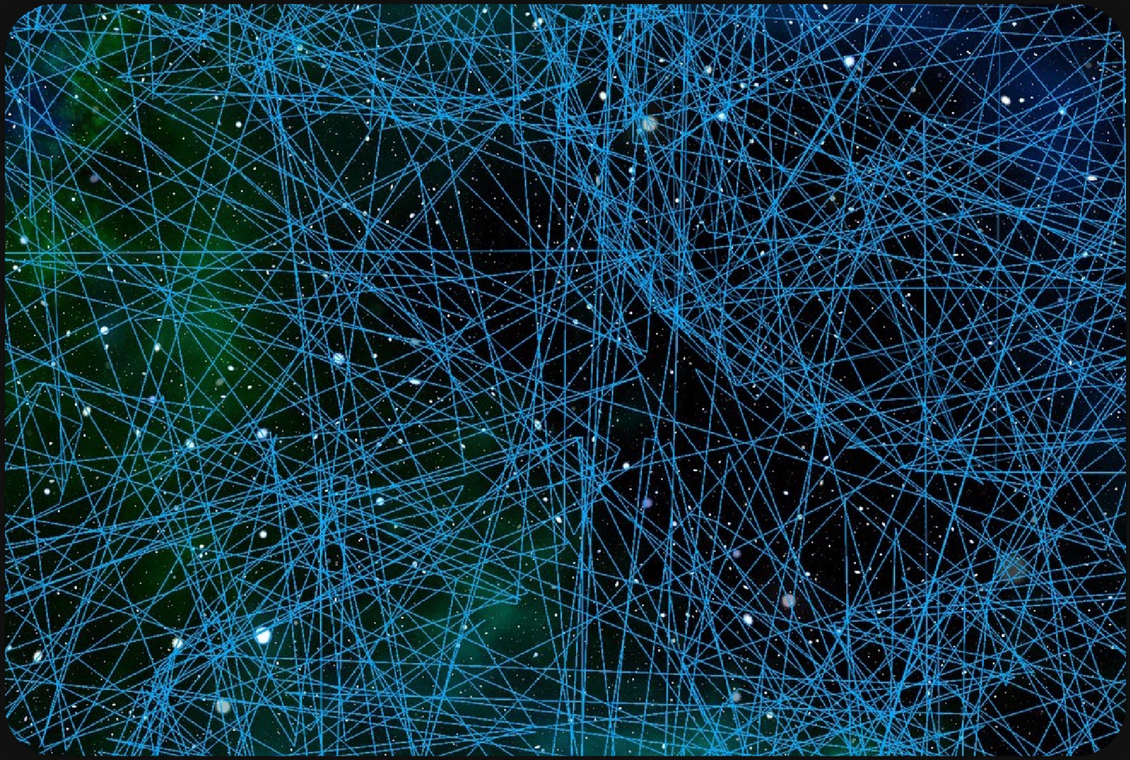
MIP* = RE : Putting Everything Together

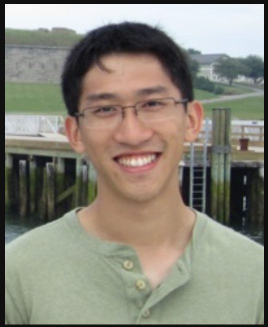


Zhengfeng Ji (UTS:QSI)

Quantum Protocols: Testing & Quantum PCPs, Simons Institute, 1 April 2020

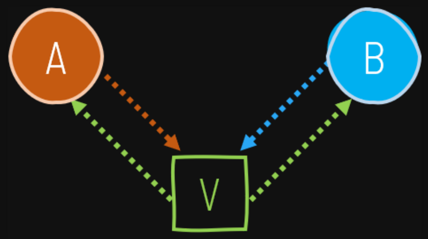
MIP* = RE

arXiv:2001.04383, 14 Jan 2020

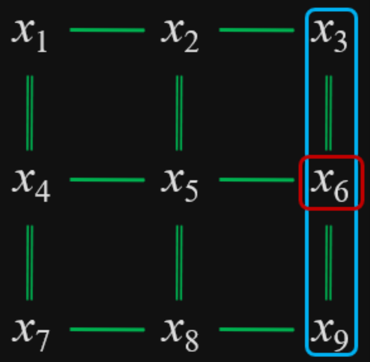
   

Background and Definitions

Multi-prover Interactive Proofs



- MIP: What can two provers prove to a verifier?
  - Completeness and Soundness
  - Known: MIP = NEXP *[Babai, Fortnow and Lund '90]*
- The power of an extra prover
- Example: Magic Square game $G_{\boxplus}$



  Nine variables and six constraints
  - Randomly sample a constraint and a variable in the constraint
  - Alice's view: the variable, x_6
  - Bob's view: the constraint, $x_3 \oplus x_6 \oplus x_9 = 1$

$$\mathrm{val}(G_{\boxplus}) = \frac{17}{18} < 1$$

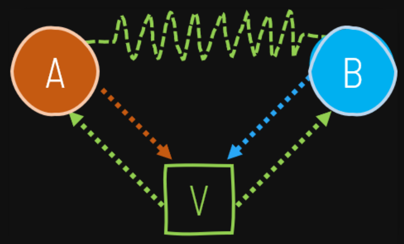
Question distribution

Quantum Multi-prover Interactive Proofs

- Entanglement among provers

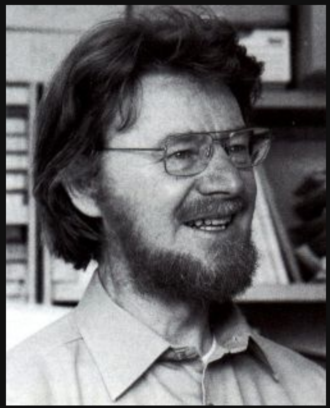
  MIP*: Entanglement vs. shared randomness

  [Cleve, Høyer, Toner and Watrous '04]



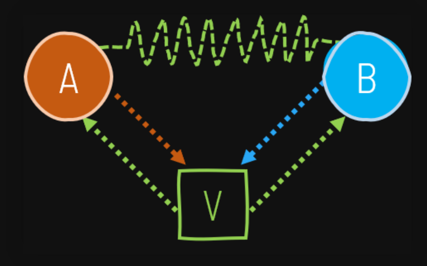
- Connects multi-prover interactive proofs to Bell inequalities!

$$\langle A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \rangle \leq 2$$



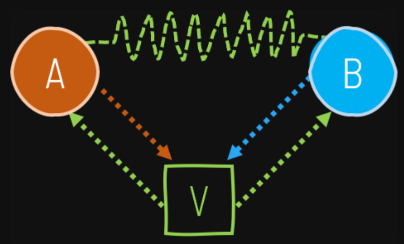
- Soundness problem of entanglement
- The development and applications of the quantum analogues of many powerful ideas in interactive proofs
  - Low-degree tests, parallel repetitions, PCPs

Nonlocal Games



- Definition of nonlocal games
  - Finite question sets $\mathcal{X}$ and $\mathcal{Y}$ and answer sets $\mathcal{A}$ and $\mathcal{B}$
  - Question distribution μ over $\mathcal{X} \times \mathcal{Y}$
  - Decider $\mathcal{D} : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times B \to \{0, 1\}$
- Family of games defined by verifier $\mathcal{V} = (\mathcal{S}, \mathcal{D})$ $\quad (L^{\mathrm{A}}(z), L^{\mathrm{B}}(z))$
  - Turing machine $\mathcal{S}$ takes input $(n, \dots)$
  - Turing machine $\mathcal{D}$ takes input (n, x, y, a, b)
  - The n-th game $\mathcal{V}_n$ defined by $\mathcal{S}_n$ and $\mathcal{D}_n$

Entangled Strategy and Value

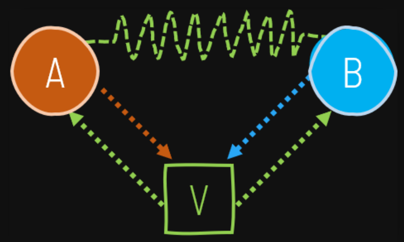


- Entangled strategy $\mathscr{S} = (|\psi\rangle, A, B)$
  - Share quantum state $|\psi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$
  - Measure $A = \{A_a^x\}$ and $B = \{B_b^y\}$ for questions x, y respectively
- Entangled value

$$\mathrm{val}^* = \sup_{\mathscr{S}} \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b \text{ accepted by } \mathcal{D}} \langle\psi|A_a^x \otimes B_b^y|\psi\rangle$$

- Entangled value of the Magic Square game $\mathrm{val}^*(G_\boxplus) = 1$
- MIP* corresponds to the approximation of val^*

Commuting Operator Strategy and Value



- Commuting operator strategy $\mathscr{S} = (|\psi\rangle, A, B)$
  - **Single** Hilbert space $\mathcal{H}$, state $|\psi\rangle \in \mathcal{H}$
  - A_a^x commutes with B_b^y for all a, b, x, y
- Commuting operator value

$$\mathrm{val}^{\mathrm{co}} = \sup_{\mathscr{S}} \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b \text{ accepted by } \mathcal{D}} \langle\psi| A_a^x B_b^y |\psi\rangle$$

- Tsirelson's problem: Is val^* equal to $\mathrm{val}^{\mathrm{co}}$ for all games?
- Two values coincide for finite-dimensional Hilbert spaces

Two Algorithms

- Algorithm 1: Exhaustively search for better tensor-product strategies of increasing Hilbert space dimensions and approximation precision

  A sequence of values approaching $\mathbf{val}^*$ from **below**

- Algorithm 2: The non-commutative sum-of-squares SDP hierarchy

  [Navascués, Pironio, and Acín '08], [Doherty, Liang, Toner, and Wehner '08]

  A sequence of values approaching $\mathbf{val}^{\mathbf{co}}$ from **above**

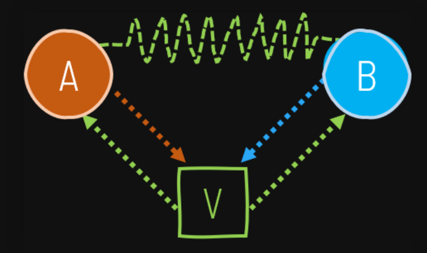
$$\text{Algorithm 1} \longrightarrow \ \mathbf{val}^* \leq \mathbf{val}^{\mathbf{co}} \ \longleftarrow \text{Algorithm 2}$$

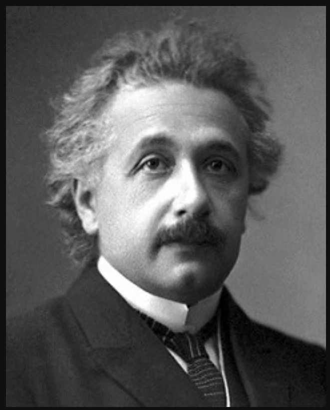
- Algorithm 1 establishes that MIP* ⊆ RE
- If Tsirelson's problem has a positive answer, we have an algorithm to approximate $\mathbf{val}^*$ (MIP* is in R = RE ∩ coRE)

Main Result

- MIP* = RE: no algorithm that can approximate val^* because it is as hard as the Halting problem
- A complete characterization of MIP*
    - "Spooky action at a distance — Einstein"
    - Spooky complexity at a distance
- Optimal violations to Bell inequalities are not computable

A computability-theoretic Bell inequality

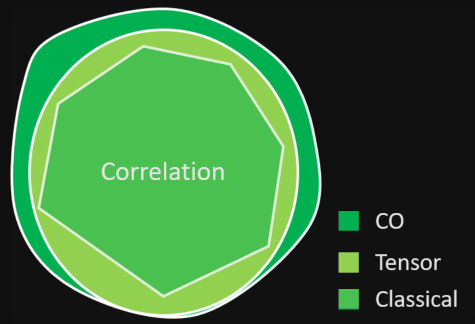




Consequences in Physics and Mathematics

- A negative answer to Tsirelson's problem

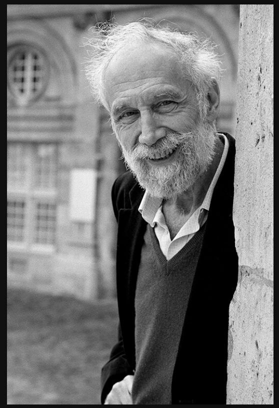
  Infinite quantum systems cannot be approximated by finite ones



- A refutation of Connes' embedding conjecture, a 44-year-old problem in operator algebra, via its known equivalence to Tsirelson's problem

[Connes '76]

[Fritz '12], [Junge, Navascués, and Palazuelos et al. '11], [Ozawa '13]



Review of Key Ideas and Techniques

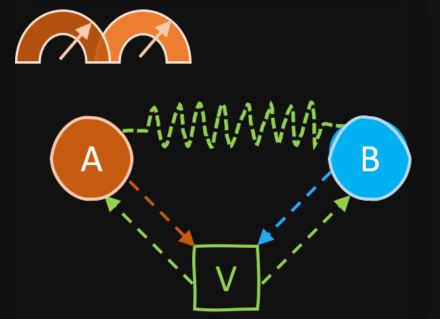
Distance Measures

- State-dependent distance:

$M_a^x \approx_\delta N_a^x$

Two collections of POVMs $\{M_a^x\}$ and $\{N_a^x\}$ acting on the same space are δ-close on state $|\psi\rangle$ under distribution μ if

$$\mathop{\mathbb{E}}_{x\sim\mu} \sum_a \left\| (M_a^x - N_a^x)|\psi\rangle \right\|^2 \leq \delta.$$

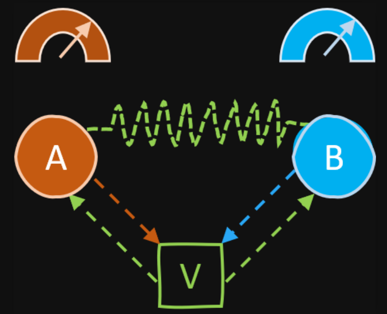


- Consistency:

$A_a^x \otimes I_{\mathrm{B}} \simeq_\delta I_{\mathrm{A}} \otimes B_a^x$

Two collections of POVMs $\{A_a^x\}$ and $\{B_a^x\}$ are δ-consistent on $|\psi\rangle$ under distribution μ if

$$\mathop{\mathbb{E}}_{x\sim\mu} \sum_{a\neq b} \langle\psi| A_a^x \otimes B_b^x |\psi\rangle \leq \delta.$$



- Cauchy-Schwarz

Entanglement Resistant Techniques

- The soundness problem of entanglement
- Confusion check: query Alice for the assignments to variables $\{x, y\}$, query Bob for x to ensure
$$R^x R^y \approx_\delta R^y R^x$$
- A third player (using monogamy of entanglement)
- Entangled games are NP-hard

[Kempe, Kobayashi, Matsumoto, Toner and Vidick '08]

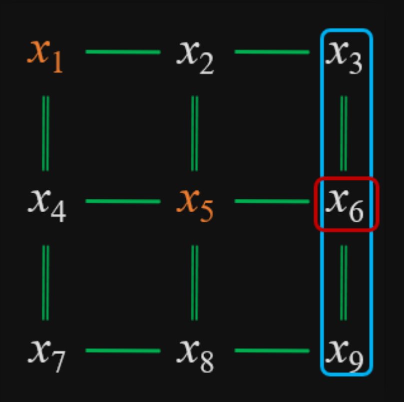
[Ito, Kobayashi and Matsumoto '09], [J. '13]

- Quantum soundness of the linearity test, multilinearity test, and low-degree test
- MIP = NEXP ⊆ MIP* *[Ito and Vidick '12]*

Rigidity and Self-testing

- The players have to measure the honest measurement to achieve a near-optimal value

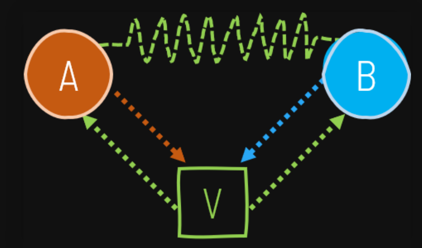
[Summers and Werner '85], [Mayers and Yao '98], [Reichardt, Unger and Vazirani '12]



- Magic Square game: all about commutativity and anticommutativity

[Wu, Bancal, McKague and Scarani '16]

- Where is the qubit? Find an anticommuting pair!



Let R_0, R_1 be two reflections, if $R_0 R_1 \approx_\delta -R_1 R_0$, then there is a local isomorphism ϕ such that up to the isomorphism

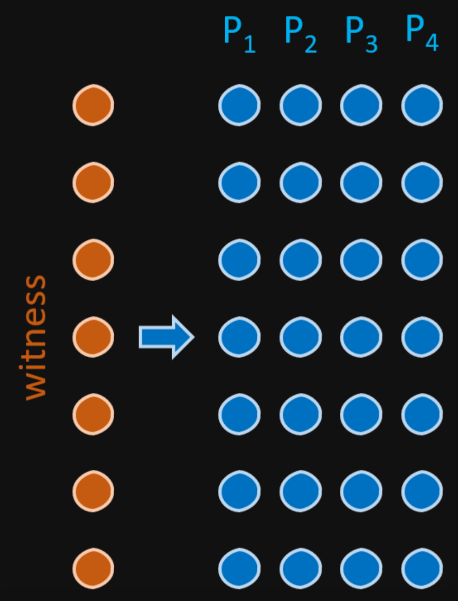
$$R_0 \approx_\delta \sigma^X \otimes I, \quad R_1 \approx_\delta \sigma^Z \otimes I.$$

Go Beyond NP Hardness

- Classical verification of QMA

  [Fitzsimons and Vidick '15], [J. '15]

- Encode each qubit in the QMA witness state with a quantum error detecting code
- Use rigidity to ensure that the provers measure Pauli X/Z's and use logical operator measurement to check the energy of the encoded state
- The initial idea emerged from discussions at a Simons Institute workshop in 2014



Pauli Basis Game

- A wrapper around the quantum low-degree test

[Natarajan and Vidick '18], [Natarajan and Wright '19]

Rigidity Theorem. For any strategy that uses measurement $\hat{A}^{\mathrm{Pauli},W}$ for the question (Pauli, W) and has value at least $1-\varepsilon$, there is a local isomorphism $\phi = \phi_A \otimes \phi_B$ such that

$$A_z^{\mathrm{Pauli},W} \otimes I_B \approx_{\delta(\varepsilon)} \sigma_z^W \otimes I_B,$$

where $A_z^{\mathrm{Pauli},W} = \phi_A \hat{A}^{\mathrm{Pauli},W} \phi_A^*$.

- An efficient self-test for Pauli X/Z measurements on EPRs

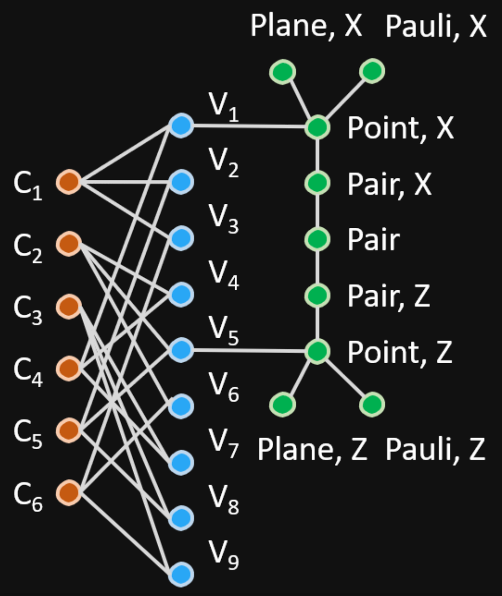
  For self-testing of n EPRs, the questions have length $\mathrm{polylog}(n)$

- (Pauli, W) primitive

Question Distribution of the Pauli Basis Game

- Random seed $z = (u_X, u_Z, v_1, v_2, r_X, r_Z) \in (\mathbb{F}^m)^4 \times \mathbb{F}^2$

Type	u_X	u_Z	v_1	v_2	r_X	r_Z
Point, X	u_X	0	0	0	0	0
Plane, X	$L^{\mathrm{Pl}}_{v_1,v_2}(u_X)$	0	v_1	v_2	0	0
Point, Z	0	u_Z	0	0	0	0
Plane, Z	0	$L^{\mathrm{Pl}}_{v_1,v_2}(u_Z)$	0	v_1	v_2	0
Pair	u_X	u_Z	0	0	r_X	r_Z
Pair, W	u_X	u_Z	0	0	r_X	r_Z
Constraint$_c$	u_X	u_Z	0	0	r_X	r_Z
Variable$_v$	u_X	u_Z	0	0	r_X	r_Z
Pauli, W	0	0	0	0	0	0



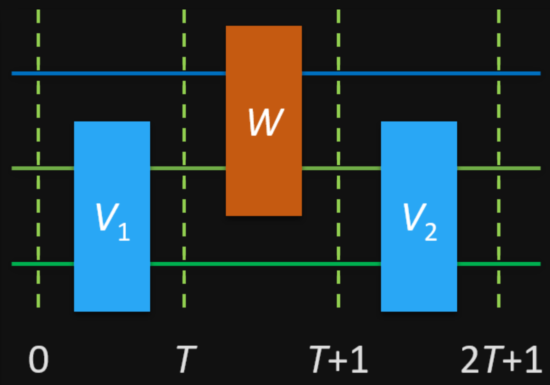
- All questions have the form (type, content) for type from a discrete set of labels and content from $\mathbb{F}^{4m+2}$

Compression

- Why compression?
- Go beyond QMA hardness
  - More sophisticated relations from rigidity: beyond anticommutativity *[Slofstra '17]*

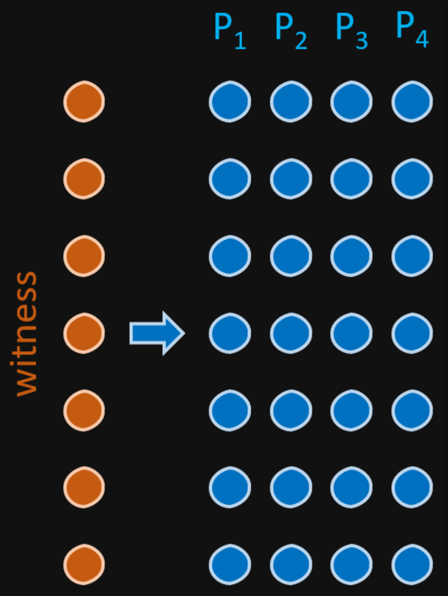
    Conjugacy relation $xyx = z$
  - QIP = QMAM is not that far from QMA *[Marriott and Watrou '05]*
- Propagation checking (circuit-to-Hamiltonian construction) for MIP*
- Compression of MIP*

[J. '16], [Fitzsimons, J., Vidick and Yuen '18]



- A comparison between quantum and classical

	MIP	Classical Games	MIP*	Entangled Games
Msg size	poly	log	poly	log
Hardness	NEXP	NP	MIP*	MIP*
Gap	const	poly^{-1} or const	const	poly^{-1}



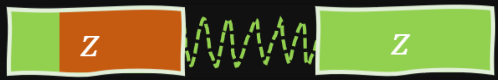
- Gap amplification (or social distancing for the completeness and soundness)?
- Throw in some PCPs?

Introspection

- Let the players sample from the question distribution themselves!

  [Natarajan and Wright '19]

- Utilize the Heisenberg Uncertainty Principle to design what to reveal and what to hide



- Let L^{A} and L^{B} be functions such that $(L^{\mathrm{A}}(z), L^{\mathrm{B}}(z))$ is the desired question distribution μ for uniformly random z
- The Intro primitive

The player receiving (Intro, v) replies (y, a) where for $v \in \{\mathrm{A}, \mathrm{B}\}$

1. the introspectively sampled question y is supposedly $L^{v}(z)$ and,
2. a is the answer in the original game of player v for question y.

Putting Everything Together

Four Steps of Compression

1. Introspection

   Question reduction

2. Oracularisation

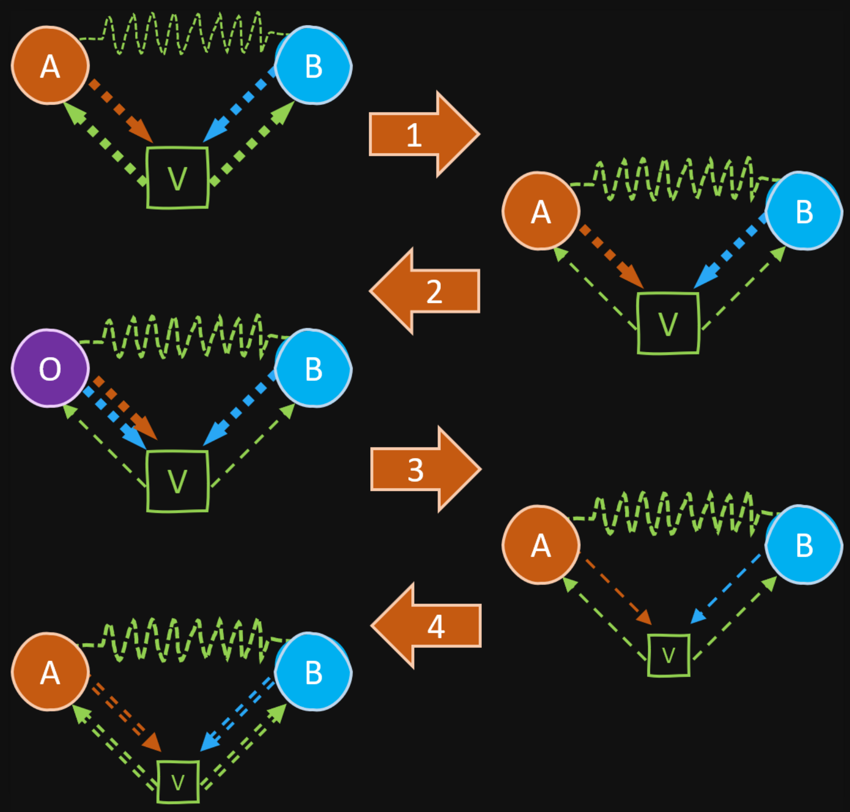
   Preprocessing for PCP

3. PCP

   Answer reduction

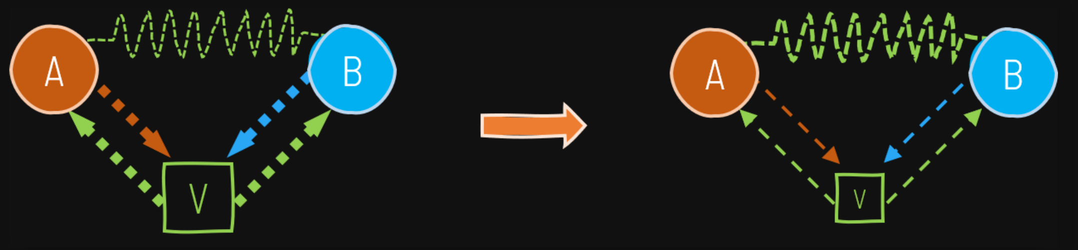
4. Parallel repetition

   Gap recovery



Recursive Gap-preserving Compression of Normal-form Games

- What is missing from $\mathrm{Compress}^{\mathrm{NW}}$?

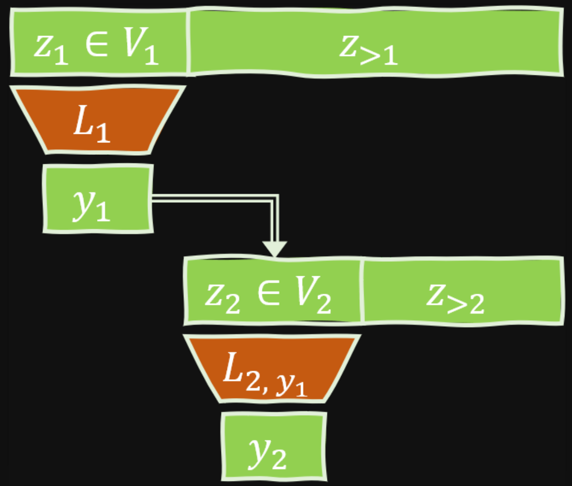


- What normal form?
- Two problems are important

$$\left(L^{\mathrm{A}}(z), L^{\mathrm{B}}(z)\right)$$

  1. What kind of distributions/functions can be introspectively sampled
  2. What is the distribution of the compressed game
- Match the two?

Conditionally Linear Functions



- Choose a register subspace V_1 of $\mathbb{F}^n$
- Apply a linear function $L_1 : V_1 \to V_1$ and get $y_1 = L_1(z^{V_1}) \in V_1$
- Conditioned on y_1, choose another subspace $V_{2,\,y_1}$ that has trivial intersection with V_1
- Apply linear function $L_{2,\,y_1}(z^{V_{2,\,y_1}})$ to get $y_2 \in V_{2,\,y_1}$
- Repeat the above ℓ times (levels) to get $y_1, y_2, \ldots, y_\ell$
- Define the output of the function to be $y = y_1 + y_2 + \cdots + y_\ell$
- Such a function $L : z \mapsto y$ is call conditionally linear

Why CL Functions?

- Linear functions

  Revealing and hiding linear information is easy

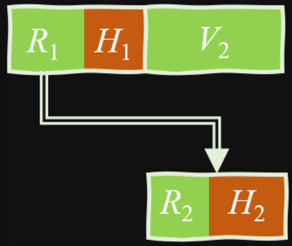
- Linear functions aren't enough

Type	u_X	u_Z	v_1	v_2	r_X	r_Z
Plane, X	$L^{\text{Pl}}_{v_1,v_2}(u_X)$	0	v_1	v_2	0	0
Plane, Z	0	$L^{\text{Pl}}_{v_1,v_2}(u_Z)$	0	v_1	v_2	0

- CL functions work as they can model all question distributions we use and have nice closure properties
  - Most importantly, the question distribution of Pauli Basis game is CL for fixed types

Introspection for CL Distributions (2-level)

	R_1	H_1	R_2	H_2	aux	answer format
Intro, A	Z	I	Z	I	yes	(y, a)
Sample, A	Z	Z	Z	Z	yes	(z, a)
Read, A	Z	X	Z	X	yes	$(y, y^{\perp}, a)$
Hide_2	Z	X	I	X	no	$(y, y^{\perp}, x)$
Hide_1	I	X	X	X	no	$(y, y^{\perp}, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z



1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection for CL Distributions (2-level)

	R_1	H_1	R_2	H_2	aux	answer format
$\mathrm{Intro, A}$	Z	I	Z	I	yes	(y, a)
$\mathrm{Sample, A}$	Z	Z	Z	Z	yes	(z, a)
$\mathrm{Read, A}$	Z	X	Z	X	yes	$(y, y^{\perp}, a)$
Hide_2	Z	X	I	X	no	$(y, y^{\perp}, x)$
Hide_1	I	X	X	X	no	$(y, y^{\perp}, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

$L^{\mathrm{A}}(z) = y$

1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection for CL Distributions (2-level)

	R_1	H_1	R_2	H_2	aux	answer format
Intro, A	Z	I	Z	I	yes	(y, a)
Sample, A	Z	Z	Z	Z	yes	(z, a)
Read, A	Z	X	Z	X	yes	$(y, y^{\perp}, a)$
Hide_2	Z	X	I	X	no	$(y, y^{\perp}, x)$
Hide_1	I	X	X	X	no	$(y, y^{\perp}, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection for CL Distributions (2-level)

	R_1	H_1	R_2	H_2	aux	answer format
$\mathrm{Intro, A}$	Z	I	Z	I	yes	(y, a)
$\mathrm{Sample, A}$	Z	Z	Z	Z	yes	(z, a)
$\mathrm{Read, A}$	Z	X	Z	X	yes	$(y, y^\perp, a)$
Hide_2	Z	X	I	X	no	$(y, y^\perp, x)$
Hide_1	I	X	X	X	no	$(y, y^\perp, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection for CL Distributions (2-level)

	R_1	H_1	R_2	H_2	aux	answer format
Intro, A	Z	I	Z	I	yes	(y, a)
Sample, A	Z	Z	Z	Z	yes	(z, a)
Read, A	Z	X	Z	X	yes	$(y, y^{\perp}, a)$
Hide_2	Z	X	I	X	no	$(y, y^{\perp}, x)$
Hide_1	I	X	X	X	no	$(y, y^{\perp}, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection for CL Distributions (2-level)

	R_1	H_1	R_2	H_2	aux	answer format
Intro, A	Z	I	Z	I	yes	(y, a)
Sample, A	Z	Z	Z	Z	yes	(z, a)
Read, A	Z	X	Z	X	yes	$(y, y^\perp, a)$
Hide_2	Z	X	I	X	no	$(y, y^\perp, x)$
Hide_1	I	X	X	X	no	$(y, y^\perp, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection for CL Distributions (2-level)

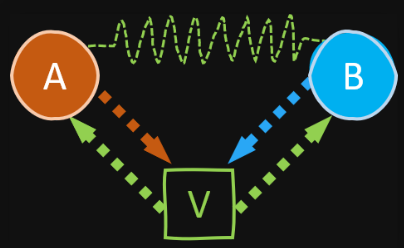
	R_1	H_1	R_2	H_2	aux	answer format
Intro, A	Z	I	Z	I	yes	(y, a)
Sample, A	Z	Z	Z	Z	yes	(z, a)
Read, A	Z	X	Z	X	yes	$(y, y^{\perp}, a)$
Hide_2	Z	X	I	X	no	$(y, y^{\perp}, x)$
Hide_1	I	X	X	X	no	$(y, y^{\perp}, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

1. Use Sample and Read types to perform data hiding for Intro
2. Cross check between Sample and Pauli, Z to ensure honest Z measurements
3. Cross check between Read, Hide_i, and Pauli, X to ensure honest X measurements

Introspection Game Review

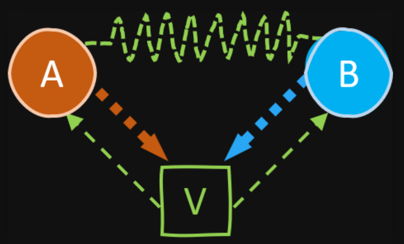
- The standard way a normal-form game $\mathcal{V}_n$ is played

1. The verifier samples $z \in \mathbb{F}^n$, calls $\mathcal{S}_n$ to compute questions $x = L^{\mathrm{A}}(z)$ and $y = L^{\mathrm{B}}(z)$,
2. Receives answers a, b and decides using $\mathcal{D}_n$.



- The introspective way a normal-form game $\mathcal{V}_n$ is played

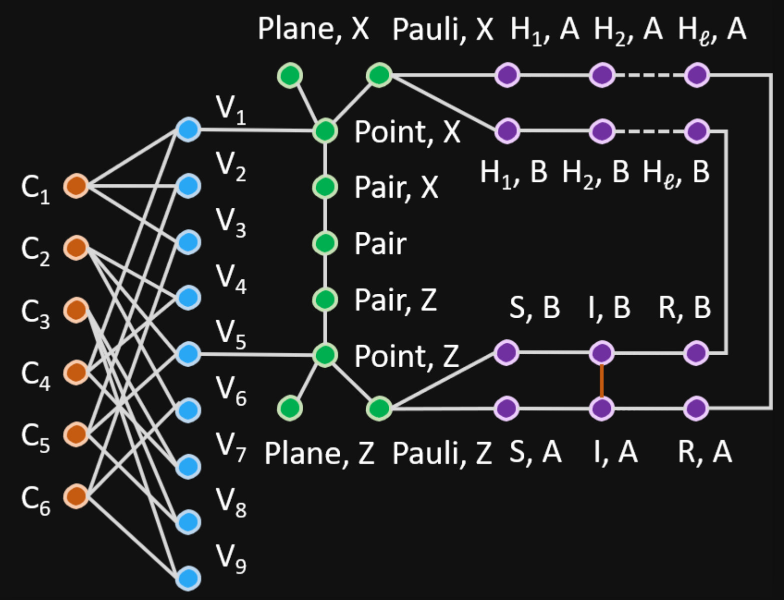
1. The verifier runs Pauli Basis game over EPRs of dimension $|\mathbb{F}|^n$, or,
2. Runs the remaining parts of the Introspection game to ensure provers respect the Intro primitives, or,
3. Sends $(\mathrm{Intro}, \mathrm{A})$ to Alice and $(\mathrm{Intro}, \mathrm{B})$ to Bob, receives (x, a), (y, b), and decides using $\mathcal{D}_n$.



Question Distribution of the Introspection Game

- Random seed $z = (u_X, u_Z, v_1, v_2, r_X, r_Z) \in (\mathbb{F}^m)^4 \times \mathbb{F}^2$

Type	u_X	u_Z	v_1	v_2	r_X	r_Z
Pauli Basis Types	-	-	-	-	-	-
Intro, v	0	0	0	0	0	0
Sample, v	0	0	0	0	0	0
Read, v	0	0	0	0	0	0
Hide_i, v	0	0	0	0	0	0



- For each type, the functions are CL
- CL distributions can simulate constant-size type distributions
- Constant (eight) levels of conditioning suffice for our purpose

Question Distribution of the Introspection Game

- Random seed $z = (u_X, u_Z, v_1, v_2, r_X, r_Z) \in (\mathbb{F}^m)^4 \times \mathbb{F}^2$

Type	u_X	u_Z	v_1	v_2	r_X	r_Z
Pauli Basis Types	-	-	-	-	-	-
Intro, v	0	0	0	0	0	0
Sample, v	0	0	0	0	0	0
Read, v	0	0	0	0	0	0
Hide_i, v	0	0	0	0	0	0

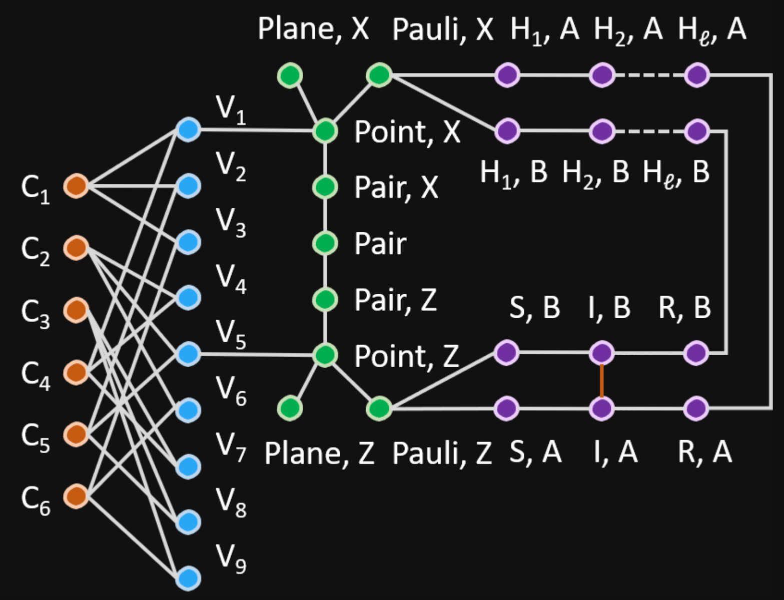
Type	u_X	u_Z	v_1	v_2
Point, X	u_X	0	0	0
Plane, X	$L^{\text{Pl}}_{v_1,v_2}(u_X)$	0	v_1	v_2
Point, Z	0	u_Z	0	0
Plane, Z	0	$L^{\text{Pl}}_{v_1,v_2}(u_Z)$	0	v_1
Pair	u_X	u_Z	0	0
Pair, W	u_X	u_Z	0	0
Constraint_c	u_X	u_Z	0	0
Variable_v	u_X	u_Z	0	0
Pauli, W	0	0	0	0

- For each type, the functions are CL
- CL distributions can simulate constant-size type distributions
- Constant (eight) levels of conditioning suffice for our purpose

Question Distribution of the Introspection Game

- Random seed $z = (u_X, u_Z, v_1, v_2, r_X, r_Z) \in (\mathbb{F}^m)^4 \times \mathbb{F}^2$

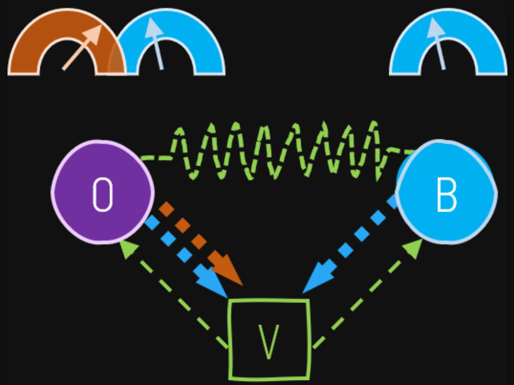
Type	u_X	u_Z	v_1	v_2	r_X	r_Z
Pauli Basis Types	-	-	-	-	-	-
Intro, v	0	0	0	0	0	0
Sample, v	0	0	0	0	0	0
Read, v	0	0	0	0	0	0
Hide_i, v	0	0	0	0	0	0



- For each type, the functions are CL
- CL distributions can simulate constant-size type distributions
- Constant (eight) levels of conditioning suffice for our purpose

Oracularisation and Commuting Strategy

- For the PCP techniques to work in answer reduction, one of the provers must compute a PCP proof that depends on x, y, a, b
- This is achieved by the oracularization and requires that, in the completeness strategies, Alice and Bob always measure commuting observables (as operators on the same space)
- Special care required in the design of the game



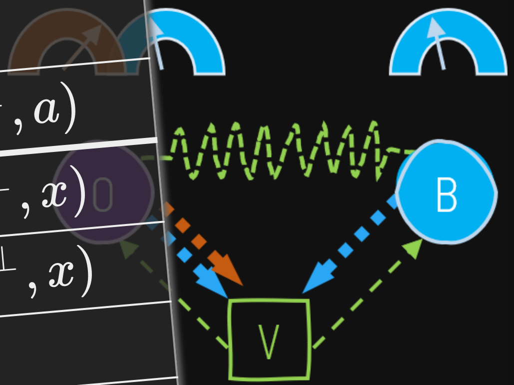
Multiple Hide types in the Introspection game

Oracularisation and Commuting Strategy

- For the PCP techniques to work in answer reduction, one of the provers must compute a PCP proof that depends on x, y, a, b
- This is achieved by the oracularization and requires that, in the completeness strategies, Alice and Bob always measure commuting observables (as operators on the same space)
- Special care required in the design of the game

  Multiple Hide types in the Introspection game

	R_1	H_1	R_2	H_2	aux	answer format
Intro, A	Z	I	Z	I	yes	(y, a)
Sample, A	Z	Z	Z	Z	yes	(z, a)
Read, A	Z	X	Z	X	yes	$(y, y^\perp, a)$
Hide_2	Z	X	I	X	no	$(y, y^\perp, x)$
Hide_1	I	X	X	X	no	$(y, y^\perp, x)$
Pauli, X	X	X	X	X	no	x
Pauli, Z	Z	Z	Z	Z	no	z

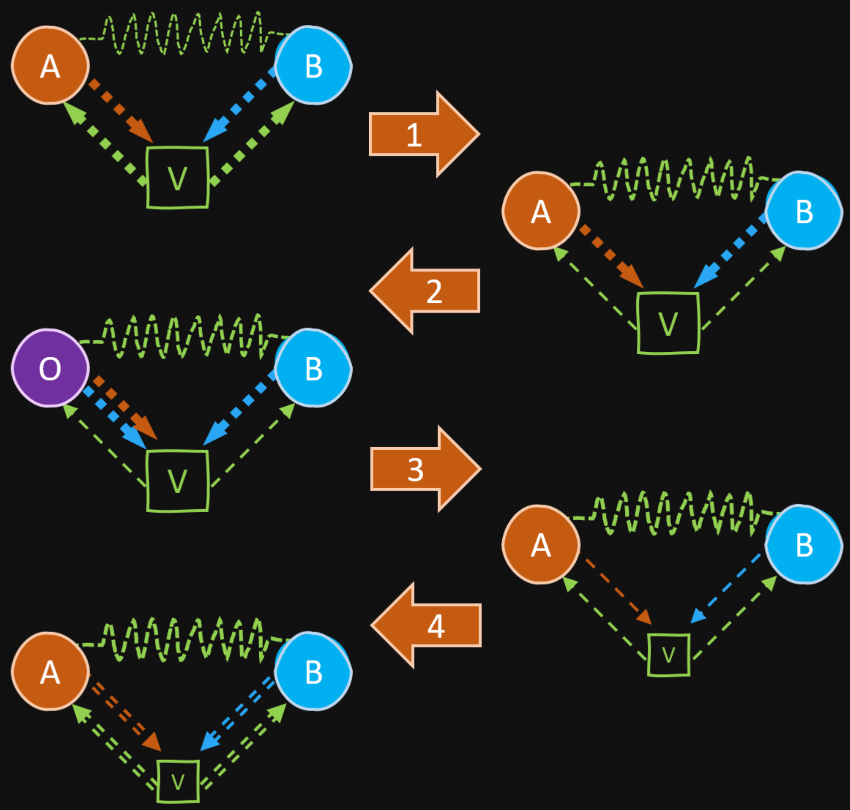


PCPs and Parallel Repetitions

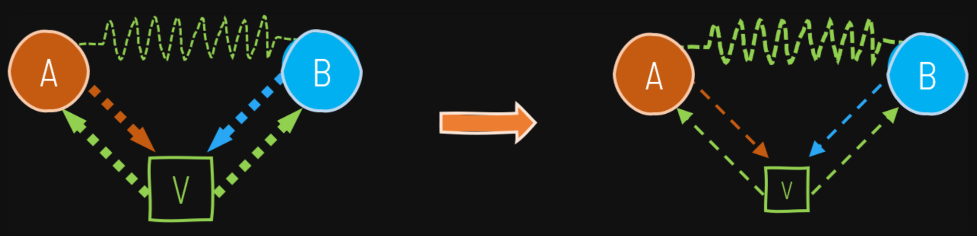
- The use of PCPs for answer reduction is similar to Natarajan-Wright
- The distribution remains CL
- Anchored parallel repetition for better entanglement bound

[Bavarian, Vidick, and Yuen '17]

- Gap-preserving compression of normal-form games



Compression Theorem



Compression Theorem. There is an algorithm Compress that on input $\mathcal{V}$ outputs $\mathcal{V}^\sharp = (\mathcal{S}^\sharp, \mathcal{D}^\sharp)$ such that for all $n \geq n_0$

1. (Completeness). If $\mathrm{val}^*(\mathcal{V}_{2^n}) = 1$ then $\mathrm{val}^*(\mathcal{V}_n^\sharp) = 1$.
2. (Soundness). If $\mathrm{val}^*(\mathcal{V}_{2^n}) \leq \frac{1}{2}$ then $\mathrm{val}^*(\mathcal{V}_n^\sharp) \leq \frac{1}{2}$.
3. (Entanglement). $\mathcal{E}(\mathcal{V}_n^\sharp) \geq \max\{\mathcal{E}(\mathcal{V}_{2^n}), 2^n\}$.

Kleene's Recursion Theorem

- For all Turing machine $\mathcal{M}$, consider verifier $\mathcal{V}^{\mathrm{Halt}}$

> Turing machine $\mathcal{D}^{\mathrm{Halt}}$:
>
> 1. Simulate $\mathcal{M}$ for n steps. If $\mathcal{M}$ halts, accept.
> 2. Compute $(\mathcal{S}^\sharp, \mathcal{D}^\sharp) = \mathrm{Compress}(\mathcal{S}^\sharp, \mathcal{D}^{\mathrm{Halt}})$.
> 3. Accept iff $\mathcal{D}^\sharp(n, x, y, a, b)$ accepts.

$\mathcal{S}^\sharp$ is universal

- Kleene's recursion theorem: $\mathcal{D}^{\mathrm{Halt}}$ above is well-defined
- For all Turing machine $\mathcal{M}$
  1. If $\mathcal{M}$ halts, $\mathrm{val}^*(\mathcal{V}_{n_0}^{\mathrm{Halt}}) = 1$

     If the Turing machine $\mathcal{M}$ halts in T steps and $n < T \leq 2^n$, then $\mathrm{val}^*(\mathcal{V}_n^{\mathrm{Halt}}) = \mathrm{val}^*(\mathcal{V}_n^\sharp) = \mathrm{val}^*(\mathcal{V}_{2^n}^{\mathrm{Halt}}) = 1.$
  2. If $\mathcal{M}$ does not halt, $\mathrm{val}^*(\mathcal{V}_{n_0}^{\mathrm{Halt}}) \leq \frac{1}{2}$

Explicit Separation Between val^* and $\mathrm{val}^{\mathrm{co}}$

- Consider verifier $\mathcal{V}^{\mathrm{Sep}} = (\mathcal{S}^\sharp, \mathcal{D}^{\mathrm{Sep}})$

Turing machine $\mathcal{D}^{\mathrm{Sep}}$:

1. Compute a description of game $\mathcal{V}^{\mathrm{Sep}}_{n_0}$.
2. Run NPA on $\mathcal{V}^{\mathrm{Sep}}_{n_0}$ for n steps. If NPA halts, then accept.
3. Compute $(\mathcal{S}^\sharp, \mathcal{D}^\sharp) = \mathrm{Compress}(\mathcal{S}^\sharp, \mathcal{D}^{\mathrm{Sep}})$.
4. Accept iff $\mathcal{D}^\sharp(n, x, y, a, b)$ accepts.

- Claim: $\mathrm{val}^*(\mathcal{V}^{\mathrm{Sep}}_{n_0}) \leq \frac{1}{2}$ and $\mathrm{val}^{\mathrm{co}}(\mathcal{V}^{\mathrm{Sep}}_{n_0}) = 1$
- If $\mathrm{val}^{\mathrm{co}}(\mathcal{V}^{\mathrm{Sep}}_{n_0}) < 1$, then $\mathrm{val}^*(\mathcal{V}^{\mathrm{Sep}}_{n_0}) = 1$, a contradiction

Conclusions

- Recursive gap-preserving compression of normal-form two-prover one-round protocols
- Compression Lemma + Kleene's recursion theorem proves $\mathrm{RE} \subseteq \mathrm{MIP}^*$
- $\mathrm{MIP}^* = \mathrm{RE}$ follows as $\mathrm{MIP}^* \subseteq \mathrm{RE}$
- Negative answers to both Tsirelson's problem and CEP
- Open problems:
    1. Simpler proofs?
    2. Does $\mathrm{MIP}^{co} = \mathrm{coRE}$?
    3. Explicit counter-examples to CEP

Physics

- 1935 EPR paradox, entanglement
- 1964 Bell inequality
- 1990's Tsirelson's problem

Computer Science

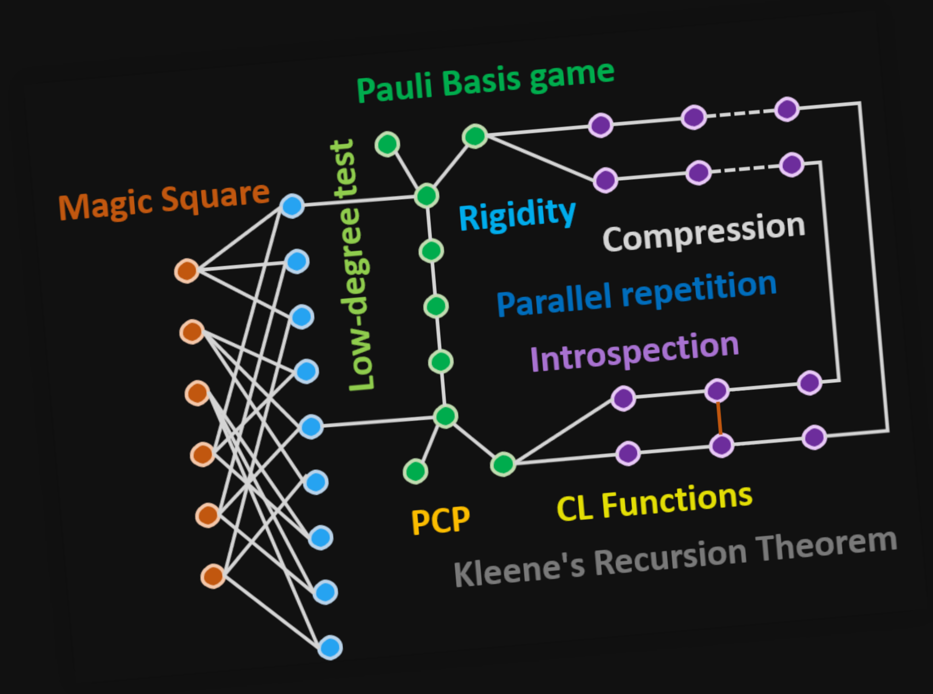
- 1936 Turing's Halting problem
- 1970's Complexity theory
- 1990's PCP theorem

Mathematics

- 1930 von Neumann algebra
- 1976 Connes
- 1993 Kirchberg

MIP* = RE

Thank you!



Pauli Basis game
Magic Square
Low-degree test
Rigidity
Compression
Parallel repetition
Introspection
PCP
CL Functions
Kleene's Recursion Theorem