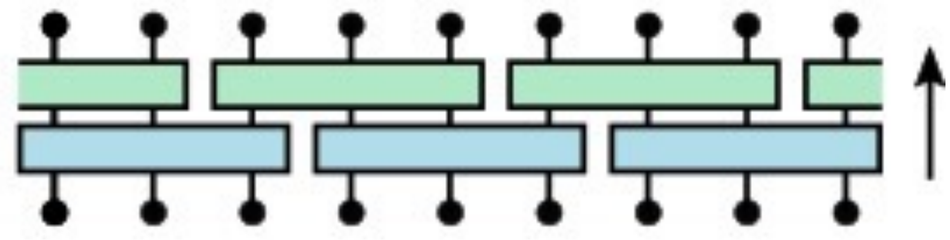
Symmetries in Quantum Information

Michael Walter



ICMP, Strasbourg, July 2024

RUHR UNIVERSITÄT BOCHUM RUB
European Research Council
Established by the European Commission
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES
NWO

Mathematics

dynamics

Quantum Physics

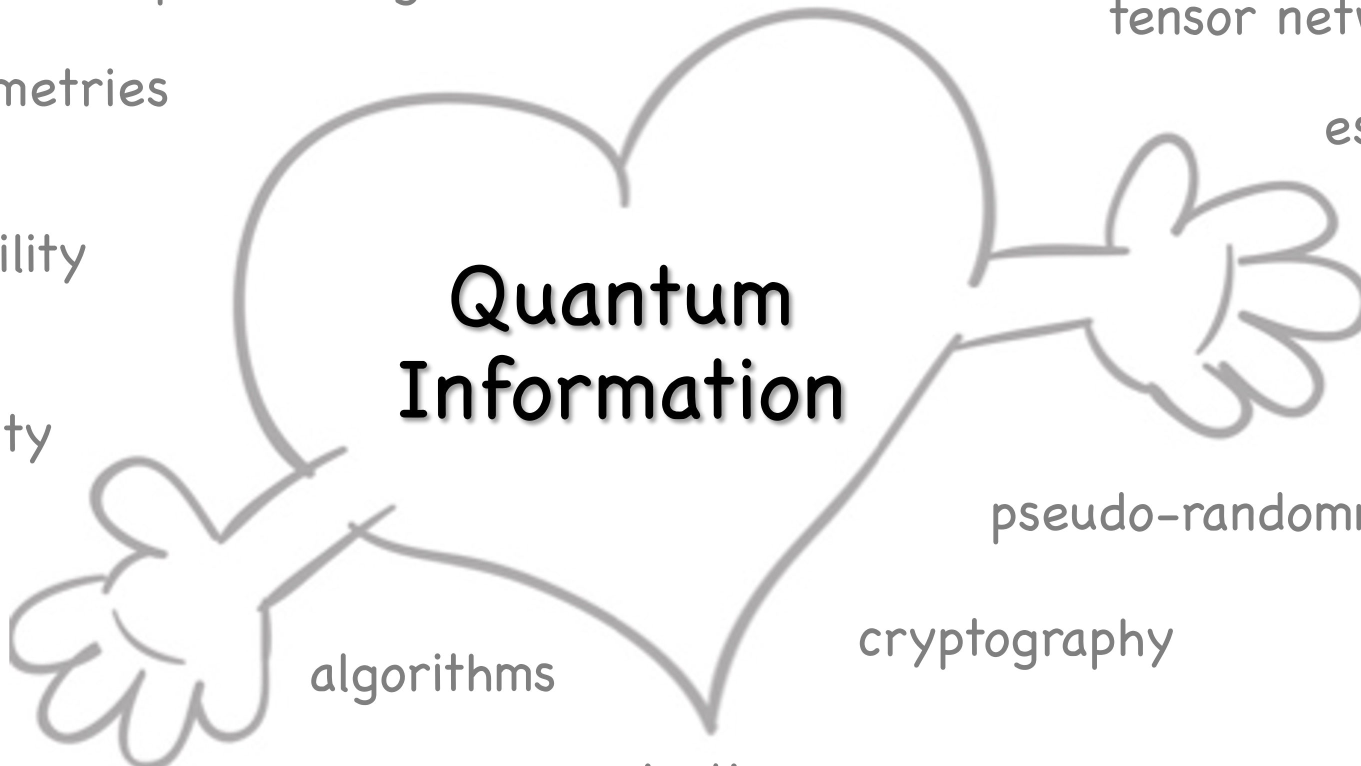
long-range entanglement

operator algebras

tensor networks

symmetries

estimation



probability

complexity

pseudo-randomness

cryptography

algorithms

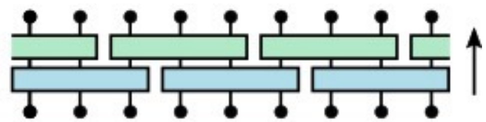
communication

Theory of Computation

The plan

Three little pieces of quantum information, where **hidden structure** plays an important role:

Invariants hiding in local quantum dynamics



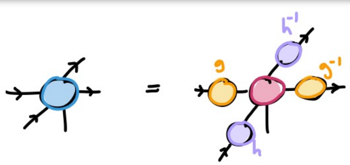
many-body physics

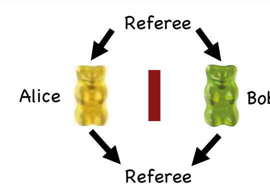
approximate algebras

Symmetries in tensor networks

algorithms & complexity

Rigidity of correlations in space and (polynomial) time





Biased selection of topics, but illustrative of general perspectives, problems, connections.

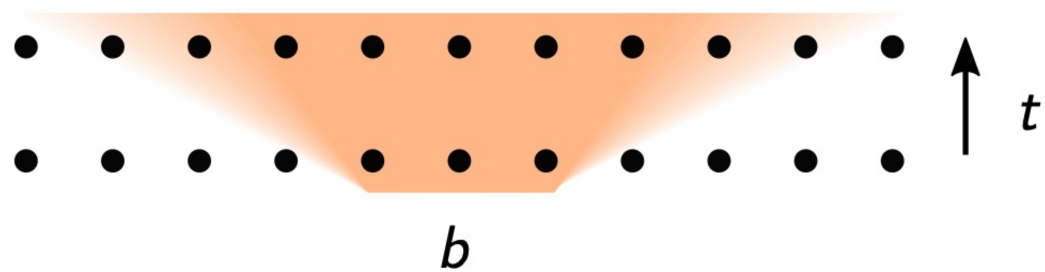
Breaking and Making Locality

Local dynamics vs local Hamiltonians

Relativistic systems have sharp light cones - as do quantum circuits.

Lieb-Robinson: Local Hamiltonian dynamics still have "fuzzy" light cones.

$$b(t) = e^{iHt} b e^{-iHt}$$



→ e.g. for short-range interactions, LR velocity and exponential tails

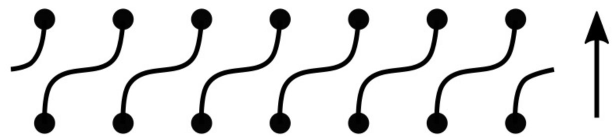
Question: Is any local dynamics (discrete time evolutions with sharp or fuzzy light cone) generated by a local Hamiltonians?

Converse to Lieb-Robinson bounds?

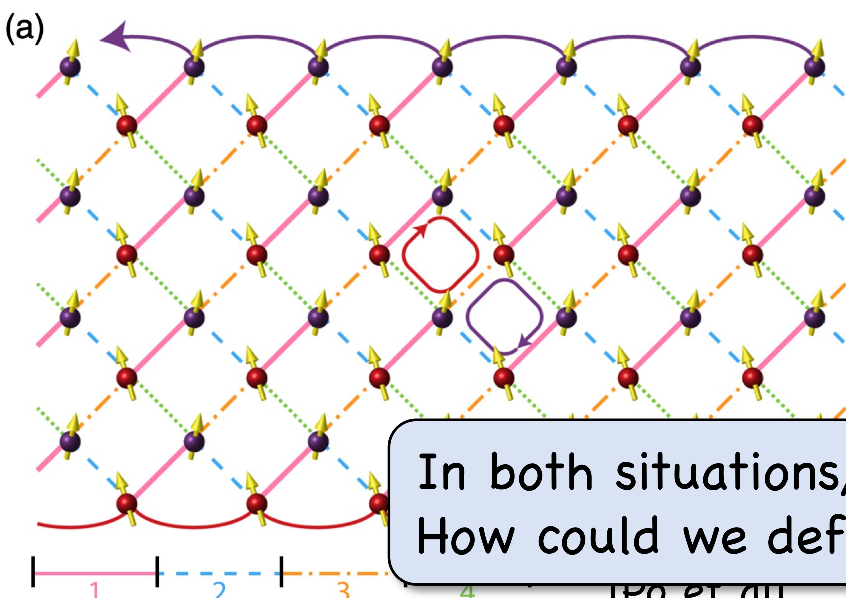
Classification of local dynamics?

Some interesting 1D dynamics

For example, can lattice shifts be realized by a local Hamiltonian?



This can even arise on the boundary of a 2D Hamiltonian dynamics:



[Po et al]

"MBL" Floquet dynamics of 4 layers of SWAP gates.

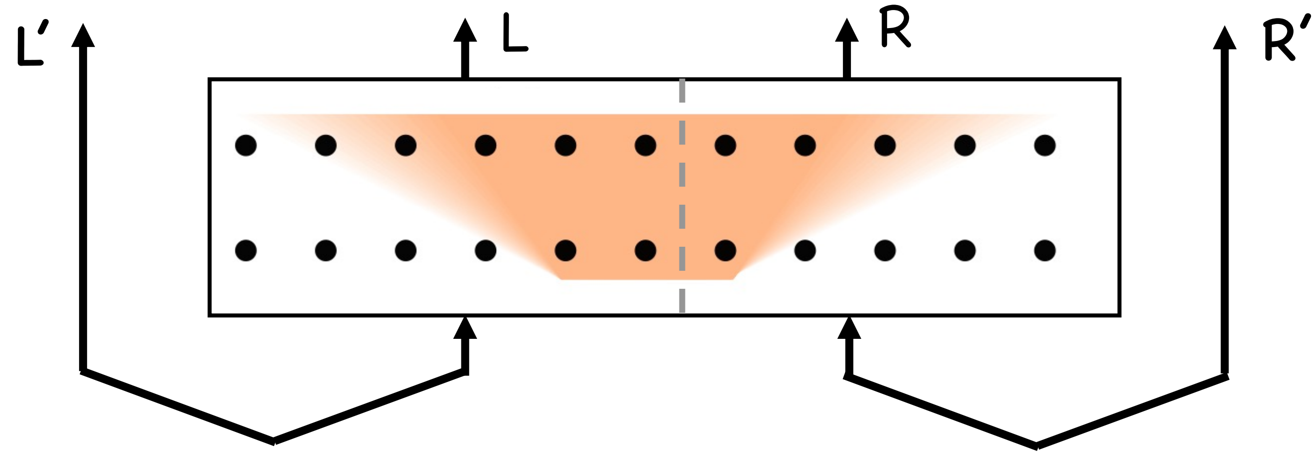
Trivial in the bulk, but has a "chiral edge".

In both situations, there is a clear **information flow**. How could we define this in general?

Information flow

[Kitaev, GNVW, …, RWW]

Consider dynamics of an infinite spin chain in 1D:



Step 1: Cut chain arbitrarily into halves.

Step 2: Consider Choi state $\Omega_{L'R'LR}$

Step 3: Compute $\boxed{\Delta = ½\,(I(L':R) - I(R':L))}$

net flow of quantum information, "index"

$I(A{:}B) = S(\rho_{AB} || \rho_A \otimes \rho_B)$ mutual information

Amazingly, Δ is quantized and **characterizes** the dynamics!

e.g. for qubit systems always an integer

e.g. dynamics is Hamiltonian iff $\Delta = 0$

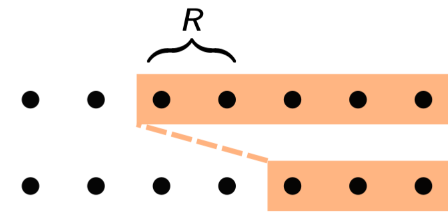
[Kitaev, GNVW]

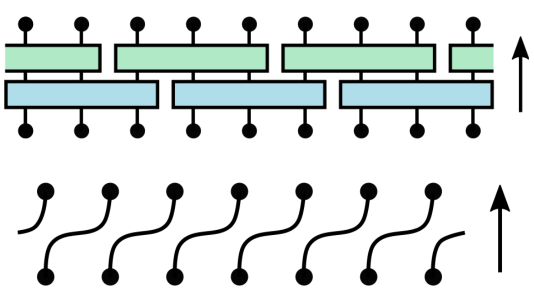
Warmup: Sharp light cones

Quasi-local algebra on infinite 1D lattice: $\mathcal{A} = \text{``}\bigotimes_{n\in\mathbb{Z}} \mathcal{A}_n\text{''}$

Quantum cellular automaton (QCA) with radius R
is automorphism $\alpha\colon \mathcal{A} \to \mathcal{A}$ if for all $X \subseteq \mathbb{Z}$:

$$\alpha(\mathcal{A}_X) \subseteq \mathcal{A}_{R\text{-Neighborhood}(X)}$$





Theorem (Gross–Nesme–Vogts–Werner):

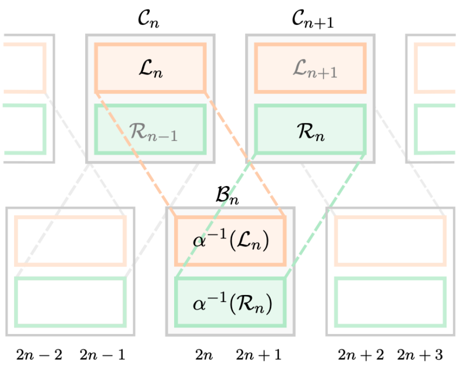
- Any QCA is composition of circuit and shifts.
- Shifts cannot be implemented by circuits.
- QCAs mod circuits are classified by **index**.

Does this theory survive passing to fuzzy light cones?

[Kitaev, GNVW]

Warmup: Sharp light cones

Quasi-local algebra on infinite 1D lattice: $\mathcal{A} = \text{“}\bigotimes_{n\in\mathbb{Z}} \mathcal{A}_n\text{”}$



Quantum cellular automaton (QCA) with radius R is automorphism $\alpha\colon \mathcal{A} \to \mathcal{A}$ if for all $X \subseteq \mathbb{Z}$:

$$\alpha(\mathcal{A}_X) \subseteq \mathcal{A}_{R\text{-Neighborhood}(X)}$$

Why not obvious?

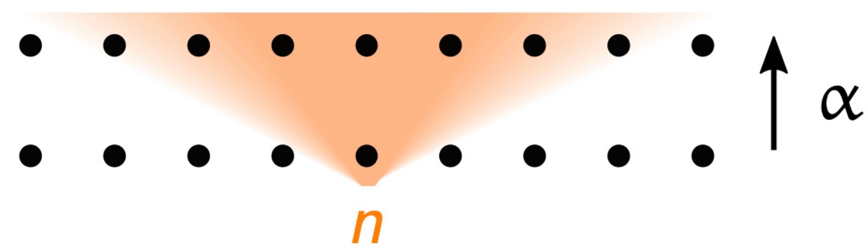
- Techniques algebraic & sensitive to perturbations
- Local Hamiltonian dynamics are **not** quantum circuits
  Can always approximate by circuits… but how about general dynamics?
- Previous definitions of index do **not** apply.
  Entropic definition applies… but does it remain quantized?

Does this theory survive passing to fuzzy light cones?

First attempt at tackling fuzzy light cones

Approximately locality preserving unitary (ALPU) with tails f(r) is automorphism $\alpha\colon \mathcal{A} \to \mathcal{A}$ if for all $X \subseteq \mathbb{Z}$ and $r > 0$:

$$\alpha(\mathcal{A}_X) \subseteq_{f(r)} \mathcal{A}_{r\text{-Neighborhood}(X)}$$



For any fixed site n, can "truncate tails" to obtain **approximate** morphism:

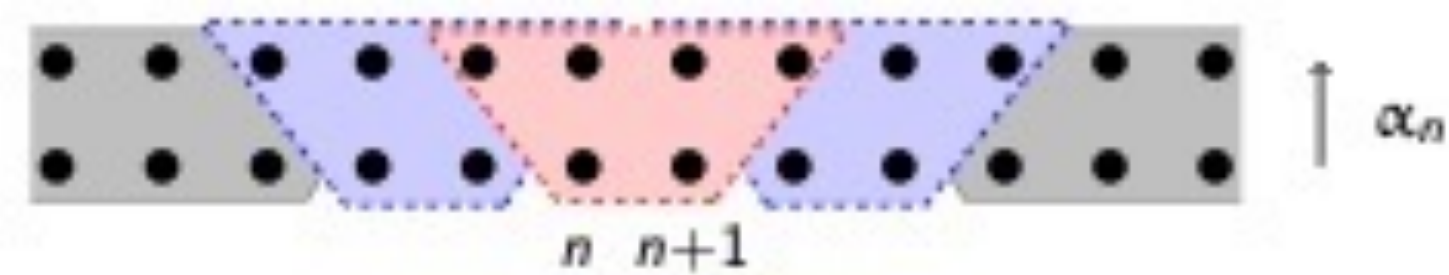
$$\mathcal{A}_n \to \mathcal{A}_{\{n-r,\ldots,n+r\}}$$

By a version of Ulam stability, can find nearby **exact** morphism.

Key challenge: For different sites n, the images of these morphisms need **not** commute → cannot patch together.

A better approach

A more clever strategy allows us to deform ALPU to one that looks like QCA *near any fixed cut*:



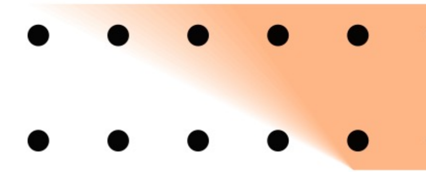
Left and right are decoupled – stronger than what we had before!

This allows us to glue different automorphism together:

Rounding Theorem (Ranard-Witteveen-W):
Any 1D ALPU α can be approximated by sequence of QCAs β_r of radius r such that $\beta_r \to \alpha$ strongly.

Main tool: Stability for approx. inclusions of hyperfinite algebras. [Christensen]

Result: Classification of 1D dynamics with fuzzy light cones



"ALPUs / time-dep. quasi-local Hamiltonian dynamics = QCAs / circuits"

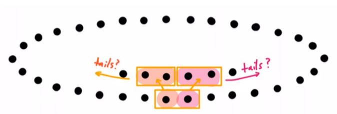
Theorem (Ranard-Witteveen-W): ALPUs…
- are classified by **index** that is quantized and robust;
- are composition of time-dep. quasi-local Hamiltonian dynamics & shifts;
- can always be approximated by sequence of QCAs of same index.

➔ Converse to Lieb-Robinson bound: ALPU generated by Hamiltonian ⇔ index = 0. *(Always the case for finite chain!)*

➔ Cannot even approximate lattice shift by Hamiltonian with LR bounds.

What do we know?

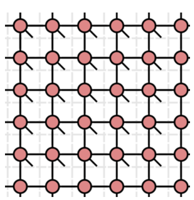
Quantum dynamics in 1D are classified by an index theory – even when the light cones are fuzzy! In particular, converse to LR bounds.



Main techniques are stability/rounding results for approx. (sub)algebras. Recent progress allows extension to periodic chains, edge dynamics of 2D systems & implies algorithms!

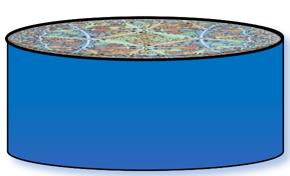
Kitaev (→ Friday talk), Ranard-Witteveen-W (in prep.)

Open questions and connections:



Higher dimensions? Beyond automorphisms?

structure gets increasingly complicated [Freedman-Hastings, Haah et al]

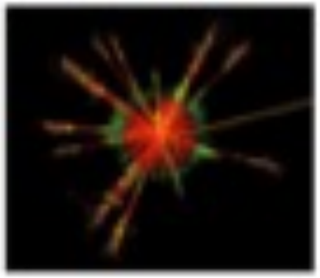


Other uses of stability results for algebras?

apart from QI e.g. also in AdS/CFT (approximate bulk algebras)

Symmetries in Tensor Networks

Complexity of many-body quantum states

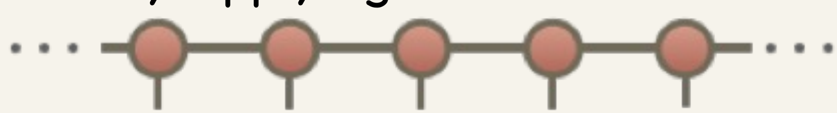
Many-body quantum states have exponentially large description:

$$|\Psi\rangle = \sum_{i_1,\dots,i_n} \boxed{\Psi_{i_1,\dots,i_n}} \, |i_1,\dots,i_n\rangle$$

For most states of interest, entanglement local → compact description?

1. Start with local entangled pairs

2. "Glue" by applying local transformations:



Tensor networks

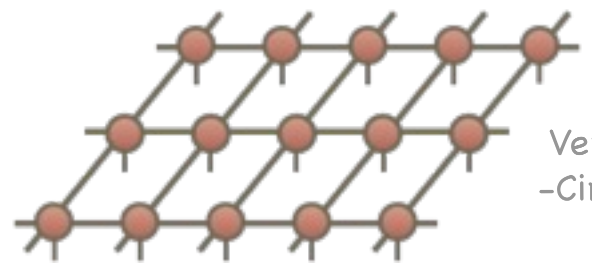
Tensor network: define many-body state by contracting "local" tensors

$$|\Psi\rangle = \sum_{i_1,\ldots,i_n} \Psi_{i_1,\ldots,i_n} |i_1,\ldots,i_n\rangle$$

Today's protagonists:

White, Fannes -Nachtergaele -Werner, ...

matrix product states (MPS)

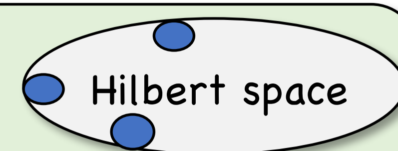


Verstraete -Cirac, ...

projected entangled pair states (PEPS)

Many other variants. Network to match entanglement structure (e.g. *area law*).

→ Numerical tool on classical and future quantum computers.

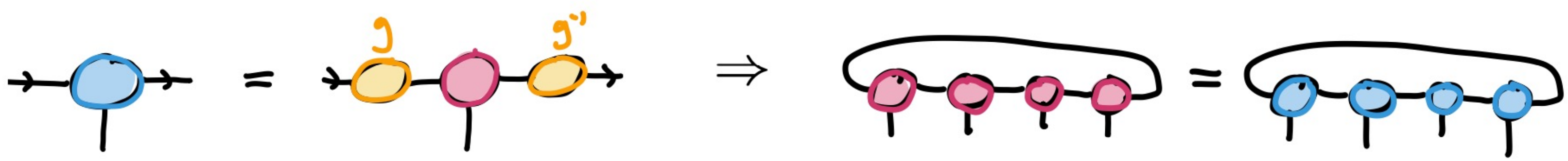


→ Analytical tool that provides "dual description" of "complex" phenomena: symmetries, topological phases, renormalization, holography, ...

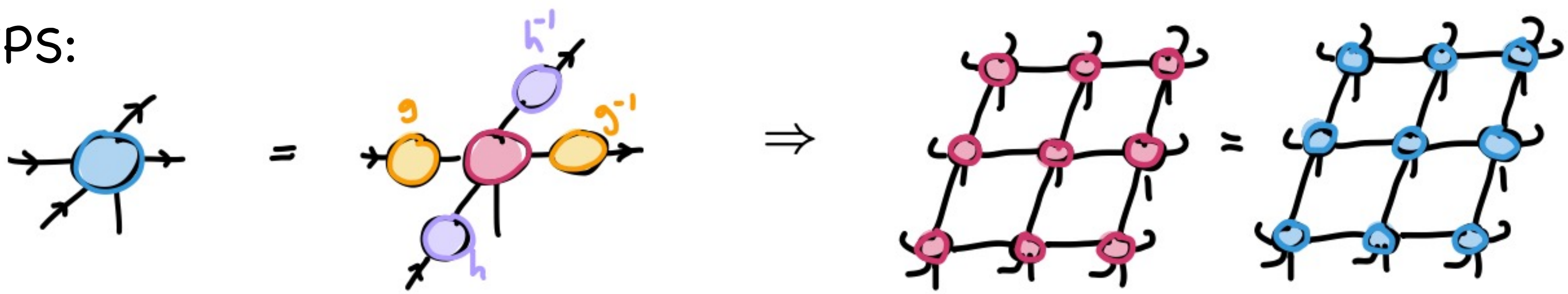
A fundamental question

Question: Given two tensors, when do they generate the *same* tensor network states?

Easy to find such situations! MPS:



PEPS:



These gauge symmetries preserve the quantum state for any system size!

Moreover can take limits...

Fundamental theorem for MPS

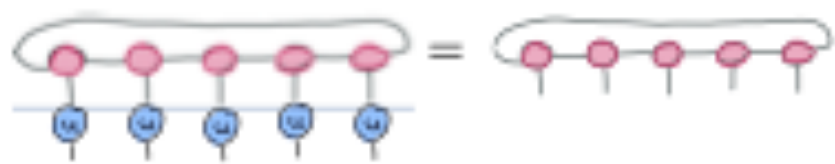
In 1D, gauge symmetry and taking limits is the only redundancy! Can even efficiently pick a canonical form. It is unique up to unitaries & satisfies:

> **Fundamental Theorem of MPS** (Cirac-PG-Schuch, de las Cuevas):
> Two tensors give rise to the same quantum states for all system sizes
> ⇔ same canonical form ⇔ related by gauge symmetry & limits.

Many theoretical and practical applications.

E.g. suppose MPS has global (on-site) symmetry for any system size n:

$$u^{\otimes n} |M_n\rangle = |M_n\rangle$$



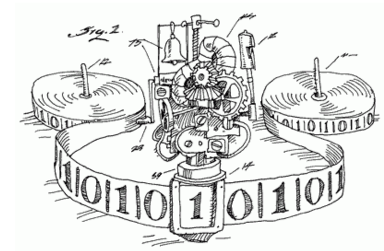
Fundamental theorem implies there is a unitary U such that…

➔ reduce classification of SPT phases to projective representations ☺

[Chen-Gu-Wen, Schuch et al, Pollman et al]

Gauge symmetry in higher dimensions

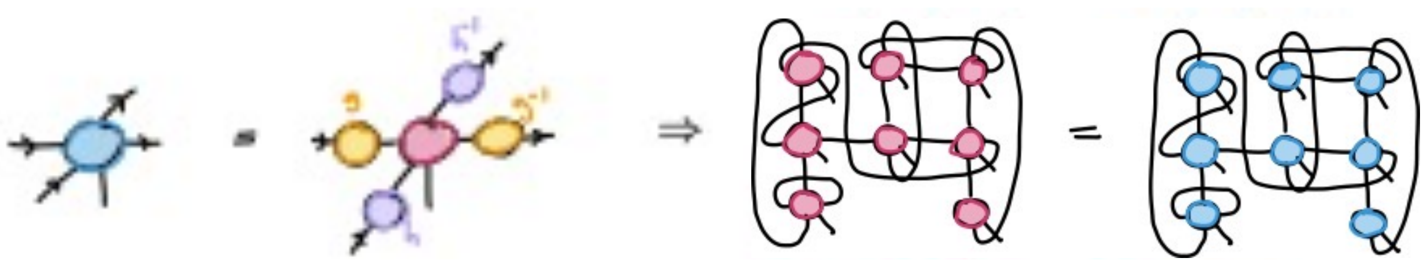
Bad news: No algorithm can decide if two PEPS tensors generate the same state for all system sizes m x n. The problem is undecidable by any Turing machine!



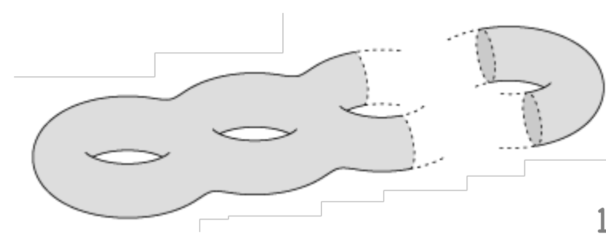
Scarpa et al

Long seen as "no go" result for going beyond 1D.

However: When two PEPS tensors are related by a gauge symmetry, they not only determine the same states on grids... but on *"any"* graph:



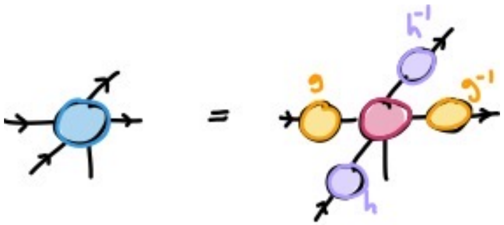
Punchline: If we allow for arbitrary "manifolds", get a good theory!



Result: Fundamental theorem and canonical form in higher dimensions

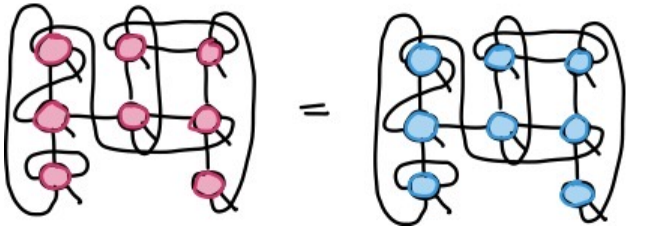
Define **minimal canonical form** of PEPS tensor T by minimizing ℓ^2-norm over all tensors obtained by applying gauge group G = GL(D) x GL(D):

$$T_{\min} := \operatorname{argmin}\{\|S\|_2 : S \in \overline{G \cdot T}\}$$



First generally defined canonical form in 2D and higher!

Theorem (Acuaviva-...-W): Get same quantum states on "any" graph ⇔ same canonical form ⇔ related by gauge symmetry & limits.



Theorem: For fixed bond dimension, can approximate $T_{\min}$ in poly time.

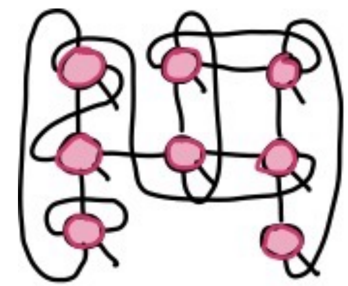
Bonus: If two MPS are distinct, this can already be seen at a system size *linear* in the bond dimension. For PEPS, can be *exponential*.

How does it work?

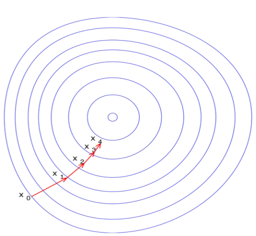
Geometric invariant theory: Field of math that studies equivalence for actions of group G on vector space V. Hilbert, Mumford, Kirwan, ...

e.g. V = tensors of fixed format & G = gauge group

Equivalence is captured by G-invariant polys, and those are precisely coefficients of tensor network states! ☺

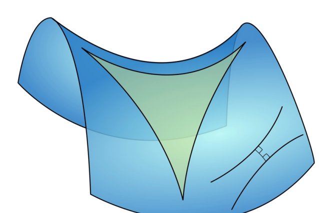


Algorithms: To compute canonical forms, combine recent progress in optimization algorithms with ideas from solution of Paulsen's problem.



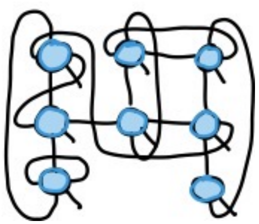
Key idea: ℓ^2-norm is convex on symmetric space associated with gauge group orbits.

Bürgisser-...-W-Wigderson



What do we know?

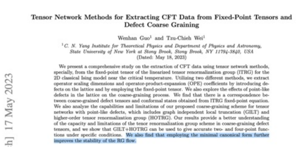
Tensor networks describe many-body states succinctly, with applications from physics to numerics to CS. Fundamental theorems and canonical forms are key tools. They can be generalized beyond 1D, but with a *twist*.



Main techniques are geometric invariant theory combined with recent progress on convex optimization in curved spaces in theoretical computer science. ✓

Cf. Bürgisser–…–W–Wigderson

Open questions and connections:


Tensor Network Methods for Extracting CFT Data from Fixed-Point Tensors and Defect Coarse Graining

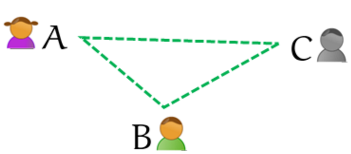
Wenhan Guo and Tzu-Chieh Wei

17 May 2023

Canonical forms are useful for numerics – how about this one?

cf. Guo et al

Topological order connection?



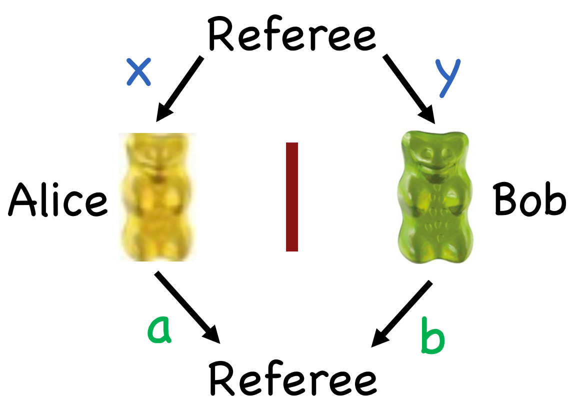
Techniques also apply to quantum marginal problems, entanglement, algebraic complexity, extremal combinatorics…

Playing Games with Locality

What is entanglement, really?

[Bell, Clauser-Horne -Shimony-Holt, ...]

Two players play against a referee:



Winning Condition (**CHSH Game**)

x	y	$a + b$
0	0	even
0	1	even
1	0	even
1	1	odd

Question: Can the players win this game?

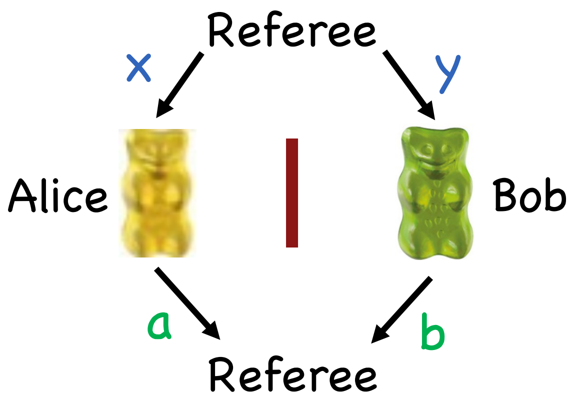
Are there suitable "answer functions" $a(x)$, $b(y)$? If so, then...

$$\big(a(0) + b(0)\big) + \big(a(0) + b(1)\big) + \big(a(1) + b(0)\big) + \big(a(1) + b(1)\big)$$

...would be **odd**. But each answer appears **twice**. **Contradiction!**

What is entanglement, really?

Two players play against a referee:



Winning Condition (**CHSH Game**)

x	y	a + b
0	0	even
0	1	even
1	0	even
1	1	odd

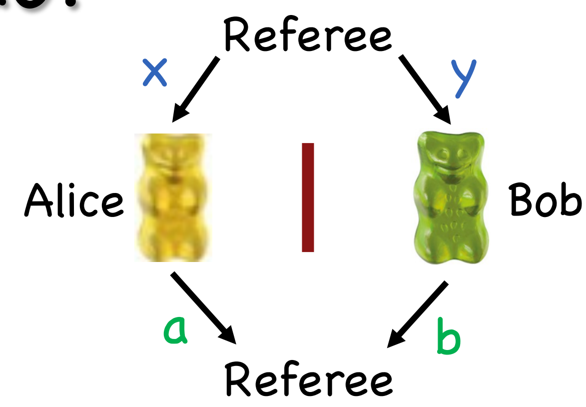
There is no "classical" way to win CHSH game: $p_{\text{win}}^{\text{classical}} \leq \frac{3}{4}$

This is a Bell inequality!

[TU Delft]

If the players share quantum entanglement they can do better!

How well can quantum players do?



If they share EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and use complementary measurements, can achieve:

$$p_{\text{win}}^{\text{quantum}} \approx 85\%$$

and this is optimal [Tsirelson]

Amazingly, optimal quantum strategy is "unique" and "rigid"!

"Operational" characterization of entanglement!

Classical verifier can verify & control untrusted pair of quantum devices

Fine print: So long they can't communicate (are spacelike). Really hard to enforce…

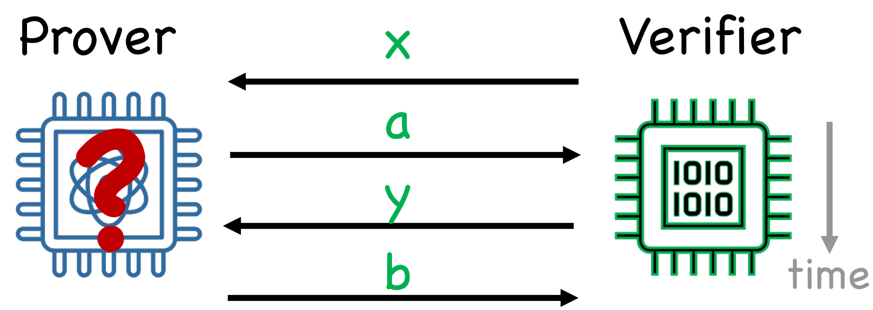
Reason: Hidden symmetry! Roughly, ϵ-optimal strategy ⇔ ϵ-representation of G = <X,Z>, and there is a nearby exact representation [Gowers-Hatami] ☺

Trading Space for Time

Question: Can we get rid of spacelike separation?

Motivation: Can a classical "verifier", by interacting with a single "prover", convince themselves that prover follows particular quantum strategy?

No!? Any quantum computation can be simulated classically…



…but in general only *inefficiently*. Indeed, ingenious work gave first classical verification protocol *under computational assumptions*. [Mahadev]

Is there any **systematic link** between nonlocal (info-theoretic, spacelike) & local (computationally-bounded) setting?

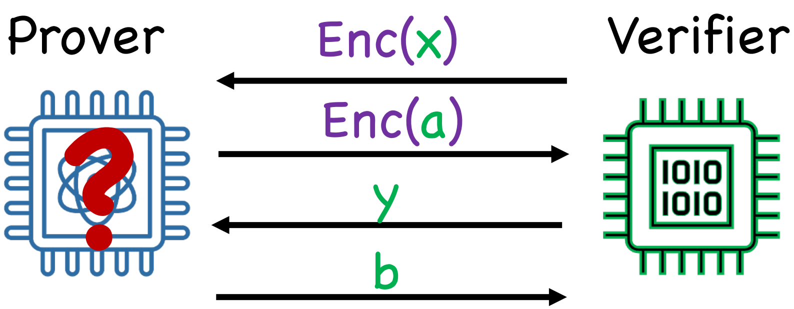
Cf. QKD vs computational cryptography

Trading Space for Time

[Kalai et al]

Idea: Use cryptography to force one prover to "simulate" two spacelike players (as long as they are unable to break the cryptography)!

long history in crypto



Intuition: Encrypted message cannot usefully be "combined" with plain one.

Use "homomorphic encryption" so that prover can simulate honest strategy.

➔ general "compiler" that applies to any nonlocal game ☺

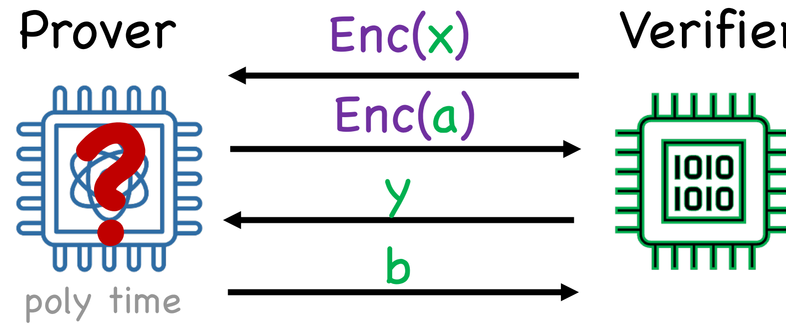
But does it work? Not obvious!

- At first glance, cryptography only ensures "non-signaling".
- But this is **not** enough! [Popescu-Rohrlich]
- Natural variations do **not** work ("spooky" encryption)!

Results: Trading Space for (Polynomial) Time

Theorem (Kalai et al):
Classical provers cannot cheat.

Thus, if observe $p_{win} > 3/4$, this constitutes proof of non-classicality!



Computational Tsirelson Theorem (Natarajan-Zhang, Cui-…-**W**):

- Quantum provers cannot cheat – for broad class of XOR games
- Near optimal strategies yield "logical qubits" inside prover!

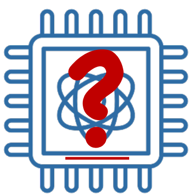
$$B_0 B_1 \approx -B_1 B_0$$

→ general method for classical verification of q. computation

Two proofs; both use "block encodings" to relate "solution algebra" to crypto.

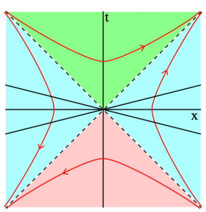
What do we know?

Nonlocal games are a foundational tool in quantum information and complexity. Recent results establish links between traditional space-like (information theoretic) and time-like (computational) setting.



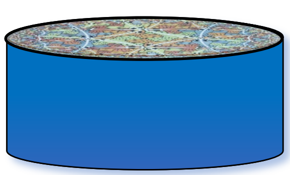
This enables theoretical applications, but also gives new insights into the math of nonlocality. Techniques combine algebra & crypto. Beyond XOR games, new ideas required.

Open problems and connections:



Tsirelson's conjecture is famously false (MIP*=RE). Any manifestation in the computational setting?

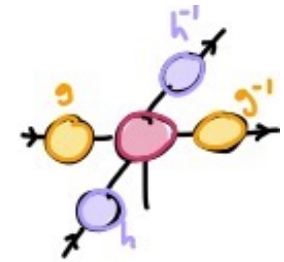
[Ji et al]



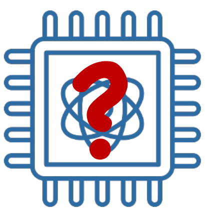
Speculative thought: In quantum gravity, locality emerges in *effective* description. Can one make a connection?

see recent works on complexity, pseudorandomness, holography [May, Bouland et al, ...]

Summary



Hidden symmetries and algebraic structure lie at the heart of math challenges & puzzles...



...which when uncovered and explored, can give new insights into quantum information.

Motivation ranges from trying to understand mathematical structure of quantum information, to learning how to leverage it for theoretical and practical applications.

Thank you for your attention!