

Cartan Decomposition of $SU(2^n)$, Constructive Controllability of Spin Systems and Universal Quantum Computing

Navin Khaneja,^{*} Steffen J. Glaser[†]

February 1, 2008

Abstract

In this paper we provide an explicit construction of any arbitrary unitary transformation on n qubits from one qubit and a single two qubit quantum gate. Building on the previous work demonstrating the universality of two qubit quantum gates, we present here an explicit implementation. The construction is based on the Cartan decomposition of the semi-simple Lie group $SU(2^n)$ and uses the geometric structure of the Riemannian Symmetric Space $\frac{SU(2^n)}{SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)}$. The decomposition highlights the geometric aspects of the problem of building an arbitrary unitary transformations out of quantum gates and makes explicit the choice of pulse sequences for the implementation of arbitrary unitary transformation on n coupled $\frac{1}{2}$ spins in *NMR* quantum computing. Finally we make observations on the optimality of the design procedure.

1 Introduction

Recent interests in quantum computing have been fostered by the prospects of building a computational theory which is different and more powerful than the classical computational theory. The vision of solving a class of problems using quantum computing, which have been known to be computationally hard in the classical setting, has been advanced by the recent work of [18], [19]. Any quantum computation involves evolution of the initial state under a series of unitary transformations. Absolutely essential to the design of an universal quantum computer is the ability to synthesize any arbitrary unitary transformations from simple quantum gates (lower dimensional unitary transformations). The search for such universal components was initiated by Deutsch's original discovery [20] of a three-bit universal quantum logic gate. Following which DiVincenzo [23] showed that two-bit universal quantum gates also exist. This result was then generalized by the work of Barenco et al. [22], Lloyd [21] and Deutsch et al. [20] showing that almost any two bit gate is also universal. The central idea behind demonstrating the universality of these gates rests on the fact that the generators of the unitary transformations produced by these gates generate the Lie algebra of the unitary

^{*}Department of Mathematics, Dartmouth College, Hanover, NH 03755, email: Navin.Khaneja@dartmouth.edu
This work was supported by Burke Fellowship from Dartmouth College

[†]Institute of Organic Chemistry and Biochemistry II, Technical University Munich, 85747 Garching, Germany.
This work was funded by the Fonds der Chemischen Industrie and the Deutsche Forschungsgemeinschaft under grant Gl 203/1-6.

group and therefore by suitable composition of these gates, we can produce any arbitrary unitary transformation. This is basically the notion of controllability in mathematical control theory— that is, whether available Hamiltonians can prepare an arbitrary state of the quantum system [24, 25]. The conditions of controllability of a quantum system were rediscovered as the conditions for the universality of a quantum computer.

Problems of similar nature arise in coherent spectroscopy. Many areas of spectroscopic fields, such as nuclear magnetic resonance (NMR), electron magnetic resonance and optical spectroscopy rely on a limited set of control variables in order to create desired unitary transformations [5, 6, 7]. In NMR, unitary transformations are used to manipulate an ensemble of nuclear spins, e.g. to transfer coherence between coupled spins in multidimensional NMR-experiments [5] or to implement quantum-logic gates in NMR quantum computers [8]. However, the design of a sequence of radio-frequency pulses that generate a desired unitary operator is not trivial [9]. So far, no general design approach is known for the implementation of a desired unitary transformation [6]. During the last decade the questions of controllability of quantum systems have generated considerable interest [16, 17]. In particular, coherence or polarization transfer in pulsed coherent spectroscopy has received lot of attention [6, 9]. Algorithms for determining bounds quantifying the maximum possible efficiency of transfer between non-Hermitian operators have been determined [6]. There is utmost need for design strategies for pulse sequences that can achieve these bounds. From a control theory perspective, all these are constructive controllability problems [14].

In this paper, we present a constructive solution to the problem of producing an arbitrary 2^n dimensional unitary transformation acting on n qubits from unitary transformations acting on individual and pair of qubits (elements of $SU(2)$ and $SU(4)$ respectively). The design strategy presented here is a generalization of well known Euler angle decomposition for rotations. Recall if

$$\begin{aligned} I_x &= \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ I_y &= \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ I_z &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

represent the standard Pauli spin matrices, then any $V \in SU(2)$ has a decomposition

$$V = \exp(-i\alpha I_x) \exp(-i\beta I_z) \exp(-i\gamma I_x).$$

where $\alpha, \beta, \gamma \in \mathbb{R}$. Similarly any $W \in SU(2^n)$, has a decomposition

$$W = K_1 A K_2.$$

Where $K_1, K_2 \in SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)$ and $A \in \exp(\mathfrak{h})$, where \mathfrak{h} is a Cartan subalgebra of the Riemannian symmetric space

$$\frac{SU(2^n)}{SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)}.$$

We will elaborate on all these notions. The point to be emphasized here is that we then obtain a recursive formula for the decomposition. Given the decomposition $W = K_1 A K_2$, we can further decompose K_1 and K_2 in terms of the elements of $SU(2^{n-2}) \otimes SU(2^{n-2}) \otimes U(1)$ and so on. Finally we will be left with only one and two qubit operations. We will see that this recursive formulation highlights the geometric structure of the problem.

We are also interested in the implementation of these unitary transformations in a network of coupled spins in the context of NMR. The emphasis being NMR quantum computers and coherence transfer experiments in multidimensional spectroscopy. We emphasize again that from a control theory viewpoint, these are constructive controllability problems. The dynamical system to be controlled is defined through the time-dependent Schrödinger equation

$$\dot{U}(t) = -iH(t)U(t), \quad U(0) = I,$$

where $H(t)$ and $U(t)$ are the Hamiltonian and the unitary displacement operators, respectively. In this paper, we will only be concerned with finite-dimensional quantum systems. In this case, we can choose a basis and think of $H(t)$ as a Hermitian matrix. We can split the Hamiltonian

$$H = H_d + \sum_{i=1}^m v_i(t)H_i,$$

where H_d is the part of Hamiltonian that is internal to the system and we call it the *drift* or *free evolution Hamiltonian* and $\sum_{i=1}^m v_i(t)H_i$ is the part of Hamiltonian that can be externally changed. It is called the *control* or *rf Hamiltonian*. The equation for $U(t)$ dictates the evolution of the density matrix according to

$$\dot{\rho}(t) = U(t)\rho(0)U^\dagger(t).$$

where

$$\dot{U} = -i(H_d + \sum_{i=1}^m v_i H_i) U; U(0) = I. \quad (1)$$

In a network of coupled spin $\frac{1}{2}$ nuclei, the control terms H_i correspond to the Hamiltonian that effect each spin individually (we assume that resonance frequencies of the spins are well separated so that selective excitation is possible). The group K generated by the Lie algebra $\{H_i\}_{LA}$ corresponds to n direct copies of $SU(2)$, which we denote by

$$[SU(2)]^{\otimes n}.$$

The drift term H_d is the part of the Hamiltonian that corresponds to couplings among the spins. It is known that if the Lie algebra $\{H_d, H_i\}_{LA}$ equals $\mathfrak{su}(2^n)$, the algebra of $2^n \times 2^n$, traceless skew Hermitian matrices, then we can steer the system (1), from identity to any point $U_F \in SU(2^n)$. The problem we will address in this paper is explicit construction of a pulse sequence or in other words control laws v_i , that steer the system (1) from $U(0) = I$ to some U_F , in finite time.

We begin by reviewing some important facts about Lie groups and Lie algebras, which will be used in the remaining part of the paper. The exposition is very brief and follows [26]. The reader is advised to refer to [1, 2, 3] for more details and a rigorous treatment on the subject.

2 Cartan Decomposition and Riemannian Symmetric Spaces

We will assume that the reader is familiar with the basic facts about Lie groups and homogeneous spaces [1].

Notation 1 Throughout the paper, G will denote a compact semi-simple Lie group and e its identity element (we use I to denote the identity matrix when working with the matrix representation of the

group). As is well known there is a naturally defined bi-invariant metric on G , given by the Killing form. We denote this bi-invariant metric by \langle, \rangle_G . We will use K to denote a compact closed subgroup of G . Let $L(G)$ be the Lie algebra of right invariant vector fields on G and similarly $L(K)$ the Lie algebra of right invariant vector fields on K . There is a one to one correspondence between these vector fields and the tangent spaces $T_e(G)$ and $T_e(K)$, which we denote by \mathfrak{g} and \mathfrak{k} respectively. There is a direct sum decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$ such that $\mathfrak{m} = \mathfrak{k}^\perp$ with respect to the metric.

To fix ideas, let $G = SU(n)$ and $\mathfrak{g} = \mathfrak{su}(n)$ be its associated Lie algebra of $n \times n$ traceless skew-Hermitian matrices. Then $\langle A, B \rangle_G = \text{trace}(A^\dagger B)$, $A, B \in \mathfrak{su}(n)$ (which is proportional to the Killing metric) represents a bi-invariant metric on $SU(n)$.

Definition 1 (Cartan decomposition of \mathfrak{g}) Let \mathfrak{g} be a real semi-simple Lie algebra and let the decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$, $\mathfrak{m} = \mathfrak{k}^\perp$ satisfy the commutation relations

$$[\mathfrak{k}, \mathfrak{k}] \subset \mathfrak{k} \quad (2)$$

$$[\mathfrak{m}, \mathfrak{k}] = \mathfrak{m} \quad (3)$$

$$[\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{k}. \quad (4)$$

We will refer to this decomposition as a Cartan decomposition of \mathfrak{g} . The pair $(\mathfrak{g}, \mathfrak{k})$ will be called an orthogonal symmetric Lie algebra pair [26, 2].

Definition 2 (Adjoint orbit) The Lie group G acts on its Lie algebra \mathfrak{g} by conjugation $Ad_G : \mathfrak{g} \rightarrow \mathfrak{g}$ (called the adjoint action). This is defined as follows. Given $U \in G$, $X \in \mathfrak{g}$, then

$$Ad_U(X) = \left. \frac{d}{dt} U \exp(tX) U^{-1} \right|_{t=0}.$$

We use the notation

$$Ad_K(X) = \bigcup_{k \in K} Ad_k(X).$$

$Ad_K(X)$ is called the adjoint orbit of X .

For example if $U \in SU(n)$, $A \in \mathfrak{su}(n)$, its associated Lie algebra of $n \times n$ traceless skew-Hermitian matrices. Then $Ad_U(A) = UAU^T$, such that

$$\exp(Ad_U(A)) = U \exp(A) U^T = Ad_U(\exp(A)).$$

Definition 3 (Cartan subalgebra) Consider the semi-simple Lie algebra \mathfrak{g} and its Cartan decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$. If \mathfrak{h} is a subalgebra of \mathfrak{g} contained in \mathfrak{m} , then \mathfrak{h} is Abelian because $[\mathfrak{m}, \mathfrak{m}] \in \mathfrak{k}$. A maximal Abelian subalgebra contained in \mathfrak{m} is called a Cartan subalgebra of the pair $(\mathfrak{g}, \mathfrak{k})$.

It is well known [2, 3] that:

Theorem 1 If \mathfrak{h} and \mathfrak{h}' are two maximal Abelian subalgebras contained in \mathfrak{m} , then

1. There is an element $k \in K$ such that $Ad_k(\mathfrak{h}) = \mathfrak{h}'$.

$$2. \mathfrak{m} = \bigcup_{k \in K} Ad_k(\mathfrak{h}).$$

Remark 1 It is also well known that the homogeneous coset space $G/K = \{KU : U \in G\}$ admits the structure of a differentiable manifold [1]. Let $\pi : G \rightarrow G/K$ denote the natural projection map. Define $o \in G/K$ by $o = \pi(e)$. Given the decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$, the tangent space plane $T_o(G/K)$ can be then identified with the vector subspace \mathfrak{m} . If $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$ is a Cartan decomposition then the homogeneous space $G/K = \exp(\mathfrak{m})$, and is called a *globally Riemannian symmetric space* [3]. From above stated theorem 1, the maximal Abelian subalgebras of \mathfrak{m} are all Ad_K conjugate and in particular they have the same dimension. The dimension is called the *rank* of the globally Riemannian symmetric space G/K .

Theorem 2 Given the semi-simple Lie algebra \mathfrak{g} and its cartan decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$, let \mathfrak{h} be a Cartan subalgebra of the pair $(\mathfrak{g}, \mathfrak{k})$ and define $A = \exp(\mathfrak{h}) \subset G$. Then $G = KAK$.

Proof: $G = KP$, where $P = \exp(\mathfrak{m}) = \exp(\bigcup_{k \in K} Ad_k(\mathfrak{h})) = \bigcup_{k \in K} Ad_k(\exp(\mathfrak{h})) = \bigcup_{k \in K} Ad_k(A) \subset KAK$. Now $G = KKA = KAK$. **Q.E.D.**

Definition 4 (Cartan decomposition of G) The decomposition $G = KAK$ of the semi-simple Lie group $G = KAK$, will be our most important tool in this paper. We will call this decomposition the *Cartan decomposition* of the Lie group G [2]

Definition 5 (Weyl orbit) Given the Cartan decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$, let \mathfrak{h} be a Cartan subalgebra of $(\mathfrak{g}, \mathfrak{k})$ containing X . We use the notation $W(X) = \mathfrak{h} \cap Ad_K(X)$ to denote the maximal commuting set contained in the adjoint orbit of X . The set $W(X)$ is called the Weyl orbit of X .

3 Product Operator Basis

The Lie Group G which we will be most interested in is $SU(2^n)$, the special unitary group describing the evolution of n interacting spin $\frac{1}{2}$ particles (Please note that we focus on $SU(2^n)$ instead of $U(2^n)$ because a global phase is not of interest to us). The Lie algebra $\mathfrak{su}(2^n)$ is a $4^n - 1$ dimensional space of traceless $n \times n$ skew-Hermitian matrices. The orthonormal bases which we will use for this space is expressed as tensor products of Pauli spin matrices [12](product operator bases). We choose to work in these bases because of their widespread use in the NMR literature and our desire to look at the implementations of NMR quantum computers. Recall the Pauli spin matrices I_x, I_y, I_z defined by

$$\begin{aligned} I_x &= \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ I_y &= \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ I_z &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

are the generators of the rotation in the two dimensional Hilbert space and basis for the Lie algebra of traceless skew-Hermitian matrices $\mathfrak{su}(2)$. They obey the well known relations

$$[I_x, I_y] = iI_z ; [I_y, I_z] = iI_x ; [I_z, I_x] = iI_y \quad (5)$$

$$I_x^2 = I_y^2 = I_z^2 = \frac{1}{4} \mathbf{1} \quad (6)$$

where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Notation 2 The orthogonal basis $\{iB_s\}$, for $\mathfrak{su}(2^n)$ take the form

$$B_s = 2^{q-1} \prod_{k=1}^n (I_{k\alpha})^{a_{ks}}, \quad (7)$$

$\alpha = x, y, \text{ or } z$ and

$$I_{k\alpha} = \mathbf{1} \otimes \cdots \otimes I_\alpha \otimes \mathbf{1}, \quad (8)$$

where I_α the Pauli matrix appears in the above expression only at the k^{th} position, and $\mathbf{1}$ the two dimensional identity matrix, appears everywhere except at the k^{th} position. a_{ks} is 1 in q of the indices and 0 in the remaining. Note that $q \geq 1$ as $q = 0$ corresponds to the identity matrix and is not a part of the algebra.

Example 1 As an example for $n = 2$ the basis for $\mathfrak{su}(4)$ takes the form

$$\begin{aligned} q = 1 & \quad i\{I_{1x}, I_{1y}, I_{1z}, I_{2x}, I_{2y}, I_{2z}\} \\ q = 2 & \quad i\{I_{1x}I_{2x}, I_{1x}I_{2y}, I_{1x}I_{2z} \\ & \quad I_{1y}I_{2x}, I_{1y}I_{2y}, I_{1y}I_{2z} \\ & \quad I_{1z}I_{2x}, I_{1z}I_{2y}, I_{1z}I_{2z}\} \end{aligned}$$

Remark 2 It is very important to note that the expression $I_{k\alpha}$ depends on the dimension n . To illustrate what this means, the expression for I_{2z} for $n = 2$ and $n = 3$ is $\mathbf{1} \otimes I_z$, and $\mathbf{1} \otimes I_z \otimes \mathbf{1}$ respectively. Also observe that these operators are only normalized for $n = 2$ as

$$\text{tr}(B_r B_s) = \delta_{rs} 2^{n-2} \quad (9)$$

To fix ideas, lets compute one of these operators explicitly for $n = 2$

$$I_{1z} = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

which takes the form

$$I_{1z} = \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

4 The Two Qubit Example

Before we consider the most general case of n qubits, let us make concrete the ideas developed in the previous section with the help of an example.

Example 2 Suppose we have two heteronuclear interacting qubits and the interaction between them produces a unitary transformation of the form

$$\exp(-i\alpha J I_{1z} I_{2z}), \quad \alpha \in \mathbb{R}.$$

This is a typical scenario of two nuclear spins coupled by a scalar J coupling. Furthermore assume we can individually excite each spin, i.e. perform one qubit operations. The goal now is to produce any arbitrary unitary transformation $U \in SU(4)$, from this specified coupling and one qubit operations. This structure appears often in the NMR situation. The unitary propagator U , describing the evolution of the system in a suitable rotating frame is described by

$$\dot{U} = -i(H_d + \sum_{i=1}^4 u_i H_i)U, \quad U(0) = I \tag{10}$$

where

$$\begin{aligned} H_d &= 2\pi J I_{1z} I_{2z} \\ H_1 &= 2\pi I_{1x} \\ H_2 &= 2\pi I_{1y} \\ H_3 &= 2\pi I_{2x} \\ H_4 &= 2\pi I_{2y}, \end{aligned}$$

The symbol J represents the strength of the scalar coupling between I_1 and I_2 . Observe that the subgroup K generated by $\{H_i\}_{i=1}^4$ is $SU(2) \otimes SU(2)$. Therefore the unitary transformations belonging to $SU(2) \otimes SU(2)$ can be produced very fast by hard pulses that excite each of the spins individually.

The Lie algebra $\mathfrak{g} = \mathfrak{su}(4)$, has the direct sum decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$. Where

$$\begin{aligned} \mathfrak{k} &= \text{span } i\{I_{1x}, I_{1y}, I_{1z}, I_{2x}, I_{2y}, I_{2z}\} \\ \mathfrak{m} &= \text{span } i\{I_{1x}I_{2x}, I_{1x}I_{2y}, I_{1x}I_{2z}, \\ &\quad I_{1y}I_{2x}, I_{1y}I_{2y}, I_{1y}I_{2z}, \\ &\quad I_{1z}I_{2x}, I_{1z}I_{2y}, I_{1z}I_{2z}\} \end{aligned}$$

Please note that span in above equations and in the rest of the paper denotes all linear combinations with real coefficients. Using the well known commutation relations

$$[A \otimes B, C \otimes D] = [A, C] \otimes (B.D) + (C.A) \otimes [B, D],$$

and equations (5, 6), it is easily verified

$$[\mathfrak{k}, \mathfrak{k}] \subset \mathfrak{k}, \quad [\mathfrak{m}, \mathfrak{k}] = \mathfrak{m}, \quad [\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{k}.$$

Therefore the decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{k}$ is a Cartan decomposition of $\mathfrak{su}(4)$. As the subalgebra $\mathfrak{k} = \mathfrak{su}(2) \oplus \mathfrak{su}(2)$, generates the group $K = SU(2) \otimes SU(2)$, the coset space

$$\frac{SU(4)}{SU(2) \otimes SU(2)}$$

is a Riemannian symmetric space. Note that the Abelian subalgebra \mathfrak{h} generated by

$$i\{I_{1x}I_{2x}, I_{1y}I_{2y}, I_{1z}I_{2z}\}$$

is contained in \mathfrak{m} and is maximal Abelian and hence a Cartan subalgebra of the Symmetric Space $\frac{SU(4)}{SU(2) \otimes SU(2)}$. Therefore using the corollary 1 any $U_F \in SU(4)$ can be decomposed as

$$U_F = K_1 \exp(-i(\alpha_1 I_{1x}I_{2x} + \alpha_2 I_{1y}I_{2y} + \alpha_3 I_{1z}I_{2z})) K_2.$$

where $K_1, K_2 \in SU(2) \otimes SU(2)$.

Now lets see how this decomposition makes obvious the choice of pulse sequences for producing this propogator. Note that for $K_y = \exp(-i\frac{\pi}{2}I_{1y}) \exp(-i\frac{\pi}{2}I_{2y})$, we have

$$K_y \exp(-i\alpha_1 I_{1z}I_{2z}) K_y^{-1} = \exp(-i\alpha_1 I_{1x}I_{2x})$$

and similarly for $K_x = \exp(-i\frac{\pi}{2}I_{1x}) \exp(-i\frac{\pi}{2}I_{2x})$ we have

$$K_x^{-1} \exp(-i\alpha_2 I_{1z}I_{2z}) K_x = \exp(-i\alpha_2 I_{1y}I_{2y}).$$

This makes transparent, as to how one should generate the unitary transformation U_F above using the unitary evolution in equation (10). This can be summarized by writing U_F as

$$U_F = K_1 \cdot K_y \cdot \exp(-i\alpha_1 I_{1z}I_{2z}) \cdot K_y^{-1} \cdot K_x^{-1} \cdot \exp(-i\alpha_2 I_{1z}I_{2z}) \cdot K_x \cdot \exp(-i\alpha_3 I_{1z}I_{2z}) \cdot K_2. \quad (11)$$

The unitary propogators K_x, K_y, K_1 and K_2 can be produced by selective hard pulses, i.e. one qubit gates.

Remark 3 In [27], it was shown that synthesizing U_F using the decomposition given above, is indeed the fastest way to generate U_F . Time optimality is an important consideration in presence of decoherence. Observe that the Hamiltonians $I_{1x}I_{2x}$ and $I_{1y}I_{2y}$ are the elements of Weyl orbit of $I_{1z}I_{2z}$ under the adjoint action of $SU(2) \otimes SU(2)$.

Now lets proceed to the general case of n qubits.

5 How does $[SU(2)]^{\otimes n}$ sit inside $SU(2^n)$

In this section we would like to use the machinery developed in the previous section to decompose the group $SU(2^n)$, into smaller unitary transformations, which can be produced. This will be achieved through successive Cartan decompositions of $SU(2^n)$ into smaller and smaller unitary transformations till we are only left with unitary operations corresponding to one and two bit operations.

Main Idea: Suppose we are given n qubits. In NMR quantum computing this will be a network of n coupled spin $\frac{1}{2}$ particles. Let us label these qubits as $q_1, q_2 \dots q_n$. Let \mathbb{H}_1 denote the two dimensional Hilbert space of a single qubit. Similarly let \mathbb{H}_n denote the 2^n dimensional Hilbert space of n qubits. These are related by

$$\mathbb{H}_n = \mathbb{H}_1 \otimes \mathbb{H}_1 \otimes \dots \mathbb{H}_1.$$

To understand the decomposition of $SU(2^n)$, suppose we can generate an arbitrary unitary transformation on the Hilbert space \mathbb{H}_{n-1} of qubits $q_1, q_2 \dots q_{n-1}$ i.e. an arbitrary element of $SU(2^{n-1})$. Also assume, we can independently manipulate the n^{th} qubit. Furthermore assume we have a two qubit gate that will act on the qubit q_n and q_{n-1} . In the context of NMR, this corresponds to evolution under a coupling between the spin q_n and q_{n-1} . To be more specific let this unitary evolution be of the form

$$\exp(-i\alpha J I_{(n-1)z} I_{nz}),$$

caused due to a scalar J coupling.

We now explicitly build any $U \in SU(2^n)$ from elements of $SU(2^{n-1}) \otimes SU(2)$ and this interaction between q_{n-1} and q_n . Notice this will essentially solve our main problem because to generate any element $V \in SU(2^{n-1})$ we will use this divide and conquer strategy again, building V from $SU(2^{n-2}) \otimes SU(2)$ and interaction between $(n-1)^{th}$ and $(n-2)^{th}$ qubit and so on. Let us look at the geometry of the situation

Notation 3 The Lie algebra $\mathfrak{su}(2^n)$ consists of the elements

$$\mathfrak{su}(2^n) = \text{span} \{A \otimes I_x, B \otimes I_y, C \otimes I_z, D \otimes \mathbf{1}, iI_{nx}, iI_{ny}, iI_{nz} | A, B, C, D \in \mathfrak{su}(2^{n-1})\}$$

The Lie algebra $\mathfrak{su}(2^n)$ has a direct sum decomposition into the following two vector spaces

$$\mathfrak{su}_{\mathfrak{t}}(2^n) = \text{span} \{A \otimes I_z, B \otimes \mathbf{1}, iI_{nz} | A, B \in \mathfrak{su}(2^{n-1})\},$$

$$\mathfrak{su}_{\mathfrak{m}}(2^n) = \text{span} \{A \otimes I_x, B \otimes I_y, iI_{nx}, iI_{ny} | A, B \in \mathfrak{su}(2^{n-1})\}.$$

We emphasize again that *span* denotes the vector space generated by the elements of the set by taking linear combinations over the field of reals.

Lemma 1 The vector space $\mathfrak{su}_{\mathfrak{t}}(2^n)$ is a Lie algebra of dimension $2 \times 4^{n-1} - 1$ such that

$$\exp(\mathfrak{su}_{\mathfrak{t}}(2^n)) = SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)$$

Proof: The proof is a direct consequence of following commutation relations. Let $A, B, C \in \mathfrak{su}(2^{n-1})$, if $A \neq B$

$$\begin{aligned} [A \otimes I_z, B \otimes I_z] &= C \otimes \mathbf{1}; \\ [A \otimes I_z, B \otimes \mathbf{1}] &= C \otimes I_z; \\ [A \otimes \mathbf{1}, B \otimes \mathbf{1}] &= C \otimes \mathbf{1}; \\ [A \otimes I_z, I_{nz}] &= 0; \\ [A \otimes \mathbf{1}, I_{nz}] &= 0; \\ [A \otimes I_z, A \otimes \mathbf{1}] &= 0. \end{aligned}$$

Now observe that I_{nz} and elements of the type

$$A \otimes \left(\frac{1}{2} \mathbf{1} + I_z \right) = A \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

and

$$B \otimes \left(\frac{1}{2} \mathbf{1} - I_z \right) = B \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

commute. Therefore the Lie Algebra

$$\mathfrak{su}_{\mathfrak{t}}(2^n) = \mathfrak{su}(2^{n-1}) \oplus \mathfrak{su}(2^{n-1}) \oplus \mathfrak{u}(1),$$

and the last part of the lemma follows.

Q.E.D.

Theorem 3 The decomposition $\mathfrak{su}(2^n) = \mathfrak{su}_m(2^n) \oplus \mathfrak{su}_t(2^n)$ is a Cartan decomposition of the Lie algebra $\mathfrak{su}(2^n)$

Proof: From equation (9), it is clear that $\mathfrak{su}_t(2^n) \perp \mathfrak{su}_m(2^n)$. We have already shown in Lemma 1 that $\mathfrak{su}_t(2^n)$ is a Lie subalgebra of $\mathfrak{su}(2^n)$. All that we need to show is that the commutation rules

$$\begin{aligned} [\mathfrak{su}_m(2^n), \mathfrak{su}_t(2^n)] &= \mathfrak{su}_m(2^n) \\ [\mathfrak{su}_m(2^n), \mathfrak{su}_m(2^n)] &\subset \mathfrak{su}_t(2^n). \end{aligned}$$

are satisfied. The proof follows from the following commutation relations and the fact that $\mathfrak{su}(n)$ is semi-simple (implies $[\mathfrak{su}(n), \mathfrak{su}(n)] = \mathfrak{su}(n)$). Let $A, B, C \in \mathfrak{su}(2^{n-1})$, $c \in \mathbb{R}$ and $\alpha \in \{x, y\}$. If $A \neq B$, then

$$\begin{aligned} [A \otimes I_\alpha, B \otimes I_\alpha] &= C \otimes \mathbf{1} ; \\ [A \otimes I_x, B \otimes I_y] &= C \otimes I_z ; \\ [A \otimes I_x, B \otimes I_z] &= C \otimes I_y ; \\ [A \otimes I_y, B \otimes I_z] &= C \otimes I_x ; \\ [A \otimes I_\alpha, B \otimes \mathbf{1}] &= C \otimes I_\alpha. \end{aligned}$$

If $A = B$ then

$$\begin{aligned} [A \otimes I_x, A \otimes I_y] &= c i I_{nz} ; \\ [A \otimes I_x, A \otimes I_z] &= c i I_{ny} ; \\ [A \otimes I_y, A \otimes I_z] &= c i I_{nx} ; \\ [A \otimes I_\alpha, A \otimes \mathbf{1}] &= 0. \end{aligned}$$

Corollary 1 Any $U \in SU(2^n)$ has a decomposition

$$U = K_1 A K_2,$$

where $K_1, K_2 \in \exp(\mathfrak{su}_t(2^n)) \cong SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)$ and $A = \exp(Y)$, for some $Y \in \mathfrak{h}$, a maximal Cartan subalgebra of the pair $(\mathfrak{su}(2^n), \mathfrak{su}_t(2^n))$.

Proof: We have already shown that $\mathfrak{su}(2^n) = \mathfrak{su}_t(2^n) \oplus \mathfrak{su}_m(2^n)$ is a Cartan decomposition. Hence the proof follows from theorem 2. **Q.E.D.**

The key observation is that $K_1, K_2 \in \exp(\mathfrak{su}_t(2^n))$ again has a decomposition. This is stated in the following theorem.

Notation 4 Let us denote

$$\begin{aligned} \mathfrak{su}_{t1}(2^n) &= \text{span} \{A \otimes I_z | A \in \mathfrak{su}(2^{n-1})\} \\ \mathfrak{su}_{t0}(2^n) &= \text{span} \{A \otimes \mathbf{1} | A \in \mathfrak{su}(2^{n-1})\} \\ \overline{\mathfrak{su}_t(2^n)} &= \text{span} \{A \otimes \mathbf{1}, A \otimes I_z | A \in \mathfrak{su}(2^{n-1})\} \end{aligned}$$

Notice $\mathfrak{su}_t(2^n)$ is just $\overline{\mathfrak{su}_t(2^n)} \oplus \mathfrak{u}(1)$ (I_{nz} commutes with everything in $\mathfrak{su}_t(2^n)$ and generates $\mathfrak{u}(1)$) and therefore

$$\exp(\mathfrak{su}_t(2^n)) = \exp(\overline{\mathfrak{su}_t(2^n)}) \otimes U(1).$$

Theorem 4 The direct sum decomposition $\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)} = \mathfrak{su}_{k_0}(2^n) \oplus \mathfrak{su}_{k_1}(2^n)$ is a Cartan decomposition of the Lie algebra $\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)}$.

Proof: Recall that

$$\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)} = \text{span} \{A \otimes I_z, B \otimes \mathbf{1} \mid A, B \in \mathfrak{su}(2^{n-1})\}$$

If $A, B, C \in \mathfrak{su}(2^{n-1})$ such that $A \neq B$, then

$$\begin{aligned} [A \otimes I_z, B \otimes \mathbf{1}] &= C \otimes I_z; \\ [A \otimes I_z, A \otimes \mathbf{1}] &= 0; \\ [A \otimes I_z, B \otimes I_z] &= C \otimes \mathbf{1} \end{aligned}$$

Therefore from the above relations and the fact that $\mathfrak{su}(n)$ is semi-simple, it can be verified that

$$\begin{aligned} [\mathfrak{su}_{\mathfrak{f}1}(2^n), \mathfrak{su}_{\mathfrak{f}1}(2^n)] &\subset \mathfrak{su}_{\mathfrak{f}0}(2^n) \\ [\mathfrak{su}_{\mathfrak{f}1}(2^n), \mathfrak{su}_{\mathfrak{f}0}(2^n)] &= \mathfrak{su}_{\mathfrak{f}1}(2^n) \\ [\mathfrak{su}_{\mathfrak{f}0}(2^n), \mathfrak{su}_{\mathfrak{f}0}(2^n)] &\subset \mathfrak{su}_{\mathfrak{f}0}(2^n) \end{aligned}$$

Hence the result follows. **Q.E.D**

Corollary 2 Any $U \in \exp(\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)})$ has a unique decomposition

$$U = K_1 A K_2,$$

where $K_1, K_2 \in SU(2^{n-1})$ and $A = \exp(Y)$, for some $Y \in \mathfrak{f}$, a Cartan subalgebra of the pair $(\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)}, \mathfrak{su}_{\mathfrak{f}0}(2^n))$.

Proof: The proof follows directly from theorem 2.

The above stated theorems, therefore give us a recursive decomposition procedure for an element in $SU(2^n)$. To summarize what we have accomplished till now.

Corollary 3 Any $U \in SU(2^n)$ has a decomposition

$$U = K_1 \cdot \exp(Z_1) \cdot K_2 \cdot \exp(Y) \cdot K_3 \cdot \exp(Z_2) \cdot K_4,$$

where $K_1, K_2, K_3, K_4 \in SU(2^{n-1}) \otimes U(1)$, $Y \in \mathfrak{h}$, a Cartan subalgebra of the pair $(\mathfrak{su}(2^n), \mathfrak{su}_{\mathfrak{f}}(2^n))$ and $Z_1, Z_2 \in \mathfrak{f}$, a Cartan subalgebra of the pair $(\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)}, \mathfrak{su}_{\mathfrak{f}0}(2^n))$.

Proof: The result follows directly from corollaries 1 and 2.

Remark 4 We know how to produce unitary transformations K_1, K_2, K_3, K_4 as these belong to the group $SU(2^{n-1}) \otimes U(1)$, a subgroup of $SU(2^{n-1}) \otimes SU(2)$. All that needs to be shown now is that we can produce unitary transformations of the form $\exp(Z_1)$, $\exp(Z_2)$ and $\exp(Y)$, where $Y \in \mathfrak{h}$, a Cartan subalgebra of the pair $(\mathfrak{su}(2^n), \mathfrak{su}_{\mathfrak{f}}(2^n))$ and $Z_1, Z_2 \in \mathfrak{f}$, a Cartan subalgebra of the pair $(\overline{\mathfrak{su}_{\mathfrak{f}}(2^n)}, \mathfrak{su}_{\mathfrak{f}0}(2^n))$. This will be achieved by using the coupling between the n^{th} spin and the network of coupled $n - 1$ spins. We will show that the adjoint action of $SU(2^{n-1}) \otimes SU(2)$ on the coupling Hamiltonian $(I_{(n-1)z} I_{nz})$ contains commuting elements whose span is the whole Cartan subalgebra \mathfrak{h} . Same applies for the Cartan subalgebra \mathfrak{f} (Recall we used this fact in the two spin case, where we generated any element of the Cartan subalgebra, of the form $\alpha_1 I_{1x} I_{2x} + \alpha_2 I_{1y} I_{2y} + \alpha_3 I_{1z} I_{2z}$ by the adjoint action of $SU(2) \otimes SU(2)$ on $I_{1z} I_{2z}$). Now using the result of corollary (3) we will be able to generate any unitary transformation on n qubits.

5.1 Generating Cartan subalgebras from Weyl orbits

Let us now characterize a Cartan subalgebra for the pair $(\mathfrak{su}(2^n), \mathfrak{su}_{\mathfrak{t}}(2^n))$ and $(\overline{\mathfrak{su}_{\mathfrak{t}}(2^n)}, \mathfrak{su}_{\mathfrak{t}0}(2^n))$, in our product operator basis. This will be done in a recursive way. For this we use the following notation

Notation 5 Let

$$\begin{aligned} \mathfrak{a}(2) &= \pm\{iI_{1x}I_{2x}, iI_{1y}I_{2y}, iI_{1z}I_{2z}\} \\ \mathfrak{s}(2) &= \mathfrak{a}(2) \\ \mathfrak{a}(n) &= \{\pm iI_{nx}, A \otimes I_x | A \in \mathfrak{s}(n-1)\} \\ \mathfrak{b}(n) &= \{A \otimes I_z | A \in \mathfrak{s}(n-1)\} \\ \mathfrak{s}(n) &= \{\mathfrak{s}(n-1) \otimes \mathbf{1}, \mathfrak{a}(n)\} \\ \mathfrak{h}(n) &= \text{span } \mathfrak{a}(n) \\ \mathfrak{f}(n) &= \text{span } \mathfrak{b}(n) \end{aligned}$$

Remark 5 To avoid confusion, we remind the reader that for $A \in \mathfrak{s}(n-1)$, the elements $A \otimes I_x$ and $A \cdot I_{nx}$ represent the same object.

Example 3 To fix ideas, we give here the explicit expressions for $\mathfrak{a}(n)$ and $\mathfrak{b}(n)$ for $n = 3$ and $n = 4$

$$\begin{aligned} \mathfrak{a}(3) &= \pm i\{I_{3x}, I_{1x}I_{2x}I_{3x}, I_{1y}I_{2y}I_{3x}, I_{1z}I_{2z}I_{3x}\} \\ \mathfrak{a}(4) &= \pm i\{I_{4x}, I_{3x}I_{4x}, I_{1x}I_{2x}I_{4x}, I_{1y}I_{2y}I_{4x}, I_{1z}I_{2z}I_{4x}, I_{1x}I_{2x}I_{3x}I_{4x}, I_{1y}I_{2y}I_{3x}I_{4x}, I_{1z}I_{2z}I_{3x}I_{4x}\} \\ \mathfrak{b}(3) &= \pm i\{I_{1x}I_{2x}I_{3z}, I_{1y}I_{2y}I_{3z}, I_{1z}I_{2z}I_{3z}\} \\ \mathfrak{b}(4) &= \pm i\{I_{3x}I_{4z}, I_{1x}I_{2x}I_{4z}, I_{1y}I_{2y}I_{4z}, I_{1z}I_{2z}I_{4z}, I_{1x}I_{2x}I_{3x}I_{4z}, I_{1y}I_{2y}I_{3x}I_{4z}, I_{1z}I_{2z}I_{3x}I_{4z}\} \end{aligned}$$

Lemma 2 The subspaces $\mathfrak{h}(n)$ and $\mathfrak{f}(n)$ are a Cartan subalgebra for the Lie algebra pair $(\mathfrak{su}(2^n), \mathfrak{su}_{\mathfrak{t}}(2^n))$ and $(\overline{\mathfrak{su}_{\mathfrak{t}}(2^n)}, \mathfrak{su}_{\mathfrak{t}0}(2^n))$ respectively.

Proof: We first show that $\mathfrak{h}(n)$ is a Cartan subalgebra of $(\mathfrak{su}(2^n), \mathfrak{su}_{\mathfrak{t}}(2^n))$. The proof is inductive. We saw that $\mathfrak{h}(2)$ is a Cartan subalgebra of the pair $(\mathfrak{su}(4), \mathfrak{su}(2) \oplus \mathfrak{su}(2))$. We assume that the span of $\mathfrak{s}(n-1)$ is maximally Abelian in $\mathfrak{su}(2^{n-1})$ (easily verified for $\mathfrak{s}(2)$). We now show $\mathfrak{h}(n)$ is Abelian. Observe, it suffices to prove that all the elements of $\mathfrak{a}(n)$ commute. The commutation relations

$$\begin{aligned} [I_{nx}, A \cdot I_{nx}] &= 0, \quad A \in \mathfrak{s}(n-1), \\ [B \cdot I_{nx}, A \cdot I_{nx}] &= 0, \quad A, B \in \mathfrak{s}(n-1), \end{aligned}$$

and

$$[B, A \cdot I_{nx}] = 0, \quad A, B \in \mathfrak{s}(n-1),$$

suffice to show that $\mathfrak{a}(n)$ and $\mathfrak{s}(n)$ are Abelian too.

To show $\mathfrak{h}(n)$ is maximally Abelian in $\mathfrak{su}_{\mathfrak{m}}(2^n)$, we use induction again. Recall that

$$\mathfrak{su}_{\mathfrak{m}}(2^n) = \text{span}\{A \otimes I_x, A \otimes I_y, iI_{nx}, iI_{ny} | A \in \mathfrak{su}(2^{n-1})\},$$

and I_{nx} does not commute with I_{ny} , I_{nz} and $A \otimes I_y$, $A \otimes I_z$, where $A \in \mathfrak{su}(2^{n-1})$. The set $\mathfrak{s}(n-1) \cdot I_{nx}$ is maximally Abelian in $\mathfrak{su}(2^{n-1}) \otimes I_x$ (Because $\mathfrak{s}(n-1)$ is maximally Abelian in $\mathfrak{su}(2^{n-1})$ by assumption). Therefore the span of $\mathfrak{a}(n) = \{\pm i I_{nx}, A \cdot I_{nx} | A \in \mathfrak{s}(n-1)\}$ is maximally Abelian in $\mathfrak{su}_m(2^n)$ and the span of $\mathfrak{s}(n) = \{\mathfrak{a}(n), \mathfrak{s}(n-1) \otimes \mathbf{1}\}$ is maximally Abelian in $\mathfrak{su}(2^n)$. Hence the induction argument is complete.

The proof $\mathfrak{f}(n)$ is a Cartan subalgebra of the pair $(\overline{\mathfrak{su}_\mathbb{R}(2^n)}, \mathfrak{su}_{\mathbb{R}0}(2^n))$ follows exactly on same lines, and we leave it for the reader to verify it. **Q.E.D.**

Remark 6 We now show that we can generate any element of the Cartan Subalgebras $\mathfrak{h}(n)$ and $\mathfrak{f}(n)$, via the adjoint action of $SU(2^{n-1}) \otimes SU(2)$ on the coupling Hamiltonian $I_{(n-1)z} I_{nz}$. To be more precise, any element $Y \in \mathfrak{h}$ can be written as

$$Y = \sum_{j=1}^p \beta_j Ad_{K_j}(I_{(n-1)z} I_{nz}), \quad \beta_j \geq 0, \quad K_j \in SU(2^{n-1}) \otimes SU(2),$$

such that $Ad_{K_j}(I_{(n-1)z} I_{nz})$ all commute (elements of a Weyl orbit under the adjoint action of $SU(2^{n-1}) \otimes SU(2)$) and therefore

$$\exp(Y) = \prod_{j=1}^p K_j \cdot \exp(\beta_j I_{(n-1)z} I_{nz}) \cdot K_j^\dagger.$$

Lemma 3 Let $K = SU(2^{n-1}) \otimes SU(2)$, then the adjoint orbit $Ad_K(I_{(n-1)z} I_{nz})$ contains the sets $\mathfrak{s}(n-1) \otimes I_x$ and $\mathfrak{s}(n-1) \otimes I_z = \mathfrak{b}(n)$.

Proof: The proof is again inductive. Note by definition

$$\mathfrak{s}(n-1) \otimes I_z = \{\mathfrak{s}(n-2) \otimes \mathbf{1} \otimes I_z, \mathfrak{s}(n-2) \otimes I_x \otimes I_z, \pm i I_{(n-1)x} I_{nz}\}.$$

We assume that the statement of the lemma is true for $n-1$, i.e., if $H = SU(2^{n-2}) \otimes SU(2)$, then $Ad_H(I_{(n-2)z} I_{(n-1)z})$ contains the set $\mathfrak{s}(n-2) \otimes I_x$. Therefore the adjoint orbit $Ad_K(I_{(n-2)z} I_{(n-1)z} I_{nz})$ contains the set $\mathfrak{s}(n-2) \otimes I_x \otimes I_z$ (Apply H to $I_{(n-2)z} I_{(n-1)z}$ and don't do anything to last spin (qubit)!). Now observe for

$$U_1 = \exp(-i\pi I_{(n-2)z} I_{(n-1)y})$$

and

$$U_2 = \exp(i\frac{\pi}{2} I_{(n-1)y})$$

both belonging to K , we have

$$U_2 U_1 (I_{(n-1)z} I_{nz}) U_1^\dagger U_2^\dagger = I_{(n-2)z} I_{(n-1)z} I_{nz}.$$

Since the term $\pm i I_{(n-1)x} I_{nz}$ are present in adjoint orbit $Ad_K(I_{(n-1)z} I_{nz})$, (By selective $\frac{\pi}{2}$ rotation of $n-1$ qubit) we deduce that the adjoint orbit $Ad_K(I_{(n-1)z} I_{nz})$ contains the set

$$\mathfrak{a}(n-1) \otimes I_z = \{\mathfrak{s}(n-2) \otimes I_x \otimes I_z, \pm i I_{(n-1)x} I_{nz}\}.$$

Finally observe terms of the form $\mathfrak{s}(n-2) \otimes \mathbf{1} \otimes I_z$ can be produced by adjoint action of $K_1 = \exp(-i\pi I_{(n-1)x} I_{ny})$ on the set $\mathfrak{s}(n-2) \otimes I_x \otimes I_x$, which produces Hamiltonians of the form $\mathfrak{s}(n-2) \otimes \mathbf{1} \otimes I_z$. Thus we can generate the whole set $\mathfrak{s}(n-1) \otimes I_z$. That we can also generate $\mathfrak{s}(n-1) \otimes I_x$, is also obvious (by selective $\frac{\pi}{2}$ rotation of the n^{th} spin). **Q.E.D.**

Remark 7 Note that the Hamiltonian $\pm I_{nx}$ can be produced by selective excitation of the n^{th} qubit. Thus we can produce any Hamiltonian from the set $\{\mathfrak{s}(n-1) \otimes I_x, \pm I_{nx}\} = \mathfrak{a}(n)$. We have therefore shown that we can produce any Hamiltonian Y and Z belonging to the set $\mathfrak{a}(n)$ and $\mathfrak{b}(n)$ and as there positive span is the Cartan subalgebra $\mathfrak{h}(n)$ and $\mathfrak{b}(n)$ we can generate any Hamiltonian belonging to $\mathfrak{h}(n)$ and $\mathfrak{b}(n)$ by the adjoint action of the group $SU(2^{n-2}) \otimes SU(2)$ on the coupling Hamiltonian and we are done. We complete the inductive proof with the following lemma.

Lemma 4 Let $K = SU(4) \otimes SU(2)$, then the adjoint orbit $Ad_K(I_{2z}I_{3z})$ contains the sets $\mathfrak{a}(2) \otimes I_x = \mathfrak{s}(2) \otimes I_x$ and $\mathfrak{a}(2) \otimes I_z = \mathfrak{b}(3)$.

Proof: Recall

$$\begin{aligned}\mathfrak{a}(3) &= \pm i\{I_{3x}, I_{1x}I_{2x}I_{3x}, I_{1y}I_{2y}I_{3x}, I_{1z}I_{2z}I_{3x}\} \\ \mathfrak{b}(3) &= \pm i\{I_{1x}I_{2x}I_{3z}, I_{1y}I_{2y}I_{3z}, I_{1z}I_{2z}I_{3z}\}\end{aligned}$$

The result then follows from the following relations

$$\begin{aligned}\exp(-i\pi I_{1x}I_{2y}) \exp(-i\pi\alpha I_{2z}I_{3z}) \exp(i\pi I_{1x}I_{2y}) &= \exp(-i\pi\alpha I_{1x}I_{2x}I_{3z}) \\ \exp(-i\frac{\pi}{2}I_{1z}) \exp(-i\frac{\pi}{2}I_{2z}) \exp(-i\pi\alpha I_{1x}I_{2x}I_{3x}) \exp(i\frac{\pi}{2}I_{2z}) \exp(i\frac{\pi}{2}I_{1z}) &= \exp(-i\pi\alpha I_{1y}I_{2y}I_{3z}) \\ \exp(-i\frac{\pi}{2}I_{1y}) \exp(-i\frac{\pi}{2}I_{2y}) \exp(-i\pi\alpha I_{1x}I_{2x}I_{3x}) \exp(i\frac{\pi}{2}I_{2y}) \exp(i\frac{\pi}{2}I_{1y}) &= \exp(-i\pi\alpha I_{1z}I_{2z}I_{3z})\end{aligned}$$

which shows how to generate $\mathfrak{b}(3)$. Now terms in $\mathfrak{a}(2) \otimes I_x$ can be generated by selectively rotating the third spin. **Q.E.D.**

To review the ideas developed and to conclude the paper, let us explicitly work out the synthesis of any unitary propogator in a linearly scalar coupled three spin system.

Example 4 Consider three heteronuclear spin $\frac{1}{2}$ nuclei, coupled through scalar coupling . One has the ability to selectively excite each of the nuclei. Thus the system evolution in a suitable rotating frame is approximated by

$$\dot{U} = -i(H_d + \sum_{i=1}^6 u_i H_i)U, \quad (12)$$

where

$$\begin{aligned}H_d &= 2\pi J(I_{1z}I_{2z} + I_{2z}I_{3z}) \\ H_1 &= 2\pi I_{1x} \\ H_2 &= 2\pi I_{1y} \\ H_3 &= 2\pi I_{2x} \\ H_4 &= 2\pi I_{2y} \\ H_5 &= 2\pi I_{3x} \\ H_6 &= 2\pi I_{3y}\end{aligned}$$

Observe that the subgroup generated by $\{H_i\}_{i=1}^6$ is $SU(2) \otimes SU(2) \otimes SU(2)$. Thus any unitary propogator U can be decomposed as

$$U = K_1 \exp(-i(\beta_1 I_{1x} I_{2x} I_{3x} + \beta_2 I_{1y} I_{2y} I_{3x} + \beta_3 I_{1z} I_{2z} I_{3x} + \beta_4 I_{3x})) K_2$$

where

$$K_1 = P_1 \exp(-i(\alpha_1 I_{1x} I_{2x} I_{3z} + \alpha_2 I_{1y} I_{2y} I_{3z} + \alpha_3 I_{1z} I_{2z} I_{3z})) P_2$$

and

$$K_2 = P_3 \exp(-i(\gamma_1 I_{1x} I_{2x} I_{3z} + \gamma_2 I_{1y} I_{2y} I_{3z} + \gamma_3 I_{1z} I_{2z} I_{3z})) P_4,$$

where P_1, P_2, P_3, P_4 belong to $SU(4) \otimes SU(2)$, with $SU(4)$ denoting arbitrary transformation on spin 1 and 2 and $SU(2)$ representing selective local transformations on the spin I_3 .

Any element of $SU(4)$ can be produced by decoupling the spin I_3 (rapidly flipping the spin [5]) and then using the coupling $I_{1z} I_{2z}$ as in example 2. The Hamiltonians belonging to the Cartan subalgebra $\mathfrak{h}(3)$ and $\mathfrak{f}(3)$ can then be produced by using the coupling $I_{2z} I_{3z}$ as illustrated in lemma 4.

Remark 8 We have therefore demonstrated constructive controllability in a network of coupled spins. The crucial thing to note is that we have dealt with the worst case scenario. The case we have treated here is of a network of linearly coupled spins. There was no direct coupling between the n^{th} spin and say k^{th} spin for $k < n$ (In terms of quantum computing, if $k < n - 1$, we are not allowed to let k^{th} and n^{th} qubit interact with a two qubit gate directly). However interactions can be mediated through the other spins and this is what our constructive procedure is doing. It is also not difficult to see now that as long as we have a network of spins which is connected we have constructive controllability.

6 Conclusions and Future Work

Our main goal in this paper has been to put the design of quantum computers and pulse sequences in NMR on a geometrical footing. We have produced here a parameterization of the group $SU(2^n)$ in terms of unitary transformations produced by one and two qubit gates using successive Cartan decompositions of $SU(2^n)$. The first issue we would like to draw attention to is time optimality. We would like to emphasize that our constructive procedure of producing an arbitrary unitary transformation is only time optimal for the two spin case [27]. Recall that in the course of synthesizing a propagator almost all of the time is spent during the interaction of qubits and this corresponds to the two qubit gates or evolution of couplings during NMR. The one qubit operations can be produced relatively fast by external selective hard pulses. Thus from a practical viewpoint, it is of utmost importance that not only do we have a constructive procedure for synthesizing an arbitrary unitary transformation, but one which is time optimal to minimize the effects of decoherence which are always present. In [27], we developed the theory for time optimal control of spin systems and computed the time optimal control laws for two spin system (as in example 2) for any kind of coupling between the spins. The two spin case is special and elegant because $\frac{SU(4)}{SU(2) \otimes SU(2)}$ happens to be a Riemannian symmetric space. The results of time optimality for two spin systems do not extend in a natural way to higher spin systems as the coset space $\frac{SU(2^n)}{[SU(2)]^{\otimes n}}$ does not have a symmetric space structure. Finding time optimal control laws for spin networks with more than two spins will require and inspire further developments in geometric control theory.

Another question of imminent interest is – how to transform between different parameterizations of $SU(2^n)$. Suppose $U = SU(2)$, then we can express any element of $SU(2)$ in the following two ways

$$U = \exp(-i\alpha_1 I_x + \alpha_2 I_y + \alpha_3 I_z), \quad \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R} \quad (13)$$

$$U = \exp(-i\beta_1 I_x) \exp(-i\beta_2 I_y) \exp(-i\beta_3 I_x), \quad \beta_1, \beta_2, \beta_3 \in \mathbb{R}. \quad (14)$$

It is well known, how to transform between these and other ways of expressing an element of $SU(2)$. It will be very interesting to find the transformation that takes our description of $SU(2^n)$, which is in the same spirits as the last of the above descriptions, to the other standard parameterizations of $SU(2^n)$.

References

- [1] S. Kobayashi, and K. Nomizu. *Foundations of Differential Geometry Vol.1 and 2* (Interscience Publishers) (1969).
- [2] S. Helgason *Differential Geometry, Lie Groups, and Symmetric Spaces* (Academic Press) (1978).
- [3] J A. Wolf, *Spaces of Constant Curvature* (Publish or Perish, Inc., 1984).
- [4] V. Jurdjevic and H. J. Sussmann *Journal of Differential Equations* **12**, 313 (1972).
- [5] R. R. Ernst, G. Bodenhausen, A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Oxford University Press, Oxford, 1987).
- [6] S. J. Glaser, T. Schulte-Herbrüggen, M. Sieveking, O. Schedletzky, N. C. Nielsen, O. W. Sørensen and C. Griesinger, *Science* **280**, 421 (1998).
- [7] W. S. Warren, H. Rabitz, M. Dahleh, *Science* **259**, 1581 (1993).
- [8] N. A. Gershenfeld and I. L. Chuang, *Science* **275**, 350 (1997);
D. G. Cory, A. Fahmy, T. Havel, *Proc. Natl. Acad. Sci. USA* **94**, 1634 (1997).
- [9] T. Untidt, T. Schulte-Herbrüggen, B. Luy, S. J. Glaser, C. Griesinger, O. W. Sørensen and N. C. Nielsen, *Molecular Physics* **95**, 787 (1998);
T. Untidt, S. J. Glaser, C. Griesinger and N. C. Nielsen, *Molecular Physics* **96**, 1739 (1999).
- [10] J. Cavanagh, A. G. Palmer III, P. E. Wright, M. Rance, *J. Magn. Reson.* **91**, 429 (1991);
A. G. Palmer III, J. Cavanagh, P. E. Wright, M. Rance, *ibid.* **93**, 151 (1991);
L. E. Kay; *J. Am. Chem. Soc.* **115**, 2055 (1993);
M. Sattler, P. Schmidt, J. Schleucher, O. Schedletzky, S. J. Glaser and C. Griesinger, *J. Magn. Reson.* **B 108**, 235 (1995);
J. Schleucher, M. Schwendinger, M. Sattler, P. Schmidt, O. Schedletzky, S. J. Glaser, O. W. Sørensen and C. Griesinger, *J. Biomol. NMR* **4**, 30 (1994).
- [11] D. P. Weitekamp, J. R. Garbow, A. Pines, *J. Chem. Phys.* **77**, 2870 (1982), *ibid.* **80**, 1372 (1984);
P. Caravatti, L. Braunschweiler, R. R. Ernst, *Chem. Phys. Lett.* **100**, 305 (1983);
S. J. Glaser and J. J. Quant, in *Advances in Magnetic and Optical Resonance*, W. S. Warren, Ed. (Academic Press, New York, 1996), vol. 19, pp. 59-252.
- [12] O.W. Sørensen, G.W. Eich, M.H. Levitt, G.Bodenhausen and R.R. Ernst, *Progr. NMR Spectrosc.* **16**, 163 (1983).
- [13] G.W. Haynes and H. Hermes, *SIAM J. Control and Optimization* **8**, 450 (1970).
- [14] R.W. Brockett and Navin Khaneja, “Stochastic Control of Quantum Ensembles” *System Theory: Modeling, Analysis and Control* (Kluwer Academic Publishers, Inc., 1999).
- [15] Navin Khaneja, *Geometric Control in Classical and Quantum Systems* (Ph.d. Thesis, Harvard University, 2000).

- [16] R. S. Judson, K. K. Lehmann, H. Rabitz, W. S. Warren, *J. Mol. Struct.* **223**, 425 (1990).
- [17] T. Schulte-Herbrüggen *Aspects and Prospects of High-Resolution NMR* (Ph.d. Thesis, ETH Zurich, 1998).
- [18] P.W. Shor, “Algorithms for quantum computation: discrete log and factoring”, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (IEEE Computer Society Press, Los Alamitos, CA, 1994), p.124.
- [19] L.K. Grover, “Quantum mechanics helps in searching for a needle in a haystack” *Phys. Rev. Lett.* **79**, 325-328
- [20] D.Deutsch, “Quantum Computational networks”,*Proc. Roy. Soc. Lond.* **A425**, 73 (1989).
- [21] S.Lloyd, “Almost any quantum logic gate is universal”, *Phys. Rev. Lett.*, **75**, 346-349
- [22] A. Barenco, C.H. Bennett, R. Cleve, D.P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, “Elementary gates for quantum computation”, *Physical Review A*, **28**, 1996
- [23] D.P. DiVincenzo, “Two-bit gates are universal for quantum computation”, *Phys. Rev. A* **50**, 1015 (1995).
- [24] V. Ramakrishna, M.V. Salapaka, M. Dahleh, H. Rabitz, and A. Peirce, *Phys. Rev. A* **51**, 960 (1995)
- [25] G.M. Huang, T.J. Tarn, and J.W. Clark, *J. Math. Phys.* **24** , 2608 (1983)
- [26] Robert Gilmore, *Lie Groups, Lie algebras and Some of Their Applications*, (Wiley-Interscience, 1974).
- [27] Navin Khaneja, Roger Brockett, and Steffen. J. Glaser, “Time optimal control of spin systems”, quant-ph/0006114, *submitted to Physical Review A*.