Holant problems and quantum information theory

Miriam Backens

University of Oxford

Queen Mary Algorithms Day, 17 July 2018





European Research Council

Outline

Introduction to holant problems

Basic quantum information theory

The new results

Conclusions

Outline

Introduction to holant problems

Basic quantum information theory

The new results

Conclusions

(Boolean) holant problems

Fix a set of functions \mathcal{F} .

Throughout, functions take Boolean inputs and yield algebraic complex outputs.

Name HOLANT (\mathcal{F}) Instance a signature grid $\Omega = (G, \mathcal{F}, \pi)$, where

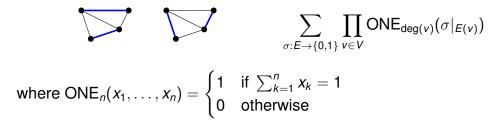
- G = (V, E) is a finite multigraph
- *π*: *V* → *F*:: *v* → *f_v* is a map that furthermore creates a bijection between *E*(*v*) and the arguments of *f_v*

Output the number

$$\mathsf{Holant}_{\Omega} := \sum_{\sigma: E \to \{0,1\}} \prod_{v \in V} f_v\left(\sigma|_{E(v)}\right)$$

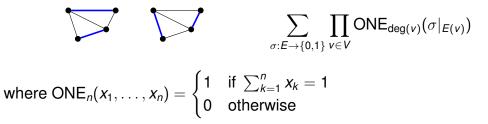
Problems expressible in the holant framework

counting perfect matchings:



Problems expressible in the holant framework

counting perfect matchings:



also:

- many other counting problems defined on graphs
- counting graph homomorphisms
- counting constraint satisfaction problems
- partition functions from statistical physics
- classical simulation of quantum computations

▶ ...

Counting complexity dichotomies

Complexity classes

- FP: counting problems that can be solved in polynomial time
- #P: counting complexity equivalent of NP

Unless FP is equal to #P, there exist intermediate problems in $\#P \setminus FP$, which are not #P-complete (by a variant of Ladner's theorem).

In the holant framework, all existing complexity classifications are dichotomies, partitioning families of functions into

- those that are polynomial-time solvable, and
- those that are #P-hard

(without any #P-intermediate problems)

Holant families and existing results

No full complexity classification for HOLANT (\mathcal{F}) yet

Allowing additional unary functions:

- $\mathsf{HOLANT}^*(\mathcal{F}) := \mathsf{HOLANT}(\mathcal{F} \cup \{\mathsf{all unaries}\})$
- ► HOLANT⁺ (\mathcal{F}) := HOLANT ($\mathcal{F} \cup \{\delta_0, \delta_1, \delta_+, \delta_-\}$)

• HOLANT^c
$$(\mathcal{F}) :=$$
 HOLANT $(\mathcal{F} \cup \{\delta_0, \delta_1\})$

[Cai, Lu, Xia 2011] [here] [here]

where

$$\begin{cases} \delta_0(0) = 1 \\ \delta_0(1) = 0, \end{cases} \quad \begin{cases} \delta_1(0) = 0 \\ \delta_1(1) = 1, \end{cases} \quad \begin{cases} \delta_+(0) = 1 \\ \delta_+(1) = 1, \end{cases} \text{ and } \begin{cases} \delta_-(0) = 1 \\ \delta_-(1) = -1. \end{cases}$$

Holant families and existing results

No full complexity classification for HOLANT (\mathcal{F}) yet

Allowing additional unary functions:

- ► HOLANT^{*} $(\mathcal{F}) :=$ HOLANT $(\mathcal{F} \cup \{ all unaries \})$ [Cai, l
- ► HOLANT⁺ (\mathcal{F}) := HOLANT ($\mathcal{F} \cup \{\delta_0, \delta_1, \delta_+, \delta_-\}$)

• HOLANT^c
$$(\mathcal{F}) :=$$
 HOLANT $(\mathcal{F} \cup \{\delta_0, \delta_1\})$

[Cai, Lu, Xia 2011] [here] [here]

where

$$\begin{cases} \delta_0(0) = 1 \\ \delta_0(1) = 0, \end{cases} \quad \begin{cases} \delta_1(0) = 0 \\ \delta_1(1) = 1, \end{cases} \quad \begin{cases} \delta_+(0) = 1 \\ \delta_+(1) = 1, \end{cases} \text{ and } \begin{cases} \delta_-(0) = 1 \\ \delta_-(1) = -1. \end{cases}$$

Allowing additional equality functions:

- ► #CSP $(\mathcal{F}) =$ Holant $(\mathcal{F} \cup \{ EQ_k \mid k \in \mathbb{N} \})$ [Cai, Lu, Xia 2009]
- $\models \# \mathsf{CSP}_2^c(\mathcal{F}) := \mathsf{HOLANT} \left(\mathcal{F} \cup \{ \delta_0, \delta_1 \} \cup \{ \mathsf{EQ}_{2k} \mid k \in \mathbb{N} \} \right)$

[Cai, Lu, Xia 2017]

Holographic transformations

There is a bijection between functions and lists of their values

$$f: \{0,1\}^n \to \mathbb{C} \qquad \leftrightarrow \qquad \mathbf{f} \in \mathbb{C}^{2^n}$$

Example: $g(x, y) = 2x + y \quad \leftrightarrow \quad \mathbf{g} = (0, 1, 2, 3)^T$

Holographic transformations

There is a bijection between functions and lists of their values

$$f: \{0,1\}^n \to \mathbb{C} \qquad \leftrightarrow \qquad \mathbf{f} \in \mathbb{C}^{2^r}$$

Example: $g(x, y) = 2x + y \quad \leftrightarrow \quad \mathbf{g} = (0, 1, 2, 3)^T$

The holographic transformation of an *n*-ary function *f* by an invertible 2×2 matrix *M* over \mathbb{C} is

$$M \circ f \qquad \leftrightarrow \qquad (\underbrace{M \otimes \ldots \otimes M}_{n}) \mathbf{f}.$$

Holographic transformations

There is a bijection between functions and lists of their values

$$f: \{0,1\}^n \to \mathbb{C} \qquad \leftrightarrow \qquad \mathbf{f} \in \mathbb{C}^{2^n}$$

Example: $g(x, y) = 2x + y \quad \leftrightarrow \quad \mathbf{g} = (0, 1, 2, 3)^T$

The holographic transformation of an *n*-ary function *f* by an invertible 2×2 matrix *M* over \mathbb{C} is

$$M \circ f \qquad \leftrightarrow \qquad (\underbrace{M \otimes \ldots \otimes M}_{n}) \mathbf{f}.$$

Example: If $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, then $(M \circ g)(x, y) = 3 - 4x - 5y + 6xy$, because

$$(M \otimes M)\mathbf{g} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \\ -1 \\ 0 \end{pmatrix}$$

Holographic transformations and complexity

Valiant's holant theorem

Suppose \mathcal{F},\mathcal{G} are sets of functions and suppose M is an invertible 2 \times 2 matrix. Then

HOLANT
$$(\mathcal{F} \mid \mathcal{G}) \equiv_{\mathcal{T}} \text{HOLANT} (M \circ \mathcal{F} \mid (M^{\mathcal{T}})^{-1} \circ \mathcal{G})$$
.

If O is a 2 \times 2 orthogonal matrix, then

HOLANT $(\mathcal{F}) \equiv_{\mathcal{T}} \text{HOLANT} (\mathcal{O} \circ \mathcal{F})$.

Holographic transformations and complexity

Valiant's holant theorem

Suppose \mathcal{F}, \mathcal{G} are sets of functions and suppose *M* is an invertible 2 \times 2 matrix. Then

HOLANT
$$(\mathcal{F} \mid \mathcal{G}) \equiv_{\mathcal{T}} \text{HOLANT} (\mathcal{M} \circ \mathcal{F} \mid (\mathcal{M}^{\mathcal{T}})^{-1} \circ \mathcal{G})$$

If O is a 2 \times 2 orthogonal matrix, then

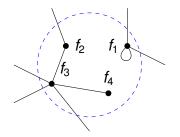
HOLANT
$$(\mathcal{F}) \equiv_{\mathcal{T}} \text{HOLANT} (\mathcal{O} \circ \mathcal{F})$$
.

Example: As $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is orthogonal,

 $\mathsf{HOLANT}\left(\{g,\mathsf{EQ}_3\}\right) \equiv_{\mathcal{T}} \mathsf{HOLANT}\left(\{M \circ g, M \circ \mathsf{EQ}_3\}\right),$

where g(x, y) = 2x + y and $(M \circ g)(x, y) = 3 - 4x - 5y + 6xy$.

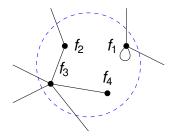
Holant gadgets



for any
$$\mathbf{x}: E_{\text{ext}} o \{0,1\}$$
: $g(\mathbf{x}) = \sum_{\mathbf{y}: E_{\text{int}} o \{0,1\}} \prod_{v \in V} f_v(\mathbf{x}, \mathbf{y}|_{E(v)})$

Let $\langle \mathcal{F} \rangle$ be the closure of \mathcal{F} under taking holant gadgets, then HOLANT $(\mathcal{F}) \equiv_{\mathcal{T}} \text{HOLANT} (\langle \mathcal{F} \rangle)$

Holant gadgets

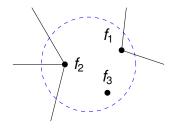


for any
$$\mathbf{x}: E_{\text{ext}} o \{0, 1\}$$
: $g(\mathbf{x}) = \sum_{\mathbf{y}: E_{\text{int}} o \{0, 1\}} \prod_{v \in V} f_v(\mathbf{x}, \mathbf{y}|_{E(v)})$

Let $\langle \mathcal{F} \rangle$ be the closure of \mathcal{F} under taking holant gadgets, then

$$\mathsf{HOLANT}\left(\mathcal{F}
ight)\equiv_{\mathcal{T}}\mathsf{HOLANT}\left(\langle\mathcal{F}
ight)$$

A holant gadget with zero internal edges is called a tensor product



Tractable families, part 1

HOLANT (\mathcal{F}) can be solved in polynomial time in the following cases:

- unary and binary functions: $\mathcal{F} \subseteq \langle \{f \mid arity(f) = 1 \text{ or } arity(f) = 2 \} \rangle$
- Generalised equality functions: there exists *M* satisfying *M^TM* ∈ { (¹₀ ⁰₁) , (⁰₁ ¹₀) }, such that

$$\mathcal{F} \subseteq \left\langle \boldsymbol{M} \circ \left\{ f \, \middle| \, \exists \mathbf{a} \in \{0, 1\}^{\operatorname{arity}(f)} \text{ s.t. } \forall \mathbf{x} \notin \{\mathbf{a}, \bar{\mathbf{a}}\}, f(\mathbf{x}) = \mathbf{0} \right\} \right\rangle$$

► generalised matching functions: there exists *M* satisfying *M^TM* = (⁰₁), such that

$$\mathcal{F} \subseteq \langle M \circ \{ f \mid f(\mathbf{x}) = 0 \text{ unless } |\mathbf{x}| \leq 1 \} \rangle$$

[Cai, Lu, Xia 2011]

Tractable families, part 2

Let $\ensuremath{\mathcal{A}}$ be the set of affine functions

$$f(\mathbf{x}) = c \ \chi_{A\mathbf{x}=\mathbf{b}} \ i^{l(\mathbf{x})} \ (-1)^{q(\mathbf{x})}$$

HOLANT (\mathcal{F}) can be solved in polynomial time in the following cases:

transformable to affine: there exists invertible M satisfying

$$M^{\mathsf{T}} \circ \{\mathsf{EQ}_2, \delta_0, \delta_1\} \subseteq \mathcal{A} \quad \text{and} \quad \mathcal{F} \subseteq M \circ \mathcal{A}$$

[Cai, Huang, Lu 2012]

local affine: *F* is a subset of

$$\bigcup_{n\in\mathbb{N}} \{f \mid \text{ if } f(x_1,\ldots,x_n) \neq 0 \text{ then } (T^{x_1}\otimes\ldots\otimes T^{x_n})\mathbf{f}\in\mathcal{A}\}$$

where

$$T^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
 and $T^1 = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$
[Cai, Lu, Xia 2017]

Outline

Introduction to holant problems

Basic quantum information theory

The new results

Conclusions

Quantum states and entanglement

A state of *n* qubits (quantum bits) is described by a vector in

$$\underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_n \cong \mathbb{C}^{2^n}$$

A quantum state of multiple qubits is fully entangled if it cannot be written as a tensor product.

For example:

- (1,0,0,1) is fully entangled
- $(0, 0, 0, -1, 0, 1, 0, 0) = (0, -1, 1, 0) \otimes (0, 1)$ is not fully entangled

Entanglement classification under SLOCC

SLOCC = 'stochastic local operations and classical communication'

Define an equivalence relation on vectors in \mathbb{C}^{2^n} :

$$\mathbf{f} \sim \mathbf{g} \quad \Longleftrightarrow \quad \mathbf{f} = (A_1 \otimes \ldots \otimes A_n)\mathbf{g}$$

for some invertible 2 by 2 matrices A_1, \ldots, A_n

Entanglement classification under SLOCC

SLOCC = 'stochastic local operations and classical communication'

Define an equivalence relation on vectors in \mathbb{C}^{2^n} :

$$\mathbf{f} \sim \mathbf{g} \quad \Longleftrightarrow \quad \mathbf{f} = (A_1 \otimes \ldots \otimes A_n)\mathbf{g}$$

for some invertible 2 by 2 matrices A_1, \ldots, A_n

Fully entangled three-qubit states: If $\mathbf{f} \in \mathbb{C}^{2^3}$ is fully entangled, then either

- $\mathbf{f} \sim \mathsf{EQ}_3$, or
- $\mathbf{f} \sim \mathsf{ONE}_3$

Correspondences

Counting complexity theory	Quantum information theory
function	quantum state
degenerate function	product state
non-degenerate function	entangled state
affine function	stabiliser state
EQ ₃	GHZ state
ONE ₃	W state
holographic transformation	stochastic local operation with classical communication (SLOCC)
Holant problem	(strong) classical simulation of quantum circuits

Outline

Introduction to holant problems

Basic quantum information theory

The new results

Conclusions

The dichotomy for HOLANT⁺

Theorem

Let \mathcal{F} be a set functions, then $\text{HOLANT}^+(\mathcal{F}) = \text{HOLANT} (\mathcal{F} \cup \{\delta_0, \delta_1, \delta_+, \delta_-\})$ is $\#\text{P-hard unless } \mathcal{F}$ is in one of the following tractable families:

unary and binary functions

$$\mathcal{F} \subseteq \langle \{f \mid \operatorname{arity}(f) = 1 \text{ or } \operatorname{arity}(f) = 2 \} \rangle$$

• generalised equality functions: $\exists M \text{ such that } M^T M \in \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}$ and

$$\mathcal{F} \subseteq \left\langle \boldsymbol{M} \circ \left\{ f \, \middle| \, \exists \mathbf{a} \in \{0,1\}^{\mathsf{arity}(f)} \text{ s.t. } \forall \mathbf{x} \notin \{\mathbf{a}, \bar{\mathbf{a}}\}, f(\mathbf{x}) = \mathbf{0} \right\} \right\rangle$$

• generalised matching functions: $\exists M$ such that $M^T M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and

$$\mathcal{F} \subseteq \langle \boldsymbol{M} \circ \{ f \mid f(\mathbf{x}) = 0 \text{ unless } |\mathbf{x}| \leq 1 \} \rangle$$

affine functions

$$\mathcal{F} \subseteq \mathcal{A}$$
.

Proof approach

There is a full dichotomy for HOLANT ($\{f\} | \{g\}$), where *f* is a symmetric ternary function and *g* is a symmetric binary function [Cai, Huang, Lu 2012]

To get a dichotomy for HOLANT⁺ (\mathcal{F}):

- Assume \mathcal{F} is not one of the tractable families
- ▶ Then there exists a fully entangled function in $\langle \mathcal{F}, \delta_0, \delta_1, \delta_+, \delta_- \rangle$ which has arity ≥ 3
- Find f, g ∈ ⟨F, δ₀, δ₁, δ₊, δ_−⟩ with arity(f) = 3 and arity(g) = 2, which are symmetric and fully entangled
- Reduce from HOLANT $({f} | {g})$ to show hardness

Proof approach

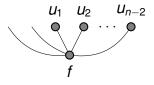
There is a full dichotomy for HOLANT ($\{f\} | \{g\}$), where *f* is a symmetric ternary function and *g* is a symmetric binary function [Cai, Huang, Lu 2012]

To get a dichotomy for HOLANT⁺ (\mathcal{F}):

- Assume \mathcal{F} is not one of the tractable families
- ▶ Then there exists a fully entangled function in $\langle \mathcal{F}, \delta_0, \delta_1, \delta_+, \delta_- \rangle$ which has arity ≥ 3
- Find f, g ∈ ⟨F, δ₀, δ₁, δ₊, δ_−⟩ with arity(f) = 3 and arity(g) = 2, which are symmetric and fully entangled
- Reduce from HOLANT $({f} | {g})$ to show hardness

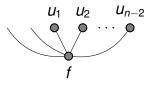
Gadget constructions from quantum theory

Theorem (Popescu & Rohrlich, 1992; Gachechiladze & Gühne, 2017) Let *f* be a fully entangled *n*-ary function. Then, for any two of the inputs, there exists some fully entangled binary gadget over { $f, \delta_0, \delta_1, \delta_+, \delta_-$ }.



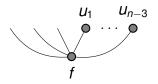
Gadget constructions from quantum theory

Theorem (Popescu & Rohrlich, 1992; Gachechiladze & Gühne, 2017) Let *f* be a fully entangled *n*-ary function. Then, for any two of the inputs, there exists some fully entangled binary gadget over { $f, \delta_0, \delta_1, \delta_+, \delta_-$ }.



Theorem

Let f be a fully entangled n-ary function with $n \ge 3$. Then there exists a fully entangled ternary gadget over $\{f, \delta_0, \delta_1, \delta_+, \delta_-\}$ for some choice of three of the inputs.



'Virtual gadgets'

It can be convenient to think of functions as gadgets even if they are not defined that way, e.g. for a fully entangled ternary function:

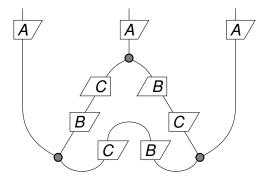


'Virtual gadgets'

It can be convenient to think of functions as gadgets even if they are not defined that way, e.g. for a fully entangled ternary function:



Then (up to a holographic transformation) the following gadget is determined by 2 cases with 4 parameters each:

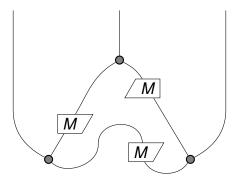


'Virtual gadgets'

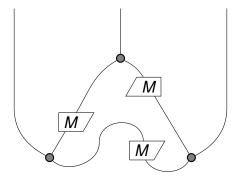
It can be convenient to think of functions as gadgets even if they are not defined that way, e.g. for a fully entangled ternary function:



Then (up to a holographic transformation) the following gadget is determined by 2 cases with 4 parameters each:



Gadgets for symmetric entangled ternary functions



Given a set \mathcal{F} containing a fully entangled ternary function, can show with a bit of effort:

- either it is possible to realise a symmetric fully entangled ternary function over $\mathcal{F} \cup \{\delta_0, \delta_1, \delta_+, \delta_-\}$ using the above gadget (possibly with some extra effort), or
- $\mathcal{F} \cup \{\delta_0, \delta_1, \delta_+, \delta_-\}$ is one of the known tractable families

The dichotomy for HOLANT^c

Theorem

Let \mathcal{F} be a set of functions, then HOLANT^{*c*}(\mathcal{F}) := HOLANT ($\mathcal{F} \cup \{\delta_0, \delta_1\}$) is #P-hard unless \mathcal{F} is in one of the following tractable families:

unary and binary functions

$$\mathcal{F} \subseteq \langle \{ f \mid \operatorname{arity}(f) = 1 \text{ or } \operatorname{arity}(f) = 2 \} \rangle$$

• generalised equality functions: $\exists M \text{ such that } M^T M \in \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}$ and

$$\mathcal{F} \subseteq \left\langle \textit{\textit{M}} \circ \left\{ \textit{f} \, \middle| \, \exists \mathbf{a} \in \{0,1\}^{\mathsf{arity}(\textit{f})} \text{ s.t. } \forall \mathbf{x} \notin \{\mathbf{a}, \bar{\mathbf{a}}\}, \textit{f}(\mathbf{x}) = \mathbf{0} \right\} \right\rangle$$

• generalised matching functions: $\exists M$ such that $M^T M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and

$$\mathcal{F} \subseteq \langle \boldsymbol{M} \circ \{ f \mid f(\mathbf{x}) = 0 \text{ unless } |\mathbf{x}| \leq 1 \} \rangle$$

- 'transformable to affine' functions: ∃M such that M^T ∘ {EQ₂, δ₀, δ₁} ⊆ A and F ⊆ M ∘ A
- local affine functions.

Combine methods from real-valued HOLANT^c dichotomy [Cai, Lu, Xia 2017] and HOLANT⁺ dichotomy [B 2017]

• Assume \mathcal{F} is not one of the tractable families

- ► Assume *F* is not one of the tractable families
- ▶ Pick a function $f \in \langle \mathcal{F}, \delta_0, \delta_1 \rangle$ with arity $(f) \ge 3$ which is fully entangled

- ► Assume *F* is not one of the tractable families
- ▶ Pick a function $f \in \langle \mathcal{F}, \delta_0, \delta_1 \rangle$ with arity $(f) \ge 3$ which is fully entangled
- Use pinning and self-loops to reduce arity while preserving properties of being fully entangled and having arity ≥ 3

- Assume *F* is not one of the tractable families
- ▶ Pick a function $f \in \langle \mathcal{F}, \delta_0, \delta_1 \rangle$ with arity $(f) \ge 3$ which is fully entangled
- Use pinning and self-loops to reduce arity while preserving properties of being fully entangled and having arity ≥ 3
- Either get ternary function, or get 4-ary function which is non-zero only on inputs 0000, 0011, 1100, 1111 (up to permutation of arguments)

- ► Assume *F* is not one of the tractable families
- ▶ Pick a function $f \in \langle \mathcal{F}, \delta_0, \delta_1 \rangle$ with arity $(f) \ge 3$ which is fully entangled
- Use pinning and self-loops to reduce arity while preserving properties of being fully entangled and having arity ≥ 3
- Either get ternary function, or get 4-ary function which is non-zero only on inputs 0000, 0011, 1100, 1111 (up to permutation of arguments)
 - With ternary function, can show hardness using techniques from HOLANT⁺ dichotomy

- ► Assume *F* is not one of the tractable families
- ▶ Pick a function $f \in \langle \mathcal{F}, \delta_0, \delta_1 \rangle$ with arity $(f) \ge 3$ which is fully entangled
- Use pinning and self-loops to reduce arity while preserving properties of being fully entangled and having arity ≥ 3
- Either get ternary function, or get 4-ary function which is non-zero only on inputs 0000, 0011, 1100, 1111 (up to permutation of arguments)
 - With ternary function, can show hardness using techniques from HOLANT⁺ dichotomy
 - ▶ With 4-ary function, can reduce from #CSP^c₂

Outline

Introduction to holant problems

Basic quantum information theory

The new results

Conclusions

 Knowledge from quantum theory, particularly about entanglement, is useful for analysing counting problems

- Knowledge from quantum theory, particularly about entanglement, is useful for analysing counting problems
- This approach has already led to dichotomies for HOLANT⁺ and HOLANT^c

- Knowledge from quantum theory, particularly about entanglement, is useful for analysing counting problems
- This approach has already led to dichotomies for HOLANT⁺ and HOLANT^c
- Hopefully stepping stone towards full dichotomy for all holant problems, together with dichotomy for symmetric HOLANT [Cai, Guo, Williams 2016] and dichotomy for non-negative real-valued HOLANT [Lin, Wang 2017]

- Knowledge from quantum theory, particularly about entanglement, is useful for analysing counting problems
- This approach has already led to dichotomies for HOLANT⁺ and HOLANT^c
- Hopefully stepping stone towards full dichotomy for all holant problems, together with dichotomy for symmetric HOLANT [Cai, Guo, Williams 2016] and dichotomy for non-negative real-valued HOLANT [Lin, Wang 2017]

Thank you.