Quantum logic and computability of noncommutative sums of squares

Tobias Fritz

August 2017

Overview

Main messages:

- Advertise complexity theory as a tool for proving nonconstructive existence results.
- I will use it to prove that there exist finite configurations of subspaces of a Hilbert space that can only be realized in infinite dimensions.

Propositional Logic

- Propositional variables $p, q, \ldots$
- Connectives $\vee, \wedge, \neg$.
- We suggestively write $p^\perp$ instead of $\neg p$.
- Semantics in Boolean algebras, satisfying in particular the law of excluded middle,

$$p \vee p^\perp = 1,$$

De Morgan duality,

$$(p \wedge q)^\perp = p^\perp \vee q^\perp, \qquad (p \vee q)^\perp = p^\perp \wedge q^\perp,$$

and distributivity,

$$(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r).$$

Distributivity of $\vee$ over $\wedge$ is automatic.

Example

The projections in a commutative von Neumann algebra form a Boolean algebra,

$$p \wedge q := pq, \qquad p^{\perp} := 1 - p,$$

and $p \vee q$ defined via De Morgan duality.

Theorem

The Boolean algebras that arise in this way are precisely the complete Boolean algebras.

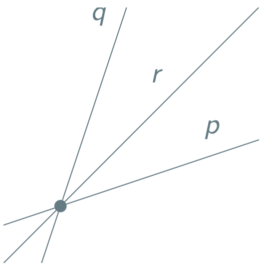
In a *noncommutative* von Neumann algebra, projections still form a lattice,

$$p \wedge q := \sup \{ \, r \mid r \leq p, \; r \leq q \, \},$$
$$p \vee q := \inf \{ \, r \mid r \geq p, \; r \geq q \, \},$$

and De Morgan duality still holds with $p^{\perp} := 1 - p$. Excluded middle holds as well, $p \vee p^{\perp} = 1$.

In the case of $\mathcal{B}(\mathcal{H})$, it helps to identify projections with closed subspaces.

Distributivity fails already in $M_2(\mathbb{C})$:



But the lattice still enjoys the weaker property of **orthomodularity**:

$$\text{If } p \leq q, \text{ then } p \vee (p^{\perp} \wedge q) = q.$$

In an **orthomodular lattice**, the complementation $p \mapsto p^{\perp}$ is not determined by $\leq$ and therefore an extra part of structure.

But the projection lattices of von Neumann algebras are a very special kind of orthomodular lattice! Many sophisticated equations have been discovered.

To give one concrete example:[1]

Theorem

If $a \perp b$, $c \perp d$ and $e \perp f$, then

$$(a \vee b) \wedge (c \vee d) \wedge (e \vee f) \leq b \vee (a \wedge (c \vee (((a \vee c) \wedge (b \vee d)) \wedge (((a \vee e) \wedge (b \vee f)) \vee ((c \vee e) \wedge (d \vee f))))))$$

What I will show is that classifying these 'laws of noncommutative logic' is impossible (in a precise sense).

[1] Norman D. Megill and Mladen Pavičić. *Equations and State and Lattice Properties That Hold in Infinite Dimensional Hilbert Space*. arXiv:quant-ph/0009038.

Satisfiability

To study the complexity of these projection lattices, let's look at some associated decision problems.

Definition

A system of atomic formulas $F_1, \dots, F_n$ in the signature $(\vee, \wedge, {}^\perp, =)$ is *(commutatively) unsatisfiable* if

$$F_1 \text{ and } \dots \text{ and } F_n \text{ implies } 0 = 1$$

holds for projections in every (commutative) von Neumann algebra.

Example

The system

$$p \vee q = 1, \qquad p \vee q^\perp = 1, \qquad p^\perp \vee q = 1, \qquad p^\perp \vee q^\perp = 1$$

is satisfiable, but not commutatively satisfiable.

Lemma

A system is

- commutatively satisfiable if and only if it is has a solution in $\mathbb{C}$.
- satisfiable if and only if it has a solution in $\mathcal{B}(\mathcal{H})$ for infinite-dimensional separable $\mathcal{H}$.

This makes commutative satisfiability Turing decidable: it is enough to check all truth assignments in $\{0, 1\}$. (This also shows it to be in NP.)

However,[2]

Theorem

Satisfiability is undecidable.

Intuitively, this says that the structure of closed subspaces of $\mathcal{B}(\mathcal{H})$ is very intricate. I do not even know whether the problem is semi-decidable!

---

[2] Tobias Fritz. *Quantum logic is undecidable*. arXiv:1607.05870; Albert Atserias, Phokion G. Kolaitis, and Simone Severini. *Generalized Satisfiability Problems via Operator Assignments*. arXiv:1704.01736.

A system of the form

$$p_1 \vee \ldots \vee p_n = 1, \qquad p_i \leq p_j^{\perp} \quad \forall i \neq j$$

expresses the constraint that the $p_1, \ldots, p_n$ should form a **partition of unity**,

$$\sum_{i=1}^{n} p_i = 1.$$

We form a subclass of satisfiability problems by considering partition of unity relations only, which are amenable to an algebraic treatment.

A set of such relations is determined by a **hypergraph** $H = (V, E)$ consisting of

- a set of vertices V indexing the variables p_v, $v \in V$;
- a set of edges $E \subseteq 2^V$ indexing the partition of unity relations

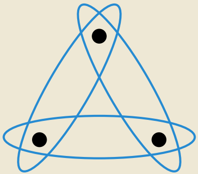
$$\sum_{v \in e} p_v = 1.$$

---

[2] Antonio Acín, Tobias Fritz, Anthony Leverrier, and Ana Belén Sainz, *A Combinatorial Approach to Nonlocality and Contextuality*, arXiv:1212.4084.

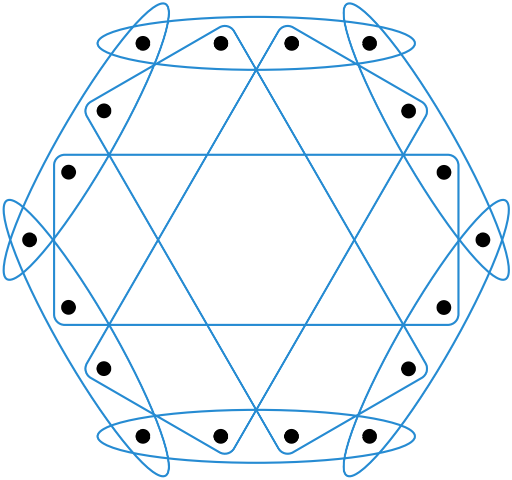
Example

The hypergraph



does not have any representations (in positive dimension), i.e. the associated satisfiability problem is unsatisfiable.

Many hypergraphs are known which only have noncommutative representations. Here is one of the simpler ones[3]:



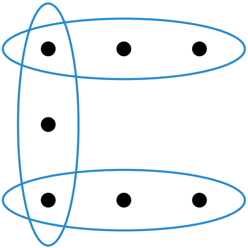
[3] Adán Cabello, José Estebaranz, and Guillermo García-Alcaine. *Bell-Kochen-Specker theorem: a proof with* 18 *vectors*. arXiv:quant-ph/9706009.

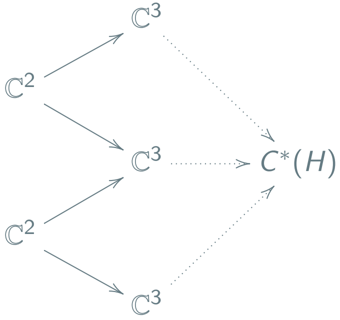
Definition

The *hypergraph C*-algebra* associated to a hypergraph $H = (V, E)$ is

$$C^*(H) := \left\langle (p_v)_{v \in V} \;\middle|\; p_v = p_v^* = p_v^2,\ \sum_{v \in e} p_v = 1 \right\rangle$$

The hypergraph C*-algebras are precisely those C*-algebras that are finite colimits of finite-dimensional commutative C*-algebras. For example:





Question

Given a hypergraph H, does it have a representation in $\mathcal{B}(\mathcal{H})$? Or is $C^*(H) = 0$?

We have previously studied this and related questions from a graph-theoretic perspective[4] and conjectured it to be undecidable, which we can now prove:

Theorem

There is no algorithm to answer this question for any given H.

This proves in particular the undecidability of noncommutative logic.

This theorem is a corollary of a recent result in combinatorial group theory due to Slofstra[5].

---

[4] Antonio Acín et al. *A Combinatorial Approach to Nonlocality and Contextuality*. arXiv:1212.4084.

[5] William Slostra. *Tsirelson's problem and an embedding theorem for groups arising from non-local games*. arXiv:1606.03140.

Slofstra's Theorem

The following class of groups plays an important role:[6]

Definition

Let $Ax = b$ be a system of linear equations over $\mathbb{Z}_2$ with $A \in \mathbb{Z}_2^{m \times n}$. The associated *solution group* is the finitely presented group with generators $x_1, \ldots, x_n$ and a central element J such that

- $x_k^2 = 1$ for all k, and $J^2 = 1$,
- x_k and x_ℓ commute if they appear jointly in one equation of the system,
- Every equation k holds in the multiplicative form $\prod_\ell x_\ell^{A_{k\ell}} = J^{b_\ell}$.

Then Slofstra has shown in particular that:

Theorem

- Every finitely presented group embeds into a solution group.
- Determining whether $J \neq 1$ is undecidable.

---

[6] Richard Cleve, Li Liu, and William Slofstra. *Perfect Commuting-Operator Strategies for Linear System Games*. arXiv:1606.02278.

Sums of squares, anywhere?

Let's switch gears a bit and consider an arbitrary Archimedean quadratic module generated by noncommutative polynomials $r_1, \ldots, r_m \in \mathbb{C}\langle x_1, \ldots, x_n \rangle$,

$$Q(\underline{r}) = \left\{ \sum_j \sum_i w_{ij}^* r_j w_{ij} + \sum_i v_i^* v_i \right\}.$$

Lemma

Determining whether a given $f \in \mathbb{C}\langle \underline{x} \rangle$ is of this form with the degrees of w_{ij} and v_i at most n is a semidefinite program.

Letting n increase shows that membership in $Q(\underline{r})$ is semi-decidable: if $f \in Q(\underline{r})$, then these semidefinite programs will eventually detect this.

We also equip $\mathbb{C}\langle \underline{X} \rangle$ with the seminorm

$$\|f\| := \sup_{\underline{a} \in \mathcal{B}(\mathcal{H}) \mid \underline{r}(\underline{a}) \geq 0} \|f(\underline{a})\|.$$

This completes to a C*-algebra $C^*(\underline{x}|\underline{r})$, the universal unital C*-algebra with generators $\underline{x}$ and positivity relations $\underline{r}$. The semidefinite programs above give a convergent sequence of upper bounds on $\|f\|$.[7]

Definition

A C*-algebra A is *residually finite-dimensional* if

$$\|a\| = \sup_{d} \sup_{\pi : A \to M_d} \|\pi(a)\|$$

for every $a \in A$.

In the case of $C^*(\underline{x}|\underline{r})$, it is enough to check this on polynomials,

$$\|f\| \stackrel{?}{=} \sup_{d} \sup_{\underline{a} \in M_d \mid \underline{r}(\underline{a}) \geq 0} \|f(\underline{a})\|.$$

[7] Konrad Schmüdgen. *Non-commutative Real Algebraic Geometry - Some Basic Concepts and First Ideas*. arXiv:0709.3170.

We can also obtain lower bounds the norm by considering increasing d and computing

$$\sup_{\underline{a} \in M_d \mid \underline{r}(\underline{a}) \geq 0} \|f(\underline{a})\|.$$

Thanks to real quantifier elimination, there is an actual algorithm to do this.

If $C^*(\underline{x}|\underline{r})$ is residually finite-dimensional, then this sequence of lower bounds converges to the actual norm. Hence we have proven:[8]

Proposition

If $C^*(\underline{x}|\underline{r})$ is residually finite-dimensional, then its norm is computable.

[8] Tobias Fritz, Tim Netzer, and Andreas Thom. *Can you compute the operator norm?* arXiv:1207.0975.

Proposition

If $C^*(\underline{x}|\underline{r})$ is residually finite-dimensional, then its norm is computable.

Why is this interesting?

One reason is the group algebra case: for a finitely presented group G, the computability of $\|\cdot\|$ on $C^*(G)$ implies solvability of the word problem.

$\Rightarrow$ For G with unsolvable word problem, there are no computable bounds on the degrees of the polynomials in sum of squares representations.

Another reason is the relation with Connes' Embedding Problem:[9]

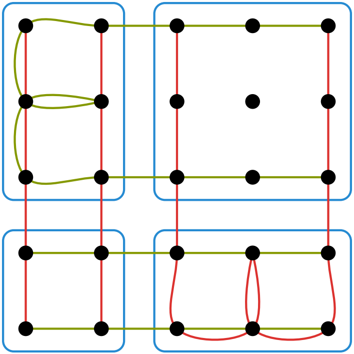
Theorem

Connes' Embedding Problem $\Leftrightarrow$ $C^*(\mathbb{F}_2 \times \mathbb{F}_2)$ residually finite-dimensional.

---

[9] Eberhard Kirchberg. *On nonsemisplit extensions, tensor products and exactness of group C^*-algebras.* Invent. Math. 112(3), 449–489 (1993).

Changing the group $\mathbb{F}_2$ e.g. to $PSL_2(\mathbb{Z})$ results in an equivalent question, and then we get a hypergraph C*-algebra:



So can we say something about the residual finite-dimensionality of hypergraph C*-algebras in general?

Corollary

- There is H such that $C^*(H)$ is not residually finite-dimensional.
- In fact, determining whether a given H is of this type is also undecidable.

Proof.

It is enough to prove the second statement. If there was such an algorithm, then we could use it to determine whether $C^*(H) \neq 0$: yes if it is not RFD; otherwise, use previous algorithm to compute $\|1\|$. □

In a similar vein:

Corollary

- There is H which has *only* infinite-dimensional representations.
- In fact, determining whether a given H is of this type is also undecidable.

What would be a concrete example?

Theorem

For each of the following properties, it is undecidable to determine whether a given hypergraph enjoys the property:

- H has a representation;
- H has only infinite-dimensional representations;
- $C^*(H)$ is residually finite-dimensional.

This suggests that many properties of $C^*(H)$ are undecidable, which is reminiscent of the Adian–Rabin theorem: "All nontrivial properties of finitely presented groups are undecidable." Is there a similar theorem in this context?