Unitary groups

Hermitian inner product on $\mathbb{C}^n$

$$\langle x, y \rangle = \sum_{i=1}^{n} \bar{x}_i \cdot y_i$$

Unitary group: matrices A such that

$$\langle Ax, Ay \rangle = \langle x, y \rangle \qquad \forall x, y$$

Just preserve length?

$$\langle x+y, x+y \rangle = \langle A(x+y), A(x+y) \rangle$$

$$\langle x, x \rangle + \langle y, y \rangle + \langle x, y \rangle + \langle y, x \rangle = \langle Ax, Ax \rangle + \langle Ay, Ay \rangle + \langle Ax, y \rangle + \langle Ay, x \rangle$$

So $\langle Ax, y\rangle + \langle Ay, x\rangle = \langle x, y\rangle + \langle y, x\rangle$

Use $ix+y$ in place of $x+y$:

$$-i\langle Ax, y\rangle + i\langle Ay, x\rangle = -i\langle x, y\rangle + i\langle y, x\rangle.$$

If U is unitary, $U^*U = I \Rightarrow |\det(U)| = 1$.

Constructing unitary matrices

1) Use an orthonormal basis

2) If $H^* = -H$ (skew Hermitian) then $\exp(H)$ is unitary

3) If $H^* = -H$ and $H+I$ is invertible, then

$$U = (I+H)(I-H)^{-1}$$

Cayley transform

$(H = -(I-U)(I+U)^{-1})$

is unitary.

4) Diagonal, diagonal entries of norm 1.

5) reflections

$$\tau_{a,\alpha}(v) = v - (1-\alpha)\frac{\langle a, v\rangle}{\langle a, a\rangle} a$$

So $\tau(v) = v$ if $\langle a, v\rangle = 0$ and

$$\tau(a) = \alpha a$$

over $\mathbb{R}$,
take $\alpha = -1$

Claim: $\tau_{a,\alpha}$ is unitary if $|\alpha| = 1$

It's called a reflection if α has finite order.

If $|\alpha| = 1$ and P is a projection

$$((1-\bar{\alpha})P - I)((1-\alpha)P - I)$$

$$= (1-\bar{\alpha})(1-\alpha)P - (1-\bar{\alpha})P - (1-\alpha)P + I$$

but $(1-\bar{\alpha})(1-\alpha) = 2 - \alpha - \bar{\alpha}$ and therefore

$(1-\alpha)P - I$ is unitary.

Neighbourhood of identity in $U(n)$.

If $U = I + H$ then

$$I = U^*U = (I+H^*)(I+H) = I + H + H^* + HH^*$$

Hence $U \approx I$ then $H + H^* \approx 0$.

If $H + H^* = 0$, then $\exp(H)$ is unitary.

If $H^* = -H$ & $K^* = -K$, then

$$(HK - KH)^* = (-K)(-H) - (-H)(-K) = -(HK - KH)$$

If M & N are $n \times n$ matrices $MN - NM$ is their **Lie bracket**, denoted $[M, N]$.

A Lie algebra is a vector space V with a bilinear map $V \times V \to V$, denoted $[M, N]$ such that

(a) $[N, M] = -[M, N]$

(b) $[L, [M, N]] + [M, [N, L]] + [N, [L, M]] = 0$ Jacobi identity

$$\cancel{LMN} - \cancel{LNM} - \cancel{MNL} + \cancel{NML}$$
$$\cancel{MNL} - \cancel{MLN} - \cancel{NLM} + \cancel{LNM}$$
$$\cancel{NLM} - \cancel{NML} - \cancel{LMN} + \cancel{MLN}$$

e.g. square matrices with

$$[M, N] = [MN - NM]$$

A **derivation** on an algebra $\mathcal{A}$ is a linear map δ in $\mathrm{End}(\mathcal{A})$ such that

$$\delta(AB) = \delta(A)B + A\delta(B)$$

Note that

$$\delta(I) = \delta(I^2) = \delta(I)I + I\delta(I) = 2\delta(I)$$

$$\Rightarrow \delta(I) = 0.$$

Claim The set $D(\mathcal{A})$ of derivations of $\mathcal{A}$ is a Lie algebra.

Example: $\delta_A : M \mapsto AM - MA$ is a derivation on $\mathrm{Mat}_{n\times n}(\mathbb{C})$.

Claim If L is a Lie algebra, then

$$\exp(L) := \{\exp(M) : M \in L\}$$

is a group. (A Lie group.)

A better (not the official) definition is that a **Lie group** is a closed subgroup of $Mat_{n \times n}(\mathbb{C})$.

Gates A set of gates (for quantum computing) is set of unitary matrices that generates a dense subgroup Γ of $U(n)$.

What do want from Γ?

- given a unitary matrix U, a short expression for U as a product of gates.
- an algorithm for finding the expression.

Gates from controllable graphs

Let X be a graph on n vertices.

If $S \subseteq V(X)$ with characteristic vector z

then (X, S) is controllable if the walk matrix

$$M_S(X) = [z \;\; Az \; \cdots \; A^{n-1}z]$$

is invertible.

Theorem If $(X, \mathfrak{z})$ is controllable and $\mathfrak{z}$ is the characteristic vector of S, then the Lie algebra generated A & $\mathfrak{z}\mathfrak{z}^T$ is $Mat_{n\times n}(\mathbb{R})$.
The real Lie algebra generated by iA & $i\mathfrak{z}\mathfrak{z}^T$ is the algebra of a skew-Hermitian matrices.

Remark: if (X, S) is controllable, the matrices $A^i \mathfrak{z}\mathfrak{z}^T A^j$ $(0 \leq i, j \leq n-1)$ are a basis for $Mat_{n\times n}(\mathbb{R})$.

1-12-21

Proof (of theorem) Set $Z = \xi\xi^T$

We prove by induction on k that, for each k the Lie algebra $\mathfrak{L}$ generated by A & Z contains

$$A^{k-i} Z A^i, \qquad (i = 0, \dots, k)$$

There are integers c_r such that

$$Z A^r Z = c_r Z$$

We work through the cases $k = 0, 1, 2, 3$

$(k=0)$ $\quad Z$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ Z

$(k=1)$ If $Z \in \mathcal{L}$, so is $AZ - ZA$ and

$$[Z,[A,Z]] = Z(AZ-ZA) - (AZ-ZA)Z$$
$$= ZAZ - Z^2A - AZ^2 - ZAZ$$

Here $ZAZ = cZ$ and $Z^2 = |S|Z$. So $ZA + AZ \in \mathcal{L}$

Therefor AZ & $ZA \in \mathcal{L}$. $\qquad\qquad\qquad$ $AZ \quad ZA$

$(k=2)$ We have

$$A^2Z - AZA, \quad AZA - ZA^2 \Rightarrow A^2Z - ZA^2 \in \mathcal{L}$$

Then $[Z, A^2Z - ZA^2] = ZA^2Z - Z^2A^2 - A^2Z^2 + ZA^2Z$ and

so $A^2Z + ZA^2 \in \mathcal{L}$. Consequently, in $\mathcal{L}$ we have: A^2Z, AZA, ZA^2

$(k=3)$ $A^3Z - A^2ZA,\ A^2ZA - AZA^2,\ AZA^2 - ZA^3 \in \mathcal{L} \to A^3Z - ZA^3 \in \mathcal{L}$,

Hence we also have

$$[Z, A^3Z - ZA^3] = ZA^3Z - Z^2A^3 - A^3Z^2 + ZA^3Z \to A^3Z + ZA^3 \in \mathcal{L}.$$

T for $A^3Z \in \mathcal{L}$ $\longrightarrow$ $A^3Z,\ A^2ZA,\ AZA^2,\ ZA^3$

Lemma If (X,S) is controllable, the Lie algebra generated by iA & iZ is the Lie algebra of all skew-Hermitian matrices

Proof Define the degree of an element of $\mathcal{L}$ inductively

degree 0 : A, Z

1 : $[A, Z]$

$r+1$: $[A, X], [Z, X]$, $\deg(X) = r$

Commutators of even weight are symmetric, those of odd weight are skew-symmetric.

It follows that the even-weight subspace of $\mathfrak{L}$ consists of the real symmetric matrices, the odd-weights give the skew-symmetric matrices.

Consider the Lie algebra generated by iA & iZ. Even weights are skew-Hermitian, odd weights are real and skew-symmetric. So its the Lie algebra of skew Hermitian matrices

Theorem [Godsil, Severini] If (X, S) is controllable, and s, t are positive reals, the group G generated by

$$\exp(isA), \exp(itZ)$$

is a dense subgroup of $U(n)$.

Proof The closure of G is a Lie group and iA & iZ generate its tangent space...

Remark If $v \in V(X)$, then $(X, \{v\})$ is controllable if & only if $\phi(X,t)$ & $\phi(X \setminus v, t)$ are coprime.
So the end-vertices of paths are controllable.