2008

Lie algebra decompositions with applications to quantum dynamics

Mehmet Dağlı
Iowa State University

Lie algebra decompositions with applications to quantum dynamics

by

Mehmet Dağlı

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:
Domenico D'Alessandro, Co-major Professor
Jonathan D. H. Smith, Co-major Professor
Sung-Yell Song
Siu-Hung Ng
Umesh Vaidya

Iowa State University

Ames, Iowa

2008

DEDICATION

Dedicated to my family, especially to my wife Burcu.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like express my gratitude to those who helped me, both directly and indirectly, with conducting this research and writing this dissertation. First, I would like to thank my advisors, Domenico D'Alessandro and Jonathan D. H. Smith, for their guidance and support. I would also like to thank my committee members for their interest and contributions to this work: Sung-Yell Song, Siu-Hung Ng, and Umesh Vaidya. In addition, I would like to thank to Department of Mathematics at Iowa State University for providing me with an outstanding working environment. I gratefully acknowledge the scholarship provided by the Turkish Ministry of National Education. Finally, I thank my wife, Burcu, for her patience and support.

ABSTRACT

Lie group decompositions are useful tools in the analysis and control of quantum systems. Several decompositions proposed in the literature are based on a recursive procedure that systematically uses the Cartan decomposition theorem. In this dissertation, we establish a link between Lie algebra gradings and recursive Lie algebra decompositions, and then we formulate a general scheme to generate Lie group decompositions. This scheme contains some procedures previously proposed as special cases and gives a virtually unbounded number of alternatives to factor elements of a Lie group.

CHAPTER 1. Introduction

Decompositions of a Lie group $\mathbf{G}$ serve to factorize every element X_f of $\mathbf{G}$ into a product

$$X_f = X_1 X_2 \cdots X_n \,, \tag{1.1}$$

where X_j, $j = 1, \ldots, n$, is an elementary factor belonging to a low dimensional subgroup of $\mathbf{G}$. In recent years, Lie group decompositions have generated a considerable amount of interest for several reasons. In control theory, such decompositions allow the task of designing a control to steer a state of the system to a final target state to be reduced into a sequence of subtasks that are easier to handle. More formally, consider a right invariant bilinear system

$$\dot{X} = AX + \left(\sum_{i=1}^{m} B_i u_i \right) X \,, \qquad X(0) = \mathbf{1} \,, \tag{1.2}$$

on a Lie group $\mathbf{G}$, where $A, B_1, \ldots, B_m$ are elements of the Lie algebra corresponding to $\mathbf{G}$, $u_1, \ldots, u_m$ are the control functions, and $\mathbf{1}$ is the identity in $\mathbf{G}$. Assume that the task is to steer the state X of (1.2) to a desired value X_f. If a decomposition of X_f into simpler factors as in (1.1) is known, it may be easier to find controls to steer to the factors X_j. Then, the concatenation of these control functions give the full control that drives X to the desired target state X_f. It is clear that some decompositions may be more convenient than others, depending on the particular situation at hand. Hence, it is important to have several ways to decompose the Lie group $\mathbf{G}$ and to be able to choose the best one for a specific situation.

Lie group decompositions have been extensively used in quantum control and information theory in which the relevant Lie group is the Lie group $\mathbf{U}(n)$ of $n \times n$ unitary matrices. Decompositions of $\mathbf{U}(n)$ are often used to analyze the dynamics of quantum systems [9]. In particular, for multipartite quantum systems such decompositions allow the identification of the local and entangling parts of a given unitary evolution. In this context, one can analyze the entanglement dynamics [4, 5, 11, 28]. In quantum information theory, Lie group decompositions can be used to design *quantum circuits*, that is, sequences of gates which perform operations on the quantum state. In particular, assuming that a certain quantum algorithm corresponds to a unitary transformation X_f on the state of a quantum system, a decomposition of the type (1.1) allows to break X_f into a sequence of simple operations $X_1, X_2, \ldots, X_n$ [19, 20, 25].

Lie group decompositions also have applications in the control of switching lossless electrical networks [1]. In this case, the relevant Lie group is the Lie group $\mathbf{SO}(n)$ of $n \times n$ orthogonal matrices with determinant equal to 1, and the evolution of the system is naturally of the form (1.1), where $X_j = e^{A_j t}$, $j = 1, \ldots, r$, with A_j a skew-symmetric matrix, depending on the current configuration of the network. By changing the configuration we drive the system to a desired state. The Lie group decomposition determines the type of configuration used and the time for a network to be in a given configuration.

For these reasons, several Lie group decompositions have been introduced in recent years [4, 5, 10, 11, 16]. In [4, 5] a decomposition called the *concurrence canonical decomposition (CCD)* was studied in the context of entanglement theory. The *concurrence* is a measure that quantifies the amount of entanglement [14, 26]. The CCD decomposes every unitary evolution on N qubits into a part that does not change the concurrence on the N qubits and a part that does. It is a Cartan decomposition in that it corresponds to a symmetric space of $\mathbf{SU}(2^N)$ [13]. In [10] the CCD was further studied and generalized to multipartite systems of arbitrary dimensions. The resulting decomposition was called an *odd-even decomposition (OED).* The OED is a decomposition of unitary evolutions on multipartite systems constructed in terms of decompositions on the single subsystems. As the CCD is related to the concurrence on N qubits, the OED has the same meaning for the generalized concurrences studied by Uhlmann in [24]. *Recursive* decompositions apply the Cartan decomposition theorem successively in order to decompose the factors into simpler ones. One of the first works in this direction is [16], where it was shown how to decompose the unitary operators on a quantum system of N qubits as a product of evolutions acting on a single qubit and two qubits. In the spirit of this study, another recursive decomposition was presented in [11] to display the local and entangling parts of unitary operators on a bipartite system of arbitrary dimensions.

This dissertation is devoted to recursive decompositions. Using the relation between Cartan decompositions of Lie algebras and Lie algebra gradings, we show that the recursive decompositions of [11, 16] are a special case of a general scheme from which several other recursive decompositions can be obtained. The main results of this dissertation are already published in [8]. Here, we extend and fill the gaps of the presentation of [8].

1.1 Outline

This dissertation is organized as follows: In Chapter 2, we provide the background material concerning the basic concepts of Cartan decompositions of a Lie algebra and KAK decompositions of a Lie group. Then, we describe the recursive decompositions of Khaneja and Glaser [16], and D'Alessandro and Romano [11].

In Chapter 3, we briefly review some basic concepts of quantum mechanics, and then we discuss a controllability problem. In particular, we show how the two qubit canonical decomposition can be used in the solution of this problem. We also review the main ingredients of the CCD, a generalization of the two qubit canonical decomposition to N qubits [4, 5].

In Chapter 4, we illustrate the dual structures between the Lie algebra $\mathfrak{u}(n)$ of $n \times n$ skew-Hermitian matrices and the Jordan algebra $i\mathfrak{u}(n)$ of $n \times n$ Hermitian matrices, and then we use this duality to construct the OED for multipartite quantum systems in arbitrary dimensions [8, 10]. We also present the linear algebra tools involved in the actual calculation of the factors of the OED, and we give a numerical example.

In Chapter 5, we describe the Lie algebra gradings and establish a link between gradings and recursive decompositions. This gives a general method to develop recursive decompositions of $\mathbf{U}(n)$. Then, we show how the recursive decompositions of [11, 16] are special cases of this general procedure and how new recursive decompositions can be obtained. We also give a numerical example illustrating the calculation of the recursive decompositions. In particular, we obtain several decompositions of the generalized SWAP operator acting on three qubits.

In Chapter 6, we summarize our results and present some concluding remarks.

CHAPTER 2. Background on Lie algebras

Lie algebras and their decompositions play an important role in analyzing quantum mechanical systems. In this chapter, we recall first the basic facts and definitions about Lie algebras, and then we review the basic concepts of Cartan decompositions of Lie algebras, with particular emphasis on decompositions of $\mathfrak{u}(n)$. Next, we describe the Khaneja Glaser and D'Alessandro Romano decompositions, which are based on recursive procedures that systematically apply Cartan decompositions. In order to illustrate the concept, we present several examples. We mainly follow [9, 12, 13].

2.1 Lie Algebras

Definition 2.1.1. *A Lie algebra $\mathcal{L}$ is a vector space over a field $\mathbb{F}$ with a bilinear map*

$$[\,\cdot\,,\cdot\,] : \mathcal{L} \times \mathcal{L} \longrightarrow \mathcal{L}\,,$$

called the commutator *or the* Lie bracket*, satisfying the following conditions:*

1. *Anticommutativity:* $[x\,,y] = [y\,,x]\,,$

2. *Jacobi identity:* $[x\,,[y\,,z]\,] + [y\,,[z\,,x]\,] + [z\,,[x\,,y]\,] = 0\,,$

for all $x, y, z \in \mathcal{L}$.

In the special case where the groundfield $\mathbb{F}$ is of characteristic 2, the anticommutativity condition is replaced by the condition $[x, x] = 0$, for all $x \in \mathcal{L}$. In this dissertation, we shall be concerned with the Lie algebras over the field $\mathbb{R}$ of real numbers and $\mathbb{C}$ of complex numbers.

Example 2.1.1. *Any vector space $\mathcal{V}$ can be made into a Lie algebra by setting $[x\,,y] = 0$, for all $x, y \in \mathcal{V}$. Such a Lie algebra is called an* Abelian *Lie algebra. In particular, any one-dimensional Lie algebra is necessarily Abelian.*

Definition 2.1.2. *A subspace $\mathcal{K}$ of $\mathcal{L}$ is called a* Lie subalgebra *if $\mathcal{K}$ is closed under the commutator. In other words, $[\mathcal{K}\,,\mathcal{K}] \subseteq \mathcal{K}$, where $[\mathcal{K}\,,\mathcal{K}] = \{[x\,,y] : x, y \in \mathcal{K}\}$.*

Definition 2.1.3. *A Lie subalgebra $\mathcal{I}$ of $\mathcal{L}$ is called an* ideal *if $[\mathcal{I}\,,\mathcal{L}] \subseteq \mathcal{I}$, i.e., if $x \in \mathcal{I}$ and $y \in \mathcal{L}$, then $[x\,,y] \in \mathcal{I}$. In particular, Lie algebra ideals are two-sided, that is, $[\mathcal{I}\,,\mathcal{L}] = [\mathcal{L}\,,\mathcal{I}]$.*

Example 2.1.2. *The center $Z(\mathcal{L})$ of a Lie algebra $\mathcal{L}$ defined by*

$$Z(\mathcal{L}) := \operatorname{span}\{x \in \mathcal{L} : [x\,,y] = 0 \text{ for all } y \in \mathcal{L}\}$$

is an ideal of $\mathcal{L}$.

2.1.1 Linear Lie algebras

The vector space $M_n(\mathbb{F})$ of $n \times n$ matrices over a field $\mathbb{F}$ forms a Lie algebra under the matrix commutator defined by

$$[A\,,B] := AB - BA\,. \tag{2.1}$$

This Lie algebra is called the *general linear Lie algebra* over $\mathbb{F}$ and is denoted by $\mathfrak{gl}(n,\mathbb{F})$. The subalgebras of $\mathfrak{gl}(n,\mathbb{F})$ are called the *linear Lie algebras*, which will be reviewed next.

Let us consider the subspace $\mathfrak{sl}(n,\mathbb{F})$ of trace zero matrices in $\mathfrak{gl}(n,\mathbb{F})$, that is,

$$\mathfrak{sl}(n,\mathbb{F}) = \operatorname{span}\{A \in \mathfrak{gl}(n,\mathbb{F}) : \operatorname{tr}(A) = 0\}\,.$$

Let $A, B \in \mathfrak{gl}(n,\mathbb{F})$. Then, it can easily be seen that $\operatorname{tr}([A,B]) = 0$, i.e., $\mathfrak{sl}(n,\mathbb{F})$ is closed under the Lie bracket, and, therefore, it is a Lie subalgebra of $\mathfrak{gl}(n,\mathbb{F})$. This subalgebra is known as the *special linear Lie algebra.* The dimension of $\mathfrak{sl}(n,\mathbb{F})$ is $n^2 - 1$.

Another very important linear Lie algebra is the *special unitary Lie algebra* $\mathfrak{su}(n)$ of $n \times n$ skew-Hermitian matrices with trace zero, i.e.,

$$\mathfrak{su}(n) = \{A \in \mathfrak{gl}(n,\mathbb{C}) : A^\dagger = -A \text{ and } \operatorname{tr}(A) = 0\}\,.$$

The dimension of $\mathfrak{su}(n)$ is $n^2 - 1$. In particular, $\mathfrak{su}(n)$ is a subalgebra of the *unitary Lie algebra* $\mathfrak{u}(n)$ of $n \times n$ skew-Hermitian matrices.

Example 2.1.3. *The special unitary Lie algebra* $\mathfrak{su}(2)$ *is spanned by the matrices*

$$\bar{\sigma}_x = \frac{1}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad \bar{\sigma}_y = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \bar{\sigma}_z = \frac{1}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

The commutator relations of $\bar{\sigma}_x$, $\bar{\sigma}_y$ *and* $\bar{\sigma}_z$ *are given by*

$$[\bar{\sigma}_x\,, \bar{\sigma}_y] = \bar{\sigma}_z\,, \qquad [\bar{\sigma}_y\,, \bar{\sigma}_z] = \bar{\sigma}_x\,, \qquad [\bar{\sigma}_z\,, \bar{\sigma}_x] = \bar{\sigma}_y\,. \tag{2.2}$$

These relations completely describe $\mathfrak{su}(2)$*.*

The skew-symmetric matrices in $\mathfrak{su}(n)$ form another linear Lie algebra called the *special orthogonal Lie algebra*, that is,

$$\mathfrak{so}(n) = \{A \in \mathfrak{gl}(n, \mathbb{R}) : A^T = -A\}\,. \tag{2.3}$$

The dimension of $\mathfrak{so}(n)$ is $n(n-1)/2$.

Example 2.1.4. *The special orthogonal Lie algebra* $\mathfrak{so}(3)$ *is spanned by the matrices*

$$s_x = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \qquad s_y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \qquad s_z = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{2.4}$$

satisfying the commutation relations

$$[s_x\,, s_y] = s_z\,, \qquad [s_y\,, s_z] = s_x\,, \qquad [s_z\,, s_x] = s_y\,. \tag{2.5}$$

Another example of a linear Lie algebra is the *symplectic Lie algebra* $\mathfrak{sp}(n)$, namely the subalgebra of $2n \times 2n$ skew-Hermitian matrices A in $\mathfrak{gl}(2n, \mathbb{C})$, satisfying the condition

$$AJ + JA^T = 0\,,$$

where J is the $2n \times 2n$ matrix

$$J := \begin{pmatrix} 0 & \mathbf{1}_n \\ -\mathbf{1}_n & 0 \end{pmatrix}. \tag{2.6}$$

Here and in the rest of this dissertation, $\mathbf{1}_n$ denotes the $n \times n$ identity matrix. The dimension of $\mathfrak{sp}(n)$ is $n(2n+1)$.

2.1.2 Lie algebra homomorphisms

A *homomorphism* ψ between two Lie algebras $\mathcal{L}_1$ and $\mathcal{L}_2$ is a linear map compatible with the commutator, that is, $\psi : \mathcal{L}_1 \longrightarrow \mathcal{L}_2$ such that

$$\psi([x\,,y]_1) = [\psi(x)\,,\psi(y)]_2\,,$$

for all $x, y \in \mathcal{L}_1$. Here, $[\cdot\,,\cdot]_1$ and $[\cdot\,,\cdot]_2$ denote the commutators in $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively. A bijective homomorphism is called an *isomorphism*.

Example 2.1.5. *The special unitary Lie algebra* $\mathfrak{su}(2)$ *and the special orthogonal Lie algebra* $\mathfrak{so}(3)$ *are isomorphic. Indeed, the isomorphism is given by the map*

$$\bar{\sigma}_x \longmapsto s_x\,, \qquad \bar{\sigma}_y \longmapsto s_y\,, \qquad \bar{\sigma}_z \longmapsto s_z\,.$$

This can be seen by comparing the commutation relations given in (2.2) and (2.5).

Definition 2.1.4. *Let* $\mathcal{L}$ *be a Lie algebra and* $x \in \mathcal{L}$*. The map* $\mathrm{ad}_x : \mathcal{L} \longrightarrow \mathcal{L}$*, defined by*

$$\mathrm{ad}_x(y) = [x\,,y]\,, \tag{2.7}$$

is called the adjoint *map. The adjoint map is linear.*

Let $x, y, z \in \mathcal{L}$. Then, using the Jacobi identity, it can be verified that

$$\mathrm{ad}_{[x\,,y]} = [\mathrm{ad}_x\,,\mathrm{ad}_y]\,,$$

i.e., the adjoint map is a homomorphism; however, it is not an isomorphism in general.

2.1.3 Semisimple Lie algebras

A non-Abelian Lie algebra $\mathcal{L}$ is called *simple* if it has no nontrivial ideals. Furthermore, $\mathcal{L}$ is said to be *semisimple* if it is a direct sum of simple Lie algebras, i.e.,

$$\mathcal{L} = \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus \cdots \oplus \mathcal{I}_n\,,$$

where each subalgebra $\mathcal{I}_i$ is simple for all $i = 1, \ldots, n$. Note that $[\mathcal{I}_i\,,\mathcal{I}_j] = 0$ for distinct i and j since $[\mathcal{I}_i\,,\mathcal{I}_j]$ is a subalgebra of both $\mathcal{I}_i$ and $\mathcal{I}_j$.

The following theorem provides a convenient tool to check whether a Lie algebra $\mathcal{L}$ is semisimple or not. It is based on the *Killing form*, a symmetric bilinear form defined by

$$\kappa(x, y) = \mathrm{tr}(\mathrm{ad}_x \cdot \mathrm{ad}_y)\,, \tag{2.8}$$

with $x, y \in \mathcal{L}$.

Theorem 2.1.1 (Cartan's semisimplicity criterion)**.** *A Lie algebra $\mathcal{L}$ is semisimple if and only if the Killing form κ on $\mathcal{L}$ is non-degenerate.*

2.2 Cartan decomposition of a Lie algebra

Let $\mathcal{L}$ be a finite dimensional semisimple Lie algebra. A vector space decomposition

$$\mathcal{L} = \mathcal{K} \oplus \mathcal{P} \tag{2.9}$$

is called a *Cartan decomposition* if the subspaces $\mathcal{K}$ and $\mathcal{P}$ satisfy the commutation relations

$$[\mathcal{K}\,, \mathcal{K}] \subseteq \mathcal{K}\,, \qquad [\mathcal{K}\,, \mathcal{P}] \subseteq \mathcal{P}\,, \qquad [\mathcal{P}\,, \mathcal{P}] \subseteq \mathcal{K}\,. \tag{2.10}$$

The pair $(\mathcal{K}\,, \mathcal{P})$ of subspaces is called a *Cartan pair* of $\mathcal{L}$. In particular, $\mathcal{K}$ is closed under the commutator, and, therefore, it is a Lie subalgebra. The subspace $\mathcal{P}$ does not have the structure of a Lie algebra since it is not closed under the commutator. Therefore, any subalgebra contained in $\mathcal{P}$ is necessarily Abelian. A maximal Abelian subalgebra $\mathcal{A}$ contained in $\mathcal{P}$ is called a *Cartan subalgebra*, and the common dimension of all the maximal subalgebras is called the *rank* of the decomposition (2.9). The Cartan subalgebra is not unique. However, it may be shown that two Cartan subalgebras $\mathcal{A}$ and $\mathcal{A}'$ are conjugate via an element of the Lie group associated with the Lie subalgebra $\mathcal{K}$, which we denote by $e^{\mathcal{K}}$. In other words, there exists $T \in e^{\mathcal{K}}$ such that $\mathcal{A}' = T^{\dagger}\mathcal{A}T$.

Associated with every Cartan decomposition is a *Cartan involution* θ, a Lie algebra homomorphism from $\mathcal{L}$ to itself such that $\theta^2 = \mathbf{1}$, but $\theta \neq \mathbf{1}$. Here, $\mathbf{1}$ denotes the identity map on $\mathcal{L}$. In particular, θ has eigenvalues -1 and $+1$. Accordingly, θ splits $\mathcal{L}$ into two orthogonal subspaces $\mathcal{K}$ and $\mathcal{P}$ that are the $+1$ and -1 eigenspaces of θ, respectively. In other words,

$$\theta(\sigma) = \sigma \qquad \text{and} \qquad \theta(S) = -S\,,$$

for all $\sigma \in \mathcal{K}$ and $S \in \mathcal{P}$. Consequently, a Cartan decomposition determines a Cartan involution and vice versa.

2.2.1 KAK decomposition of a Lie group

The Cartan decomposition (2.9) of a semisimple Lie algebra $\mathcal{L}$ induces a decomposition of the connected Lie group $e^{\mathcal{L}}$. In particular, every element $X \in e^{\mathcal{L}}$ can be written as

$$X = KP\,, \tag{2.11}$$

where K belongs to the connected Lie subgroup $e^{\mathcal{K}}$ associated with the Lie subalgebra $\mathcal{K}$ and P is the exponential of element of $\mathcal{P}$. The coset space $e^{\mathcal{L}}/e^{\mathcal{K}}$ is called a *symmetric space*. The decomposition in (2.11) is the right coset decomposition often called the *KP decomposition* of $e^{\mathcal{L}}$. Note that $e^{\mathcal{P}}$ does not have the structure of a subgroup in general.

Let $\mathcal{A}$ be a Cartan subalgebra contained in $\mathcal{P}$. Then, it can be shown that

$$\mathcal{P} = \bigcup_{T \in e^{\mathcal{K}}} T\mathcal{A}T^{\dagger}$$

and, therefore,

$$e^{\mathcal{P}} = \bigcup_{T \in e^{\mathcal{K}}} Te^{\mathcal{A}}T^{\dagger}.$$

It follows that P in (2.11) is of the form $TAT^{\dagger}$, where A belongs to the Abelian group $e^{\mathcal{A}}$. Hence, (2.11) refines as $X = KTAT^{\dagger}$, in particular $KT \in e^{\mathcal{K}}$.

The following theorem summarizes the content of this section.

Theorem 2.2.1 (Cartan decomposition theorem)**.** *Let $\mathcal{L}$ be a semisimple Lie algebra with the Cartan decomposition (2.9). Then, each element X of $e^{\mathcal{L}}$ admits a decomposition*

$$X = K_1 A K_2\,, \tag{2.12}$$

where $K_1\,, K_2 \in e^{\mathcal{K}}$ and $A \in e^{\mathcal{A}}$.

This decomposition is known as the *KAK decomposition* of the connected Lie group $e^{\mathcal{L}}$.

2.2.2 Cartan decompositions of the classical Lie algebras

All the symmetric spaces of the classical Lie groups $\mathbf{SU}(n)$, $\mathbf{SO}(n)$, and $\mathbf{Sp}(n)$, and, therefore, the Cartan decompositions of their corresponding Lie algebras $\mathfrak{su}(n)$, $\mathfrak{so}(n)$, and $\mathfrak{sp}(n)$, were classified by Cartan [6, 7, 13]. In particular, up to a conjugation, the special unitary Lie algebra $\mathfrak{su}(n)$ has three types of Cartan decompositions. These are labeled by **AI**, **AII**, and **AIII**. The special orthogonal Lie algebra $\mathfrak{so}(n)$ has two types of Cartan decompositions labeled by **BI** and **BDI**, and the symplectic Lie algebra $\mathfrak{sp}(n)$ has two types of Cartan decompositions labeled by **CI** and **CII**.

Each Cartan decomposition of $\mathfrak{su}(n)$ is conjugate to one of the types **AI**, **AII**, and **AIII**. In other words, if

$$\mathfrak{su}(n) = \mathcal{K} \oplus \mathcal{P} \tag{2.13}$$

is a Cartan decomposition, then there exists $T \in \mathbf{SU}(n)$ such that the decomposition $\mathfrak{su}(n) = T\mathcal{K}T^\dagger \oplus T\mathcal{P}T^\dagger$ is in one of the forms **AI**, **AII**, and **AIII**, which we shall consider next.

A decomposition of type **AI** is the Cartan decomposition of $\mathfrak{su}(n)$ into purely real and purely imaginary subspaces, that is,

$$\mathfrak{su}(n) = \mathfrak{so}(n) \oplus \mathfrak{so}(n)^\perp. \tag{2.14}$$

A maximal Abelian subalgebra contained in $\mathfrak{so}(n)^\perp$ is spanned by the diagonal matrices, and, therefore, the rank of this decomposition is $n-1$. In the general case, the Cartan involution associated with the decomposition in (2.13) is of the form

$$\theta_{AI}(X) = (TT^T)\bar{X}(TT^T)^\dagger\,. \tag{2.15}$$

The Cartan involution associated with (2.14) is obtained when $T = \mathbf{1}_n$. In this case, the subspaces $\mathfrak{so}(n)$ and $\mathfrak{so}(n)^\perp$ are the $+1$ and -1 eigenspaces of θ_{AI}, respectively.

A Cartan decomposition of type **AII** is of the form

$$\mathfrak{su}(n) = \mathfrak{sp}(\frac{n}{2}) \oplus \mathfrak{sp}(\frac{n}{2})^\perp, \tag{2.16}$$

where n is even. The diagonal matrices in $\mathfrak{sp}(\frac{n}{2})^\perp$ form a maximal Abelian subalgebra.[1] Consequently, the rank of the decomposition is $\frac{n}{2}-1$. In the general case, the associated

[1] The diagonal matrices in $\mathfrak{sp}(\frac{n}{2})^\perp$ are of the form $\left(\begin{smallmatrix} D & 0 \\ 0 & D \end{smallmatrix}\right)$, where D is diagonal.

Cartan involution of (2.13) is of the form

$$\theta_{AII}(X) = (TJT^T)\bar{X}(TJT^T)^\dagger, \tag{2.17}$$

with J defined in (2.6). The Cartan involution associated with (2.16) is obtained when $T = \mathbf{1}_n$.

A Cartan decomposition of type **AIII** is defined in terms of two fixed positive integers p and q with $p + q = n$. The decomposition is

$$\mathfrak{su}(n) = \mathfrak{k} \oplus \mathfrak{p}\,, \tag{2.18}$$

where $\mathfrak{k}$ and $\mathfrak{p}$ are respectively spanned by block diagonal and block antidiagonal matrices of forms

$$\sigma := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \qquad \text{and} \qquad S := \begin{pmatrix} 0 & C \\ -C^\dagger & 0 \end{pmatrix}, \tag{2.19}$$

where $A \in \mathfrak{u}(p)$, $B \in \mathfrak{u}(p)$ with $\mathrm{tr}(\sigma) = 0$, and C is an arbitrary $p \times q$ complex matrix. Let E_{ij} denote the $n \times n$ matrix with all entries equal to 0 except the entry on the position (i, j) is 1. If $p \leq q$, then the matrices $E_{i,p+i} - E_{p+i,i}$ span a maximal Abelian subalgebra where $i = 1, \ldots, p$. On the other hand, if $p > q$, then the space spanned by $E_{i,p+i} - E_{p+i,i}$ with $i = 1, \ldots, q$ can be taken as a Cartan subalgebra. Consequently, the rank of the decomposition is $\min\{p, q\}$. In the general case, the associated Cartan involution is given by

$$\theta_{AIII}(X) = (TI_{p,q}T^\dagger)X(TI_{p,q}T^\dagger)^\dagger\,, \tag{2.20}$$

where

$$I_{p,q} := \begin{pmatrix} \mathbf{1}_p & 0 \\ 0 & -\mathbf{1}_q \end{pmatrix}. \tag{2.21}$$

A decomposition of type **BDI** of $\mathfrak{so}(n)$, $n > 2$, is constructed essentially the same as the type **AIII** decompositions of $\mathfrak{su}(n)$. In this case, A and B in (2.19) are skew-symmetric, i.e., $A \in \mathfrak{so}(p)\,,\ B \in \mathfrak{so}(q)$, and C is an arbitrary $p \times q$ real matrix. The rank of this decomposition is again $\min\{p, q\}$. We refer to [13] for the decompositions of types **BI**, **CI**, and **CII**.

In the following, we shall find it convenient to extend the decompositions of $\mathfrak{su}(n)$ to the decompositions of $\mathfrak{u}(n) = \mathfrak{su}(n) \oplus \mathrm{span}\{i\,\mathbf{1}_n\}$. Since $i\,\mathbf{1}_n$ commutes with each element of $\mathfrak{su}(n)$, the extension can be done naturally by including the subspace $\mathrm{span}\{i\,\mathbf{1}_n\}$ into either $\mathcal{K}$ or $\mathcal{P}$ in (2.13). For our goals, we extend the decompositions of type **AI** and **AII** by replacing $\mathcal{P}$ with $\mathcal{P} \oplus \mathrm{span}\{i\,\mathbf{1}_n\}$. Accordingly, the ranks of these decompositions become n and $n/2$, respectively. For decompositions of type **AIII**, we include $\mathrm{span}\{i\,\mathbf{1}_n\}$ into $\mathcal{K}$ rather than $\mathcal{P}$ so as to lift the restriction $\mathrm{tr}(\sigma) = 0$ in (2.19). With the abuse of terminology, we call the decompositions of $\mathfrak{u}(n)$ as the Cartan decompositions of types **AI**, **AII**, and **AIII** again.

2.3 Recursive decompositions

Recursive decompositions repeatedly apply the Cartan decomposition theorem in order to decompose the factors into simpler ones. Informally speaking, this procedure allows one to write "large" matrices as a product of "small" matrices. The basic outline of such a procedure is as follows. Recall that the Cartan decomposition (2.9) of $\mathcal{L}$ writes each X in $e^{\mathcal{L}}$ as

$$X = K_1 A K_2\,,$$

with $K_j \in e^{\mathcal{K}}$, $j = 1, 2$, and $A \in e^{\mathcal{A}}$ where $\mathcal{A}$ is a Cartan subalgebra in $\mathcal{P}$. Assume that the Lie subalgebra $\mathcal{K}$ is semisimple. Introducing a Cartan decomposition

$$\mathcal{K} = \mathcal{K}' \oplus \mathcal{P}'\,,$$

one can write each K_j as

$$K_j = K_{j1} A_j K_{j2}\,,$$

where $K_{j1}\,, K_{j2} \in e^{\mathcal{K}'}$, and A_j belongs to the connected Lie group corresponding to the Cartan subalgebra contained in $\mathcal{P}'$. One then repeats the procedure for $\mathcal{K}'$ and so on. The resulting decomposition of $X \in e^{\mathcal{L}}$ will have several simple factors. Such decompositions are often useful to analyze and control the dynamics of quantum systems [9]. In this context, recursive decompositions of $\mathfrak{su}(2^N)$ and $\mathfrak{u}(n_1 n_2)$ were introduced in [16] and [11], respectively. In the following, we shall review such decompositions.

2.3.1 The Khaneja Glaser decomposition

A recursive procedure to decompose any unitary evolutions acting on N qubits into one qubit and two qubit operations was introduced by N. Khaneja and S. Glaser in [16]. Such procedure begins with the type **AIII** decomposition

$$\mathfrak{su}(2^N) = \mathcal{K} \oplus \mathcal{P}\,, \tag{2.22}$$

where

$$\mathcal{K} = \text{span}\{\mathbf{1}_2 \otimes A,\, \sigma_z \otimes B : A \in \mathfrak{su}(2^{N-1}),\, B \in \mathfrak{u}(2^{N-1})\}\,,$$

and

$$\mathcal{P} = \text{span}\{\sigma_{x,y} \otimes C : C \in \mathfrak{u}(2^{N-1})\}.$$

The rank of this decomposition is 2^{N-1}. A Cartan subalgebra contained in $\mathcal{P}$ is given by $\mathcal{A} = \text{span}\{\sigma_x \otimes D : D \text{ diagonal}\}$. Thus, any $X \in \mathbf{SU}(2^N)$ can be decomposed as

$$X = K_1 A K_2\,, \tag{2.23}$$

where K_j, $j = 1, 2$, and A are of the form

$$K_j = \begin{pmatrix} K_{j1} & 0 \\ 0 & K_{j2} \end{pmatrix} \qquad \text{and} \qquad A = \begin{pmatrix} D_1 & D_2 \\ D_2 & D_1 \end{pmatrix}.$$

Here, K_{jk}, $k = 1, 2$, is a 4×4 unitary matrix, and D_k is a diagonal matrix with $D_1^2 - D_2^2 = \mathbf{1}_4$.

The subalgebra $\mathcal{K}$ is not semisimple. However, it is a direct sum of two copies of the semisimple Lie algebra $\mathfrak{su}(2^{N-1})$ and $\text{span}\{i\sigma_z \otimes \mathbf{1}_{2^{N-1}}\}$ commuting with every element of $\mathcal{K}$. Thus, finer decompositions of each K_j can be obtained by applying the Cartan decomposition

$$\mathcal{K} = \mathcal{K}' \oplus \mathcal{P}'\,, \tag{2.24}$$

where $\mathcal{K}' = \text{span}\{\mathbf{1}_2 \otimes A : A \in \mathfrak{su}(2^{N-1})\}$ and $\mathcal{P}' = \text{span}\{\sigma_z \otimes B : B \in \mathfrak{u}(2^{N-1})\}$. A Cartan subalgebra in this case is given by $\mathcal{A}' = \text{span}\{\sigma_z \otimes D : D \text{ diagonal}\}$. Accordingly, each K_j admits the decomposition

$$K_j = L_{j1} A_j L_{j2}\,, \tag{2.25}$$

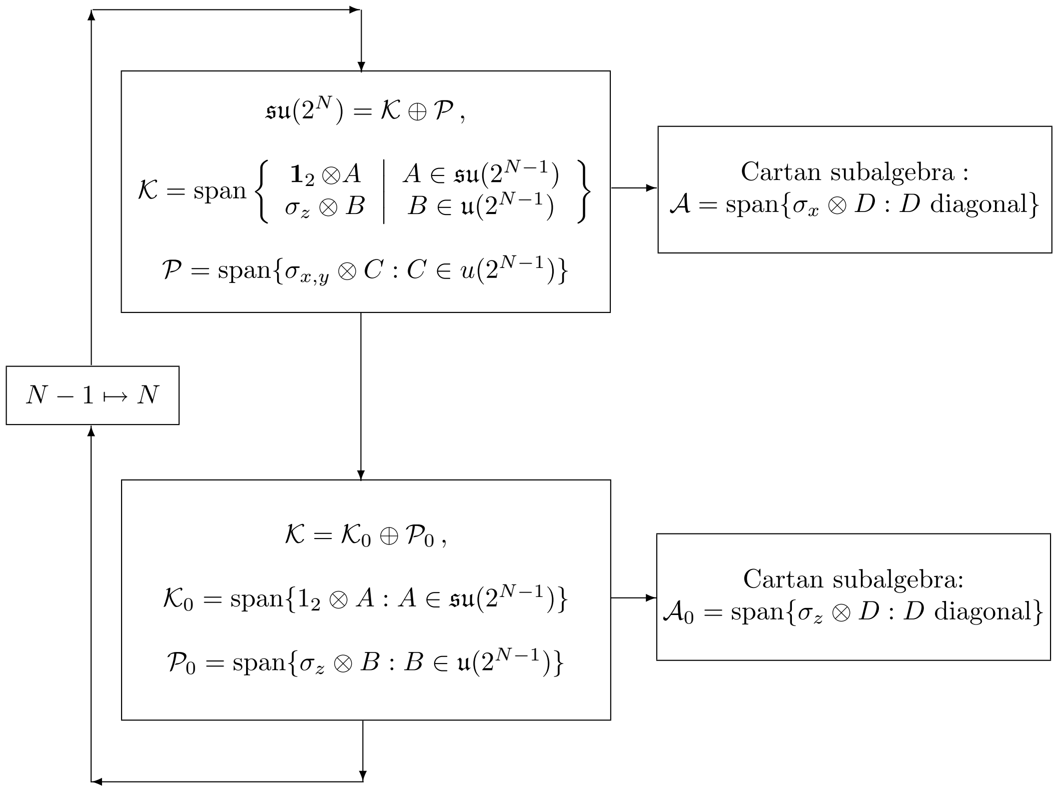

Figure 2.1 A schematic representation of the Khaneja Glaser decomposition. The procedure starts with a Cartan decomposition of type **AIII** of $\mathfrak{su}(2^N)$ and continues with a Cartan decomposition of $\mathcal{K}$. In particular, $\mathcal{K}_0$ is isomorphic to $\mathfrak{su}(2^{N-1})$. Hence, the procedure repeats for $N - 1$ and so on.

where L_{jk} and A_j are of the form

$$L_{jk} = \begin{pmatrix} U_{jk} & 0 \\ 0 & U_{jk} \end{pmatrix} \qquad \text{and} \qquad A_j = \begin{pmatrix} D_{jj} & 0 \\ 0 & D_{jj}^{-1} \end{pmatrix} .$$

Here, U_{jk} is a unitary matrix with determinant equal to 1, and D_{jj} is a diagonal matrix.

At this point, the key observation is that $\mathcal{K}'$ and $\mathfrak{su}(2^{N-1})$ are isomorphic. Thus, the procedure can be repeated by replacing N with $N - 1$ to decompose each $U_{jk} \in \mathbf{SU}(2^{N-1})$ and so on. The resulting decomposition of $X \in \mathbf{SU}(2^N)$ will have several factors. We present a schematic representation of the Khaneja Glaser decomposition in Figure 2.3.1.

The Khaneja Glaser decomposition requires two applications of the KAK decompositions. The following algorithm of [9] can be used to compute the KAK decomposition given in (2.23):

Algorithm 1

(1) Partition X_{sw} into four 4×4 blocks, i.e. $X_{sw} := \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}$. Then, the equation (2.23) is equivalent to the four matrix equations:

$$X_{11} = K_{11}D_1K_{21}, \qquad X_{12} = K_{11}D_2K_{22}, \qquad X_{21} = K_{12}D_1K_{21}, \qquad X_{22} = K_{12}D_2K_{22}.$$

(2) From the first matrix equation of (1), obtain $(X_{11}X_{11}^\dagger)K_{11} = K_{11}(D_1D_1^\dagger)$, where $D_1D_1^\dagger$ is diagonal. This is an eigenvalue problem that determines K_{11} and D_1 up to signs.

(3) Determine D_2 up to signs from the condition $D_1^2 - D_2^2 = \mathbf{1}_4$.

(4) Use K_{11} and D_2 in the second matrix equation of (1) to determine K_{22} up to signs and so on. Finally, adjust the signs so that the equations in the previous steps are consistent.

To compute the KAK decomposition given in (2.25), one can use the following algorithm:

Algorithm 2

(1) Set the matrix equation

$$\begin{pmatrix} K_{j1} & 0 \\ 0 & K_{j2} \end{pmatrix} = \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & P^\dagger \end{pmatrix},$$

with unitary K and P to obtain two matrix equations $K_{j1} = KP$ and $K_{j2} = KP^\dagger$.

(2) Compute $P^2 = K_{j2}^\dagger K_{j1}$.

(3) Compute P as follows: diagonalize P^2 with a unitary matrix T to write $P^2 = T\Lambda T^\dagger$, and choose $D = \Lambda^{\frac{1}{2}}$ with $\det(D) = 1$ so that $P = TDT^\dagger$.

(4) Compute $K = K_{j2}P$.

(5) Choose $U_{j1} = KT$, $U_{j2} = T^\dagger$, and $D_{jj} = D$ to obtain the desired decomposition in (2.25).

We shall use the above algorithms to compute the Khaneja Glaser decomposition of the generalized SWAP operator in section 5.3.

2.3.2 The D'Alessandro Romano decomposition

Another recursive decomposition method was presented by D. D'Alessandro and R. Romano in [11]. Such a method displays the local and entangling parts of a quantum involution acting on bipartite quantum system composed of subsystems of dimensions n_1 and n_2. In this case, the Lie algebra associated with the dynamics is $\mathfrak{u}(n_1 n_2)$. The recursive decomposition procedure starts with a decomposition of type **AI** of $\mathfrak{u}(n_1 n_2)$ and continues with successive decompositions of type **BDI** of $\mathfrak{so}(n_1 n_2)$. We shall discuss this next.

Initial step: In this step, we perform a decomposition of type **AI** for the total system as follows. First, we apply Cartan decompositions of type **AI** on each single system, i.e.,

$$\mathfrak{u}(n_1) = \mathfrak{so}(n_1) \oplus \mathfrak{so}(n_1)^{\perp} \qquad \text{and} \qquad \mathfrak{u}(n_2) = \mathfrak{so}(n_2) \oplus \mathfrak{so}(n_2)^{\perp}.$$

Let us denote the generic basis elements of the subspaces $\mathfrak{so}(n_j)$ and $\mathfrak{so}(n_j)^{\perp}$ by σ_j and S_j, $j = 1, 2$, respectively. Then, a Cartan decomposition of $\mathfrak{u}(n_1 n_2)$ is given by

$$\mathfrak{u}(n_1 n_2) = i\mathcal{I}_o \oplus i\mathcal{I}_e \,, \tag{2.26}$$

where $i\mathcal{I}_o = \operatorname{span}\{i\sigma_1 \otimes S_2,\, iS_1 \otimes \sigma_2\}$ and $i\mathcal{I}_e = \operatorname{span}\{i\sigma_1 \otimes \sigma_2,\, iS_1 \otimes S_2\}$. This decomposition is called the odd-even decomposition of $\mathfrak{u}(n_1 n_2)$.[2] The Lie subalgebra $i\mathcal{I}_o$ is conjugate to $\mathfrak{so}(n_1 n_2)$, and the rank of the decomposition is $n_1 n_2$.

Recursive step: In this step, we choose two positive integers p_j and q_j with $p_j + q_j = n_j$, $j = 1, 2$, to separate block diagonal and block antidiagonal elements of the Lie subalgebra $i\mathcal{I}_o$. In particular, let

$$\mathcal{K} = \operatorname{span}\{i\sigma_1^D \otimes S_2^D,\, iS_1^D \otimes \sigma_2^D,\, i\sigma_1^A \otimes S_2^A,\, iS_1^A \otimes \sigma_2^A\}\,,$$

and

$$\mathcal{P} = \operatorname{span}\{i\sigma_1^D \otimes S_2^A,\, iS_1^A \otimes \sigma_2^D,\, i\sigma_1^A \otimes S_2^D,\, iS_1^D \otimes \sigma_2^A\}\,,$$

[2] A detailed discussion of the odd-even decomposition will be given in Chapter 4.

where the superscripts D and A denote the block diagonal and block antidiagonal matrices, respectively. Therefore, we write

$$i\mathcal{I}_o = \mathcal{K} \oplus \mathcal{P}\,. \tag{2.27}$$

Under an appropriate conjugacy transformation, it was shown in [11] that this decomposition is of type **BDI** and $\mathcal{K}$ is conjugate to the semisimple sum $\mathfrak{so}(p_1p_2 + q_1q_2) \oplus \mathfrak{so}(p_1q_2 + p_2q_1)$.

The next step is to apply the Cartan decomposition $\mathcal{K} = \mathcal{K}' \oplus \mathcal{P}'$, where

$$\mathcal{K}' = \mathrm{span}\{i\sigma_1^D \otimes S_2^D,\, iS_1^D \otimes \sigma_2^D\} \qquad \text{and} \qquad \mathcal{P}' = \mathrm{span}\{i\sigma_1^A \otimes S_2^A,\, iS_1^A \otimes \sigma_2^A\}.$$

In particular, the subalgebra $\mathcal{K}'$ is conjugate to the semisimple sum

$$\mathfrak{so}(p_1p_2) \oplus \mathfrak{so}(q_1q_2) \oplus \mathfrak{so}(p_1q_2) \oplus \mathfrak{so}(p_2q_1)\,,$$

each of which is spanned by elements of form $i\sigma \otimes S$ and $iS \otimes \sigma$ as in the case of the Lie subalgebra $i\mathcal{I}_o$. One then iterates the procedure.

We have described the D'Alessandro Romano decomposition at the algebraic level. Accordingly, decompositions of $\mathbf{U}(n_1n_2)$ can be obtained by applying the Cartan decomposition theorem repeatedly. Unlike the Khaneja Glaser decomposition, the D'Alessandro Romano decomposition applies to bipartite systems of arbitrary dimensions, and at the end of the procedure one obtains a decomposition of unitary evolutions with several simple factors where the local and nonlocal contributions of each factor is transparent. We refer to [11] for the computation of the KAK decompositions induced by the D'Alessandro Romano decomposition.

CHAPTER 3. The concurrence canonical decomposition and entanglement

3.1 Basics of quantum mechanics

In this section, we shall briefly review some of the basic concepts of quantum mechanics that we use in the rest of this dissertation. A detailed treatment of the material presented here can be found in [2, 9, 20].

3.1.1 The state of a quantum system

The *state* of a quantum mechanical system is represented by a unit vector in a Hilbert space $\mathcal{H}$, a complex inner product space that is complete with respect to the norm defined by the inner product. The system is identified by its Hilbert space $\mathcal{H}$, and it is assumed that the state vector completely describes the physical system. The *dimension* of the system is the dimension of the associated Hilbert space, which may be finite or infinite.

In what follows, we shall be concerned with finite dimensional systems.

3.1.1.1 Kets

The state vector of a quantum system is called a *ket*, and denoted by Dirac's notation $|\psi\rangle$. The space spanned by kets is called the *ket space*.

Consider a Hilbert space $\mathcal{H}$ with an orthonormal basis $\{|e_1\rangle, |e_2\rangle, \ldots, |e_n\rangle\}$. Then, every $|\psi\rangle$ in $\mathcal{H}$ can uniquely be written as

$$|\psi\rangle = \sum_{j=1}^{n} \alpha_j |e_j\rangle\,, \tag{3.1}$$

where α_j is a complex number. In the given basis, $|\psi\rangle$ may be represented by its expansion coefficients α_j as the column vector

$$|\psi\rangle := \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}. \tag{3.2}$$

Thus, the kets may be viewed as column vectors.

The inner product of two kets $|\psi_1\rangle$ and $|\psi_2\rangle$ is denoted by $\langle\psi_1|\psi_2\rangle$.

Definition 3.1.1. *The kets $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal if $\langle\psi_1|\psi_2\rangle = 0$.*

3.1.1.2 Two level quantum systems

The simplest example of quantum systems is the two dimensional quantum system called a *two level system* or a *qubit* which has two degrees of freedom. More formally, the associated Hilbert $\mathcal{H}$ is spanned by two orthonormal state vectors $|0\rangle$ and $|1\rangle$, which are known as the *computational basis states*. Then, each state vector can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.3}$$

where α and β are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$.

A hydrogen atom and spin$-\frac{1}{2}$ particles are two common examples for two level systems. The ground and the excited states of the hydrogen atom and the spin-up and the spin-down states of spin$-\frac{1}{2}$ particles form bases for the associated Hilbert spaces.

The state equation (3.3) may be rewritten as

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle, \tag{3.4}$$

(see [20, §1.2]). In this representation, the numbers $0 \le \theta \le 2\pi$, and $0 \le \phi \le \pi$, define a point on a three-dimensional unit sphere called the *Bloch sphere*. Indeed, the state $|0\rangle$ is the North pole, the state $|1\rangle$ is the South pole, and $|\psi\rangle$ in (3.4) is the pure state given in Figure 3.1.1.2.

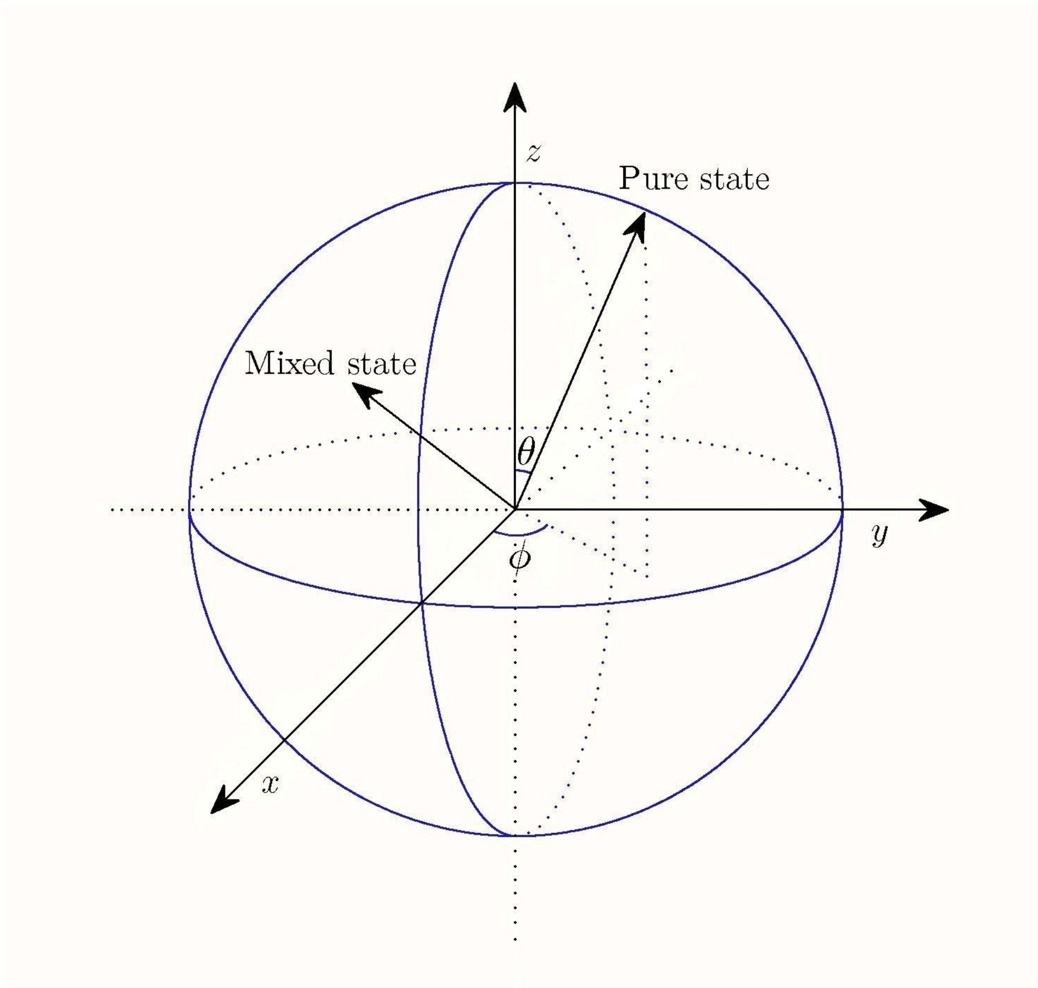

Figure 3.1 Pure and mixed states on the Bloch sphere.

3.1.2 Linear Operators

A linear operator X between two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ is a map that preserves the addition and multiplication by a scalar, i.e.

$$X(|\psi\rangle + |\phi\rangle) = X|\psi\rangle + X|\phi\rangle \qquad \text{and} \qquad X(c|\psi\rangle) = cX|\psi\rangle,$$

where c is a complex number.

The sum $X+Y$ and the multiplication XY of linear operators X and Y are associative linear operators. Here XY is defined as $(XY)|\psi\rangle := X(Y|\psi\rangle)$. Note that the multiplication is not commutative in general, i.e., $XY \neq YX$.

3.1.2.1 Bras

Associated with each ket $|\phi\rangle$ is a linear functional $\langle\psi| : \mathcal{H} \longrightarrow \mathbb{C}$, called a *bra.* When applied to a ket $|\phi\rangle$ gives the complex number $\langle\psi|\phi\rangle$. In the matrix formulation, the bra $\langle\psi|$ corresponds to a unique raw vector representation obtained by the complex conjugate transpose of the ket $|\psi\rangle$ in (3.2), i.e.,

$$\langle\psi| := |\psi\rangle^\dagger = \begin{pmatrix} \bar{\alpha}_1 & \bar{\alpha}_2 & \cdots & \bar{\alpha}_n \end{pmatrix}. \tag{3.5}$$

Similar to the equation (3.1), one can write $\langle\psi|$ as

$$\langle\psi| = \sum_{j=1}^{n} \alpha_j \langle e_j|\,,$$

where $\langle e_j| = |e_j\rangle^\dagger$. The space spanned by row vectors $\langle e_j|$, $j = 1, \ldots, n$, is called the *bra space.* In particular, the bra space is the dual space of the associated ket space.

3.1.2.2 Outer product

The outer product of a ket $|\psi\rangle$ and bra $|\phi\rangle$, denoted by $|\phi\rangle\langle\psi|$, is a linear operator acting on both kets and bras. It maps the ket $|\varphi\rangle$ to another ket $|\phi\rangle\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle|\phi\rangle$. Note that $\langle\psi|\varphi\rangle$ is a complex number. Similarly, $|\phi\rangle\langle\psi|$ transforms the a bra $\langle\varphi|$ to another bra $\langle\varphi|\phi\rangle\langle\psi|$.

In the matrix representation, the outer product is a rank-one operator obtained by right-multiplying a column matrix by a row matrix.

3.1.3 State of a composite quantum system

Consider a bipartite quantum system composed of two subsystems with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ of dimensions m and n, respectively. Then, a state of the composite system is a vector in the Hilbert space $\mathcal{H}_{tot}$ that is the tensor product of $\mathcal{H}_1$ and $\mathcal{H}_2$, i.e.,

$$\mathcal{H}_{tot} := \mathcal{H}_1 \otimes \mathcal{H}_2 .$$

Let $\{|e_i\rangle\}$, $1 \leq i \leq m$, and $\{|f_j\rangle\}$, $1 \leq i \leq n$, be orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the tensor product space $\mathcal{H}_{tot}$ is spanned by the orthonormal basis

$$\{|e_i\rangle \otimes |f_j\rangle : 1 \leq i \leq m, 1 \leq j \leq n\} .$$

Consequently, the dimension of $\mathcal{H}_{tot}$ is equal to mn, and any element of $\mathcal{H}_{tot}$ is of the form

$$|\psi\rangle = \sum_{i,j} \alpha_{ij} |e_i\rangle \otimes |f_j\rangle.$$

This definition analogously extends to the multipartite quantum systems composed of N subsystems for a general N.

3.1.4 Density operator

A state of a quantum system represented by a ket $|\psi\rangle$ is called a *pure state*. However, in general quantum systems are in statistical mixtures of pure states. In this case, the density matrix formalism is used to represent a state of the system. More precisely, consider a quantum system that is a collection of a large number of non-interacting identical quantum systems. This type of system is called an *ensemble*. In the ensemble, let w_j be the probability of finding the system in the state $|\psi_j\rangle$. Then, the *density operator* (or *density matrix*) is defined as

$$\rho := \sum_j w_j |\psi_j\rangle\langle\psi_j| , \tag{3.6}$$

where $0 \leq w_j \leq 1$, and $\sum_j w_j = 1$. It is clear from the definition that if $w_j = 1$ for some j, then the density matrix ρ represents a *pure ensemble* or *pure state*, i.e., $\rho = |\psi_j\rangle\langle\psi_j|$. Density matrices that are not pure ensembles are called *mixed ensembles* or *mixed states*.

The density matrix ρ has the following properties:

1. ρ is a positive semi-definite Hermitian operator acting on the Hilbert space of the system.

2. $\mathrm{tr}(\rho) = 1$.

3. For pure ensembles, $\rho^2 = \rho$.

4. For mixed ensembles, $\mathrm{tr}(\rho^2) < 1$.

Example 3.1.1. *Let us compute the density matrix representation ρ of a qubit. Let*

$$\vec{s} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \qquad \textit{and} \qquad \vec{\sigma}^S = \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix},$$

where $s_{1,2,3}$ are real numbers and $\sigma_{x,y,z}$ are the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then, any Hermitian 2×2 matrix ρ with trace equal to 1 can be written as

$$\rho = \frac{1}{2}\left[\, \mathbf{1}_2 + \vec{s} \cdot \vec{\sigma}^S \right].$$

Note that $\det(\rho) = \left(1 - \|s\|^2\right)/4$. Since ρ is positive semi-definite, a necessary and sufficient condition for ρ to have nonnegative eigenvalues is that $\|s\|^2 \leq 1$. Therefore, there is a one-to-one correspondence between the density matrices of the qubit and the Bloch sphere given in Figure 3.1.1.2. The vectors of length one represent the pure ensembles, while the others represent mixed ensembles. This representation of qubits is also known as the coherence vector representation.

3.1.5 Entanglement

Recall that a state of a bipartite quantum system is a vector in the Hilbert space $\mathcal{H}_{tot}$, the tensor product of the Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ of the subsystems. Suppose that the first system is in the state $|\psi_1\rangle$ and the second system is in the state $|\psi_2\rangle$. Then, the total state of both systems is in the state

$$|\psi_1\rangle \otimes |\psi_2\rangle. \tag{3.7}$$

These type of states are called *product states* or *separable states*. However, there are states in $\mathcal{H}_{tot}$ that cannot be written in the product form (3.7). Such states are called *entangled states*.

Example 3.1.2. *The generalized Bell states*

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |0\rangle \pm |1\rangle \otimes |1\rangle\big) \qquad \textit{and} \qquad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |1\rangle \pm |1\rangle \otimes |0\rangle\big) \tag{3.8}$$

are the most standard examples for entangled pure states of two qubits. To show that they are entangled, we consider the computational basis states

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \textit{and} \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.9}$$

for the Hilbert space of a qubit. Then, it can be easily verified that the equation

$$|\psi\rangle = \big(\alpha_1|0\rangle + \alpha_2|1\rangle\big) \otimes \big(\beta_1|0\rangle + \beta_2|1\rangle\big)$$

has no solution for $|\psi\rangle = |\Phi^{\pm}\rangle$ and $|\psi\rangle = |\Psi^{\pm}\rangle$. Therefore, the Bell states are entangled states.

The formal definition of entanglement for pure and mixed states is as follows. Consider a multipartite system composed of N quantum systems with Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_N$. Then, the Hilbert space of the total system is $\mathcal{H}_{tot} := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N$.

Definition 3.1.2. *A pure state $|\psi\rangle$ of $\mathcal{H}_{tot}$ is called* separable *if and only if*

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle,$$

where $|\psi_j\rangle \in \mathcal{H}_j$ with $j = 1, \dots, N$. A pure state that is not separable is called entangled.

Definition 3.1.3. *A mixed state ρ of $\mathcal{H}_{tot}$ is called* separable *if ρ can be written as*

$$\rho = \sum_{j=1}^{N} w_j \rho_{j_1} \otimes \rho_{j_2} \otimes \cdots \otimes \rho_{j_N}\,, \qquad w_j > 0\,, \qquad \sum_{j=1}^{N} w_j = 1\,,$$

where each ρ_{j_k}, $k = 1, \dots, N$, is itself a state in $\mathcal{H}_k$. A mixed state that is not separable is called entangled.

3.1.6 Evolution of a quantum system

The state $|\psi(t)\rangle$ of a quantum system that does not interact with the outside world evolves according to the time dependent *Schrödinger's equation*

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \tag{3.10}$$

where $\hbar$ is the Plank's constant and $H(t)$ is an Hermitian operator called the *Hamiltonian operator* of the system. The solution of the Schrödinger's equation is

$$|\psi(t)\rangle = X(t)|\psi(0)\rangle,$$

where $X(t)$ is an operator that satisfies the differential equation

$$i\hbar \frac{d}{dt}X(t) = H(t)X(t)\,, \qquad X(0) = \mathbf{1}\ .$$

Since $H(t)$ is an Hermitian operator for all t, it follows that $X(t)$ is a unitary operator called the *evolution operator* or the *propagator* of the quantum system. In the finite dimensional case, the operators $X(t)$ and $H(t)$ are represented by a unitary matrix in $\mathbf{U}(n)$ and a Hermitian matrix in $i\mathfrak{u}(n)$, respectively.

For a multipartite quantum system of N systems of dimensions $n_1, \ldots, n_N$, every Hamiltonian can be written as the linear span of the tensor products of the form

$$H_1 \otimes H_2 \otimes \cdots \otimes H_N\,,$$

where $H_j \in i\mathfrak{u}(n_j)$, $j = 1, \ldots, N$. In particular, the linear span of the tensor products where all the factors equal to identity except one generates the subgroup

$$\mathbf{U}(n_1) \otimes \mathbf{U}(n_1) \otimes \cdots \otimes \mathbf{U}(n_N)\,,$$

called the *local unitary Lie group*. Elements of the local unitary group are called the *local evolutions*, and they correspond to operations on the single subsystems. The evolutions that are not local are called the *nonlocal evolutions*.

Decompositions of unitary operators into local and nonlocal parts are useful tools in quantum control theory, as we shall see in the next section.

3.2 Incoherent control of two entangling qubits

In this section, we investigate the controllability of a two level quantum system S by means of a quantum probe P. The total system varies according to a given Hamiltonian H_{tot}. The assumption is that only the initial state of P is controllable and the controllability problem is to give conditions on H_{tot} so that, by modifying the initial state of the probe P it is possible to drive the state of S to any value. Our goal is to show how the Cartan decomposition theorem can be used in the solution of this controllability problem. This problem was studied in [21].

Consider two initially uncorrelated two level quantum systems S and P. We assume that the initial state ρ_P of the quantum probe P can be modified at will by the control $u \in \mathcal{U}$. We study the controllability of S using the interactions between the system and the probe. The controls do not enter the dynamics of S directly; therefore, this scheme is called *incoherent control*. In this setting, the time evolution of a state ρ_S of S is given by

$$\rho_S(t,u) = \mathrm{tr}_S\left[X(t)\rho_S \otimes \rho_P(u) X(t)^\dagger\right], \tag{3.11}$$

where $X(t) = e^{-itH_{tot}}$ is the unitary propagator of the composite system $T = S + P$, acting on $\mathcal{H}_S \otimes \mathcal{H}_P$. Here, tr_S is the *partial trace operator* over the degrees of freedom of the probe. In other words, it is a linear operator $\mathrm{tr}_S : \mathcal{H}_S \otimes \mathcal{H}_P \longrightarrow \mathcal{H}_S$, defined by

$$\mathrm{tr}_S(A \otimes B) = \mathrm{tr}(B)A\,.$$

The system is controllable if, by varying ρ_P, it is possible to achieve every possible density matrix ρ_S with (3.11). The problem is to give necessary and sufficient conditions on H_{tot} so that this is the case.

Observe that any iH_{tot} is contained in

$$\mathfrak{su}(4) = \mathrm{span}\{i\sigma^S \otimes \mathbf{1}_2\,,\, i\,\mathbf{1}_2 \otimes \sigma^P,\, i\sigma^S \otimes \sigma^P\}\,, \tag{3.12}$$

where $\sigma^{S,P} = \sigma^{S,P}_{x,y,z}$ are the Pauli matrices acting on the Hilbert spaces $\mathcal{H}_S$ and $\mathcal{H}_P$, respectively. The special unitary Lie algebra $\mathfrak{su}(4)$ has the type **AI** Cartan decomposition

$$\mathfrak{su}(4) = \mathcal{K} \oplus \mathcal{P}\,, \tag{3.13}$$

where $\mathcal{K} = \mathrm{span}\{i\sigma^S \otimes \mathbf{1}_2\,,\, i\,\mathbf{1}_2 \otimes \sigma^P\}$ and $\mathcal{P} = \mathrm{span}\{i\sigma^S \otimes \sigma^P\}$.[1] Applying the Cartan decomposition theorem, we can write the unitary propagator $X(t)$ in (3.11) as

$$X(t) = \left[L^S_{11}(t) \otimes L^P_{12}(t)\right]\left[e^{iat}\right]\left[L^S_{21}(t) \otimes L^P_{22}(t)\right], \tag{3.14}$$

where $L^S_{k1}(t)$, $L^P_{k2}(t) \in \mathbf{SU}(2)$ with $k = 1, 2$, and

$$a = c_x\sigma^S_x \otimes \sigma^P_x + c_y\sigma^S_y \otimes \sigma^P_y + c_z\sigma^S_z \otimes \sigma^P_z\,,$$

where c_x, c_y, and c_z are real constants. The decomposition given in (3.14) is known as the *two qubit canonical decomposition* and allows to reduce the time evolution in (3.11) to

$$\rho_S(t,u) = L^S_1\,\mathrm{tr}_P\left[e^{at}\,\tilde{\rho}_S \otimes \tilde{\rho}_P(u)\,e^{a^\dagger t}\right]L^{S\dagger}_1\,, \tag{3.15}$$

where $\tilde{\rho}_S = L^S_2\rho_S L^{S\dagger}_2$ and $\tilde{\rho}_P(u) = L^P_2\rho_P(u)L^{P\dagger}_2$. Then, we have the following theorem of [21].

Theorem 3.2.1. *The system evolving under (3.11) is controllable for any Hermitian H_{tot} if and only if it is controllable for $L^S_1 = L^S_2 = \mathbf{1}_2$, that is, under the time evolution*

$$\rho_S(t,u) = \mathrm{tr}_P\left[e^{at}\,\rho_S \otimes \rho_P(u)\,e^{a^\dagger t}\right]. \tag{3.16}$$

In summary, the unitary evolution $X(t)$ in (3.11) is characterized by 15 parameters. An application of the Cartan decomposition theorem along with Theorem 3.2.1 reduces 15 parameters to 3 parameters, which significantly simplifies the task in the control procedure. In order to compute the reachable set under the time evolution (3.16), we use the coherence vector representation for the states of the systems S and P, i.e.,

$$\rho_S(t,u) = \frac{1}{2}\left[\,\mathbf{1}_2 + \vec{s}(t,u)\cdot\vec{\sigma}^S\right] \qquad \text{and} \qquad \rho_P(u) = \frac{1}{2}\left[\,\mathbf{1}_2 + \vec{p}(u)\cdot\vec{\sigma}^P\right],$$

where $\vec{s}(t,u)$ and $\vec{p}(u)$ are real vectors and $\vec{\sigma}^S$ and $\vec{\sigma}^P$ are the vectors of the Pauli matrices. In this representation, the sets $\mathcal{P}_S$ and $\mathcal{P}_P$ are given by two Bloch spheres

$$S_S = \{\vec{s} \in \mathbb{R}^3 :\ ||\vec{s}|| \le 1\} \qquad \text{and} \qquad \mathcal{S}_P = \{\vec{p} \in \mathbb{R}^3 :\ ||\vec{p}|| \le 1\}$$

[1] Associated with this decomposition is the Cartan involution $\theta_S : \mathfrak{su}(4) \longrightarrow \mathfrak{su}(4)$, defined by $\theta_S(F) := S\bar{F}S^\dagger$, where $S = (-i\sigma_y) \otimes (-i\sigma_y)$.

(see Figure 3.1.1.2) and the time evolution (3.16) of ρ_S is given by

$$\vec{s}(t,u) = A(t,\vec{s}_0)\vec{p}(u) + \vec{a}(t,\vec{s}_0)\,, \tag{3.17}$$

where

$$A(t,\vec{s}_0) = \begin{pmatrix} \sin(2c_y t)\sin(2c_z t) & -s_z\sin(2c_y t)\cos(2c_z t) & s_y\cos(2c_y t)\sin(2c_z t) \\ s_z\sin(2c_x t)\cos(2c_z t) & \sin(2c_x t)\sin(2c_z t) & -s_x\cos(2c_x t)\sin(2c_z t) \\ -s_y\sin(2c_x t)\cos(2c_y t) & s_x\cos(2c_x t)\sin(2c_y t) & \sin(2c_x t)\sin(2c_y t) \end{pmatrix},$$

and

$$a(t,\vec{s}_0) = \begin{pmatrix} s_x\cos(2c_y t)\cos(2c_z t) \\ s_y\cos(2c_x t)\cos(2c_z t) \\ s_z\cos(2c_x t)\cos(2c_y t) \end{pmatrix}.$$

Using the dynamics (3.17), the controllability conditions under the time evolution (3.11) can be characterized in the following theorem of [21].

Theorem 3.2.2. *The system evolving under (3.11) is controllable if and only if there exists integers k_1, k_2, and k_3 such that*

$$\frac{c_x}{c_y} = \frac{2k_1+1}{2k_2+1}\,, \qquad \frac{c_x}{c_z} = \frac{2k_1+1}{2k_3+1}\,, \qquad \frac{c_y}{c_z} = \frac{2k_2+1}{2k_3+1}\,.$$

In conclusion, we initially let the system and probe interact to create entanglement in the incoherent control scheme of the quantum system discussed above. In particular, Theorem 3.2.1 states that the local evolutions do not create entanglement. Using nonlocal evolutions under the conditions of Theorem 3.2.2, we are able to create the necessary amount of entanglement to drive the initial state of the system S to a final state.

3.3 Concurrence

Entanglement is the crucial resource in the control procedure discussed in the previous section. Not all the unitary evolutions can create the necessary amount of entanglement. This is only one of the important properties of entanglement. Therefore, using mathematical tools, it is important to quantify the amount of entanglement and study how much entanglement a given unitary operator can create. The latter is referred as the *entanglement capacity* of a unitary operator [4]. In this context, we focus on a measure of the entanglement, the concurrence. The concurrence was introduced in [14] to provide a measure of the entanglement for pure and mixed states of two qubits and was generalized to the systems of N qubits in [26]. Different generalizations can also be found in [22, 24]. We shall discuss this next.

Consider an $N-$qubit multipartite quantum system with Hilbert space $\mathcal{H}_N$. Then, the *concurrence* is a map $C_N : \mathcal{H}_N \longrightarrow [0,1]$, defined by

$$C_N(|\psi\rangle) := \big|\, \overline{\langle\psi|}(-i\sigma_y) \otimes \cdots \otimes (-i\sigma_y)|\psi\rangle \,\big|.$$

It is possible to prove that the concurrence is identically 0 when N is odd. Moreover, it gives 0 on separable states and does not increase under the local operations.

Example 3.3.1. *Let $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ be a separable state of two qubits. In the computational basis $\{|0\rangle, |1\rangle\}$, each $|\psi_j\rangle$, $j = 1, 2$, can be represented by the column vectors*

$$|\psi_j\rangle = \begin{pmatrix} c_j \\ d_j \end{pmatrix},$$

where c_j and d_j are complex numbers. Note that

$$\big|\, \overline{\langle\psi_j|}(-i\sigma_y)|\psi_j\rangle \,\big| = \big| \begin{pmatrix} c_j & d_j \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} c_j \\ d_j \end{pmatrix} \big| = 0\,,$$

and, therefore,

$$C_2(|\psi\rangle) = \big|\, \overline{\langle\psi|}(-i\sigma_y) \otimes (-i\sigma_y)|\psi\rangle \,\big| = \big|\, \overline{\langle\psi_1|}(-i\sigma_y)|\psi_1\rangle \otimes \overline{\langle\psi_2|}(-i\sigma_y)|\psi_2\rangle \,\big| = 0\,.$$

Example 3.3.2. *The generalized Bell states (3.8) have maximal concurrence. For example,*

$$C_2(|\Psi^+\rangle) = \big| \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \big| = \big| -1 \big| = 1\,.$$

The concurrence can be used to determine the entanglement capability of unitary evolutions. In this context, the concurrence canonical decomposition was introduced in [4, 5].

3.4 The concurrence canonical decomposition

The *concurrence canonical decomposition (CCD)* was introduced as a generalization of two qubit canonical decomposition to N qubits. It is the Cartan decomposition associated with the Cartan involution $\theta_S : \mathfrak{u}(2^N) \longrightarrow \mathfrak{u}(2^N)$, defined by

$$\theta_S(X) := S\bar{X}S^\dagger \,, \tag{3.18}$$

where $S := (-i\sigma_y) \otimes (-i\sigma_y) \otimes \cdots \otimes (-i\sigma_y)$, N factors. To describe the CCD, we consider the orthogonal basis of $\mathfrak{u}(2^N)$ given by the tensor products of the form $F := iF_1 \otimes F_2 \otimes \cdots \otimes F_N$, where $F_j = \sigma_{x,y,z}$ or $F_j = \mathbf{1}_2$, for all $j = 1, \ldots, N$. We can write

$$\theta_S(F) = -i\big[\,(-i\sigma_y)\bar{F}_1(-i\sigma_y)^\dagger\,\big] \otimes \cdots \otimes \big[\,(-i\sigma_y)\bar{F}_N(-i\sigma_y)^\dagger\,\big]\,. \tag{3.19}$$

Let us denote by $i\mathcal{I}_o^N$ and $i\mathcal{I}_e^N$ the corresponding subspaces of $\mathfrak{u}(2^N)$ that are the linear span of tensor products with an odd or even number of factors of $\sigma_{x,y,z}$, and the remaining factors are equal to $\mathbf{1}_2$. Here, the superscript N denotes the number of qubits. It can be easily seen that

$$(-i\sigma_y)\bar{\mathbf{1}}_2(-i\sigma_y)^\dagger = \mathbf{1}_2 \qquad \text{and} \qquad (-i\sigma_y)\bar{\sigma}(-i\sigma_y)^\dagger = -\sigma\,,$$

for $\sigma = \sigma_{x,y,z}$. Therefore, the involution θ_S leaves the elements of $\mathcal{I}_o^N$ unchanged and negates the elements of $\mathcal{I}_e^N$. Then, the CCD is the decomposition,

$$\mathfrak{u}(2^N) = i\mathcal{I}_o^N \oplus i\mathcal{I}_e^N. \tag{3.20}$$

In conclusion, we have the following theorem of [4].

Theorem 3.4.1. *The CCD is a Cartan decomposition associated with the Cartan involution θ_S defined in (3.18), that is,*

$$[i\mathcal{I}_o^N, i\mathcal{I}_o^N] \subseteq i\mathcal{I}_o^N, \qquad [i\mathcal{I}_o^N, i\mathcal{I}_e^N] \subseteq i\mathcal{I}_e^N, \qquad [i\mathcal{I}_e^N, i\mathcal{I}_e^N] \subseteq i\mathcal{I}_o^N.$$

Remark 3.4.1. *As the CCD is a Cartan decomposition, it has to be up to conjugacy one of the types* ***AI****,* ***AII****, or* ***AIII****. It turns out that the type of the CCD depends on the number N of qubits. If N is even, the CCD is of type* ***AI*** *and $i\mathcal{I}_o^N$ is conjugate to $\mathfrak{so}(2^N)$. Otherwise, the CCD is of type* ***AII*** *and $i\mathcal{I}_o^N$ is conjugate to $\mathfrak{sp}(2^{N-1})$.*

The subalgebra $i\mathcal{I}_o^N$ contains all the tensor products of type $\mathbf{1}_2 \otimes \cdots \otimes \mathbf{1}_2 \otimes i\sigma \otimes \mathbf{1}_2 \otimes \cdots \otimes \mathbf{1}_2$, and, therefore, the corresponding Lie subgroup $e^{i\mathcal{I}_o^N}$ of $\mathbf{U}(2^N)$ contains all the local transformations. This means that

$$\mathbf{SU}(2) \otimes \mathbf{SU}(2) \otimes \cdots \otimes \mathbf{SU}(2) \subseteq e^{i\mathcal{I}_o^N},$$

where the inclusion is strict for $N > 2$. For any $X \in \mathbf{U}(2^N)$, the KP decomposition (2.11) holds with $K = e^k$ and $P = e^p$, where $k \in i\mathcal{I}_o^N$ and $p \in i\mathcal{I}_e^N$. In particular, the factor K does not modify the concurrence, that is,

$$C_N(K|\psi\rangle) = C_N(|\psi\rangle),$$

for all $|\psi\rangle \in \mathcal{H}_N$ [4]. In conclusion, X and P have the same entanglement capability.

The CCD concerns decompositions of $N-$qubit quantum systems. In the next chapter, we shall be concerned with decompositions for multipartite quantum systems in arbitrary dimensions. In particular, we construct a decomposition that contains the CCD as a special case.

CHAPTER 4. The odd-even decomposition

Consider a multipartite quantum system composed of N subsystems with Hilbert spaces $\mathcal{H}_1, \dots, \mathcal{H}_N$ of dimensions $n_1, \dots, n_N$, respectively. The Hilbert space of the total system is

$$\mathcal{H}_{tot} := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N \,.$$

The set of Hermitian operators acting on the Hilbert space $\mathcal{H}_j$ of the jth system is the Jordan algebra $i\mathfrak{u}(n_j)$ where $j = 1, \dots, N$. Furthermore, the set of possible Hamiltonian operators acting on the Hilbert space $\mathcal{H}_{tot}$ of total system is the Jordan algebra $i\mathfrak{u}(n_1 n_2 \cdots n_N)$ of $n_1 n_2 \cdots n_N \times n_1 n_2 \cdots n_N$ Hermitian matrices. The Lie algebra associated with the dynamics of the composite system is $\mathfrak{u}(n_1 n_2 \cdots n_N)$, and the corresponding group of evolutions is the unitary Lie group $\mathbf{U}(n_1 n_2 \cdots n_N)$. Recall that three possible types of Cartan decompositions of $\mathfrak{u}(n_1 n_2 \cdots n_N)$ exist and result in decompositions of $\mathbf{U}(n_1 n_2 \cdots n_N)$. However, when dealing with multipartite systems, it is useful to have decompositions constructed in terms of the decompositions on the single subsystems. In this context, the odd-even decomposition (OED) was introduced in [10] as a generalization of the concurrence canonical decomposition. The main idea of [10] is to construct a decomposition for the Lie algebra $\mathfrak{u}(n_1 n_2 \cdots n_N)$ associated with the overall system starting from decompositions of type **AI** and **AII** performed on $\mathfrak{u}(n_j)$, the Lie algebra associated with the jth system. In [8], similar ideas of OED were used to construct a decomposition for $\mathfrak{u}(n_1 n_2 \cdots n_N)$ starting from decompositions of **AIII** applied on $\mathfrak{u}(n_j)$.

The present chapter is devoted to the construction of the odd-even decompositions and is organized as follows. In section 4.1, we recall the definition of a Jordan algebra and a Cartan symmetry, and we introduce the Cartan type decomposition of a Jordan algebra. Then, we illustrate the dual structures between the unitary Lie algebra $\mathfrak{u}(n)$ of skew-Hermitian matrices and the Jordan algebra $i\mathfrak{u}(n)$ of Hermitian matrices, and we discuss the correspondence between the Cartan involutions and the Cartan symmetries. In section 4.2, we use this duality to construct decompositions for multipartite systems by combining Cartan decompositions of types **AI** and **AII** performed on subsystems, and we show that the CCD is a special case of this construction. We also show how similar constructions can be obtained starting from decompositions of type **AIII** applied to subsystems. In section 4.3, we give the outline of the computation of the KAK decompositions and present a numerical example.

4.1 Quantum symmetries and Cartan symmetries: duality

Definition 4.1.1. *A real vector space $\mathcal{J}$ with a binary product $\bullet : \mathcal{J} \times \mathcal{J} \longrightarrow \mathcal{J}$ is called a Jordan algebra if the following conditions hold:*

1. *Commutativity:* $x \bullet y = y \bullet x$,
2. *Jordan identity:* $(x^2 \bullet y) \bullet x = x^2 \bullet (y \bullet x)$,

for all $x, y \in \mathcal{J}$.

Perhaps the simplest nontrivial example of a Jordan algebra is the vector space $i\mathfrak{u}(n)$ of $n \times n$ Hermitian matrices under the binary product

$$A \bullet B := \frac{1}{2}\big(AB + BA\big)\,, \tag{4.1}$$

called the *anticommutator*. It is customary to denote the anticommutator by the curly bracket, that is, $\{A\,, B\} := A \bullet B$.

Definition 4.1.2. *A homomorphism ψ between two Jordan algebras $\mathcal{J}_1$ and $\mathcal{J}_2$ is a linear map compatible with the anticommutator, that is, $\psi : \mathcal{J}_1 \longrightarrow \mathcal{J}_2$*

$$\psi(\{x, y\}_1) = \{\psi(x), \psi(y)\}_2\,,$$

for all $x, y \in \mathcal{J}_1$. Here, $\{\cdot\,,\cdot\}_1$ and $\{\cdot\,,\cdot\}_2$ denote the anticommutators on $\mathcal{J}_1$ and $\mathcal{J}_2$, respectively.

A detailed presentation of Jordan algebras can be found in [18]. In the rest of this dissertation, we shall be concerned with the Jordan algebra $i\mathfrak{u}(n)$. Recall that the Hermitian matrices in $i\mathfrak{u}(n)$ represent the observables of $n-$dimensional quantum systems. On the space of observables, *quantum symmetries* are defined as Jordan algebra homomorphisms

$$\Theta : i\mathfrak{u}(n) \longrightarrow i\mathfrak{u}(n)\,.$$

A particular type of quantum symmetry of interest is a Cartan symmetry.

Definition 4.1.3. *A quantum symmetry* Θ *on* $i\mathfrak{u}(n)$ *is called a* Cartan symmetry *if applied twice is the identity on* $i\mathfrak{u}(n)$*, that is,* $\Theta^2 = \boldsymbol{1}$.

In the following, we shall illustrate the correspondence between Cartan involutions and Cartan symmetries. For this purpose, we begin with a Cartan decomposition

$$\mathfrak{u}(n) = \mathcal{K} \oplus \mathcal{P}\,. \tag{4.2}$$

Let us denote the corresponding Cartan involution by θ. Associated with this decomposition is a decomposition of the Jordan algebra $i\mathfrak{u}(n_j)$,

$$i\mathfrak{u}(n) = i\mathcal{K} \oplus i\mathcal{P}\,, \tag{4.3}$$

called a *Cartan type* decomposition of $i\mathfrak{u}(n)$. Suppose that the decomposition in (4.2) is of type either **AI** or **AII**. Then, it can be verified that the map Θ defined by

$$\Theta(iA) = -i\theta(A)\,,$$

is a Cartan symmetry on $i\mathfrak{u}(n)$ where $A \in \mathfrak{u}(n)$. In particular, the subspaces $i\mathcal{P}$ and $i\mathcal{K}$ in (4.3) are, respectively, the $+1$ and -1 eigenspaces of Θ. Therefore, it follows that

$$\{i\mathcal{K}\,, i\mathcal{K}\} \subseteq i\mathcal{P}\,, \qquad \{i\mathcal{K}\,, i\mathcal{P}\} \subseteq i\mathcal{K}\,, \qquad \{i\mathcal{P}\,, i\mathcal{P}\} \subseteq i\mathcal{P}\,. \tag{4.4}$$

Note that the subspace $i\mathcal{P}_j$ has the structure of a Jordan algebra. On the other hand, if (4.2) is of type **AIII**, then a Cartan symmetry Θ can be constructed by defining

$$\Theta(iA) = i\theta(A)\,.$$

In this case, the subspaces $i\mathcal{K}$ and $i\mathcal{P}$ in (4.3) become the $+1$ and -1 eigenspaces of Θ, respectively. Equivalently, $i\mathcal{K}$ and $i\mathcal{P}$ have the anticommutator relations

$$\{i\mathcal{K}\,, i\mathcal{K}\} \subseteq i\mathcal{K}\,, \qquad \{i\mathcal{K}\,, i\mathcal{P}\} \subseteq i\mathcal{P}\,, \qquad \{i\mathcal{P}\,, i\mathcal{P}\} \subseteq i\mathcal{K}\,. \tag{4.5}$$

In conclusion, there is a duality between the decompositions of the unitary Lie algebra $\mathfrak{u}(n)$ and the Jordan algebra $i\mathfrak{u}(n)$ and a correspondence between the Cartan involutions on $\mathfrak{u}(n)$ and Cartan symmetries on $i\mathfrak{u}(n)$. This duality was studied in [10] and is of fundamental importance in the remainder of this chapter for the construction of the odd-even type decompositions.

4.2 Odd-even type decompositions

4.2.1 The OED of type AI and AII

The purpose of this section is to construct a Cartan decomposition for the Lie algebra $\mathfrak{u}(n_1 n_2 \cdots n_N)$ associated with a multipartite system composed of a number N of subsystems by performing decompositions on Lie algebras $\mathfrak{u}(n_j)$, $j = 1, \ldots, N$, associated with the single subsystems. To this purpose, we begin with the Cartan decomposition

$$\mathfrak{u}(n_j) = \mathcal{K}_j \oplus \mathcal{P}_j\,, \tag{4.6}$$

of type either **AI** or **AII**. The corresponding decomposition of the Jordan algebra $i\mathfrak{u}(n_j)$ is

$$i\mathfrak{u}(n_j) = i\mathcal{K}_j \oplus i\mathcal{P}_j\,. \tag{4.7}$$

Let us denote by θ_j and Θ_j the associated Cartan involution on $\mathfrak{u}(n_j)$ and the corresponding Cartan symmetry on $i\mathfrak{u}(n_j)$, respectively. Let σ_j and S_j denote the generic elements of orthonormal bases of the subspaces $i\mathcal{K}_j$ and $i\mathcal{P}_j$, respectively. An orthonormal basis of $i\mathfrak{u}(n_1 n_2 \cdots n_N)$ can be obtained by the tensor products of the form

$$F := F_1 \otimes F_2 \otimes \cdots \otimes F_N\,, \tag{4.8}$$

where $F_j = \sigma_j$ or $F_j = S_j$ for all possible combinations of σ_j and S_j in the N places. Define $\mathcal{I}_o$ and $\mathcal{I}_e$ to be the respective vector spaces spanned by tensor products of form (4.8) with an odd or even number of elements of σ_j. Thus, we write the direct sum decomposition

$$i\mathfrak{u}(n_1 n_2 \cdots n_N) = \mathcal{I}_o \oplus \mathcal{I}_e \,. \tag{4.9}$$

This decomposition, together with the dual decomposition

$$\mathfrak{u}(n_1 n_2 \cdots n_N) = i\mathcal{I}_o \oplus i\mathcal{I}_e \,, \tag{4.10}$$

is called the *odd-even* decomposition (OED) of $\mathfrak{u}(n_1 n_2 \ldots n_N)$. We are now ready to state the following theorem of [10].

Theorem 4.2.1. *The decomposition given in (4.9) is a Cartan type decomposition of the Jordan algebra* $i\mathfrak{u}(n_1 n_2 \cdots n_N)$ *that has the anticommutator relations*

$$\{\mathcal{I}_o \,, \mathcal{I}_o\} \subseteq \mathcal{I}_e \,, \qquad \{\mathcal{I}_o \,, \mathcal{I}_e\} \subseteq \mathcal{I}_o \,, \qquad \{\mathcal{I}_e \,, \mathcal{I}_e\} \subseteq \mathcal{I}_e \,.$$

Therefore, the corresponding decomposition (4.10) of the unitary Lie algebra $\mathfrak{u}(n_1 n_2 \cdots n_N)$ *is a Cartan decomposition, that is,*

$$[i\mathcal{I}_o \,, i\mathcal{I}_o] \subseteq i\mathcal{I}_o \,, \qquad [i\mathcal{I}_o \,, i\mathcal{I}_e] \subseteq i\mathcal{I}_e \,, \qquad [i\mathcal{I}_e \,, i\mathcal{I}_e] \subseteq i\mathcal{I}_o \,.$$

Proof. Let us define Θ_{tot} to be the tensor product of Cartan symmetries Θ_j, $j = 1, \ldots, N$, i.e,

$$\Theta_{tot} := \Theta_1 \otimes \Theta_2 \otimes \cdots \otimes \Theta_N \,. \tag{4.11}$$

Let $F = F_1 \otimes F_2 \otimes \cdots \otimes F_N$ be a generic basis element of $i\mathfrak{u}(n_1 n_2 \cdots n_N)$ where $F_j = \sigma_j$ or $F_j = S_j$. Then,

$$\Theta_{tot}(F) = \Theta_1(F_1) \otimes \Theta_2(F_2) \otimes \cdots \otimes \Theta_N(F_N) \,.$$

Since we apply a decomposition of type either **AI** or **AII** on $i\mathfrak{u}(n_j)$, we have $\Theta_j(\sigma_j) = -\sigma_j$ and $\Theta_j(S_j) = S_j$. Let k be the number of the elements of σ_j in F. Then, it can be verified that

$$\Theta_{tot}(F) = (-1)^k F \,.$$

The foregoing argument shows that $\Theta_{tot}^2 = \mathbf{1}$, i.e., Θ_{tot} is a Cartan symmetry which negates the elements of $\mathcal{I}_o$ and leaves the elements of $\mathcal{I}_e$ unchanged as the subspaces $\mathcal{I}_o$ and $\mathcal{I}_e$ are the linear span of tensor products with an odd or even number of elements of σ_j, respectively. In other words, $\mathcal{I}_o$ and $\mathcal{I}_e$ are the -1 and $+1$ eigenspaces of the Θ_{tot}, respectively. This means that the decomposition given in (4.9) is a Cartan type decomposition of the Jordan algebra $\mathfrak{u}(n_1 n_2 \ldots n_N)$. Consequently, the corresponding decomposition (4.10) is a Cartan decomposition of $\mathfrak{u}(n_1 n_2 \cdots n_N)$. □

Remark 4.2.1. *Since the unitary Lie algebra $\mathfrak{u}(n_1 n_2 \cdots n_N)$ has three possible types of Cartan decompositions, the OED (4.10) must fall in one of the types **AI**, **AII**, or **AIII**. It turns out that the type of the OED depends on the number r of the decompositions of type **AII** performed on subsystems. If r is even, then the OED is of type **AI** and the Lie subalgebra $i\mathcal{I}_o$ is conjugate to $\mathfrak{so}(n_1 n_2 \ldots n_N)$. Otherwise, the OED is of type **AII** and $i\mathcal{I}_o$ is conjugate to $\mathfrak{sp}(n_1 n_2 \ldots n_N/2)$.*

We give schematic representation of the construction of the OED in Figure 4.2.1. In view of the previous theorem, we shall construct several odd-even decompositions and identify their types for the Lie algebra $\mathfrak{u}(4)$ associated with a quantum system composed of two qubits using one or both of the Cartan decompositions

$$\mathfrak{u}(2) = \mathrm{span}\{i\sigma_x\} \oplus \mathrm{span}\{i\sigma_y\,, i\sigma_z\,, i\,\mathbf{1}_2\} \qquad \text{and} \qquad \mathfrak{u}(2) = \mathrm{span}\{i\sigma_x\,, i\sigma_y\,, i\sigma_z\} \oplus \mathrm{span}\{i\,\mathbf{1}_2\}\,, \tag{4.12}$$

which are of types **AI** and **AII** respectively.

Example 4.2.1. *Consider an OED $\mathfrak{u}(4) = i\mathcal{I}_o \oplus i\mathcal{I}_e$. If this decomposition is constructed by applying decompositions of type **AII** on both qubits, then the subspaces $\mathcal{I}_o$ and $\mathcal{I}_e$ are given by*

$$\mathcal{I}_o = \mathrm{span}\{\sigma_{x,y,z} \otimes \mathbf{1}_2\,, \mathbf{1}_2 \otimes \sigma_{x,y,z}\} \quad \textit{and} \quad \mathcal{I}_e = \mathrm{span}\{\sigma_{x,y,z} \otimes \sigma_{x,y,z}\,, \mathbf{1}_2 \otimes \mathbf{1}_2\}.$$

*Indeed, this OED is the same as the decomposition given in (3.13) which is associated with the two qubit canonical decomposition. Due to the even number of type **AII** decompositions performed on subsystems, $i\mathcal{I}_o$ is conjugate to $\mathfrak{so}(4)$.*

*Suppose now that the OED is constructed by applying the decomposition of type **AI** on the first qubit and the decomposition of type **AII** on the second qubit. Then we obtain*

$$\mathcal{I}_o = \mathrm{span}\{\sigma_x \otimes \mathbf{1}_2\,, \sigma_{y,z} \otimes \sigma_{x,y,z}\,, \mathbf{1}_2 \otimes \sigma_{x,y,z}\} \quad \textit{and} \quad \mathcal{I}_e = \mathrm{span}\{\sigma_x \otimes \sigma_{x,y,z}\,, \sigma_{y,z} \otimes \mathbf{1}_2\,, \mathbf{1}_2 \otimes \mathbf{1}_2\}.$$

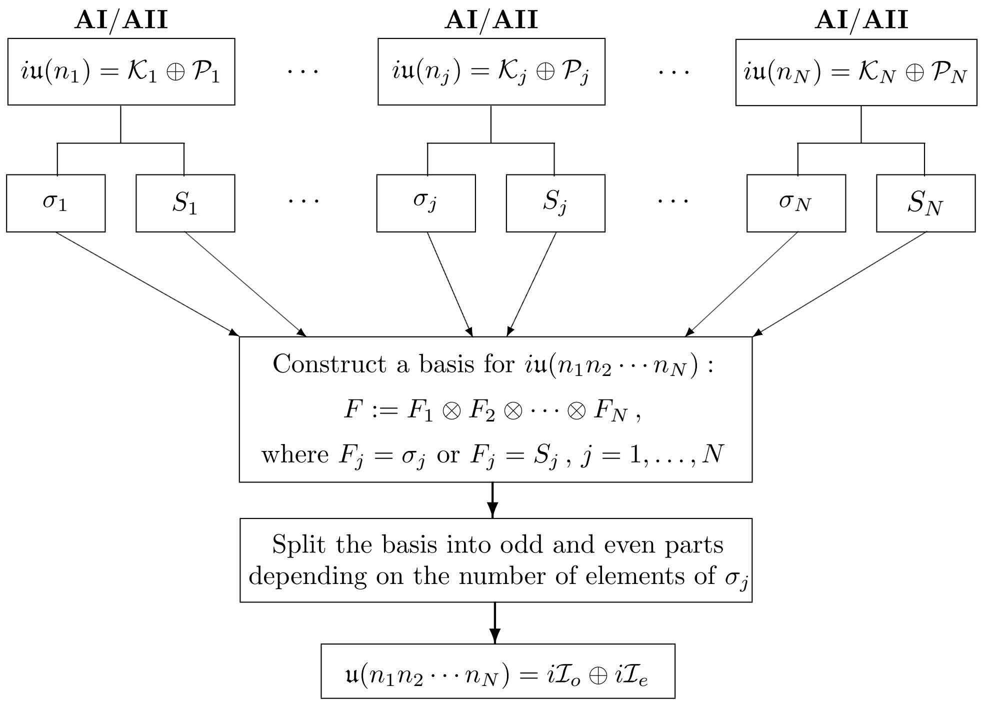

Figure 4.1 A scheme of the odd-even decomposition of type either **AI** or **AII**. The procedure starts by performing decompositions of type either **AI** or **AII** on each single subsystem. Then, we form a basis of the overall system by taking the tensor products of the generic basis elements σ_j and S_j, $j = 1, \ldots, N$. Finally, we split the basis elements of $\mathfrak{u}(n_1 n_2 \cdots n_N)$ into even and odd parts depending on the number of elements of σ_j.

Consequently, the OED is of type ***AII*** *and the subalgebra* $i\mathcal{I}_o$ *is conjugate to* $\mathfrak{sp}(2)$ *as the number of the decompositions of type* ***AII*** *performed on the single subsystems is odd. Similarly, if the OED is constructed by performing decompositions of type* ***AI*** *on both qubits, we obtain*

$$\mathcal{I}_o = \mathrm{span}\{\sigma_{y,z} \otimes \sigma_x \,, \sigma_x \otimes \sigma_{y,z} \,, \boldsymbol{1}_2 \otimes \sigma_x \,, \sigma_x \otimes \boldsymbol{1}_2\} \quad \textit{and} \quad \mathcal{I}_e = \mathrm{span}\{\sigma_{y,z} \otimes \sigma_{y,z} \,, \boldsymbol{1}_2 \otimes \boldsymbol{1}_2\}\,,$$

with the Lie subalgebra $i\mathcal{I}_o$ *conjugate to* $\mathfrak{so}(4)$.

Remark 4.2.2. *The CCD is a special case of the OED when all the subsystems are two dimensional, i.e.,* $n_j = 2$ *for all* $j = 1, 2, \ldots N$*, and (4.2) is of type* ***AII****, that is,* $\mathcal{K}_j$ *is conjugate to* $\mathfrak{sp}(1)$. *More precisely, the construction of the CCD is as follows. The Pauli matrices* $\sigma_{x,y,z}$ *with* $\boldsymbol{1}_2$ *form a basis of the Jordan algebra* $i\mathfrak{u}(2)$. *An orthogonal basis of* $i\mathfrak{u}(2^N)$ *is given by the tensor products of the form (4.8) where* $F_j = \sigma_{x,y,z}$ *or* $F_j = \boldsymbol{1}_2$ *for all* $j = 1, \ldots, N$. *Since* $\mathfrak{sp}(1) = \mathfrak{su}(2)$*, the first decomposition in (4.12) can be seen as a Cartan decomposition of type* ***AII*** *of* $\mathfrak{u}(2)$. *Then, the CCD of* $\mathfrak{u}(2^N)$ *is the decomposition*

$$\mathfrak{u}(2^N) = i\mathcal{I}_o^N \oplus i\mathcal{I}_e^N \tag{4.13}$$

where $\mathcal{I}_o^N$ *(*$\mathcal{I}_e^N$*) is the span of the tensor products, which contains an odd (even) number of elements* $\sigma_{x,y,z}$. *Here, the superscript* N *stands for the number of qubits. The type of the CCD depends on the number* N *of qubits. If* N *is even, then the CCD (4.13) is of type* ***AI*** *and* $i\mathcal{I}_o$ *is conjugate to* $\mathfrak{so}(2^N)$. *Otherwise, it is of type* ***AII*** *and* $i\mathcal{I}_o$ *is conjugate to* $\mathfrak{sp}(2^{N-1})$.

4.2.2 The OED of type AIII

The OED discussed in the previous section is a generalization of the CCD and is constructed by performing decompositions of type **AI** and **AII** on each single subsystem. We observe here that the procedure followed to construct the OED can be applied with few changes to construct an overall decomposition of type **AIII** starting from decompositions of type **AIII** performed on subsystems. We start with a motivating example for the case of a bipartite system of two qubits, and then we generalize this idea to multipartite systems.

Example 4.2.2. *Consider a quantum system composed of two qubits. On each qubit, let us apply the type* ***AIII*** *decomposition*

$$\mathfrak{u}(2) = \mathrm{span}\{i\,\boldsymbol{1}_2, i\sigma_z\} \oplus \mathrm{span}\{i\sigma_x, i\sigma_y\}$$

and collect in the respective subspaces $\mathcal{J}_e$ and $\mathcal{J}_o$ the linear combinations of the tensor products with an even or odd number of factors in the subspace $\mathrm{span}\{i\sigma_x\,, i\sigma_y\}$ *(modulo i), that is,*

$$\mathcal{J}_e = \mathrm{span}\{\boldsymbol{1}_2 \otimes \boldsymbol{1}_2\,, \boldsymbol{1} \otimes \sigma_z\,, \sigma_z \otimes \boldsymbol{1}_2\,, \sigma_z \otimes \sigma_z\,, \sigma_x \otimes \sigma_x\,, \sigma_x \otimes \sigma_y\,, \sigma_y \otimes \sigma_x\,, \sigma_y \otimes \sigma_y\}\,,$$

and

$$\mathcal{J}_o = \mathrm{span}\{\boldsymbol{1}_2 \otimes \sigma_x\,, \boldsymbol{1}_2 \otimes \sigma_y\,, \sigma_x \otimes \boldsymbol{1}_2\,, \sigma_y \otimes \boldsymbol{1}_2\,, \sigma_z \otimes \sigma_x\,, \sigma_z \otimes \sigma_y\,, \sigma_x \otimes \sigma_z\,, \sigma_y \otimes \sigma_z\}\,.$$

A straightforward calculation shows that the decomposition $\mathfrak{u}(4) = i\mathcal{J}_e \oplus i\mathcal{J}_o$ is a Cartan decomposition of type ***AIII*** *where $i\mathcal{J}_e$ is the Lie subalgebra.*

Unlike the construction of the OED discussed in the previous section, we performed decompositions of type **AIII** on both subsystems and obtained a decomposition of type **AIII** for the total system. In particular, we collected the tensor products with an even number of elements of σ_x and σ_y in the subspace $\mathcal{J}_e$. This example motivates the search of similar constructions for multipartite systems of arbitrary dimensions. We shall consider this next.

Consider again a multipartite quantum system composed of N quantum systems of dimensions $n_1\,, \ldots, n_N$. Suppose that the Cartan decomposition given in (4.6) is of type **AIII** for all $j = 1, \ldots, N$. Recall that σ_j and S_j denote the generic elements of orthonormal bases of $i\mathcal{K}_j$ and $i\mathcal{P}_j$, respectively. Define $\mathcal{J}_e$ and $\mathcal{J}_o$ to be the subspaces that are the linear combinations of the tensor products with an even and odd number of factors S_j, respectively. Thus, we write

$$i\mathfrak{u}(n_1 n_2 \ldots n_N) = \mathcal{J}_e \oplus \mathcal{J}_o\,. \tag{4.14}$$

The corresponding decomposition of $\mathfrak{u}(n_1 n_2 \ldots n_N)$ is given by

$$\mathfrak{u}(n_1 n_2 \ldots n_N) = i\mathcal{J}_e \oplus i\mathcal{J}_o\,. \tag{4.15}$$

Theorem 4.2.2. *The decomposition given in (4.14) is a Cartan type decomposition of the Jordan algebra* $i\mathfrak{u}(n_1 n_2 \ldots n_N)$ *with the anticommutator relations*

$$\{\mathcal{J}_e\,,\mathcal{J}_e\} \subseteq \mathcal{J}_e\,, \quad \{\mathcal{J}_e\,,\mathcal{J}_o\} \subseteq \mathcal{J}_o\,, \quad \{\mathcal{J}_o\,,\mathcal{J}_o\} \subseteq \mathcal{J}_e\,.$$

Therefore, the dual decomposition (4.15) is a Cartan decomposition of $\mathfrak{u}(n_1 n_2 \ldots n_N)$*, that is,*

$$[i\mathcal{J}_e\,,i\mathcal{J}_e] \subseteq i\mathcal{J}_e\,, \quad [i\mathcal{J}_e\,,i\mathcal{J}_o] \subseteq i\mathcal{J}_o\,, \quad [i\mathcal{J}_o\,,i\mathcal{J}_o] \subseteq i\mathcal{J}_e\,.$$

We shall give a proof by transforming the subspaces $i\mathcal{J}_e$ and $i\mathcal{J}_o$ into the standard block diagonal and block anti diagonal form of the Cartan decomposition of type **AIII**. In doing this, we will make use of the following corollary whose proof can be found in [15, §4.3].

Corollary 4.2.1. *Given square matrices* A *and* B *of respective sizes* $p \times p$ *and* $q \times q$*, there exists a permutation similarity matrix* $P(p,q) := \sum_{i=1}^{p}\sum_{j=1}^{q} E_{ij} \otimes E_{ij}^T$*, such that*

$$B \otimes A = P(p,q)^T \big(A \otimes B\big)\, P(p,q)\,.$$

Proof of Theorem 4.2.2. We give a proof by induction on the number N of the subsystems. For simplicity, we assume that all the initial decompositions are in the standard form of type **AIII** decompositions. If $N = 1$ the statement is obvious. Assume the statement is true for $N-1$. We denote by $\mathcal{J}_e^{N-1}$ and $\mathcal{J}_o^{N-1}$ the respective spaces of matrices in $i\mathfrak{u}(n_1 n_2 \cdots n_{N-1})$ that are linear combinations of the tensor products of an even or odd number of matrices in the subspace $i\mathcal{P}_j$, $j = 1, \ldots, N$, where $\mathcal{P}_j$ is the orthogonal complement of the Lie subalgebra $\mathcal{K}_j$ in the Cartan decomposition of type **AIII** of $\mathfrak{u}(n_j)$. Therefore, we have

$$\mathcal{J}_e = \big(\mathcal{J}_e^{N-1} \otimes i\mathcal{K}_N\big) \oplus \big(\mathcal{J}_o^{N-1} \otimes i\mathcal{P}_N\big) \qquad \text{and} \qquad \mathcal{J}_o = \big(\mathcal{J}_e^{N-1} \otimes i\mathcal{P}_N\big) \oplus \big(\mathcal{J}_o^{N-1} \otimes i\mathcal{K}_N\big)\,.$$

By the inductive assumption, there exists a unitary matrix R in $\mathbf{U}(n_1 n_2 \cdots n_{N-1})$ such that $i\mathcal{K}' = R^\dagger \mathcal{J}_e^{N-1} R$ and $i\mathcal{P}' = R^\dagger \mathcal{J}_o^{N-1} R$, where the subspaces $\mathcal{K}'$ and $\mathcal{P}'$ are in the standard block diagonal and block antidiagonal forms, respectively, i.e.,

$$\mathcal{K}' = \operatorname{span}\left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \;\middle|\; \begin{array}{c} A \in \mathfrak{u}(p_1),\ B \in \mathfrak{u}(q_1) \\ p_1 + q_1 = n_1 n_2 \cdots n_{N-1} \end{array} \right\},$$

and

$$\mathcal{P}' = \operatorname{span}\left\{ \begin{pmatrix} 0 & F \\ -F^\dagger & 0 \end{pmatrix} \middle| \begin{array}{c} F \text{ arbitrary } p_1 \times q_1 \\ \text{complex matrix} \end{array} \right\}.$$

Suppose that the subspaces $\mathcal{K}_N$ and $\mathcal{P}_N$ are spanned, respectively, by elements of form

$$\begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & G \\ -G^\dagger & 0 \end{pmatrix}$$

with $C \in \mathfrak{u}(p_2)$, $D \in \mathfrak{u}(q_2)$ and G an arbitrary $p_2 \times q_2$ complex matrix where $p_2 + q_2 = n_N$. Let $R_1 = R \otimes \mathbf{1}_{n_N}$. Then, the subspace $R_1^\dagger \mathcal{J}_e^N R_1$ is spanned by all the Hermitian matrices of form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \otimes \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & F \\ -F^\dagger & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & G \\ -G^\dagger & 0 \end{pmatrix}.$$

Using the Corollary 4.2.1, a permutation similarity matrix $R_2 = \operatorname{diag}\left(P(p_1, n_N), P(q_1, n_N)\right)$ can be constructed so that the subspace $R_2^\dagger R_1^\dagger \mathcal{J}_e^N R_1 R_2$ is spanned by all the matrices of the form

$$\begin{pmatrix} C \otimes A & 0 & 0 & G \otimes F \\ 0 & D \otimes A & -G^\dagger \otimes F & 0 \\ 0 & -G \otimes F^\dagger & C \otimes B & 0 \\ G^\dagger \otimes F^\dagger & 0 & 0 & D \otimes B \end{pmatrix}.$$

Finally, the subspace $R_3^\dagger R_2^\dagger R_1^\dagger \mathcal{J}_e^N R_1 R_2 R_3$, where R_3 has the form

$$R_3 = \begin{pmatrix} \mathbf{1}_{p_1 p_2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1}_{p_1 q_2} \\ 0 & 0 & \mathbf{1}_{q_1 p_2} & 0 \\ 0 & \mathbf{1}_{q_1 q_2} & 0 & 0 \end{pmatrix},$$

is spanned by all Hermitian matrices of the form

$$\begin{pmatrix} C \otimes A & G \otimes F & 0 & 0 \\ G^\dagger \otimes F^\dagger & D \otimes B & 0 & 0 \\ 0 & 0 & C \otimes B & -G \otimes F^\dagger \\ 0 & 0 & -G^\dagger \otimes F & D \otimes A \end{pmatrix},$$

where the upper block is of size $p := p_1p_2 + q_1q_2$, and the lower block is of size $q := q_1p_2 + p_2q_1$. Similarly, it can be verified that the subspace $R_3^\dagger R_2^\dagger R_1^\dagger \mathcal{J}_o^N R_1R_2R_3$ is spanned by all Hermitian matrices of the form

$$\begin{pmatrix} 0 & 0 & C \otimes F & G \otimes A \\ 0 & 0 & -G^\dagger \otimes B & -D \otimes F^\dagger \\ -C \otimes F^\dagger & G \otimes B & 0 & 0 \\ -G^\dagger \otimes A & D \otimes F & 0 & 0 \end{pmatrix}.$$

In other words,

$$i\mathfrak{u}(n_1n_2 \cdots n_{N-1}n_N) = T^\dagger \mathcal{J}_e^N T \oplus T^\dagger \mathcal{J}_o^N T$$

is a Cartan decomposition of type **AIII** of the Jordan algebra $i\mathfrak{u}(n_1n_2 \cdots n_{N-1}n_N)$, where $T := R_1R_2R_3$. Hence, the corresponding decomposition

$$\mathfrak{u}(n_1n_2 \cdots n_{N-1}n_N) = iT^\dagger \mathcal{J}_e^N T \oplus iT^\dagger \mathcal{J}_o^N T$$

is a Cartan decomposition of type **AIII**. □

Remark 4.2.3. *The procedure followed to prove Theorem 4.2.1 can also be used with few changes to prove Theorem 4.2.2 as follows. Consider again the tensor product of Cartan symmetries in (4.11) where each Θ_j, $j = 1, \ldots, N$, is associated with a type* ***AIII*** *decomposition, i.e., $\Theta_j(\sigma_j) = \sigma_j$ and $\Theta_j(S_j) = -S_j$ for all $\sigma_j \in \mathcal{K}_j$ and $S_j \in \mathcal{P}_j$. Let k be the number of the elements S_j in $F = F_1 \otimes F_2 \otimes \cdots \otimes F_N$, where $F_j = \sigma_j$ or $F_j = S_j$. Then, it can be seen that*

$$\Theta_{tot}(F) = (-1)^k F\,.$$

Due to the number of factors S_j contained in F, Θ_{tot} leaves the elements of $\mathcal{J}_e$ unchanged and negates the elements of $\mathcal{J}_o$. Therefore, the subspaces $\mathcal{J}_e$ and $\mathcal{J}_o$ are the $+1$ and -1 eigenspaces of Θ_{tot}, respectively. In other words, the decomposition (4.14) is a Cartan type decomposition of the Jordan algebra $i\mathfrak{u}(n_1n_2 \ldots n_N)$, and, therefore, the associated decomposition given in (4.15) is a Cartan decomposition of $\mathfrak{u}(n_1n_2 \ldots n_N)$. Moreover, the Cartan symmetry Θ_{tot} is unitary since it is constructed by unitary symmetries. Hence, the decomposition (4.15) is of type ***AIII****.*

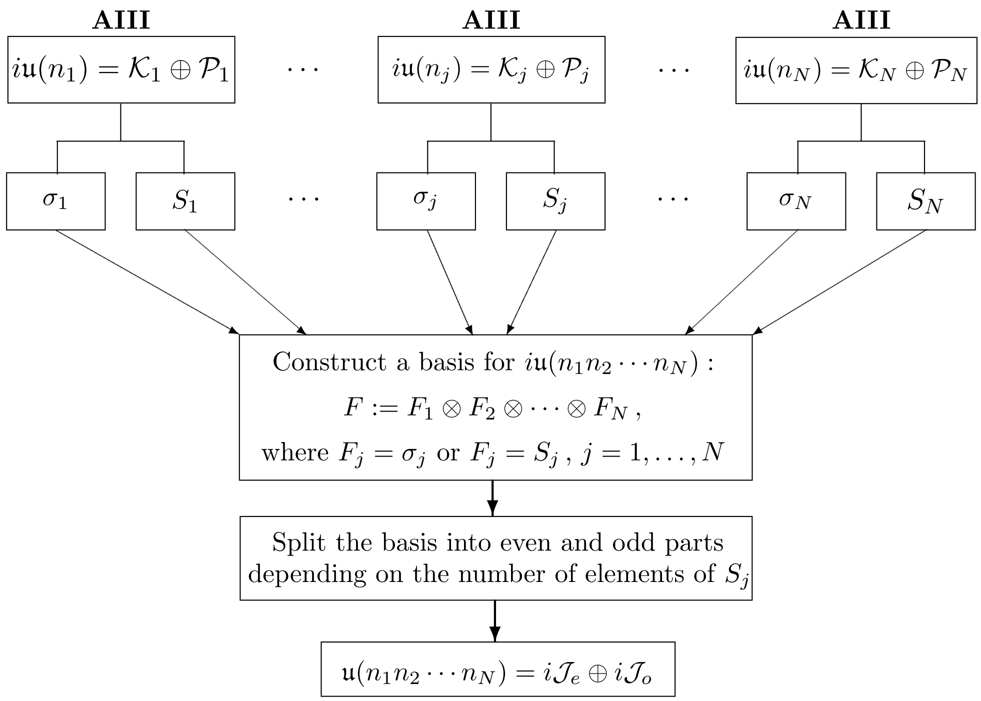

Figure 4.2 A scheme of the odd-even decomposition of type **AIII**. We start the procedure by performing type **AIII** decompositions on each single subsystem. Then, we form a basis of the overall system by taking the tensor products of the generic basis elements σ_j and S_j, $j = 1, \ldots, N$. Finally, we split the basis elements of $\mathfrak{u}(n_1 n_2 \cdots n_N)$ into even and odd parts depending on the number of elements of S_j.

In conclusion, using a method similar to the one presented in [10], we have constructed a Cartan decomposition of type **AIII** for the Lie algebra $\mathfrak{u}(n_1 n_2 \cdots n_N)$ starting from type **AIII** decompositions of Lie algebras $\mathfrak{u}(n_j)$. We also call this decomposition an *odd-even decomposition.* At this point, the question arises whether the OED decomposition can be constructed by mixing type **AI** or **AII** decompositions with type **AIII** decompositions in the odd-even sense. The following remark answers this question.

Remark 4.2.4. *The decompositions constructed by mixing type **AI** or **AII** decompositions with type **AIII** decompositions do not give rise to Cartan decompositions in the odd-even sense in general.*

In order to see this, we give the following example.

Example 4.2.3. *Let $\mathfrak{u}(4) = i\mathcal{I} \oplus i\mathcal{J}$ be obtained by performing the decompositions*

$$\mathfrak{u}(2) = \mathrm{span}\{i\sigma_x,\, i\sigma_y,\, i\sigma_z\} \oplus \mathrm{span}\{i\,\mathbf{1}_2\} \quad \textit{and} \quad \mathfrak{u}(2) = \mathrm{span}\{i\,\mathbf{1}_2,\, i\sigma_z\} \oplus \mathrm{span}\{i\sigma_x,\, i\sigma_y\}\,,$$

*of types **AII** and **AIII** on the fist system and the second system, respectively, that is,*

$$\mathcal{I} = \mathrm{span}\{\sigma_x \otimes \sigma_x,\, \sigma_x \otimes \sigma_y,\, \sigma_y \otimes \sigma_x,\, \sigma_y \otimes \sigma_y,\, \sigma_z \otimes \sigma_x,\, \sigma_z \otimes \sigma_y,\, \mathbf{1}_2 \otimes \sigma_z,\, \mathbf{1}_2 \otimes \mathbf{1}_2\}\,,$$

and

$$\mathcal{J} = \mathrm{span}\{\sigma_x \otimes \mathbf{1}_2,\, \sigma_x \otimes \sigma_z,\, \sigma_y \otimes \mathbf{1}_2,\, \sigma_y \otimes \sigma_z,\, \sigma_z \otimes \mathbf{1}_2,\, \sigma_z \otimes \sigma_z,\, \mathbf{1}_2 \otimes \sigma_x,\, \mathbf{1}_2 \otimes \sigma_y\}\,.$$

Consider the elements $i\sigma_x \otimes \sigma_x,\ i\sigma_y \otimes \sigma_x \in i\mathcal{I}$ and $i\,\mathbf{1}_2 \otimes \sigma_x,\ i\,\mathbf{1}_2 \otimes \sigma_y \in i\mathcal{J}$, then

$$[i\sigma_x \otimes \sigma_x\,, i\sigma_y \otimes \sigma_x] = -2i\sigma_z \otimes \mathbf{1}_2 \notin i\mathcal{I} \qquad \textit{and} \qquad [i\,\mathbf{1}_2 \otimes \sigma_x\,, i\,\mathbf{1}_2 \otimes \sigma_y] = -2i\,\mathbf{1}_2 \otimes \sigma_z \notin i\mathcal{J}\,,$$

i.e, none of $i\mathcal{I}$ and $i\mathcal{J}$ is closed under the commutator. Thus, the above remark holds.

Remark 4.2.5. *The procedures described in Theorems 4.2.1 and 4.2.2 allow great flexibility in the construction of various Cartan decompositions. Not only are we free to choose decompositions of appropriate types for each subsystem, but we can also choose the conjugate decompositions of the same type. This gives a method for the construction of an unbounded number of decompositions in terms of tensor product matrices, even for the case of N qubits. This flexibility is crucial in the construction of gradings and of recursive decompositions, as we shall see in the following chapter.*

4.3 Computation of the OED

Numerical algorithms exist for the computation of the KAK decompositions of $\mathbf{U}(n)$ induced by the Cartan decompositions given in the standard forms [4, 5, 9, 23]. Using such algorithms along with a change of basis matrix, we can compute the OED of $\mathbf{U}(n)$. In this section, we give the outline of how to find such change of basis matrices. This discussion was given in [9] for the odd-even decompositions of types **AI** and **AII**. Here, we extend this to the odd-even decompositions of type **AIII**. For simplicity of our calculations, in the following we assume that all the initial decompositions for the construction of the OED are performed in the standard forms as given in equations (2.14), (2.16), and (2.18).

Let us start with the OED

$$u(n_1 n_2 \cdots n_N) = i\mathcal{I}_o \oplus i\mathcal{I}_e \,. \tag{4.16}$$

It follows from the construction of the OED that the associated Cartan involution is given by

$$\theta_{tot}(F) = (U_1 \otimes U_2 \otimes \cdots \otimes U_N)\, \bar{F}\, (U_1^{-1} \otimes U_2^{-1} \otimes \cdots \otimes U_N^{-1}), \tag{4.17}$$

where $U_j = \mathbf{1}_{n_j}$ if a decomposition of type **AI** performed on the jth subsystem and $U_j = J_{n_j}$ (cf. equation (2.6)) if a decomposition of type **AII** performed on the jth subsystem for $j = 1, \ldots, N$. First, we suppose that the OED given in (4.16) is of type **AI**, i.e., the number of type **AII** decompositions performed on subsystems is even. There exists a change of basis matrix T in $\mathbf{U}(n_1 n_2 \cdots n_N)$ such that

$$i\mathcal{I}_o = T\mathfrak{so}(n_1 n_2 \cdots n_N)\, T^\dagger \qquad \text{and} \qquad i\mathcal{I}_e = T\mathfrak{so}(n_1 n_2 \cdots n_N)^\perp\, T^\dagger.$$

Comparing the involutions (2.15) and (4.17), the unitary matrix T must be chosen to satisfy

$$TT^T = U_1 \otimes U_2 \otimes \cdots \otimes U_N.$$

Analogously, for OED of type **AII**, comparing (2.17) and (4.17), we choose T such that

$$TJT^T = U_1 \otimes U_2 \otimes \cdots \otimes U_N.$$

On the other hand, for the case of OED of type **AIII**, the matrix T constructed in the proof of the Theorem 4.2.2 provides the desired change of basis matrix. Furthermore, other change of basis matrices can be found by comparing the Cartan involutions as similar to the previous cases. More specifically, a change of base matrix T must be chosen to satisfy

$$TI_{p,q}T^\dagger = I_{p_1,q_1} \otimes I_{p_2,q_2} \otimes \cdots \otimes I_{p_N,q_N}\,,$$

where p and q are the indices of the total decomposition and p_j and q_j, $j = 1, \ldots, N$, are the indices of the decomposition performed on the jth subsystem.

Once a change of base matrix T is found, the OED of $X \in \mathbf{U}(n_1 n_2 \cdots n_N)$ can be computed as follows. Using the algorithms given in the standard coordinates, one first computes the KAK the decomposition of $T^\dagger X T$, that is, $T^\dagger X T = K_1' A' K_2'$. Then, the OED of X is given by

$$X = K_1 A K_2\,,$$

where $K_j = TK_j' T^\dagger$, $j = 1, 2$, and $A = TA'T^\dagger$. In order to illustrate the concept, we give the following example.

Example 4.3.1. *We compute the decomposition of the unitary matrix*

$$X = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

induced by the OED $u(6) = i\mathcal{J}_e \oplus i\mathcal{J}_o$, for indices $n_1 = 2\,, n_2 = 3$, with $p_1 = p_2 = q_1 = 1\,, q_2 = 2$ so that $p_1 + q_1 = n_1$ and $p_2 + q_2 = n_2$. Note that the conjugation by

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

*maps the subspaces $i\mathcal{J}_e$ and $i\mathcal{J}_o$ into the standard block diagonal and block antidiagonal forms, respectively. Using the tools presented in [9], it can be shown that the KAK decomposition of $T^\dagger XT$ induced by the standard type **AIII** decomposition is given by $T^\dagger XT = K_1'A'K_2'$, where*

$$K_1' = \begin{pmatrix} i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & i \end{pmatrix}, \quad A' = \begin{pmatrix} 0 & 0 & 0 & i & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \\ i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -i & 0 & 0 & 0 \end{pmatrix}, \quad K_2' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Therefore, the OED of X is given by $X = K_1AK_2$, where $K_j = TK_j'T^\dagger$, $j = 1, 2$, and $A = TA'T^\dagger$. Finally, we write each factor in the above decomposition as exponentials of matrices to obtain

$$X = e^{k_1}e^{a}e^{k_2}\,,$$

where

$$k_1 = \frac{i\pi}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \frac{i\pi}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{-1-i}{\sqrt{2}} \\ 0 & \frac{-1+i}{\sqrt{2}} & \frac{1}{2} \end{pmatrix},$$

$$k_2 = \frac{i\pi}{4}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & i & 0 \\ -i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} - \frac{i\pi}{4}\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and

$$a = \frac{i\pi}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

It is clear that $k_2, k_2 \in i\mathcal{J}_e$ and a is in a Cartan subalgebra contained in $i\mathcal{J}_o$.

CHAPTER 5. A general framework for recursive decompositions

Cartan decomposition theorem can be applied successively to obtain finer decompositions of Lie groups, especially the unitary group $\mathbf{U}(n)$, as pointed out in section 2.3. In this context, the Khaneja Glaser and D'Alessandro Romano decompositions recursively factors unitary transformations on quantum systems of appropriate dimensions. Such decompositions are a very useful tool in quantum control theory to analyze the dynamics and design control algorithms for quantum systems. In particular, since they keep the tensor product basis structure, such decompositions allow the identification of the local and entangling character of each factor. This fact makes such decompositions appealing.

In this chapter, we study the recursive decompositions of the unitary Lie group $\mathbf{U}(n)$. Based on the observation that an appropriate grading of a Lie algebra induces a recursive decomposition, we develop a general framework that contains the Khaneja Glaser and D'Alessandro Romano decompositions as a special case. This chapter is organized as follows: In section 5.1, we recall the definition of the grading of a Lie algebra, and then we relate a recursive decomposition to a grading. Using this connection, in section 5.2, we provide a general scheme for recursive decompositions for $\mathbf{U}(n)$. In section 5.3, we present a numerical example.

5.1 Grading of a Lie algebra and recursive decompositions

5.1.1 Grading of a Lie algebra

Definition 5.1.1. *Let $\mathcal{L}$ be a Lie algebra, and let M be an additive semigroup, that is, a set M with an associative binary operation $+ : M \times M \longrightarrow M$. Any direct sum decomposition*

$$\mathcal{L} = \bigoplus_{i \in M} \mathcal{L}_i \,,$$

*is called an $M-$*grading *of $\mathcal{L}$ if the subspaces $\mathcal{L}_i$ and $\mathcal{L}_j$ satisfy the commutation relation*

$$[\mathcal{L}_i, \mathcal{L}_j] \subseteq \mathcal{L}_{i+j}\,, \tag{5.1}$$

for all $i, j \in M$. In other words, if the commutator of $x \in \mathcal{L}_i$ with $y \in \mathcal{L}_j$ is nonzero, then there exists a nonzero $z \in \mathcal{L}_{i+j}$ such that $z = [x\,, y]$.

According to (5.1), if M is a monoid, that is, a semigroup with an identity element 0, then the subspace $\mathcal{L}_0$ is a Lie subalgebra, since it naturally satisfies the commutation relation

$$[\mathcal{L}_0, \mathcal{L}_0] \subseteq \mathcal{L}_0\,.$$

Example 5.1.1. *Consider the special linear Lie algebra $\mathfrak{sl}(2, \mathbb{R})$ spanned by the matrices*

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

These basis elements have the commutation relations

$$[h\,, x] = 2x\,, \qquad [x\,, y] = h\,, \qquad [h\,, y] = -2y\,.$$

Let $M = \{-1, 0, 1\}$. Then, M becomes a monoid with the binary addition given by the following table:

$(M, +)$	0	-1	1
0	0	-1	1
-1	-1	0	0
1	1	0	0

Therefore, the choice of one dimensional subspaces

$$\mathcal{L}_{-1} = \mathrm{span}\{x\}\,, \qquad \mathcal{L}_0 = \mathrm{span}\{h\}\,, \qquad \mathcal{L}_1 = \mathrm{span}\{y\}$$

makes $\mathfrak{sl}(2, \mathbb{R})$ into an $M-$graded Lie algebra.

Definition 5.1.2. *A grading $\mathcal{L} = \bigoplus_{j \in N} \mathcal{R}_j$ is called a* refinement *of the grading $\mathcal{L} = \bigoplus_{i \in M} \mathcal{L}_i$, if for any $j \in N$ there exists $i \in M$ such that $\mathcal{R}_j \subseteq \mathcal{L}_i$.*

It is clear that any Lie algebra $\mathcal{L}$ with a Cartan decomposition (2.9) is endowed with the structure of a $\mathbb{Z}_2-$grading with $\mathcal{K} := \mathcal{L}_0$ and $\mathcal{P} := \mathcal{L}_1$, that is,

$$[\mathcal{L}_0\,, \mathcal{L}_0] \subseteq \mathcal{L}_0\,, \qquad [\mathcal{L}_0\,, \mathcal{L}_1] \subseteq \mathcal{L}_1\,, \qquad [\mathcal{L}_1\,, \mathcal{L}_1] \subseteq \mathcal{L}_0\,.$$

Example 5.1.2. *The CCD $\mathfrak{u}(4) = \mathcal{L}_0 \oplus \mathcal{L}_1$ defines a $\mathbb{Z}_2-$grading of $\mathfrak{u}(4)$. A refinement of this grading is the $\mathbb{Z}_2 \times \mathbb{Z}_2-$grading*

$$\mathfrak{u}(4) = \mathcal{L}_{00} \oplus \mathcal{L}_{01} \oplus \mathcal{L}_{10} \oplus \mathcal{L}_{11}\,,$$

where $\mathcal{L}_{00} = \mathrm{span}\{i\sigma \otimes \mathbf{1}_2\,, i\,\mathbf{1}_2 \otimes \sigma_z\}$, $\mathcal{L}_{01} = \mathrm{span}\{i\,\mathbf{1}_2 \otimes \sigma_{x,y}\}$, $\mathcal{L}_{11} = \mathrm{span}\{i\sigma \otimes \sigma_z\,, \mathbf{1}_2 \otimes \mathbf{1}_2\}$, and $\mathcal{L}_{10} = \mathrm{span}\{i\sigma \otimes \sigma_{x,y}\}$.

As discussed in the previous chapters, for a Lie algebra $\mathcal{L}$, there are many Cartan decompositions. These decompositions can be used to obtain refined gradings. More specifically, p number of Cartan decompositions of a Lie algebra $\mathcal{L}$ give a $\mathbb{Z}_2^p-$grading of $\mathcal{L}$ for a general p.

Proposition 5.1.1. *We consider p number of distinct (possibly conjugate, but not necessarily different types) Cartan decompositions $\mathcal{L} = \mathcal{L}_0^j \oplus \mathcal{L}_1^j$, where $j = 1, \ldots, p$. We define*

$$\mathcal{L}_{k_1 k_2 \ldots k_p} := \bigcap_{j=1,2,\ldots,p} \mathcal{L}_{k_j}^j\,, \qquad k_j \in \mathbb{Z}_2\,. \tag{5.2}$$

Then, the vector space decomposition

$$\mathcal{L} = \bigoplus_{k_1 k_2 \ldots k_p \in \mathbb{Z}_2^p} \mathcal{L}_{k_1 k_2 \ldots k_p} \tag{5.3}$$

forms a $\mathbb{Z}_2^p-$grading of $\mathcal{L}$.

Proof. We give a proof by induction on the number p of the decompositions. If $p = 1$, then the statement is obvious. Assume the statement is true for $p-1$. Let $A \in \mathcal{L}_{k_1 k_2 \ldots k_p}$ and $B \in \mathcal{L}_{l_1 l_2 \ldots l_p}$ with $k_i\,, l_i \in \mathbb{Z}_2$ for $i = 1, \ldots, p$. Then it follows that $A \in \mathcal{L}_{k_1 k_2 \ldots k_{p-1}}$, $A \in \mathcal{L}_{k_p}$, $B \in \mathcal{L}_{l_1 l_2 \ldots l_{p-1}}$, and $B \in \mathcal{L}_{l_p}$. Since $\mathcal{L}$ is both $\mathbb{Z}_2^{p-1}-$graded and $\mathbb{Z}_2-$graded, we have

$$[A\,, B] \in \mathcal{L}_{(k_1+l_1)(k_2+l_2)\ldots(k_{p-1}+l_{p-1})} \qquad \text{and} \qquad [A\,, B] \in \mathcal{L}_{(k_p+l_p)}\,.$$

This means that

$$[A, B] \in \mathcal{L}_{(k_1+l_1)(k_2+l_2)\dots(k_{p-1}+l_{p-1})} \cap \mathcal{L}_{(k_p+l_p)} = \mathcal{L}_{(k_1+l_1)(k_2+l_2)\dots(k_p+l_p)} \,,$$

and, therefore,

$$[\mathcal{L}_{k_1 k_2 \dots k_p}, \mathcal{L}_{l_1 l_2 \dots l_p}] \subseteq \mathcal{L}_{(k_1+l_1)(k_2+l_2)\dots(k_p+l_p)} \,.$$

Hence, the vector space decomposition (5.3) is a $\mathbb{Z}_2^p$−grading of $\mathcal{L}$. □

Summarizing the content of this section, a Cartan decomposition of a Lie algebra defines a $\mathbb{Z}_2$−grading. A combination of p Cartan decompositions gives a $\mathbb{Z}_2^p$−grading.

5.1.2 Recursive decompositions induced by Lie algebra gradings

In this section, we establish a link between a recursive decomposition and a Lie algebra grading. This connection is crucial for the general framework for the recursive decompositions. To put a recursive decomposition in this framework, we give the following definition.

Definition 5.1.3. *A* recursive decomposition *of a Lie algebra $\mathcal{L}$ consists of two sequences of subspaces of $\mathcal{L}$,*

$$\mathcal{S}_0 := \{\mathcal{L}_0\,, \mathcal{L}_{00}\,, \mathcal{L}_{000}\,, \dots, \mathcal{L}_{0^p}\} \qquad \textit{and} \qquad \mathcal{S}_1 := \{\mathcal{L}_1\,, \mathcal{L}_{01}\,, \mathcal{L}_{001}\,, \dots, \mathcal{L}_{0^{p-1}1}\}\,,$$

both of length p, such that the decomposition

$$\mathcal{L}_{0^j} = \mathcal{L}_{0^{j+1}} \oplus \mathcal{L}_{0^j 1},$$

is a Cartan decomposition of $\mathcal{L}_{0^j}$ for each $j = 0, 1, \dots, p-1$, that is,

$$[\mathcal{L}_{0^{j+1}}\,, \mathcal{L}_{0^{j+1}}] \subseteq \mathcal{L}_{0^{j+1}}\,, \qquad [\mathcal{L}_{0^{j+1}}\,, \mathcal{L}_{0^j 1}] \subseteq \mathcal{L}_{0^j 1}\,, \qquad [\mathcal{L}_{0^j 1}\,, \mathcal{L}_{0^j 1}] \subseteq \mathcal{L}_{0^{j+1}}\,.$$

Here, we have set $\mathcal{L}_{0^0} := \mathcal{L}$ and $\mathcal{L}_{0^0 1} := \mathcal{L}_1$.

The following proposition states that a $\mathbb{Z}_2^p$−grading of a Lie algebra $\mathcal{L}$ induces a recursive decomposition of $\mathcal{L}$ of length p, in the sense of the above definition.

Proposition 5.1.2. *Consider a $\mathbb{Z}_2^p-$grading*

$$\mathcal{L} = \bigoplus_{j_1 j_2 \ldots j_p \in \mathbb{Z}_2^p} \mathcal{R}_{j_1, j_2, \ldots, j_p}$$

of $\mathcal{L}$. Then, the sequences $\mathcal{S}_0 := \{\mathcal{L}_{0^k}\}$ and $\mathcal{S}_1 := \{\mathcal{L}_{0^{k-1}1}\}$ defined by

$$\mathcal{L}_{0^k} := \bigoplus \mathcal{R}_{0^k, j_{k+1}, \ldots, j_p} \qquad \textit{and} \qquad \mathcal{L}_{0^{k-1}1} := \bigoplus \mathcal{R}_{0^{k-1}1, j_{k+1}, \ldots, j_p} \tag{5.4}$$

for $k = 1, \ldots, p$, yield a recursive decomposition of $\mathcal{L}$ of length p.

A recursive decomposition of a Lie algebra $\mathcal{L}$ induces a recursive decomposition of the connected Lie group $e^{\mathcal{L}}$ associated with $\mathcal{L}$ by a repeated application of the Cartan decomposition theorem using the Cartan pair $(\mathcal{L}_{0^{j+1}}, \mathcal{L}_{0^j 1})$ of $\mathcal{L}_{0^j}$, $j = 1, \ldots, p-1$, as discussed in section 2.3. In order to apply the Cartan decomposition theorem, we make the following remark.

Remark 5.1.1. *The construction of recursive decompositions from a $\mathbb{Z}_2^p-$grading does not guarantee the semisimplicity of the subalgebras $\mathcal{L}_{0^j}$, $j = 1, \ldots, p$. Therefore, the semisimplicity of each $\mathcal{L}_{0^j}$ has to be verified independently to apply the Cartan decomposition theorem. For example, the combination of type **AI** and **AII** decompositions of $\mathfrak{su}(4)$ in the standard basis gives the subalgebra $\mathcal{L}_{00} = \mathfrak{sp}(2)$. This is not semisimple, since it has an element commuting with the whole Lie algebra $\mathfrak{sp}(2)$. However, if the Lie subalgebra $\mathcal{L}_{0^j}$ is a direct sum of a semisimple Lie algebra and an Abelian ideal, the Cartan decomposition theorem can be extended in the same fashion as we extended decompositions of $\mathfrak{su}(n)$ to decompositions of $\mathfrak{u}(n)$ in section 2.2.2. In the general case, one can always apply the Levi decomposition theorem to write any Lie algebra as the sum of a semisimple subalgebra and a solvable ideal, as described in [9, §5.4].*

5.2 A scheme for recursive decompositions of $\mathbf{U}(n)$

We now show that the recursive decompositions of Khaneja and Glaser [16], D'Alessandro and Romano [11], and the new recursive decompositions can be obtained from an appropriate grading of $\mathfrak{u}(n)$. We begin with the special cases.

5.2.1 The Khaneja Glaser decomposition

In the following, we shall construct a $\mathbb{Z}_2^p$−grading of $\mathfrak{u}(2^N)$ from $p = 2N-1$ number of Cartan decompositions using the method presented in Proposition 5.1.1. Then we show that this grading induces the Khaneja Glaser decomposition. To start with, we consider the OED

$$\mathfrak{u}(2^N) = i\mathcal{J}_e \oplus i\mathcal{J}_o \,,$$

constructed by performing decompositions of type **AIII** on each qubit. Note that the Lie subalgebra $i\mathcal{J}_e$ is of dimension 2^{2N-1}. Therefore, there exists a unitary T in $\mathbf{U}(2^N)$ such that

$$\mathfrak{u}(2^N) = \mathcal{K} \oplus \mathcal{P} \,, \tag{5.5}$$

where

$$\mathcal{K} := i\,T^\dagger \mathcal{J}_e\, T = \mathrm{span}\{\mathbf{1}_2 \otimes A,\, \sigma_z \otimes B : A,\, B \in \mathfrak{u}(2^{N-1})\} \,,$$

and

$$\mathcal{P} := i\,T^\dagger \mathcal{J}_o\, T = \mathrm{span}\{\sigma_{x,y} \otimes C : C \in \mathfrak{u}(2^{N-1})\} \,.$$

Next, we consider the decompositions $\mathfrak{su}(2^N) = \mathcal{L}_0^j \oplus \mathcal{L}_1^j$, $j = 1, \ldots, 2N-1$, given as follows:

(1) The subspaces $\mathcal{L}_0^1$ and $\mathcal{L}_1^1$ are given by $\mathcal{L}_0^1 := \mathcal{K} - \mathrm{span}\{i\,\mathbf{1}_{2^N}\}$ and $\mathcal{L}_1^1 := \mathcal{P}$.

(2) The subspaces $\mathcal{L}_0^2$ and $\mathcal{L}_1^2$ are defined in the same way as $\mathcal{L}_0^1$ and $\mathcal{L}_1^1$, except for the fact that σ_x and σ_z are interchanged,[1] that is,

$$\mathcal{L}_0^2 = \mathrm{span}\{\mathbf{1}_2 \otimes A,\, \sigma_x \otimes B : A \in \mathfrak{su}(2^{N-1}),\, B \in \mathfrak{u}(2^{N-1})\} \,,$$

and

$$\mathcal{L}_1^2 = \mathrm{span}\{\sigma_{y,z} \otimes C : C \in \mathfrak{u}(2^{N-1})\} \,.$$

Indeed, this decomposition is conjugate to the standard type **AIII** decomposition. Such a conjugation has the form $A \longmapsto (S^\dagger \otimes \mathbf{1}_{2^{N-1}}) A (S \otimes \mathbf{1}_{2^{N-1}})$, where S is the 2×2 matrix diagonalizing σ_x.

[1] There is nothing special about σ_x here. One could have chosen σ_y instead.

(3) The subspaces $\mathcal{L}_0^3$ and $\mathcal{L}_1^3$ are defined analogously to $\mathcal{L}_0^1$ and $\mathcal{L}_1^1$, using the second position in place of the first, that is,

$$\mathcal{L}_0^3 = \mathrm{span}\{A \otimes \mathbf{1}_2 \otimes C,\, B \otimes \sigma_z \otimes D : A,\, B \in \mathfrak{u}(2),\, C,\, D \in \mathfrak{u}(2^{N-2}),\, \mathrm{tr}(A \otimes C) = 0\}\,,$$

and

$$\mathcal{L}_1^3 = \mathrm{span}\{E \otimes \sigma_{x,y} \otimes F : E \in \mathfrak{u}(2),\, F \in \mathfrak{u}(2^{N-2})\}\,.$$

This decomposition is again conjugate to the standard type **AIII** decomposition under the permutation exchanging the first and second positions.

(4) The subspaces $\mathcal{L}_0^4$ and $\mathcal{L}_1^4$ are defined in the same way as $\mathcal{L}_0^3$ and $\mathcal{L}_1^3$, except for the fact that σ_x and σ_z are interchanged.

(5) $\to (2N-1)$ Moving towards the last position, alternating decompositions as in (1) and decompositions as in (2).

In this fashion, we obtain $p = 2N - 1$ number of Cartan decompositions.[2] These decompositions define a $\mathbb{Z}_2^p$–grading, which induces a recursive decomposition of $\mathfrak{su}(2^N)$ according to Proposition 5.1.2. The associated subspaces of the pair of sequences giving the recursive decomposition are

$$\begin{aligned}
\mathcal{L}_0 &= \mathrm{span}\{\mathbf{1}_2 \otimes A,\, \sigma_z \otimes B : A \in \mathfrak{su}(2^{N-1}),\, B \in \mathfrak{u}(2^{N-1})\}\,,\\
\mathcal{L}_{00} &= \mathrm{span}\{\mathbf{1}_2 \otimes A : A \in \mathfrak{su}(2^{N-1})\}\,,\\
\mathcal{L}_{000} &= \mathrm{span}\{\mathbf{1}_2 \otimes \mathbf{1}_2 \otimes A,\, \mathbf{1}_2 \otimes \sigma_z \otimes B : A \in \mathfrak{su}(2^{N-2}),\, B \in \mathfrak{u}(2^{N-2})\}\,,\\
&\ \ \vdots\\
\mathcal{L}_{0^{2N-3}} &= \mathrm{span}\{\mathbf{1}_{2^{N-1}} \otimes A,\, \mathbf{1}_{2^{N-2}} \otimes \sigma_z \otimes B : A \in \mathfrak{su}(2),\, B \in \mathfrak{u}(2)\}\,,\\
\mathcal{L}_{0^{2N-2}} &= \mathrm{span}\{\mathbf{1}_{2^{N-1}} \otimes A : A \in \mathfrak{su}(2)\}\,,\\
\mathcal{L}_{0^{2N-1}} &= \mathrm{span}\{\mathbf{1}_{2^{N-1}} \otimes \sigma_z\}\,,
\end{aligned}$$

[2] We stop at $p = 2N - 1$ because $\mathcal{L}_{0^p}$ is $\{0\}$.

and

$$\mathcal{L}_1 = \text{span}\{\sigma_{x,y} \otimes C : C \in \mathfrak{u}(2^{N-1})\}\,,$$
$$\mathcal{L}_{01} = \text{span}\{\sigma_z \otimes B : B \in \mathfrak{u}(2^{N-1})\}\,,$$
$$\mathcal{L}_{001} = \text{span}\{\mathbf{1}_2 \otimes \sigma_{x,y} \otimes C : C \in \mathfrak{u}(2^{N-2})\}\,,$$
$$\vdots$$
$$\mathcal{L}_{0^{2N-4}1} = \text{span}\{\mathbf{1}_{2^{N-2}} \otimes \sigma_{x,y} \otimes C : C \in \mathfrak{u}(2)\}\,,$$
$$\mathcal{L}_{0^{2N-3}1} = \text{span}\{\mathbf{1}_{2^{N-2}} \otimes \sigma_z \otimes B : B \in \mathfrak{u}(2)\}\,,$$
$$\mathcal{L}_{0^{2N-2}1} = \text{span}\{\mathbf{1}_{2^{N-1}} \otimes \sigma_{x,y}\}\,.$$

This sequence of subspaces corresponds to the Khaneja Glaser decomposition. In particular, each Lie subalgebra $\mathcal{L}_{0^k}$, for all $k = 1, \ldots, 2N-1$, is either semisimple or a direct sum of two copies of a semisimple Lie algebra and a one-dimensional Abelian subalgebra of elements commuting with the whole Lie algebra. Thus, the Cartan decomposition theorem applies in each case.

5.2.2 The D'Alessandro Romano decomposition

We now construct a Lie algebra grading of $\mathfrak{u}(n_1 n_2)$, and, therefore, a recursive decomposition corresponding to the D'Alessandro Romano decomposition [11]. In particular, we consider three types of Cartan decompositions as follows:

(1) An OED with a type **AI** decomposition on each system so that

$$\mathcal{L}_0^1 = i\mathcal{I}_o \qquad \text{and} \qquad \mathcal{L}_1^1 = i\mathcal{I}_e\,,$$

where the subspaces $i\mathcal{I}_o$ and $i\mathcal{I}_e$ are defined in (2.26).

(2) An OED constructed using type **AIII** decompositions on each factor with indices $\{p_1, q_1\}$ and $\{p_2, q_2\}$ as in Theorem 4.2.2 so that

$$\mathcal{L}_0^2 = i\mathcal{J}_e \qquad \text{and} \qquad \mathcal{L}_1^2 = i\mathcal{J}_o\,,$$

where the subspaces $i\mathcal{J}_e$ and $i\mathcal{J}_o$ are defined in (4.15).

(3) A type **AIII** decompositions in the standard form given in (2.18) separating block diagonal and block antidiagonal matrices, that is,

$$\mathcal{L}_0^3 = \mathcal{K} \qquad \text{and} \qquad \mathcal{L}_1^3 = \mathcal{P}\,,$$

where $\mathcal{K}$ and $\mathcal{P}$ are constructed with indices p and q, where $p =: p_1p_2 + p_1q_2$ and $q := q_1p_2 + q_1q_2$. Here, $\{p_1, q_1\}$ and $\{p_2, q_2\}$ are the indices for the type **AIII** decompositions used for $\mathcal{L}_0^2$ and $\mathcal{L}_1^2$.

(4) The subspaces $\mathcal{L}_0^4$ and $\mathcal{L}_1^4$ are constructed analogously to $\mathcal{L}_0^2$ and $\mathcal{L}_1^2$, respectively, with different indices $\{p_1, q_1\}$ and $\{p_2, q_2\}$.

(5) The subspaces $\mathcal{L}_0^5$ and $\mathcal{L}_1^5$ are constructed analogously to $\mathcal{L}_0^3$ and $\mathcal{L}_1^3$, respectively.

The same construction holds for the Cartan pairs $(\mathcal{L}_0^6, \mathcal{L}_1^6)$ and $(\mathcal{L}_0^7, \mathcal{L}_1^7)$, and so on. Each time, the indices $\{p_1, q_1\}$ and $\{p_2, q_2\}$ are changed, differing from the previous ones in order to avoid repetition of decompositions. With these decompositions, one can define a grading and, therefore, a recursive decomposition. This decomposition corresponds to the D'Alessandro Romano decomposition.

5.2.3 Construction of new recursive decompositions

It is now clear that many recursive decompositions of $\mathfrak{u}(n)$ and, therefore, $\mathbf{U}(n)$ can be obtained. As an example, we construct a recursive decomposition of $\mathbf{U}(2^N)$ that allows the identification of the local and entangling parts in every unitary evolution on N qubits [8]. For this purpose, we begin with the CCD and take various conjugation of an OED of $\mathfrak{u}(2^N)$ to construct a grading and, therefore, a recursive decomposition. More specifically, we consider the following $2N$ decompositions on $\mathfrak{u}(2^N)$:

(1) A CCD so that

$$\mathcal{L}_0^1 = i\mathcal{I}_o^N \quad \text{and} \quad \mathcal{L}_1^1 = i\mathcal{I}_e^N\,, \tag{5.6}$$

where the subspaces $\mathcal{I}_o^N$ and $\mathcal{I}_e^N$ are defined in (3.20).

(2) An OED obtained by performing decompositions of type **AII** on all qubits except the one on the Nth qubit, which is of type **AI** and of the form

$$\mathfrak{u}(2) = \text{span}\{i\sigma_z\} \oplus \text{span}\{i\sigma_x\, , i\sigma_y\, , i\, \mathbf{1}_2\}\, .$$

Then, the subspaces $\mathcal{L}_0^2$ and $\mathcal{L}_1^2$ are given by

$$\mathcal{L}_0^2 = \text{span}\{i\mathcal{I}_e^{N-1} \otimes \sigma_z,\ i\mathcal{I}_o^{N-1} \otimes \{\sigma_x, \sigma_y, \mathbf{1}_2\}\}\, ,$$

and

$$\mathcal{L}_1^2 = \text{span}\{i\mathcal{I}_o^{N-1} \otimes \sigma_z,\ i\mathcal{I}_e^{N-1} \otimes \{\sigma_x, \sigma_y, \mathbf{1}_2\}\}\, .$$

(3) The subspaces $\mathcal{L}_0^3$ and $\mathcal{L}_1^3$ are defined in the same way as in (2) but σ_z and σ_x are interchanged,[3] that is,

$$\mathcal{L}_0^3 = \text{span}\{i\mathcal{I}_e^{N-1} \otimes \sigma_x,\ i\mathcal{I}_o^{N-1} \otimes \{\sigma_y, \sigma_z, \mathbf{1}_2\}\}\, ,$$

and

$$\mathcal{L}_1^3 = \text{span}\{i\mathcal{I}_o^{N-1} \otimes \sigma_x,\ i\mathcal{I}_e^{N-1} \otimes \{\sigma_y, \sigma_z, \mathbf{1}_2\}\}\, .$$

(4) The subspaces $\mathcal{L}_0^4$ and $\mathcal{L}_1^4$ are defined in the same way as in (2) but with the Nth position replaced by the $(N-1)$th position.

(5) Same as in (4) with σ_x and σ_z interchanged.

(6) $\rightarrow$ $(2N-1)$ Moving towards the first position, alternating decompositions as in (2) and decompositions as in (3).

(2N) Same as in (2) with the first position replacing the Nth position.

Example 5.2.1. *For $N = 3$, denoting any possible Pauli matrix by σ, we obtain the following subspaces:*

$$\mathcal{L}_0^1 = \text{span}\{i\sigma \otimes \mathbf{1}_2 \otimes \mathbf{1}_2\, , \, i\, \mathbf{1}_2 \otimes \sigma \otimes \mathbf{1}_2\, , \, i\, \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma\, , \, i\sigma \otimes \sigma \otimes \sigma\}\, ,$$

$$\mathcal{L}_1^1 = \text{span}\{i\sigma \otimes \sigma \otimes \mathbf{1}_2\, , \, i\, \mathbf{1}_2 \otimes \sigma \otimes \sigma\, , \, i\sigma \otimes \mathbf{1}_2 \otimes \sigma\, , \, i\, \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \mathbf{1}_2\}\, ,$$

[3] One can use σ_y instead of σ_x.

$$\mathcal{L}_0^2 = \text{span}\{i\sigma\otimes \boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\,,\, i\,\boldsymbol{1}_2\otimes\sigma\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\,,\, i\sigma\otimes\sigma\otimes\sigma_z\,,\, i\,\boldsymbol{1}_2\otimes\boldsymbol{1}_2\otimes\sigma_z\}\,,$$

$$\mathcal{L}_1^2 = \text{span}\{i\sigma\otimes\sigma\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\,,\, i\,\boldsymbol{1}_2\otimes\boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\,,\, i\sigma\otimes\boldsymbol{1}_2\otimes\sigma_z\,,\, i\,\boldsymbol{1}_2\otimes\sigma\otimes\sigma_z\}\,,$$

$$\mathcal{L}_0^3 = \text{span}\{i\sigma\otimes \boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\,,\, i\,\boldsymbol{1}_2\otimes\sigma\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\,,\, i\sigma\otimes\sigma\otimes\sigma_x\,,\, i\,\boldsymbol{1}_2\otimes\boldsymbol{1}_2\otimes\sigma_x\}\,,$$

$$\mathcal{L}_1^3 = \text{span}\{i\sigma\otimes\sigma\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\,,\, i\,\boldsymbol{1}_2\otimes\boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\,,\, i\sigma\otimes\boldsymbol{1}_2\otimes\sigma_x\,,\, i\,\boldsymbol{1}_2\otimes\sigma\otimes\sigma_x\}\,,$$

$$\mathcal{L}_0^4 = \text{span}\{i\sigma\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\boldsymbol{1}_2\,,\, i\,\boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\sigma\,,\, i\sigma\otimes\sigma_z\otimes\sigma\,,\, i\,\boldsymbol{1}_2\otimes\sigma_z\otimes\boldsymbol{1}_2\}\,,$$

$$\mathcal{L}_1^4 = \text{span}\{i\sigma\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\sigma\,,\, i\,\boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\boldsymbol{1}_2\,,\, i\sigma\otimes\sigma_z\otimes\boldsymbol{1}_2\,,\, i\,\boldsymbol{1}_2\otimes\sigma_z\otimes\sigma\}\,,$$

$$\mathcal{L}_0^5 = \text{span}\{i\sigma\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\otimes\boldsymbol{1}_2\,,\, i\,\boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\otimes\sigma\,,\, i\sigma\otimes\sigma_x\otimes\sigma\,,\, i\,\boldsymbol{1}_2\otimes\sigma_x\otimes\boldsymbol{1}_2\}\,,$$

$$\mathcal{L}_1^5 = \text{span}\{i\sigma\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\otimes\sigma\,,\, i\,\boldsymbol{1}_2\otimes\{\boldsymbol{1}_2,\sigma_y,\sigma_z\}\otimes\boldsymbol{1}_2\,,\, i\sigma\otimes\sigma_x\otimes\boldsymbol{1}_2\,,\, i\,\boldsymbol{1}_2\otimes\sigma_x\otimes\sigma\}\,,$$

$$\mathcal{L}_0^6 = \text{span}\{i\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\sigma\otimes\boldsymbol{1}_2\,,\, i\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\boldsymbol{1}_2\otimes\sigma\,,\, i\sigma_z\otimes\sigma\otimes\sigma\,,\, i\sigma_z\otimes\boldsymbol{1}_2\otimes\boldsymbol{1}_2\}\,,$$

$$\mathcal{L}_1^6 = \text{span}\{i\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\sigma\otimes\sigma\,,\, i\{\boldsymbol{1}_2,\sigma_x,\sigma_y\}\otimes\boldsymbol{1}_2\otimes\boldsymbol{1}_2\,,\, i\sigma_z\otimes\sigma\otimes\boldsymbol{1}_2\,,\, i\sigma_z\otimes\boldsymbol{1}_2\otimes\sigma\}.$$

In the general case, with the decompositions $\mathfrak{u}(2^N) := \mathcal{L}_0^j \oplus \mathcal{L}_1^j$, $j = 1,\dots,2N$, one can construct a $\mathbb{Z}_2^{2N}-$grading and obtain a recursive decomposition. The subspaces of the sequences associated to the latter are, for $k = 0,\dots,N-1$,[4]

$$\begin{aligned}
\mathcal{L}_{0^{2k+1}} &= \text{span}\{i\mathcal{I}_o^{N-k}\otimes\mathbf{1}_{2^k}\}\,,\\
\mathcal{L}_{0^{2k}1} &= \text{span}\{i\mathcal{I}_e^{N-k}\otimes\sigma_z\otimes\mathbf{1}_{2^{k-1}}\}\,,\\
\mathcal{L}_{0^{2k+2}} &= \text{span}\{i\mathcal{I}_o^{N-k-1}\otimes\mathbf{1}_{2^{k+1}}\,,\, i\mathcal{I}_e^{N-k-1}\otimes\sigma_z\otimes\mathbf{1}_{2^k}\}\,,\\
\mathcal{L}_{0^{2k+1}1} &= \text{span}\{i\mathcal{I}_e^{N-k-1}\otimes\{\sigma_x,\sigma_y\}\otimes\mathbf{1}_{2^k}\}\,.
\end{aligned} \tag{5.7}$$

To apply the Cartan decomposition theorem, we make the following two remarks.

Remark 5.2.1. *The Lie subalgebra $\mathcal{L}_{0^{2k+1}} = \text{span}\{i\mathcal{I}_o^{N-k}\otimes\boldsymbol{1}_{2^k}\}$, $k = 1,\dots,N-1$, is isomorphic to $i\mathcal{I}_o^{N-k}$. Furthermore, $i\mathcal{I}_o^{N-k}$ is conjugate to $\mathfrak{so}(2^{N-k})$ or $\mathfrak{sp}(2^{N-k-1})$ according to whether $N-k$ is even or odd, respectively. Thus, in every case, $\mathcal{L}_{0^{2k+1}}$ is semisimple.*

Remark 5.2.2. *The Lie subalgebra $\mathcal{L}_{0^{2k}} = \text{span}\{i\mathcal{I}_o^{N-k}\otimes\boldsymbol{1}_{2^k},\, i\mathcal{I}_e^{N-k}\otimes\sigma_z\otimes\boldsymbol{1}_{2^{k-1}}\}$ is isomorphic to $\mathfrak{u}(2^{N-k})$, and the isomorphism is given by the map*

$$A\otimes\boldsymbol{1}_{2^k}\longmapsto A \qquad \textit{and} \qquad B\otimes\sigma_z\otimes\boldsymbol{1}_{2^{k-1}}\longmapsto B\,, \tag{5.8}$$

[4]If the factors on the left occupy all the N positions in the tensor products, the factors on the right do not appear.

where $A \in i\mathcal{I}_o^{N-k}$ and $B \in i\mathcal{I}_e^{N-k}$. This is the direct sum of a semisimple Lie algebra and a one dimensional subspace commuting with the elements of the Lie algebra.

In conclusion, the Cartan decomposition theorem applies in all cases. Therefore, the subspaces in (5.7) define a recursive decomposition for the unitary Lie group $\mathbf{U}(2^N)$. It is important to identify the Cartan subalgebras to obtain the KAK decomposition of the corresponding Lie group. In order to do that, we consider the commuting set

$$\mathcal{A} := \{\sigma_x \otimes \sigma_x\,, \sigma_y \otimes \sigma_y\,, \sigma_z \otimes \sigma_z\,, \mathbf{1}_2 \otimes \mathbf{1}_2\}\,.$$

Let us denote by $\mathcal{A}_l$ the set obtained by the tensor products of l elements of $\mathcal{A}$, that is, $\mathcal{A}_l := \mathcal{A} \otimes \mathcal{A} \otimes \cdots \otimes \mathcal{A}$, l times. Using induction on l along with the formula

$$[A \otimes B\,, C \otimes D] = [A\,, C] \otimes (BD) + (CA) \otimes [B\,, D]\,, \tag{5.9}$$

it is easy to see that $\mathcal{A}_l$ is also a commuting set.

Remark 5.2.3. *The decomposition*

$$\mathcal{L}_{0^{2k}} = \mathcal{L}_{0^{2k+1}} \oplus \mathcal{L}_{0^{2k}1}\,,$$

*with $k = 0, \ldots, N-1$, (modulo the isomorphism in (5.8)) is a decomposition of type **AI** or **AII** of $\mathfrak{u}(2^{N-k})$, according to whether $N-k$ is even or odd, respectively. If $N-k$ is even, then this decomposition is of type **AI** with rank 2^{N-k}. A maximal Abelian subalgebra can be given by*

$$\mathcal{A}_{\boldsymbol{AI}} := \operatorname{span}\{i\mathcal{A}_{\frac{N-k}{2}} \otimes \sigma_z \otimes \boldsymbol{1}_{2^{k-1}}\}\,,$$

*which indeed has dimension $4^{\frac{N-k}{2}} = 2^{N-k}$. On the other hand, if $N-k$ is odd, then the decomposition is of type **AII** with rank 2^{N-k-1}. A Cartan subalgebra in this case is given by*

$$\mathcal{A}_{\boldsymbol{AII}} := \operatorname{span}\{i\mathcal{A}_{\frac{N-k-1}{2}} \otimes \boldsymbol{1}_2 \otimes \sigma_z \otimes \boldsymbol{1}_{2^{k-1}}\}\,.$$

Remark 5.2.4. *The decomposition*

$$\mathcal{L}_{0^{2k+1}} = \mathcal{L}_{0^{2k+2}} \oplus \mathcal{L}_{0^{2k+1}1}\,,$$

*with $k = 0, \ldots, N-1$, is a decomposition of $\mathfrak{so}(2^{N-k})$ or $\mathfrak{sp}(2^{N-k-1})$ according to whether $N-k$ is even or odd. If $N-k$ is even, then this is a decomposition of $\mathfrak{so}(2^{N-k})$ of type **DIII** which has rank 2^{N-k-2}. A Cartan subalgebra can be taken equal to*

$$\mathcal{A}_{\boldsymbol{DIII}} := \operatorname{span}\{i\mathcal{A}_{\frac{N-k-2}{2}} \otimes \boldsymbol{1}_2 \otimes \sigma_x \otimes \boldsymbol{1}_{2^k}\}\,.$$

*Otherwise, it is a decomposition of type **CI** and the associated rank is 2^{N-k-1}. In this case, a Cartan subalgebra is given by*

$$\mathcal{A}_{\boldsymbol{CI}} := \operatorname{span}\{i\mathcal{A}_{\frac{N-k-1}{2}} \otimes \sigma_x \otimes \boldsymbol{1}_{2^k}\}\,.$$

5.3 Computational issues and examples

In this section, we illustrate by an example the Lie group decompositions induced by the recursive decompositions described in the previous section. In particular, we show how the generalized SWAP operator $X_{sw} \in \mathbf{U}(8)$ can be decomposed into the product of elementary factors. The action of X_{sw} on the states of a composite system of three qubits is defined by

$$X_{sw} : |i\rangle \otimes |j\rangle \otimes |k\rangle \longmapsto |j\rangle \otimes |k\rangle \otimes |i\rangle\,,$$

where each of $|i\rangle$, $|j\rangle$ and $|k\rangle$ belong to the Hilbert spaces of a two level quantum system spanned by the orthonormal basis $\{|0\rangle\,, |1\rangle\}$. In fact, X_{sw} is the cyclic right shift operator acting on three qubits. The matrix representation of this operator is given by

$$X_{sw} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let us first factor X_{sw} using the decomposition of Khaneja and Glaser. According to section 5.2.1, this decomposition is given by the sequences

$$\mathcal{S}_0 = \{\mathcal{L}_0,\ \mathcal{L}_{0^2},\ \mathcal{L}_{0^3},\ \mathcal{L}_{0^4},\ \mathcal{L}_{0^5}\} \qquad \text{and} \qquad \mathcal{S}_1 = \{\mathcal{L}_1,\ \mathcal{L}_{01},\ \mathcal{L}_{0^21},\ \mathcal{L}_{0^31},\ \mathcal{L}_{0^41}\}\,.$$

The first step is to compute the KAK decomposition of X_{sw} induced by the Cartan pair $(\mathcal{L}_0\,,\mathcal{L}_1)$. Using the Algorithm 1 provided in section 2.3.1, we obtain the decomposition

$$X_{sw} = \begin{pmatrix} K_{11} & 0 \\ 0 & K_{12} \end{pmatrix} \begin{pmatrix} D_1 & D_2 \\ D_2 & D_1 \end{pmatrix} \begin{pmatrix} K_{21} & 0 \\ 0 & K_{22} \end{pmatrix},$$

where

$$K_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad K_{12} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad K_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$K_{22} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The next step is to obtain the decomposition

$$\begin{pmatrix} K_{j1} & 0 \\ 0 & K_{j2} \end{pmatrix} = \begin{pmatrix} U_{j1} & 0 \\ 0 & U_{j1} \end{pmatrix} \begin{pmatrix} D_{jj} & 0 \\ 0 & D_{jj}^{-1} \end{pmatrix} \begin{pmatrix} U_{j2} & 0 \\ 0 & U_{j2} \end{pmatrix},$$

$j = 1, 2$, induced by the Cartan pair $(\mathcal{L}_{0^2}, \mathcal{L}_{01})$, where $\mathcal{L}_{0^2}$ is the subspace $\mathbf{1}_2 \otimes \mathfrak{su}(4)$. Using the Algorithm 2 given in section 2.3.1, we obtain the matrices

$$U_{11} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ i & 0 & 0 & -1 \\ 0 & i & 1 & 0 \end{pmatrix}, \qquad U_{12} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

$$U_{21} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 & 0 & -1 \\ 1 & 0 & 0 & -i \\ 0 & 1 & -i & 0 \\ 0 & -i & 1 & 0 \end{pmatrix}, \quad U_{22} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \end{pmatrix},$$

and

$$D_{jj} = \begin{pmatrix} i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The important observation is that $U_{jk} \in \mathbf{SU}(4)$. Therefore, we repeat the first two steps with the Cartan pairs $(\mathcal{L}_{0^3}, \mathcal{L}_{0^2 1})$ and $(\mathcal{L}_{0^4}, \mathcal{L}_{0^3 1})$ to decompose each U_{jk}. Finally, writing all the factors as exponentials, we obtain the desired decomposition

$$\begin{aligned} X_{sw} = {} & e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_z} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_z} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \mathbf{1}_2} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_x} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_z} \\ & \times e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_x} e^{\frac{i\pi}{4} \sigma_z \otimes \mathbf{1}_2 \otimes \sigma_z} e^{\frac{i\pi}{4} \sigma_z \otimes \sigma_z \otimes \sigma_z} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \mathbf{1}_2} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \sigma_z} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \mathbf{1}_2} \\ & \times e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_z} e^{\frac{3i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{i\pi}{4} \sigma_x \otimes \sigma_z \otimes \mathbf{1}_2} e^{\frac{-i\pi}{4} \sigma_x \otimes \mathbf{1}_2 \otimes \sigma_z} e^{\frac{i\pi}{2} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \mathbf{1}_2} \\ & \times e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_z} e^{\frac{3i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \mathbf{1}_2} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \sigma_z} e^{\frac{i\pi}{4} \sigma_z \otimes \mathbf{1}_2 \otimes \sigma_z} e^{\frac{i\pi}{4} \sigma_z \otimes \sigma_z \otimes \sigma_z} \\ & \times e^{\frac{i\pi}{2} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_z} e^{\frac{i\pi}{2} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_z} e^{\frac{i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \mathbf{1}_2} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_x \otimes \sigma_z} e^{\frac{i\pi}{2} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \mathbf{1}_2} \\ & \times e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_z} e^{\frac{-i\pi}{4} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y}. \end{aligned} \tag{5.10}$$

The D'Alessandro Romano decomposition of X_{sw} is computed in [11] as

$$\begin{aligned} X_{sw} = {} & e^{\frac{7i\pi}{8} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{-5i\pi}{8} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_y} e^{\frac{-i\pi}{8} \sigma_z \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{-i\pi}{8} \sigma_z \otimes \sigma_z \otimes \sigma_y} e^{\frac{5i\pi}{8} \sigma_y \otimes \sigma_x \otimes \mathbf{1}_2} e^{\frac{i\pi}{8} \sigma_y \otimes \sigma_x \otimes \sigma_z} \\ & \times e^{\frac{-3i\pi}{8} \sigma_x \otimes \sigma_y \otimes \mathbf{1}_2} e^{\frac{-3i\pi}{8} \sigma_x \otimes \sigma_y \otimes \sigma_z} e^{\frac{3i\pi}{8} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{-3i\pi}{8} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_y} e^{\frac{-3i\pi}{8} \sigma_z \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{3i\pi}{8} \sigma_z \otimes \sigma_z \otimes \sigma_y} \\ & \times e^{\frac{3i\pi}{4} \mathbf{1}_2 \otimes \sigma_y \otimes \mathbf{1}_2} e^{\frac{-i\pi}{2} \sigma_z \otimes \sigma_y \otimes \mathbf{1}_2} e^{\frac{-i\pi}{4} \sigma_z \otimes \sigma_y \otimes \sigma_z} e^{\frac{3i\pi}{8} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{3i\pi}{8} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_y} e^{\frac{-3i\pi}{8} \sigma_z \otimes \mathbf{1}_2 \otimes \sigma_y} \\ & \times e^{\frac{-3i\pi}{8} \sigma_z \otimes \sigma_z \otimes \sigma_y} e^{\frac{i\pi}{8} \sigma_y \otimes \sigma_x \otimes \mathbf{1}_2} e^{\frac{-i\pi}{8} \sigma_y \otimes \sigma_x \otimes \sigma_z} e^{\frac{-i\pi}{8} \sigma_x \otimes \sigma_y \otimes \mathbf{1}_2} e^{\frac{i\pi}{8} \sigma_x \otimes \sigma_y \otimes \sigma_z} e^{\frac{3i\pi}{8} \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \sigma_y} \\ & \times e^{\frac{-3i\pi}{8} \mathbf{1}_2 \otimes \sigma_z \otimes \sigma_y} e^{\frac{3i\pi}{8} \sigma_z \otimes \mathbf{1}_2 \otimes \sigma_y} e^{\frac{-3i\pi}{8} \sigma_z \otimes \sigma_z \otimes \sigma_y}. \end{aligned} \tag{5.11}$$

Finally, we factor X_{sw} using the decomposition proposed in section 5.2.3. In this case, modulo isomorphism, the sequences defining the recursive decomposition for $\mathfrak{u}(8)$ are given by

$$\begin{aligned} \mathcal{S}_0 =& \{\mathfrak{sp}(4),\, \mathfrak{u}(4),\, \mathfrak{so}(4),\, \mathfrak{u}(2),\, \mathfrak{sp}(1),\, \mathfrak{u}(1)\}\,, \\ \mathcal{S}_1 =& \{\mathfrak{sp}(4)^\perp,\, \mathfrak{u}(4)^\perp,\, \mathfrak{so}(4)^\perp,\, \mathfrak{u}(2)^\perp,\, \mathfrak{sp}(1)^\perp,\, \mathfrak{u}(1)^\perp\}\,. \end{aligned} \tag{5.12}$$

We do not have direct algorithms to compute the KAK decompositions in the original coordinates of the decomposition. However, with an orthogonal change of basis matrix, we can transform the problem into the standard coordinates, compute the decomposition using the existing algorithms, and then we transform the problem back to its original coordinates. According to [4], the associated change of basis matrix is given by

$$F = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}.$$

This matrix is sometimes called a *finagler*. After this change of coordinates, X_{sw} takes the form $\tilde{X}_{sw} = F^T X_{sw} F$, with $\tilde{X}_{sw} = \mathbf{1}_2 \otimes X'_{sw}$, where

$$X'_{sw} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

To perform the decomposition, we follow the sequence of subspaces in (5.12). It can be verified that $\tilde{X}_{sw}$ is symplectic, that is, $\tilde{X}_{sw} \in \mathbf{Sp}(4)$. Moreover, $\tilde{X}_{sw}$ is contained in the image of $\mathbf{U}(4)$ embedded into $\mathbf{Sp}(4)$,[5] and represented by X'_{sw} in $\mathbf{U}(4)$. Indeed, X'_{sw} is not only unitary but

[5] An embedding of $\mathbf{U}(n)$ into $\mathbf{Sp}(n)$ or $\mathbf{SO}(2n)$ is given by the map $U + iV \mapsto \left(\begin{smallmatrix} U & V \\ -V & U \end{smallmatrix}\right)$, where U and V are real matrices.

also orthogonal, that is, $X'_{sw} \in \mathbf{SO}(4)$. Hence, the decompositions induced by the first three Cartan pairs $(\mathfrak{sp}(4), \mathfrak{sp}(4)^{\perp})$, $(\mathfrak{u}(4), \mathfrak{u}(4)^{\perp})$, and $(\mathfrak{so}(4), \mathfrak{so}(4)^{\perp})$ are trivial. Therefore, we turn our attention to decompose $X'_{sw} = K'_1 A' K'_2$ induced by the Cartan pair $(\mathfrak{u}(2), \mathfrak{u}(2)^{\perp})$, where K'_1 and K'_2 are contained the image of $\mathbf{U}(2)$ embedding into $\mathbf{SO}(4)$, and A' is the exponential of an element of the suitable Cartan subalgebra, i.e., $A' = \operatorname{diag}\left(E, E^{-1}\right)$. Let us partition X'_{sw} into 2×2 blocks, i.e.,

$$X'_{sw} = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix} .$$

Choose $K'_2 = \mathbf{1}_4$. Then, X'_{sw} decomposes as

$$X'_{sw} = \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \begin{pmatrix} E & 0 \\ 0 & E^{-1} \end{pmatrix} , \tag{5.13}$$

where $A + iB \in \mathbf{U}(2)$. This equation is equivalent to two matrix equations

$$X_{11} - iX_{21} = (A + iB)E \qquad \text{and} \qquad X_{22} + iX_{12} = (A + iB)E^{-1} .$$

Since $A + iB$ is unitary, we have

$$E^2 = (X_{22} + iX_{12})^{-1}(X_{11} - iX_{21}) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} .$$

Once E is determined from the last equation, we obtain A and B using (5.13) so that

$$K'_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad A' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} . \tag{5.14}$$

In the next step, we decompose K'_1 using the Cartan pairs $(\mathfrak{sp}(1), \mathfrak{sp}(1)^{\perp})$ and $(\mathfrak{u}(1), \mathfrak{u}(1)^{\perp})$. Carrying out the calculations, we obtain

$$\tilde{X}_{sw} = \tilde{L}_1 \tilde{L}_2 \tilde{L}_3 \tilde{L}_4 , \tag{5.15}$$

where $\tilde{L}_1 = \frac{1}{\sqrt{2}}(\mathbf{1}_8 - i\mathbf{1}_2 \otimes \sigma_y \otimes \mathbf{1}_2)$, $\tilde{L}_2 = \frac{1}{\sqrt{2}}(\mathbf{1}_8 + i\mathbf{1}_2 \otimes \sigma_y \otimes \sigma_z)$, $\tilde{L}_3 = \frac{1}{\sqrt{2}}(\mathbf{1}_8 + i\mathbf{1}_4 \otimes \sigma_y)$, and $\tilde{L}_4 = \mathbf{1}_2 \otimes A'$. We map $\tilde{X}_{sw}$ in (5.15) back to the tensor product basis to write

$$X_{sw} = L_1 L_2 L_3 L_4, \tag{5.16}$$

where $L_k = F\tilde{L}_k F^T$, $k = 1, \ldots, 4$. Here, F is the finagler defined in (5.13). Finally, we write all the factors in (5.16) as exponentials of matrices in the tensor product basis to obtain

$$X_{sw} = e^{\frac{-i\pi}{4}\sigma_y\otimes\sigma_z\otimes\sigma_x}\, e^{\frac{i\pi}{4}\sigma_x\otimes\sigma_z\otimes\sigma_y}\, e^{\frac{i\pi}{4}\sigma_y\otimes\sigma_x\otimes\sigma_z}\, e^{\frac{-i\pi}{4}\sigma_x\otimes\sigma_y\otimes\sigma_z}\,. \tag{5.17}$$

Thus, we obtained three different decompositions (5.10), (5.11), and (5.17) for the generalized SWAP operator X_{sw}. To perform the given task, the Khaneja Glaser decomposition (5.10) uses 32 transformations, two of which are equal to $e^{\frac{i\pi}{4}\sigma_z\otimes\sigma_z\otimes\sigma_z}$, creating three-body interaction. In particular, using the formulas given in [16], it is possible to decompose $e^{\frac{i\pi}{4}\sigma_z\otimes\sigma_z\otimes\sigma_z}$ further so that we obtain a decomposition of X_{sw} into evolutions acting on a single and two qubits. The D'Alessandro Romano decomposition (5.11) uses 27 transformations to perform the task. In particular, using another basis, this decomposition displays the local and entangling parts of X_{sw} on a bipartite system composed of subsystems of dimensions 2 and 4 [11]. On the other hand, the recursive decomposition that we proposed in section 5.2.3 performs the given task with four transformations, each of which creates three-body interaction.

CHAPTER 6. Concluding Remarks

The framework presented in the previous chapter can be applied to any Lie algebra $\mathcal{L}$ once one has a certain number of Cartan decompositions of $\mathcal{L}$. The OED type of decompositions are a very useful tool to construct a great wealth of possible Cartan decompositions for $\mathfrak{u}(n)$. This abundance of decompositions is very important in the construction of recursive decompositions. A similar strategy can be used for other Lie algebras. For example, we can construct a type **BDI** decomposition for $\mathfrak{so}(n_1n_2)$ starting from a tensor product basis of $\mathfrak{so}(n_1n_2)$ as follows. Let us denote by σ_j and S_j, $j=1,2$, $n_j\times n_j$ skew-symmetric and symmetric matrices respectively. A basis of $\mathfrak{so}(n_1n_2)$ is given by the tensor products of form

$$F := F_1 \otimes F_2\,,$$

where $F_j=\sigma_j$ or $F_j=S_j$. Let us fix two positive integers p_j and q_j with $p_j+q_j=n_j$. Accordingly, we partition each σ_j or S_j in F into block diagonal matrices, which we denote by the superscript D (i.e., $\sigma_j^D\,, S_j^D$), and block antidiagonal matrices, which we denote by the superscript A (i.e., $\sigma_j^A\,, S_j^A$). Therefore, a decomposition of $\mathfrak{so}(n_1n_2)$ is given by

$$\mathfrak{so}(n_1n_2) := \mathcal{K}\oplus\mathcal{P}\,, \tag{6.1}$$

where

$$\mathcal{K} = \operatorname{span}\{\sigma_1^D\otimes S_2^D,\, S_1^D\otimes\sigma_2^D,\, \sigma_1^A\otimes S_2^A,\, S_1^A\otimes\sigma_2^A\}\,,$$

and

$$\mathcal{P} = \operatorname{span}\{\sigma_1^D\otimes S_2^A,\, S_1^A\otimes\sigma_2^D,\, \sigma_1^D\otimes S_2^A,\, S_1^D\otimes\sigma_2^A\}\,.$$

Using a similarity transformation, it was shown in [11], the above decomposition of $\mathfrak{so}(n_1n_2)$ is a Cartan decomposition of type **BDI** with indices $p=p_1p_2+q_1q_2$ and $q=p_1q_2+p_2q_1$. Furthermore, we note that this construction can be extended to decompositions of $so(n_1 n_2 \cdots n_N)$ with additional notational complexity.

In conclusion, Lie algebra gradings, Cartan decompositions, and recursive Lie group decompositions are interrelated concepts. From a set of p Cartan decompositions, we can naturally obtain a $\mathbb{Z}_2^p-$grading of a Lie algebra and a recursive decomposition of the associated Lie group. Known procedures for the recursive decomposition of the unitary group of quantum evolutions are special cases of this general scheme. In this dissertation, we enhanced the previous work on Lie group decompositions. When dealing with multipartite quantum systems, it is convenient if the decompositions used in the procedure are given in terms of tensor products of basis elements of the Lie algebras associated to the single subsystems. This is the case for the CCD on N qubits and the OED in its various forms. In this way, the factors of each element of the group are exponentials of tensor products, and one can identify local operations as well as multi-body interactions. In this context, we provided an important mathematical basis for further work in the area.

We have given a new recursive decomposition applying the general procedure, along with an example of computation. For this example, formulas (5.10), (5.11), and (5.17) give different decompositions. In general, different recursive decompositions of $\mathfrak{u}(n)$ will result in different factorizations of $\mathbf{U}(n)$. The framework presented here gives a virtually unbounded number of alternatives to decompose $\mathbf{U}(n)$ and parametrize quantum evolutions. Finally, we note that this framework is very general but uses only one type of decompositions of Lie groups, the Cartan decompositions. It is possible that different types of decompositions such as Bruhat and Iwasawa [17] could be used to obtain different schemes.

BIBLIOGRAPHY

[1] Albertini F and D'Alessandro D 2006 Lagrangian formulation and geometric control of switching LC electrical networks *Proc. 45th IEEE CDC* San Diego CA

[2] Ashok D 2003 *Lectures on Quantum Mechanics* (New Delhi: Hindustan Book Agency)

[3] Bullock S S 2004 Note on the Khaneja Glaser decomposition *Quantum Inf. Comput.* **4** 396

[4] Bullock S S and Brennen G K 2004 Canonical decompositions of n-qubit quantum computations and concurrence *J. Math. Phys.* **45** 2447

[5] Bullock S S, Brennen G K and O'Leary D P 2005 Time reversal and n-qubit canonical decompositions *J. Math. Phys.* **46** 062104

[6] Cartan E 1926 Sur une class remarkable d'espaces de Riemann *Bull. Suc. Math. France* **54** 214

[7] Cartan E 1927 Sur une class remarkable d'espaces de Riemann *Bull. Suc. Math. France* **55** 114

[8] Dağlı M, D'Alessandro D and Smith J D H 2008 A general framework for recursive decompositions of unitary quantum evolutions *J. Phys. A: Math. Theor.* **41** 15302

[9] D'Alessandro D 2008 *Introduction to Quantum Control and Dynamics* (Florida: Chapman & Hall/CRC)

[10] D'Alessandro D and Albertini F 2007 Quantum symmetries and Cartan decompositions in arbitrary dimensions *J. Phys. A: Math. Theor.* **40** 2439

[11] D'Alessandro D and Romano R 2006 Decompositions of unitary evolutions and entanglement dynamics of bipartite quantum systems *J. Math. Phys.* **47** 082109

[12] De Graaf W A 2000 *Lie Algebras: Theory and Algorithms* (Amsterdam: North-Holland)

[13] Helgason S 1978 *Differential Geometry, Lie groups and Symmetric Spaces* (New York: Academic Press)

[14] Hill S and Wootters W K 1997 Entanglement of a pair of quantum bits *Phys. Rev. Lett.* **78** 5022

[15] Horn R A and Johnson C R 1994 Topics in Matrix Analysis (Cambridge: Cambridge University Press)

[16] Khaneja N and Glaser S J 2001 Cartan decompositions of $\mathbf{SU}(2^n)$ and control of spin systems *Chem. Phys.* **267** 11

[17] Knapp A W 2002 *Lie Groups Beyond an Introduction* (Boston: Birkhäuser)

[18] McCrimmon K 2004 *A Taste of Jordan Algebras* (New York: Springer-Verlag)

[19] Nakajima Y, Kawano Y and Sekigawa H 2005 A new algorithm for producing quantum circuits using KAK decompositions *Preprint* quant-ph/0509196v4

[20] Nilesen M A and Chuang I L 2000 *Quantum Information and Quantum Computation* (Cambridge: Cambridge University Press)

[21] Romano R and D'Alessandro D 2006 Incoherent control and entanglement for two-dimensional coupled systems *Phys. Rev. A* **73** 022323

[22] Rungta P, Bužek V, Caves C M, Hillery M and Milburn G J 2001 Universal state inversion and concurrence in arbitrary dimensions *Phys. Rev. A* **64** 042315

[23] Sá Earp H N and Pachos J K 2005 A constructive algorithm for the Cartan decomposition of $\mathbf{SU}(2^N)$ *J. Math. Phys.* **46** 082108

[24] Uhlmann A 2000 Fidelity and concurrence of conjugated states *Phys. Rev. A Third Series* **62** 032307

[25] Vatan F and Williams C P 2004 Realization of a general three-qubit quantum gate *Preprint* quant-ph/0401178v2

[26] Wong A and Christensen N 2001 Potential multiparticle entanglement measure *Phys. Rev. A* **63** 044301

[27] Wootters W K 1998 Entanglement of formation of an arbitrary state of two qubits *Phys. Rev. Lett.* **80** 2245

[28] Zhang J, Vala J, Sastry S and Whaley K B 2003 Geometric theory of nonlocal two-qubit operations *Phys. Rev. A Third Series* **67** 042313