finite) set of equivalence classes of irreducible representations. We remark that the Proposition in [21] is given for a Lie group but only the hypothesis of complete reducibility is used which is automatically true for finite groups as considered here.

Consider now a class $[j] \in \hat{G}$ and a representative $j$, $(\tilde{V}_j)$, as well as the space $\text{Hom}_G(\tilde{V}_j, \tilde{V}) \otimes \tilde{V}_j$. By defining the action of $G$ as the action on the second factor, i.e., $g(u \otimes \tilde{v}) := u \otimes g\tilde{v}$, for $u \in \text{Hom}_G(\tilde{V}_j, \tilde{V})$ and $\tilde{v} \in \tilde{V}_j$, we can consider $\text{Hom}_G(\tilde{V}_j, \tilde{V}) \otimes \tilde{V}_j$ as a representation of $G$, i.e., as $G$--module. Now consider the map $M_j : \text{Hom}_G(\tilde{V}_j, \tilde{V}) \otimes \tilde{V}_j \rightarrow \tilde{V}$, which is linear and defined on tensor products as

$$M_j(u \otimes \tilde{v}) := u(\tilde{v}).$$

This is also a $G$--map since $u(g \tilde{v}) = gu(\tilde{v})$ because $u \in \text{Hom}_G(\tilde{V}_j, \tilde{V})$. In fact, this map establish a $G$--isomorphism between $\text{Hom}_G(\tilde{V}_j, \tilde{V}) \otimes \tilde{V}_j$ and $\tilde{V}_j$ (Proposition 3.10 in [21]). We have therefore

$$\text{Hom}_G(\tilde{V}_j, \tilde{V}) \otimes \tilde{V}_j \simeq \tilde{V}_j.$$

This gives formula (18) with the obvious change of notation $C_j \leftrightarrow \tilde{V}_j$. Next we need to show that

"Each $\text{Hom}_G(\tilde{V}_j, \tilde{V})$ is an irreducible representation of $\hat{R}^G$." assuming that it is not equal to $\{0\}$.

We use an idea similar to what led to Theorem 2 to infer properties of representation of a Lie algebra $\mathfrak{r}$ and $\hat{R}^G$ from properties of representations of algebras. This is because we are going to use theorems in [21] and [13] which were proved for algebra representations. Given Lie algebra (defining) representations $\mathfrak{r}$ and $\hat{R}^G$ we can extend to algebra representations $\mathfrak{r}$ and $\hat{R}^G$ which are defined by taking the algebra (over $\mathbb{C}$) generated by a basis in $\mathfrak{r}$ and $\hat{R}^G$, respectively. With $r_1$ and $r_2$ in $\mathfrak{r}$ the representation $\rho$ of $\mathfrak{r}$ is defined so that $\rho(r_1 r_2) = \rho(r_1) \rho(r_2)$. $\mathfrak{r}$ (resp. $\hat{R}^G$) is irreducible if and only if $\mathfrak{r}$ (resp. $\hat{R}^G$) is irreducible. For instance if $\mathfrak{r} = u(2^n)$ then $\mathfrak{r}$ is the complexification of $u(2^n)$, that is, $\mathfrak{gl}(2^n, \mathbb{C})$.

$\hat{R}^G$ acts on $\text{Hom}_G(\tilde{V}_j, \tilde{V})$ by left multiplication, i.e., $u \in \text{Hom}_G(\tilde{V}_j, \tilde{V})$, $r \in \hat{R}^G$, $u \rightarrow ru$. In fact, if $r \in \hat{R}^G$, $u \in \text{Hom}_G(\tilde{V}_j, \tilde{V})$, $g \in G$, we have $g(ru) = rgu = r(ug)$. The theorem says that $\text{Hom}_G(\tilde{V}_j, \tilde{V})$ is in fact an irreducible $\hat{R}^G$--module. To show irreducibility one picks two arbitrary nontrivial elements in $\text{Hom}_G(\tilde{V}_j, \tilde{V})$, $T$ and $S$ and shows that there exists an $r \in \hat{R}^G$, such that $rT = S$. This excludes the existence of proper invariant subspaces for the action of $\hat{R}^G$. This is shown by noticing that, as $T$ and $S$ act on $\tilde{V}_j$, $\text{Ker}(T) = \text{Ker}(S) = \{0\}$, since otherwise $\text{Ker}(T)$ or $\text{Ker}(S)$ will be a nontrivial sub-representation of $\tilde{V}_j$ which is excluded since $\tilde{V}_j$ is irreducible. Defined $X := TV_j$ and $Y := SV_j$, this gives an isomorphism between $X$, $\tilde{V}_j$ and $Y$, which is also a $G$-map. This gives an element of $\text{Hom}_G(X, \tilde{V})$ whose image is $Y$. According to a Lemma (Lemma 4.2.3 in [13]) which is a consequence of Jacobson density theorem (Theorem 4.1.5 in [13]) such an isomorphism can be realized as the restriction of an element $r \in \hat{R}^G$. Now consider $\tilde{V}_j$ and $S\tilde{V}_j$ which are two equivalent representations of $G$. The maps $sT : \tilde{V}_j \rightarrow S\tilde{V}_j$ and $S : \tilde{V}_j \rightarrow S\tilde{V}_j$ are both in $\text{Hom}_G(\tilde{V}_j, S\tilde{V}_j)$. It is known (Lemma 2.57 in [21]) that if $V$ and $W$ are equivalent representations of a finite group $G$, $\dim \text{Hom}_G(V, W) = 1$. Therefore $S$ is a multiple of $rT$, i.e., $S = crT$ for some complex number $c \in \mathbb{C}$ and $cr$ is the required map which maps $T$ to $S$. We refer to the proof of Theorem 4.5 of [21] for details.

Finally we have to show that $\text{Hom}_G(\tilde{V}_j, \tilde{V})$ and $\text{Hom}_G(\tilde{V}_i, \tilde{V})$ are isomorphic representations of $\hat{R}^G$ if and only if $[j] = [i]$. If $\tilde{V}_j$ and $\tilde{V}_i$ are $G$-isomorphic, there exists a $G$-isomorphism, $T : \tilde{V}_i \rightarrow \tilde{V}_j$. The map $\Phi_T$ that maps $f \in \text{Hom}_G(\tilde{V}_j, \tilde{V})$ to $fT \in \text{Hom}_G(\tilde{V}_i, \tilde{V})$ is an $\hat{R}^G$-isomorphism, since for $r \in \hat{R}^G$, $r(\Phi_T(f)) = rTf = (rf)T = \Phi_T(rf)$. If $\tilde{V}_j$ and $\tilde{V}_i$ are not $G$-isomorphic a contradiction argument (cf. Theorem 4.5 in [21]) shows that the two representations are not equivalent.

**Appendix C: Proof of Proposition 3.1**

We first introduce another $\hat{R}^G$ module: $(V^* \otimes W)^G$, the space of all elements in $V^* \otimes W$ which are invariant under $G$. Here $G$ acts on $W$ on the left and on $V^*$ on the right. $(V^* \otimes W)^G$ is a left $\hat{R}^G$-module since $\hat{R}^G$ acts on elements of $(V^* \otimes W)^G$ by $1 \otimes r$, for $r \in \hat{R}^G$, i.e., as $1 \otimes r(\phi \otimes \tilde{w}) = \phi \otimes r\tilde{w}$. This action maps elements of $(V^* \otimes W)^G$ to elements of $(V^* \otimes W)^G$ and we have, for $g \in G$, $\phi g \otimes gr\tilde{w} = g\phi \otimes r\tilde{w} = \phi \otimes r\phi \in (V^* \otimes W)^G$.

**Lemma 5.1.** As $\hat{R}^G$-modules $V^* \otimes_{\mathbb{C}[G]} W$ and $(V^* \otimes W)^G$ are isomorphic.
Proof. Consider the linear map \( P \) on \( V^* \otimes W \), defined by
\[
P(\mu \otimes \bar{w}) = \frac{1}{|G|} \sum_{g \in G} \mu g^{-1} \otimes g\bar{w},
\]
which has as its image \((V^* \otimes W)^G\). From the (Linear Algebra) first isomorphism theorem we know that \( \text{Im}(P) \cong (V^* \otimes W)/\text{Ker}(P) \). Therefore we show that \( \text{Ker}(P) = \text{span}\{\mu a \otimes \bar{w} \mid \bar{w} \in W, \mu \in V^*, a \in \mathbb{C}[G]\} \) := \( N \) (cf. \([19]\)).

\( (N \subseteq \text{Ker}(P):) \) By linearity it is enough to take an element \( x \in N \) of the form \( x = \mu h \otimes \bar{w} - \mu \otimes h\bar{w} \) with \( h \in G \). We have
\[
P(x) := \frac{1}{|G|} \sum_{g \in G} (\mu hg^{-1} \otimes g\bar{w} - \mu g^{-1} \otimes gh\bar{w}),
\]
which defining \( m = gh^{-1} \), gives
\[
P(x) = \frac{1}{|G|} \sum_{m \in G} (\mu m^{-1} \otimes mh\bar{w}) - \frac{1}{|G|} \sum_{g \in G} (\mu g^{-1} \otimes gh\bar{w}) = 0.
\]

\( (\text{Ker}(P) \subseteq N:) \) First notice that for every \( \mu \otimes \bar{w} \), and every \( g \in G \), \( \mu \otimes \bar{w} - \mu g^{-1} \otimes g\bar{w} \in N \), since, by defining \( \nu := \mu g^{-1} \) it can be written as \( \nu g \otimes \bar{w} - \nu \otimes g\bar{w} \). Write \( x \in \text{Ker}(P) \) as \( x := \sum_j \mu_j \otimes \bar{w}_j \). We have, from \( x = (1-P)x \),
\[
x = \frac{1}{|G|} \sum_j (\sum_{g \in G} \mu_j \otimes \bar{w}_j - \mu_j g^{-1} \otimes g\bar{w}_j),
\]
which is the sum of elements in \( N \) and therefore in \( N \).

The induced isomorphism which associates with \([\mu \otimes \bar{w}] \in V^* \otimes_{\mathbb{C}[G]} W\) \( P(\mu \otimes W) \in (V^* \otimes W)^G \) is an \( \mathcal{R}^G \) isomorphism since \( P \) commutes with \( 1 \otimes r \), for all \( r \in \mathcal{R}^G \).

Proof. (Proof of the Proposition) We regard \( \text{Hom}(V,W) \) as a representation of \( G \), where the (left) action of \( G \) on \( \text{Hom}(V,W) \) is defined, for \( T \in \text{Hom}(V,W) \) by \( T \rightarrow gTg^{-1} \). Therefore \( \text{Hom}_G(V,W) \) coincides with the subspace \((\text{Hom}(V,W))^G\) of elements of \( \text{Hom}(V,W) \) which are fixed by the action of any \( g \in G \), since \( gTg^{-1} = T \) is equivalent to \( gT = Tg \).

In view of the above Lemma, to prove the proposition, it is enough to display an \( \mathcal{R}^G \)-isomorphism between \((V^* \otimes W)^G \) and \((\text{Hom}(V,W))^G\). Recall that there is a canonical isomorphism \( \Psi \), between \( V^* \otimes W \) and \( \text{Hom}(V,W) \), defined as, for each \( \bar{v} \in V \),
\[
\Psi(\mu \otimes \bar{w})(\bar{v}) := \mu(\bar{v})\bar{w}.
\]
Given the actions of \( G \) on \( V^* \otimes W \) and \( \text{Hom}(V,W) \), \( \Psi \) is a \( G \)-map. In order to see this, take a general \( \mu \in V^* \), \( \bar{w} \in W \) and \( \bar{v} \in V \). We have
\[
(g\Psi)(\mu \otimes \bar{w})(\bar{v}) := g(\Psi(\mu \otimes \bar{w}))(g^{-1}\bar{v}) := g\mu(g^{-1}\bar{v})\bar{w} = (\Psi(\mu g^{-1} \otimes g\bar{w}))(\bar{v}) = (\Psi(\mu \otimes g\bar{w}))(\bar{v}).
\]
It is a general fact, easily verifiable, that given a \( G \)-isomorphism \( \Psi \) between two representations of \( G \), \( C \xrightarrow{\Psi} D \), the restriction of \( \Psi \) to the fixed set under \( G \) in \( C^G \), is an isomorphism between \( C^G \) and \( D^G \), the fixed set of \( D \) under \( G \). Applying this to our situation, we have a \( G \)-isomorphism between \((V^* \otimes W)^G \) and \((\text{Hom}(V,W))^G\). It is also easily seen that this is an \( \mathcal{R}^G \)-isomorphism since for \( r \in \mathcal{R}^G \), we have
\[
(r\Psi)(\mu \otimes \bar{w})(\bar{v}) := r\mu(\bar{v})\bar{w} = \mu(\bar{v})r\bar{w} = \Psi((1 \otimes r)(\mu \otimes \bar{w}))(\bar{v}),
\]
and therefore the proof is complete. \( \square \)