Lie theory in Quantum Gates
Part I: Introduction to Lie theory by Daniel Son

The linear Lie Group $SU(4)$ describes a quantum gate with two channels. The goal of this paper is to understand the structure of this group. For the first half of the paper, we will review the definition of Lie Groups and Algebra which will lay down the foundation to understand the killing form. The killing form will provide a method to verify if a Cartan decompositon exists.

1 Lie groups and Lie Algebras

In this section, we introduce definition and facts to understand the nature of Lie groups and Lie algebras. The definitions and facts should be considered as motivations, and we will refrain from providing a full proof of the statments.

A **group** is defined to be a set equipped with a binary operation. For the set to be called a group, the binary operation must satisfy closure, associativity. A group must have an identity (i.e. $e \in G$ s.t. $ae = a$ for all $a \in G$), and a corresponding inverse for every group element, i.e. for all $a \in G$, there exists $a^{-1} \in G$ s.t. $aa^{-1} = e$.

We introduce the concept of a **group representation**. Crudely, a group representation can be considered as a matrix snapshot of each group element. [1] Let G be a group, and M_n be the group of all n by n matricies with complex entries. Formally, a map $\Gamma : G \to M_n$ is a representation if

$$\Gamma(a \cdot b) = \Gamma(a) \cdot \Gamma(b)$$

for all elements $a, b \in G$. The operation between the matricies are defined as the natural matrix multiplication. The representation preserves the group operation.

We have the tools to consider distances between two group elements. Let Γ be a representation with degree 2 of group G. Any two elements a, b in G will have a corresponding matrix in M_2. For simplicity, assume the representation maps the group elements to matrices with real entries. Write out the representations of a, b.

$$\Gamma(a) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad \text{and} \quad \Gamma(b) = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

The natural way to define the distance between two 2 by 2 matrices is to take the Euclidean distance by considering the matrix as a tuple of four numbers. [2]

$$d(\Gamma(a), \Gamma(b)) := \sqrt{(a_{11} - b_{11})^2 + (a_{12} - b_{12})^2 + (a_{21} - b_{21})^2 + (a_{22} - b_{22})^2}$$

.

[1] Refer to A.Zee p89

[2] If the matrix entries are complex, we can replace the difference of each entries with the modulus of the difference, e.g. $|a_{ij} - b_{ij}|^2$ instead of $(a_{ij} - b_{ij})^2$

We generalize this notion of distance to n by n matricies. Generalize Γ to be a representation of degree n. For group elements $a, b \in G$, define the **distance** between a, b as follows.

$$d(a,b) := \sqrt{\sum_{i,j}(a_{ij} - b_{ij})^2}$$

We finally have the tools to define a linear lie group. Let G be a group with a representation Γ. Suppose the degree of the representation is n. G is called a linear lie group if it satisfies the following three properties. [3]

(A) Parameterization around the identity

Let $C_\delta(I)$ be all the points in G that is within a distance δ from the identity. Call this the δ-ball around the identity. There must exist an injective mapping from the δ-ball to some tuple of real numbers, $\mathbb{R}^b$. Also, the identity matrix must correspond to the zero tuple. In symbols,

$$prm(\Gamma(E)) = prm(I_n) = (0, 0, \ldots, 0)$$

where map $prm : M_n \to \mathbb{R}^b$ is the parameterization function. E denotes the identity function in the lie group. The integer b is called the degree of the linear lie group.

(B) Dense Parameterization

Consider the space $\mathbb{R}^b$. The δ-ball in the group G will fall into some points in this space. The goal of this definition is to make the parameterization bijective for some domain.

There must exist some positive real number η in which the η-ball in the $\mathbb{R}^b$ centered at the zero tuple $(0, \ldots, 0)$ in which all points fall under the image of the δ-ball under the parameterization. In other words, for every point $(x_1, x_2, \ldots, x_b)$, there exists some point $A \in C_\delta(I)$ such that

$$prm(A) = (x_1, x_2, \ldots, x_b)$$

This implies that around some wierd neighborhood of some point in the linear Lie group, the parameterization to the real tuples are bijective.

(C) Analytic Parameterization

Now that there is a one-to-one correspondence betwen the real tuples and some complex matricies, we can consider a map from the real tuples to n by n matricies. We slightly abuse notation. Let

$$A = prm(g) = (x_1, x_2, \ldots, x_b)$$

Define

$$\Gamma(x_1, x_2, \ldots, x_b) = A$$

[3] Refer to Cornwell p36-37

A is an n by n matrix. Hence, each matrix element can be considered as separate. That is, for each entry we can define

$$\Gamma_{ij}(x_1, x_2, \ldots, x_b) = A_{ij}$$

We dictate that each of the Γ_{ij} must be analytic.

The linear Lie group can be better understood in conjunction with the corresponding Lie algebra. The correspondence between the Lie algebra and Lie groups are denoted by the matrix exponention. The matrix exponential is defined as

$$\exp(A) := I + A + \frac{A^2}{2!} + \cdots = \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

We list out some useful facts about matrix exponentials.

Facts

1. Let $\{\lambda_1, \ldots, \lambda_n\}$ be the set of eigenvalues of A, then the eigenvalues of $\exp(A)$ are $\{\exp(\lambda_1), \ldots, \exp(\lambda_n)\}$

2. The determinant of the matrix exponential is the expnential of the trace. In symbols,
$$\det(\exp(A)) = e^{tr(A)}$$
.

3. The exponential map is bijective and continuous around the identity.

4. $$\exp(A)\exp(-A) = I$$

5. (Campbell-Baker-Housdorff)

   Let A, B be two square matricies. Let the commutator be defined as

   $$[A, B] := AB - BA$$

   Suppose a square matrix C satisfies the following identity.

   $$\exp(A)\exp(B) = \exp(C)$$

   Then,
   $$C = A + B + \frac{1}{2}[A, B] + \frac{1}{12}([a, [a, b]] + [b, [b, a]]) \cdots$$

We continue our discourse to understand the correlation between linear Lie groups and Lie algebras. Suppose $A(t)$ to be a curve within the linear Lie group G. That is, the map A takes a real value t and maps it to some element in the G. Also, suppose that for any real values s, t,

$$A(s + t) = A(s)A(t)$$

It is straightforward to observe that $A(t)$ is an abelian group with an identity $E = A(0)$. Our goal is to identify a quintessential property of all such curves and to generate them.

We present the following theorem. [4]

Theorem All curves that converts scalar addition to matrix multiplication are characterized by the exponential map. In symbols,

$$A(t) = \exp(at) \quad \text{where} \quad a = \frac{d}{dt}A(t)$$

Proof. It is straightforward to see that given a matrix a, the exponential map generates a nice curve. Write the following.

$$A(t)A(s) = \exp(at)\exp(as) = \exp(a(t+s)) = A(t+s)$$

Now, take any nice curve $A(t)$. It suffices to show, that for all $t \in \mathbb{R}$,

$$A(t)\exp(-at) = I$$

Clearly, if t is zero, $A(0) = I$ and $\exp(-a0) = I$ so the equality holds.

The strategy is to take the derivative of the LHS with respect to t vanishes everywhere. Beforehand, consider the derivatinve of $A(t)$.

$$\frac{d}{dt}A(t) = \lim_{s\to 0}\frac{A(t+s) - A(t)}{s}$$

Since the curve is nice it is possible to factor out $A(t)$ from the first summand.

$$\lim_{s\to 0}\frac{A(t)(A(s) - A(0))}{s} = A(t)\left[\frac{d}{dt}A(t)\right]_{t=0} = aA(t)$$

Now take the desired derivative.

$$\frac{d}{dt}A(t)\exp(-at) = \left(\frac{d}{dt}A(t)\right)\exp(-at) + A(t)(-a)\exp(-at)$$

$$= aA(t)\exp(-at) - aA(t)\exp(-at) = 0$$

□

The theorem suggests that the derivatives of the linear Lie group around the identity generates the Lie group. The derivatives of the group around the identity form an algebra.

For now, we losely define the **Lie algebra** as a vector space of linear lie Groups equipped with a **Lie bracket**. The exponential map of the lie algebra generates the lie group. For square matricies, the lie bracket is defined as the commutator. Also, the common convention is to denote the Lie group with a capital letter such as G and the Lie algebra as a lower case letter $\mathfrak{g}$.

[4] Refer to Sternberg p234-235

Let $a, b \in \mathfrak{g}$. We list out a motivation for why the lie bracket of the two elements, $[a, b]$, must also be in the Lie algebra. For $\mathfrak{g}$ generates G by the exponential map,

$$\exp(at), \exp(bt) \in G$$

G is a group, and thus

$$\exp(at)\exp(bt) = \exp(C(t)) \in G$$

By the Campbell-Baker-Housdorff expansion, we can find an expression for $C(t)$.

$$C(t) = at + bt + \frac{1}{2}[at, bt] + O(t^3) = t\left(a + b + \frac{t}{2}[a, b] + O(t^2)\right)$$

Let $C(t) := C'(t)t$. The exponential of $C(t)$ is generated by $C'(t)$. For small enough t, we claim that the element

$$a + b + \frac{t}{2}[a, b]$$

must be in the subalgebra up to a leading term of t. By the closure of vector spaces, the lie bracket $[a, b]$ must be inside the lie algebra.

2 Structure Constants and Cartan Decomosition

We wish to use Cartan Decomposition in order to decompose the group $SU(4)$ into a direct sum of two subgroups. In order to obtain a decomposition, we will use Cartan Decomposition. The Cartan decomposition comes with nice properties, but to guarantee that a Lie group has a Cartan decomposition, we must understand structure constants and Killing forms.

Recall that a lie algebra is indeed a vector space. This means that the algebra must have a basis. Let $\mathfrak{g}$ be a lie algebra with basis vectors $X_1, X_2, \ldots X_n$.

Also, the Lie bracket is bilinear. That is,

$$[\alpha X + \beta Y, Z] = \alpha[X, Z] + \beta[Y, Z]$$

along with

$$[X, Y] = -[Y, X]$$

for any elements x, y, z in the algebra $\mathfrak{g}$ and any scalars α, β. [5]

These property imply that the lie bracket of any two elements in the algebra can be represented by the elements

$$[X_i, X_j] \quad \text{where} \quad i \neq j$$

[5] It is straightforward to check that this property holds for the typical commutator bracket $[X, Y] = XY - YX$

. Also the Lie bracket guarantees closure, and the Lie bracket of the basis elements must also be a linear combination of the basis. In symbols,

$$[X_i, X_j] = C_{ij}^1 X_1 + C_{ij}^2 X_2 \dots C_{ij}^n X_n = \sum_{k \leq n} C_{ij}^k X_k$$

So the n^3 coefficients C_{ij}^k entirely determine the behavior of the Lie bracket, and therefore determines the structure of the algebra. We call these coefficients the **structure coefficients**.

Now, we introduce the Killing form of the algebra. [6] Define a linear transform $L(Y)$ as follows.

$$L\{X_i, X_j\}(Y) := [X_i, [X_j, Y]]$$

For this transform is linear, it must have a matrix with respect to the base $\{X_1, \dots X_n\}$. To construct the matrix, apply the basis elements to the transform.

$$L\{X_i, X_j\}(X_c) = [X_i, [X_j, X_c]] = \left[X_i, \sum_s C_{jc}^s X_s\right]$$

Invoking bilinearity,

$$= \sum_s C_{jc}^s [X_i, X_s] = \sum_s \sum_r C_{jc}^s C_{is}^r X_r$$

Thus, the entry at the rth row and the cth column of the matrix of L will be

$$\sum_s C_{jc}^s C_{is}^r = \sum_s C_{is}^r C_{jc}^s$$

Define a scalar function B as follows. Also, invoke the previous result to directly compute B.

$$B(X_i, X_j) = tr(L\{X_i, X_j\}) = \sum_k L_{kk} = \sum_k \sum_s C_{is}^k C_{jk}^s$$

The function B also defines a square matrix. This matrix is called the killing form. Explicitly, the matrix is

$$\begin{bmatrix} B(1,1) & B(1,2) & \cdots & B(1,n) \\ B(2,1) & B(2,2) & \cdots & B(2,n) \\ \vdots & \vdots & \vdots & \vdots \\ B(n,1) & B(n,2) & \cdots & B(n,n) \end{bmatrix}$$

Without proof, we claim that if the determinant of the killing form is nonzero, then there exists a Cartan decomposition, which will be introduced in the second part.

[6] We present a complicated definition, but our interest is to apply the mathematical result, and hence we ignore the motivation behind the definition.

3 References

[1] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, "Geometric theory of nonlocal two-qubit operations," Physical Review A, vol. 67, no. 4, Apr. 2003, doi: https://doi.org/10.1103/physreva.67.042313.

[2] J. F. Cornwell, Group Theory in Physics. Academic Press, 1997.

[3] Shlomo Sternberg, Group theory and physics. Cambridge: Cambridge University Press, 2003.

[4] A. Zee, Group Theory in a Nutshell for Physicists. Princeton University Press, 2016.