Orthogonal decompositions of sl(n) and mutually unbiased bases

Alexey Bondal

September 20, 2011

1. Two independent sources for the problem:

Lie Theory (math):

Find (maximal number of) Cartan subalgebras in sl(n) pairwise orthogonal wrt Killing form

Quantum Info Theory and quantum mechanics (phys):

Mutually unbiased bases/ Discrete version of path integral (unitary version of the problem)

Orthogonal Cartan subalgebras:

Let L be a simple Lie algebra over $\mathbb{C}$, K the Killing form on L.

Def. 1 Two Cartan subalgebras H_1 and H_2 in L are said to be *orthogonal* if $K(h_1, h_2) = 0$ for all $h_1 \in H_1, h_2 \in H_2$.

Def. 2 Decomposition of L into direct sum of Cartan subalgebras $L = \oplus_{i=1}^{h+1} H_i$ is called *orthogonal decomposition* (OD) if $K(H_i, H_j) = 0$ for all $i \neq j$.

Introduced by **J.G.Thompson** in 1960.

Winnie-the-Pooh Conjecture(A.I. Kostrikin) A simple Lie algebra $sl(n)$ has an orthogonal decomposition iff $n = p^m$, p prime. (a wordplay in Milne's book in Russian translation).

Construction of solutions

Let $n = p$ prime number, P be the matrix of cyclic permutation, D the diagonal matrix $\mathrm{diag}(1, \xi, \ldots, \xi^{p-1})$, where $\xi^p = 1$, subject to relation:

$$DP = \xi PD.$$

Let $S_{k,l} = D^k P^l$. Consider (k,l) as an element of $\mathbb{F}_p^2$. Choose a line $\mathcal{L} \subset \mathbb{F}_p^2$. Take the linear span

$$H_{\mathcal{L}} = \langle S_{k,l} | \quad (0,0) \neq (k,l) \in \mathcal{L} \rangle$$

All $H_{\mathcal{L}}, \mathcal{L} \in \mathbb{F}_p\mathbb{P}^1$ are Cartan subalgebras , pairwise orthogonal.

We have **Orthogonal Decomposition**:

$$sl(p) = \oplus_{\mathcal{L} \in \mathbb{F}_p\mathbb{P}^1} H_{\mathcal{L}}$$

Examples for higher powers of p similar: tensor products of $S_{k,l}$.

Let $q = p^m$. Take a two dimensional plane $\mathbb{F}_q^2$. Consider it as a vector space over $\mathbb{F}_p$ of dimension $2m$. Endow it with a symplectic $\mathbb{F}_p$-valued form B.

$S_{k,l} = S_{k_1,\ldots,k_m;l_1,\ldots,l_m} = D^{k_1}P^{l_1} \otimes \cdots \otimes D^{k_m}P^{l_m}$

Choose a line $\mathcal{L} \subset \mathbb{F}_q^2$. It is Lagrangian with respect to B. Take the linear span

$$H_{\mathcal{L}} = \langle S_{k,l} | \quad (0,0) \neq (k,l) \in \mathcal{L} \rangle$$

We have **Orthogonal Decomposition**:

$$sl(q) = \oplus_{\mathcal{L} \in \mathbb{F}_q\mathbb{P}^1} H_{\mathcal{L}}$$

Any decomposition of $\mathbb{F}_p^{2m} \setminus 0$ into a disjoint union of Lagrangian subspaces (minus zero) will equally work.

Protocols of Quantum Information Transmission

Let $\mathcal{H} = \mathbb{C}^n$ with a fixed Hermitian metric. Bases $\{e_i\}$ and $\{f_j\}$ in $\mathcal{H}$ are mutually unbiased if, for all (i, j),

$$|\langle e_i, f_j \rangle|^2 = \frac{1}{n}$$

Choose an *observable*, a Hermitian operator, diagonal in the bases $\{e_i\}$, with distinct eigenvalues.

Measuring this observable for any *state* f_j returns us one of the eigenvalue with equal probability $\frac{1}{n}$.

If we have a protocol - a set of pairwise mutually unbiased bases - for quantum transmitting information, then eavesdropper will get no information if he use a wrong basis from the protocol for measuring a given state.

Generalized Hadamard matrices

Denote by H_0 the Cartan subalgebra of diagonal matrices. All Cartan subalgebras are conjugate. Hence, we can choose $H_1 = H_0$ and $H_2 = AH_0A^{-1}$ for some matrix A.

Def. Matrix $A = (a_{ij})$ is said to be *generalized Hadamard* if a_{ij} satisfy relations:

$$\sum_{j=1}^{n} \frac{a_{ij}}{a_{kj}} = 0. \qquad (1)$$

for all $i \neq k$.

Cartan subalg H_1 and H_2 are orthogonal iff A is generalized Hadamard. Complicated (very symmetric!) system of algebraic equations. Algebraic Geometry enter at this point.

Reduced Tempreley-Lieb algebras of graphs

A Cartan subalgebra in $sl(n)$ gives a set of minimal orthogonal projectors. If P and Q are projectors from the sets corresponding to two *orthogonal* Cartan subalgebras, then:

$$PQP = \frac{1}{n}P, \qquad QPQ = \frac{1}{n}Q.$$

Idea: view projectors as vertices of a graph. *Edges* are between vertices corresponding to projectors of *different* Cartan subalgebras; no edge for projectors in the same Cartan.

Γ a simply laced graph.

(Reduced) Temperley-Lieb algebra $B(\Gamma)$ is a *unital* algebra over $\mathbb{C}[r, r^{-1}]$ with generators x_v numbered by vertices v of Γ, subject to relations:

1. $x_v^2 = x_v$ for any $v \in \Gamma$,

2. $x_v x_w x_v = r x_v$, $x_w x_v x_w = r x_w$, if v, w are adjacent in Γ,

3. $x_v x_w = x_w x_v = 0$, otherwise.

$B^+(\Gamma)$ is the augmentation ideal.

Representations of $B^+(\Gamma)$.

Orthogonal decompositions are interpreted as low dimensional representations of $B^+(\Gamma)$ for particular graphs.

Assume Γ is connected. Then, ranks of projectors representing all x_v are the same. Define rank of representation to be the rank of any of the projectors.

We are interested in representations of rank 1. The dimension of an irreducible representation M of a given rank might vary. It is clear that:

$$\mathrm{dim} M \leq \mathrm{rank} M \cdot |\Gamma|$$

Γ a simply laced graph.

Hecke algebra of graphs $H(\Gamma)$: Generators: $\{T_v, v \in \Gamma\}$; relations:

$$T_v T_w T_v = T_w T_v T_w, \quad \text{if } (v, w) \text{ is an edge;} \tag{2}$$

$$T_v T_w = T_w T_v, \quad \text{otherwise;} \tag{3}$$

$$(T_v + 1)(T_v - q) = 0. \tag{4}$$

For the case Γ is A_n Dynkin graph, $H(\Gamma)$ is a q-deformation of the group algebra for S_{n+1}.

Algebra $B(\Gamma)$ is the quotient of Hecke algebra by relations:

$$-1 + T_v + T_w - T_vT_w - T_wT_v + T_vT_wT_v = 0, \quad \text{if } (v,w) \text{ edge;} \quad (5)$$

$$-1 + T_v + T_w - T_vT_w = 0; \quad \text{otherwise} \quad (6)$$

The homomorphism $H(\Gamma) \to B(\Gamma)$ is given by:

$$T_v \mapsto (q+1)x_v - 1$$

while r is related with q by the formula:

$$r = (q + 2 + q^{-1})^{-1}.$$

For the case Γ is A_n Dynkin graph, $B(\Gamma)$ is the matrix algebra of the standard n-dimensional representation of S_{n+1} (q is not a root of unity).

Poincare groupoid of a graph

Consider Γ as a topological 1-dimensional complex. Let $\mathcal{P}(\Gamma)$ be its *Poincare groupoid*, i.e. the category with vertices of Γ as objects and homotopy classes of paths between vertices in Γ as morphisms. Let $\mathbb{C}\mathcal{P}(\Gamma)$ be the the groupoid algebra of Poincare groupoid with basis consisting of elements in $\mathcal{P}(\Gamma)$.

Let e_v be a generator in $\mathbb{C}\mathcal{P}(\Gamma)$ corresponding to a constant path in $\mathcal{P}(\Gamma)$. Any *oriented* edge (ij) in Γ can be interpreted as a morphism in $\mathcal{P}(\Gamma)$, hence it gives an element l_{ij} in $\mathbb{C}\mathcal{P}_r(\Gamma)(= \mathbb{C}\mathcal{P}(\Gamma)$, if $r \neq 0)$. Defining relations are:

$$e_i e_j = \delta_{ij} e_i,\ e_i l_{jk} = \delta_{ij} l_{ik},\ l_{ij} e_k = \delta_{jk} l_{ik}, \tag{7}$$

$$l_{ij} l_{ji} = r e_i,\ l_{ji} l_{ij} = r e_j,\ l_{ij} l_{km} = 0, \text{ if } j \neq k. \tag{8}$$

Given an element Δ in an algebra A, consider a new *non-unital* algebra A_Δ. The same space as A, but new multiplication:

$$a \cdot_\Delta b = a \cdot \Delta \cdot b$$

There is a homomorphism $\phi : A_\Delta \to A$ given by:

$$\phi(a) = \Delta \cdot a$$

A_Δ is an A-bimodule.

Let $A = \mathbb{C}\mathcal{P}(\Gamma)$ and $\Delta = \sum e_i + r \sum l_{ij}$, then

$$A_\Delta = B^+(\Gamma).$$

Hence, a homomorphism:

$$\phi : B^+(\Gamma) \to \mathbb{C}\mathcal{P}(\Gamma)$$

Representations

ϕ gives a pair of adjoint functors:

$$\mathrm{mod} - \phi : B^{+}(\Gamma) \rightleftarrows \mathrm{mod} - \mathbb{C}\mathcal{P}(\Gamma)$$

Let V be an irrep of $B(\Gamma)$, adjunction gives:

$$0 \to K \to B^{+}(\Gamma) \otimes_{B(\Gamma)} V \to V \to 0$$

with the kernel K a trivial representation of $B^{+}(\Gamma)$.

A rep of $\mathbb{C}\mathcal{P}(\Gamma)$ is a set of vector spaces U_v and maps $U_v \to U_w$, for any *oriented* edge of Γ, inverse for the opposite orientation of the same edge.

$\mathrm{Rep} - \mathbb{C}\mathcal{P}(\Gamma) \cong \ \mathrm{Rep} - \pi_1(\Gamma)$

Homological properties of representations

Harmonic analysis on graphs

Graphs are discrete models of Riemannian manifolds.

{**Functions**} = {functions on vertices of Γ}

{**Bundles with flat connections**} = { reps of $\mathbb{C}\mathcal{P}(\Gamma)$}

Laplace operator on a graph is an element in $\mathbb{C}\mathcal{P}(\Gamma)$:

$$L = \sum l_{ij} + N$$

where N is the valency operator:

$$N = \sum_{v \in \Gamma} N_v e_v, \quad N_v \text{ the valancy of } v.$$

If Γ is a regular graph, then N is scalar.

Problem: Given a (regular) graph, find representations with minimal polynomial of Laplace operator to be of degree $\leq$ the length of the minimal cycle in the graph.

Finite number of possible variants for minimal polynomials if the rank of rep is fixed.

For $\Gamma_2(n)$, the minimal polynomial is $(\sum l_{ij})^2 = n \cdot 1$.

Interpretation in terms of higher polars

Consider the vector space $V = \mathbb{C}^n$; n coord. y_i's, one relation:

$$\sum y_i = 0$$

Consider the pencil of quartics in V given by:

$$f(y) = f_{\lambda,\mu}(y) = \lambda \sum y_i^4 + \mu \prod y_{i_1} y_{i_2} y_{i_3} y_{i_4}$$

Let $s \in V$. Define the polar of g at s by:

$$\mathsf{P}_s(f) = \sum s_i \frac{\partial g}{\partial y_i}$$

The equations for the first 3 columns of $n \times n$ generalized Hadamard matrix give the locus of triples $s, t, u \in V$ satisfying:

$$\mathsf{P}_s \mathsf{P}_t \mathsf{P}_u(f) \equiv 0$$

A 4-dimensional family for sl(6)

Theorem (joint with I. Zhdanovskiy) There exists a 4-dimensional family of orthogonal pairs of Cartan algebras in $sl(6)$.