Hadamard matrices and Compact Quantum Groups

Uwe Franz

18 février 2014
3ème journée FEMTO-LMB

based in part on joint work with:
Teodor Banica, Franz Lehner, Adam Skalski

Quantum mechanics

If we measure on a quantum system described by the Hilbert space $\mathcal{H}$ and the state vector $\psi \in \mathcal{H}$ (with $||\psi|| = 1$) the observable corresponding to the self-adjoint operator X with spectral decomposition

$$X = \sum_{\lambda \in \sigma(X)} \lambda E_\lambda,$$

then we observe λ with probability

$$P(\text{“}X = \lambda\text{”}) = ||E_\lambda \psi||^2.$$

After the experiment, if we observed λ, the state vector is

$$\frac{E_\lambda \psi}{||E_\lambda \psi||}.$$

Mutually Unbiased Bases (MUB)

Definition

A family $\{B_k = \{e_1^{(k)}, \ldots, e_n^{(k)}\}; k = 1, \ldots, r\}$ of orthonormal bases is called mutually unbiased, if

$$\left|\langle e_i^{(k)}, e_j^{(\ell)}\rangle\right| = \frac{1}{\sqrt{n}}$$

for $k \neq \ell$, $i, j = 1, \ldots, n$.

If $n = p^k$ is a power of a prime number, then there exist $n+1$ mutually unbiased bases for $\mathbb{C}^n$.

Open Problem

Determine the maximal number of mutually unbiased bases, if n is not a power of a prime number. Still open even for $n = 6$.

Definition

A (complex) Hadamard matrix is a matrix $H = (h_{jk}) \in M_n(\mathbb{C})$ such that

(i) $|h_{jk}| = 1$ for all $1 \leq j, k \leq n$;

(ii) $\frac{1}{\sqrt{n}} H$ is unitary.

Hadamard matrices (the real ones) are defined as above, but with $h_{jk} \in \{-1, +1\}$. They exist only for $n = 2$ and n a multiple of 4.

Open Problem

Does there exists a Hadamard matrix (real!) of order $n = 4k$ for all $k \in \mathbb{N}$?

Wikipedia: As of 2008, there are 13 multiples of 4 less than or equal to 2000 for which no Hadamard matrix of that order is known. They are: 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, and 1964.

Hadamard matrices

Example

For any integer $n \geq 1$, the Fourier matrix

$$F_n = \left(\omega_n^{(j-1)(k-1)}\right)$$

with $\omega_n = \exp\left(\frac{2\pi i}{n}\right)$, defines a Hadamard matrix,

Example

If $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_n\}$ are two MUB, then

$$H = \sqrt{n} \begin{pmatrix} \langle e_1, f_1\rangle & \langle e_1, f_2\rangle & \cdots & \langle e_1, f_n\rangle \\ \langle e_2, f_1\rangle & \langle e_2, f_2\rangle & \cdots & \langle e_2, f_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle e_n, f_1\rangle & \langle e_n, f_2\rangle & \cdots & \langle e_n, f_n\rangle \end{pmatrix}$$

is a Hadamard matrix.

Hadamard matrices

- Complex Hadamard matrices play an important role in quantum information, subfactor theory, and in connection to many other aspects in combinatorics, representation theory, and mathematical physics.
- Question by Jones (1999): Does there exist an "efficient" way to compute the "invariants" of a complex Hadamard matrix?
- Banica showed that one can associate a compact quantum group $\mathbb{G}$ to any Hadamard matrix ($\rightarrow$ Hopf image), in such a way that Jones' "invariants" are equal to the moments of the trace of the fundamental corepresentation of $\mathbb{G}$,

$$c_m = \int_{\mathbb{G}} \big(\mathrm{Tr}\rho(g)\big)^m \mathrm{d}g.$$

Classification for $n \leq 5$

Definition

Two Hadamard matrices H_1, H_2 are called equivalent, if one can be obtained from the other by

1. permuting rows or columns;
2. multiplying rows or columns by a complex number of modulus one.

We write $H_1 \cong H_2$.

A Hadamard matrix is called dephased, if the first row and the first column consist of 1's.

Theorem (Haagerup, 1997)

(a) For $n = 1, 2, 3, 5$, all Hadamard matrices are equivalend to a Fourier matrix.

(b) All 4×4 Hadamard matrices are equivalent to a matrix of the form

$$H_4^q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & q & -q \\ 1 & -1 & -q & q \end{pmatrix}$$

with $|q| = 1$.

For $n \geq 6$, many inequivalent Hadamard matrices are known, but their classification is a hard open problem, even for $n = 6$ or n a prime number ≥ 7.

Let A be a C^*-algebra over $\mathbb{C}$.

Definition

(a) A square matrix $u \in M_n(A)$ is called magic, if all its entries are projections and each row or column sums up to 1.

(b) The free permutation quantum group $C(S_n^+)$ is the universal C^*-algebra generated by the entries of a $n \times n$ magic square matrix $u = (u_{jk})$. It is a compact quantum group (or Woronowicz C^*-algebra) with the coproduct

$$\Delta : C(S_n^+) \to C(S_n^+) \otimes C(S_n^+)$$

determined by $\Delta(u_{jk}) = \sum_{\ell=1}^{n} u_{j\ell} \otimes u_{\ell k}$.

Definition

(c) A matrix compact quantum group (A, v) with fundamental unitary corepresentation $v = (v_{jk}) \in M_n(A)$ is called a quantum permutation group, if the map

$$\pi : C(S_n^+) \to A, \qquad \pi(u_{jk}) = v_{jk}$$

extends to a surjective C^*-Hopf algebra morphism (or morphism of compact quantum groups), i.e. (A, v) is a sub quantum group of $(C(S_n^+), u)$.

For $n = 1, 2, 3$, $C(S_n^+)$ is commutative and $C(S_n^+) \cong C(S_n)$, i.e. S_n^+ is isomorphic to the permutation group S_n.

For $n \geq 4$, $C(S_n^+)$ is noncommutative and $\dim C(S_n^+) = \infty$, i.e. there exist (infinitely many!) genuine "quantum permutations".

The quantum permutation group of a Hadamard matrix

If $H \in M_n(C)$ is a Hadamard matrix and

$$\xi_{jk} = \left(\frac{h_{j\ell}}{h_{k\ell}}\right) \in \mathbb{C}^n$$

then $\{\xi_{j1}, \ldots, \xi_{jn}\}$ and $\{\xi_{1j}, \ldots, \xi_{nj}\}$ are o.n.b.'s of $\mathbb{C}^n$ for all $j = 1, \ldots, n$.

Therefore the orthogonal projections P_{jk} onto $\mathbb{C}\xi_{jk}$ form a magic square

$$P = (P_{jk}) \in M_n\big(B(\mathbb{C})\big) \cong M_n \otimes M_n$$

and

$$\pi_H : C(S_n^+) \to M_n(\mathbb{C}), \qquad \pi_H(u_{jk}) = P_{jk},$$

defines a representation of $C(S_n^+)$

Definition

The quantum permutation group $\mathbb{G}_H$ associated to a Hadamard matrix H is the smallest compact quantum group such that we have a factorization

$$\begin{tikzcd} C(S_n^+) \arrow[r, "\pi_H"] \arrow[d, "\pi"'] & M_n(\mathbb{C}) \\ C(\mathbb{G}_H) \arrow[ur, "\rho"'] & \end{tikzcd}$$

where $\pi : C(S_n^+) \to C(\mathbb{G}_H)$ is a C^*-Hopf algebra morphism and $\rho : C(\mathbb{G}_H) \to M_n(\mathbb{C})$ a representation.

What is known

Theorem (Banica, Bichon, Schlenker, 2009)

The following are equivalent:

(i) $C(\mathbb{G}_H)$ is commutative;

(ii) $C(\mathbb{G}_H)$ is cocommutative;

(iii) $\mathbb{G}_H \cong \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k}$ for some $n_1, \ldots, n_k$;

(iv) $H \cong F_{n_1} \otimes \cdots \otimes F_{n_k}$ for some $n_1, \ldots, n_k$.

Theorem (Banica, F, Skalski)

Let

$$\varphi = \mathrm{tr} \circ \pi_H \quad \text{and} \quad \tilde{\varphi} = \lim_{n\to\infty} \frac{1}{n} \sum_{m=0}^{n-1} \varphi^{\star m}.$$

Then $\tilde{\varphi}$ is equal to the "Haar" idempotent state on $C(S_n^+)$ induced by the Haar state of $C(\mathbb{G}_H)$ and we can construct $C(\mathbb{G}_H)$ as the quotient of $C(S_n^+)$ by the null space of $\tilde{\varphi}$,

$$C(\mathbb{G}_H) \cong C(S_n^+)/N_{\tilde{\varphi}}, \quad N_{\tilde{\varphi}} = \{a \in C(S_n^+) : \tilde{\varphi}(a^* a) = 0\}.$$

Computing the invariants

Corollary (Banica, F, Skalski)

Let

$$\begin{aligned} T_m &= \big(\varphi(u_{j_1k_1}\cdots u_{j_mk_m})\big) \\ &= \mathrm{tr}(P_{j_1k_1}\cdots P_{j_mk_m}) \\ &= \langle \xi_{j_1k_1}, \xi_{j_2k_2}\rangle\langle \xi_{j_2k_2}, \xi_{j_3k_3}\rangle\cdots\langle \xi_{j_mk_m}, \xi_{j_1k_1}\rangle \in M_{n^m}, \end{aligned}$$

then we have

$$c_m = \dim\big(\ker(T_m - \mathrm{id})\big)$$

Franz Lehner wrote a program that computes these dimensions (for "small" m).

Classification for $n = 4$

Consider

$$H_4^q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & q & -q \\ 1 & -1 & -q & q \end{pmatrix}$$

with $|q| = 1$.

Theorem (Banica& Bichon, F)

The quantum permutation group $\mathbb{G}_q$ of H_q is

- $O_{-1}(2) \cong \mathbb{Z}_2 \wr_* \mathbb{Z}_2$, if $\mathrm{ord}(q) = \infty$;
- a "Zakrzewski twist" of the dihedral group D_{2n}, if $\mathrm{ord}(q^4) = n$

Classification for $n = 4$

Examples

- if $q = \pm 1$: $\mathbb{G}_q = \mathbb{Z}_2 \times \mathbb{Z}_2$;
- if $q = \pm i$; $\mathbb{G}_q = \mathbb{Z}_4$;
- if $q \notin \{\pm 1, \pm i\}$, then $\mathbb{G}_q$ is non-commutive, non-cocommutative,
  - if $\mathrm{ord}(q) = 4n$, then $\mathbb{G}_q \cong DC_n^{-1}$,
  - if $\mathrm{ord}(q) = n$ or $2n$, then $\mathbb{G}_q \cong D_{2n}^{-1}$.

DC_n^{-1} and D_{2n}^{-1} are twists of the dicyclic and dihedral groups, they were constructed by Nikshych in 1998.

References

- Teodor Banica and Julien Bichon, Quantum groups acting on 4 points, Journal für die reine und angewandte Mathematik (Crelle's Journal) 626, 75-114, 2009.
- Teodor Banica, Quantum permutations, Hadamard matrices, and the search for matrix models, arXiv:1109.4888, 2011.
- Teodor Banica, Uwe Franz, Adam Skalski, Idempotent States and the Inner Linearity Property, Bull. Polish Acad. Sci. Math. 60, 123-132, 2012.
- Teodor Banica and Julien Bichon, Quantum invariants of deformed Fourier matrices, arXiv:1310.6278, 2013.