The quantum moment problem

Stephanie Wehner

Joint work with Andrew Doherty, Yeong-Cherng Liang and Ben Toner (0803.4373)

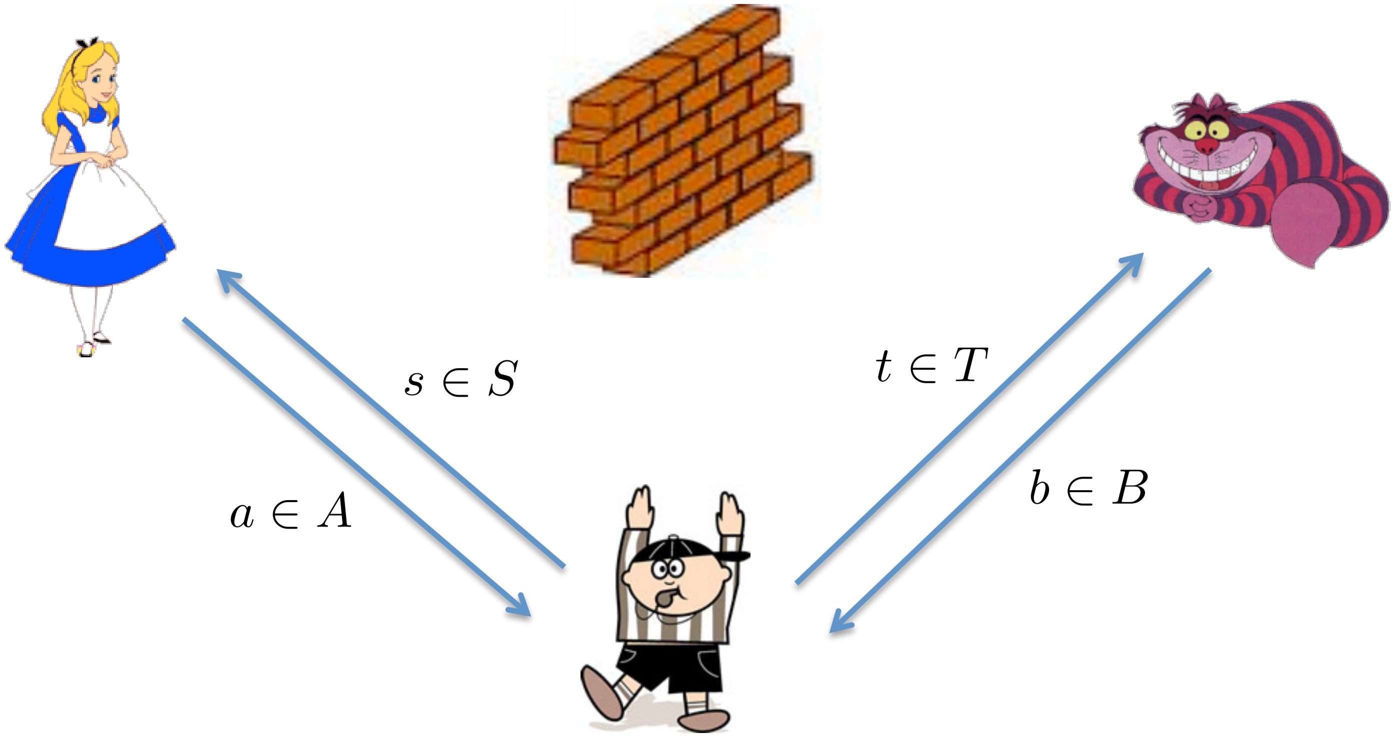
Centre for Quantum Technologies

NUS
National University of Singapore

Outline

- Motivation: non-local games
- What was known
- Optimization and non-local games
- The general quantum moment problem
- Open questions

Motivation: non-local games



Distribution $\pi(s,t)$

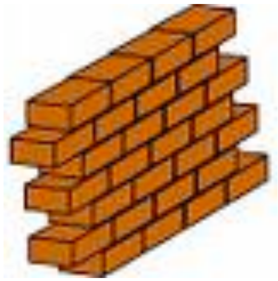
Rules of the game given by predicate $V : A \times B \times S \times T \to \{0,1\}$

Alice and Bob win if and only if $V(a,b|s,t) = 1$

What's the probability that Alice and Bob win the game?

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \Pr[a,b|s,t]$$

Non-signaling strategies



$s \in S$ $\quad$ $t \in T$

$a \in A$ $\quad$ $b \in B$

$$\Pr[a|s,t] = \sum_b \Pr[a,b|s,t]$$

$$\Pr[b|s,t] = \sum_a \Pr[a,b|s,t]$$

Distribution $\pi(s,t)$

Any non-signaling distribution is allowed

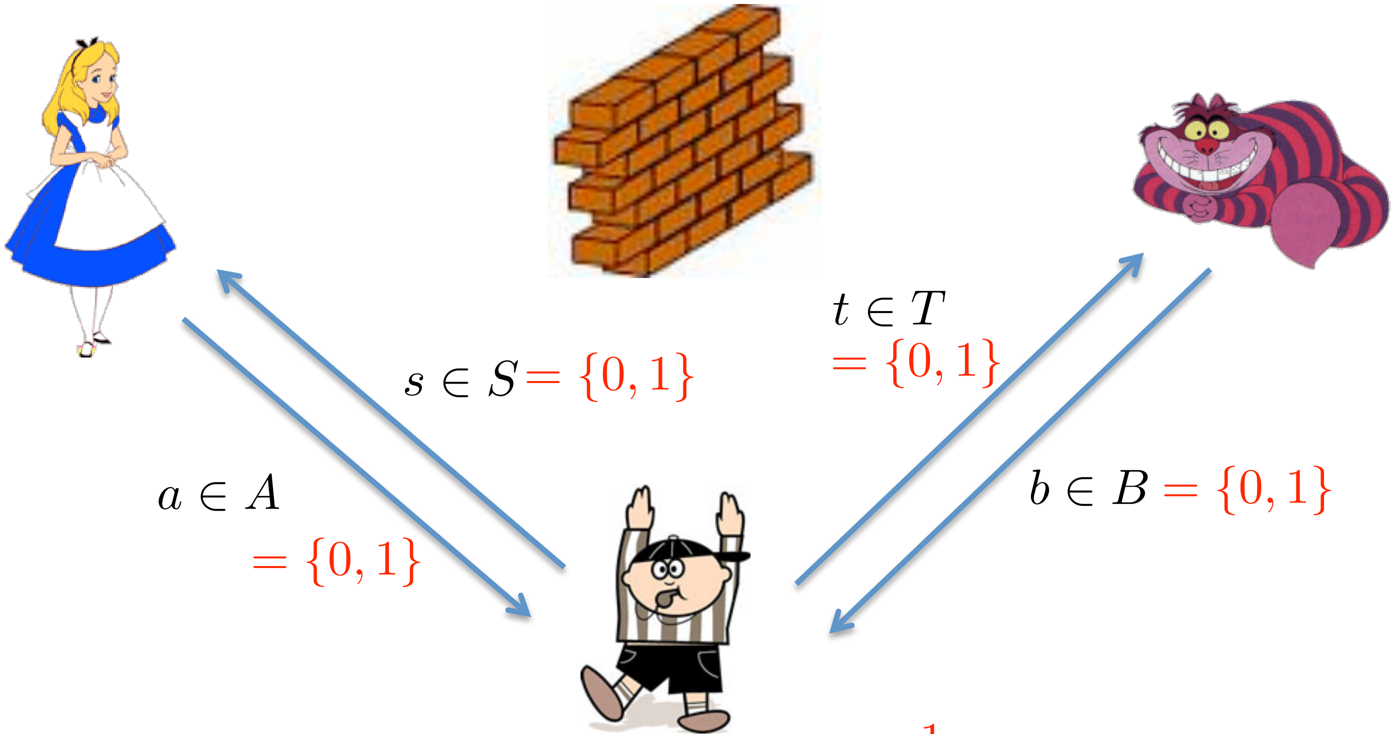
$\forall a, s \forall t, t' \qquad \Pr[a|s,t] = \Pr[a|s,t']$

$\forall b, t \forall s, s' \qquad \Pr[b|s,t] = \Pr[b|s',t]$

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \Pr[a,b|s,t]$$

Linear program!

Example: The CHSH game (no-signaling)

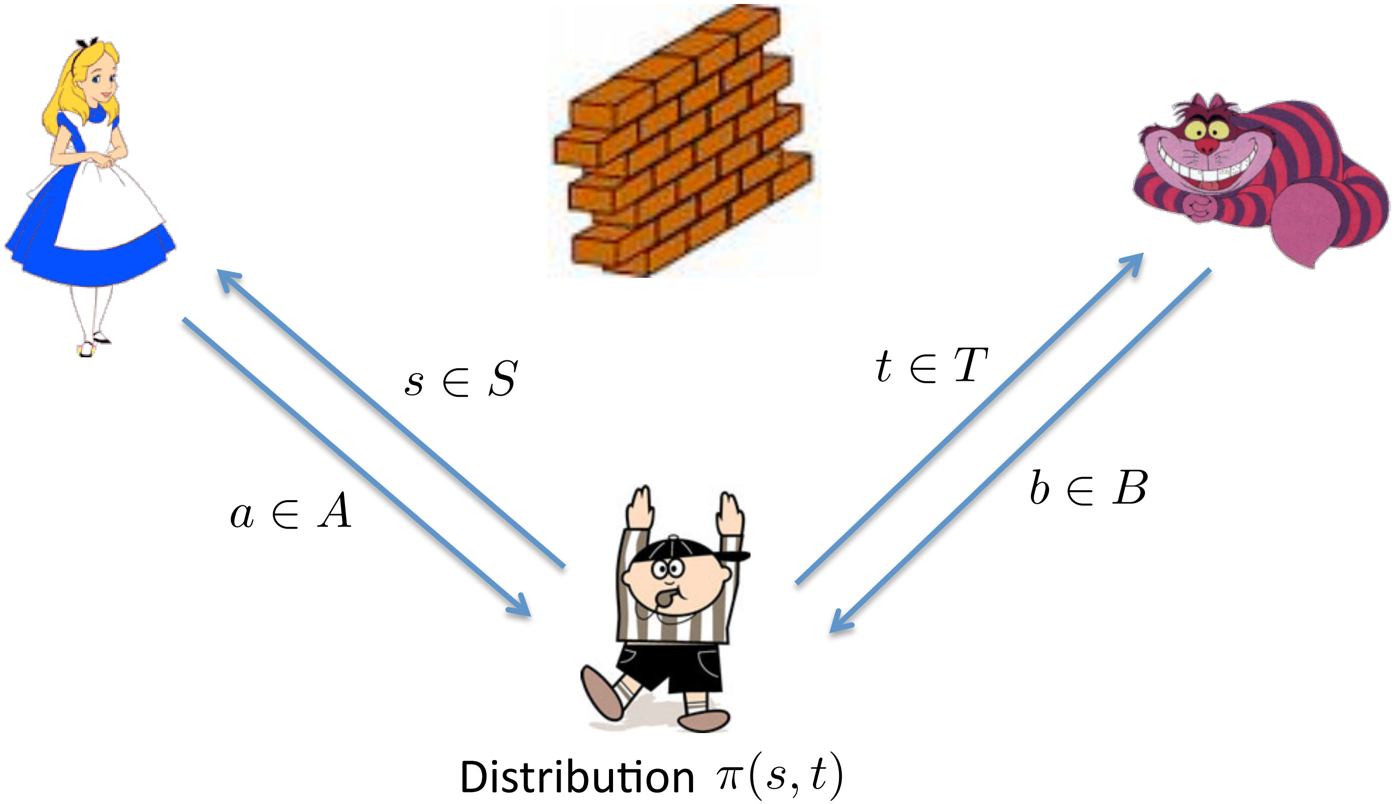


Distribution $\pi(s,t) = \frac{1}{4}$

Rules: Alice and Bob win if and only if $s \cdot t = a + b \mod 2$

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \Pr[a,b|s,t] = 1$$

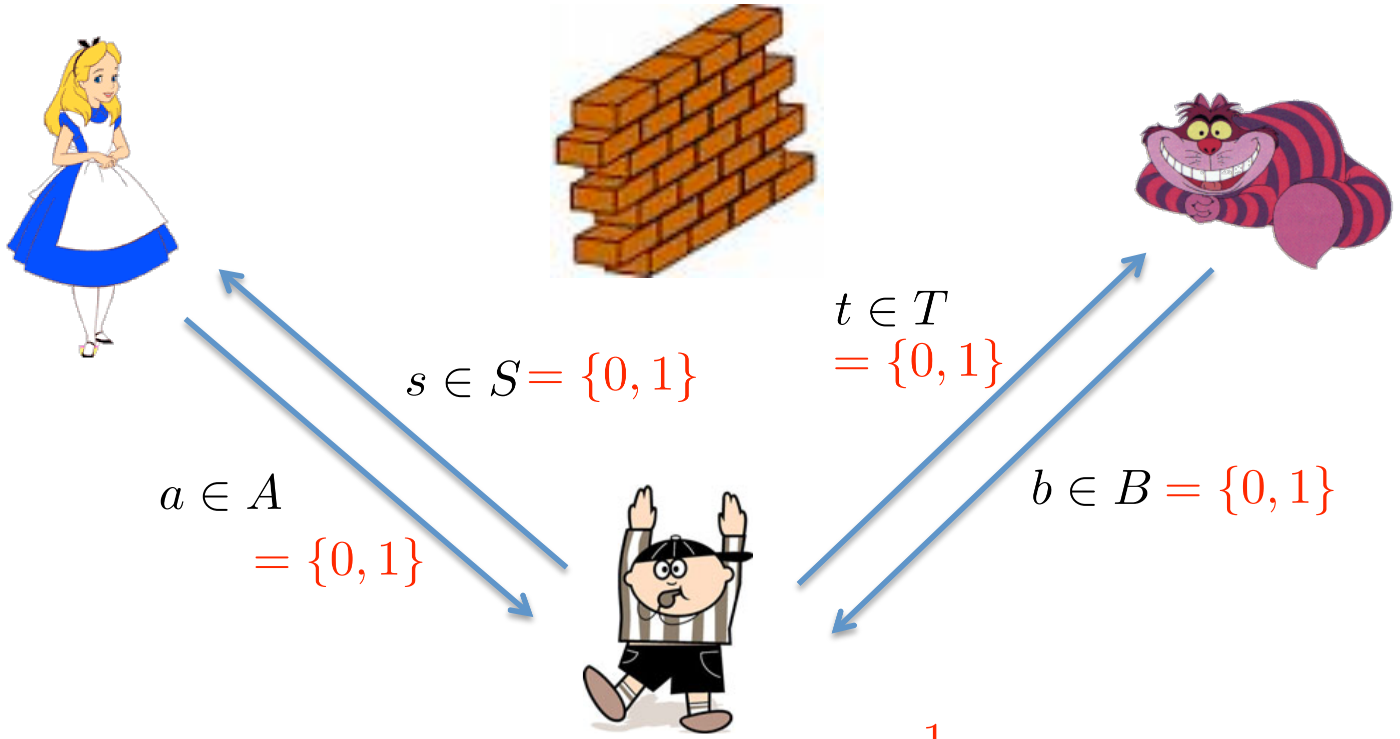
Classical strategies



$$a_r : S \to A$$
$$b_r : T \to B$$

$$p = \max \sum_{s,t} \pi(s,t) V(a_r(s), b_r(t) | s,t)$$

Example: The CHSH game (classical)



Distribution $\pi(s,t) = \frac{1}{4}$

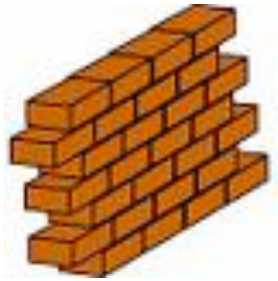
Rules: Alice and Bob win if and only if $s \cdot t = a + b \mod 2$

$$p = \max \sum_{s,t} \pi(s,t) V(a_r(s), b_r(t)|s,t) = \frac{3}{4}$$

$$a_r(s) = 0$$

$$b_r(s) = 0$$

Quantum strategies



$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle$$

$b \in B$

Distribution $\pi(s,t)$

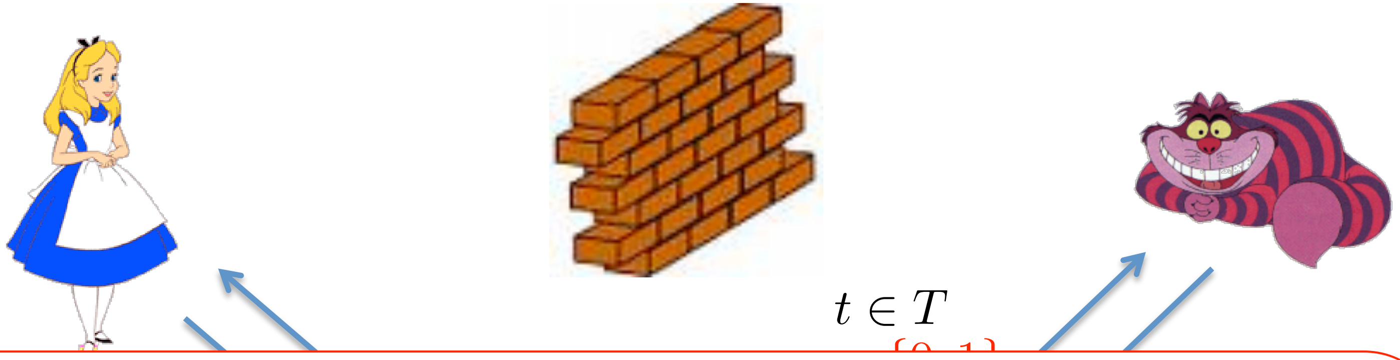
1. Shared quantum state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$
2. Quantum measurements

$$A_s = \{A_s^a \in \mathcal{B}(\mathcal{H}_A)\}_{a \in A} \qquad \forall s, a \ A_s^a \geq 0 \qquad \forall s \ \sum_a A_s^a = \mathbb{I}$$

$$B_t = \{B_t^b \in \mathcal{B}(\mathcal{H}_B)\}_{b \in B} \qquad \forall t, b \ B_t^b \geq 0 \qquad \forall t \ \sum_b B_t^b = \mathbb{I}$$

$$\Pr[a,b|s,t] = \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle$$

Example: The CHSH game (quantum)



In quantum mechanics, Alice and Bob are more restricted than no-signaling: For CHSH, $p_{\text{classical}} < p_{\text{quantum}} < p_{\text{nosignaling}}$

In general,

$$p_{\text{classical}} \leq p_{\text{quantum}} \overset{?}{\leq} p_{\text{nosignaling}}$$

Rules: Alice and Bob win if and only if $s \cdot t = a + b \mod 2$

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$$

$$\left(> \frac{3}{4} \text{ classical} \right)$$

Non-local games in physics

- Known as Bell inequalities (Bell ’65)
- Experimentally verify that nature is not classical

  (Aspect, Grangier, Roger ‘82….)

  - Play game many times
  - Estimate success probability

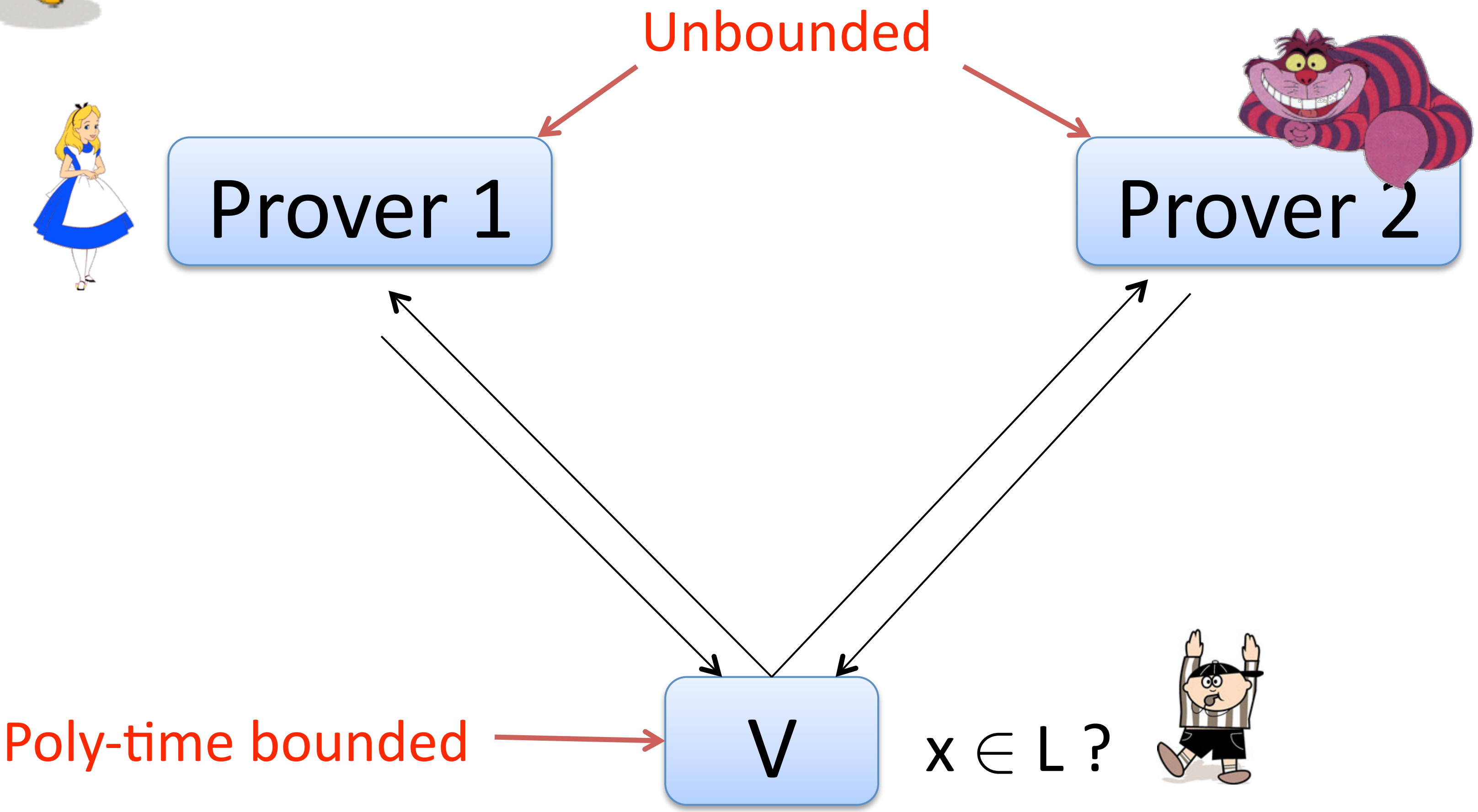
- What is the maximum success probability?
- What is the difference to the classical case?

Non-local games in information theory and cryptography

- Cryptography: If Alice and Bob can win the game with high probability, they are uncorrelated with an eavesdropper.

- Information theory: Bounds on the success probability give bounds on coding problems.

Non-local games in computer science

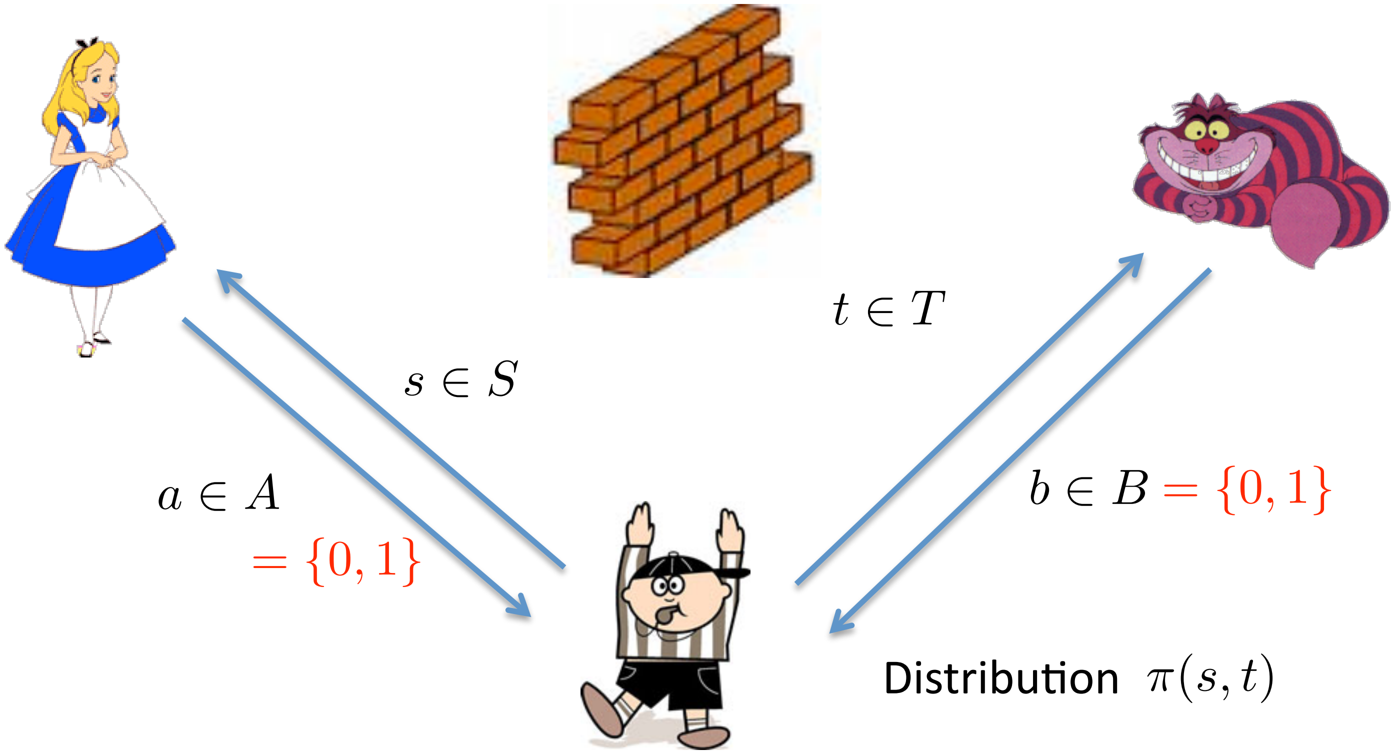


- If $x \in L$, then there exists a strategy for the provers to win with probability $p \geq c$
- Otherwise, then for any strategy of the provers, they win only with probability $p \leq s$

Outline

- Motivation: non-local games
- What was known
- Optimization and non-local games
- The general quantum moment problem
- Open questions

XOR-games



Decide whether Alice and Bob win based on $c = a + b \mod 2$

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle$$

$$= \max_{\substack{\{a_s\}_{s \in S} \\ \{b_t\}_{t \in T}}} \frac{1}{2} \sum_{s,t} \pi(s,t) \sum_{c} V(c|s,t)(1 + (-1)^c \, a_s \cdot b_t)$$

$$a_s, b_t \in \mathbb{R}^{\min |T|,|S|} \quad \|a_s\|_2, \|b_t\|_2 = 1$$

Optimal solution is easy to find!

Wehner, quant-ph/0510076

What is known

- $\oplus\mathrm{MIP}^* \subseteq \mathrm{QIP}$ (Wehner quant-ph/0508201)
- QIP = PSPACE (Jain, Ji, Upadhyay, Watrous 0907.4737)
- Can approximate the value of a unique game to within a certain accuracy in polynomial time (Kempe, Regev, Toner 0710.0655)
- … but nothing for general games!

Outline

- Motivation: non-local games
- What was known
- Optimization and non-local games
- The general quantum moment problem
- Open questions

Goal

- Find upper bound on the winning probability

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle$$

$$\text{minimize } \nu$$

$$\nu \mathbb{I} - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_s^a \otimes B_t^b \geq 0$$

Quantum measurements

$$\forall s,a \; A_s^a \geq 0 \qquad \forall t,b \; B_t^b \geq 0$$

$$\forall s \; \sum_a A_s^a = \mathbb{I} \qquad \forall t \; \sum_a B_t^b = \mathbb{I}$$

Goal

- Find upper bound on the winning probability

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle$$

$$\text{minimize } \nu$$

$$\nu \mathbb{I} - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_s^a \otimes B_t^b \geq 0$$

Quantum measurements

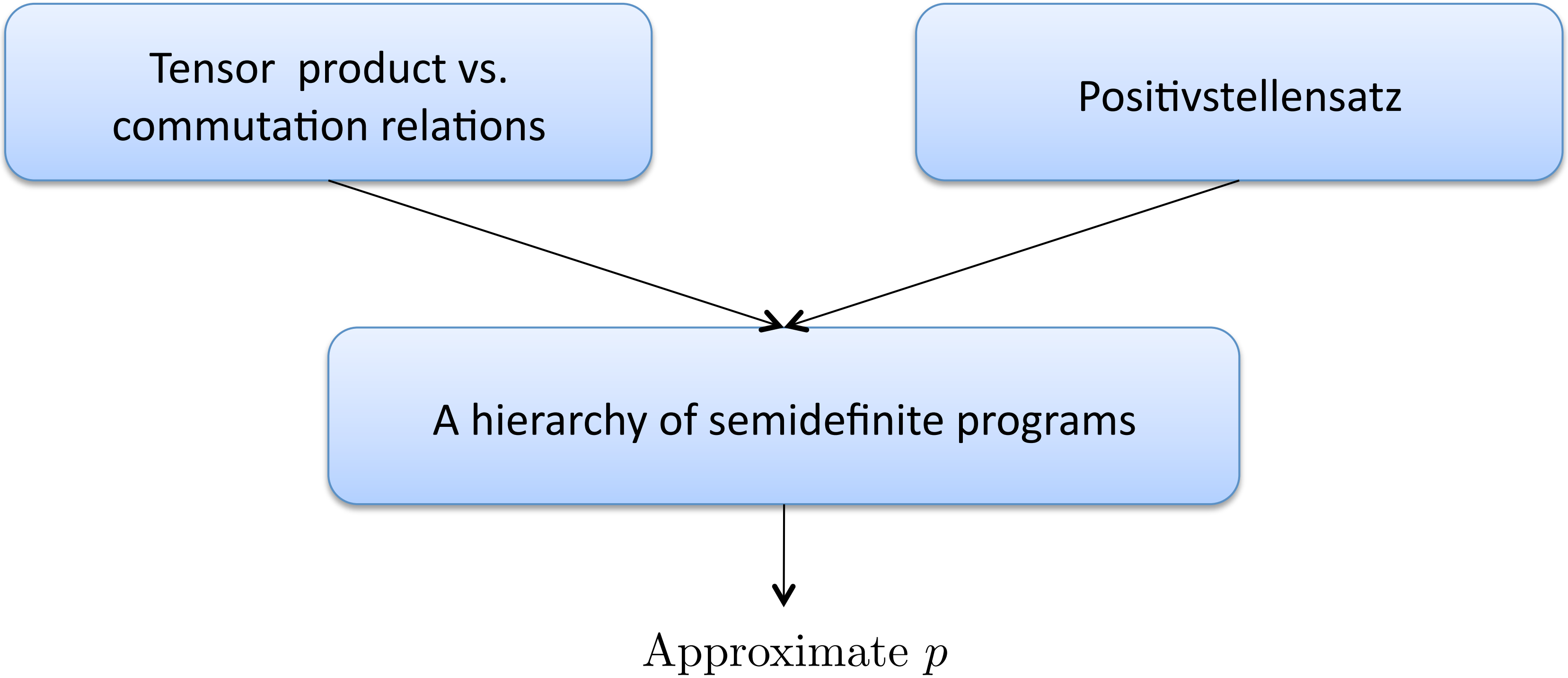
$$\forall s, a \; (A_s^a)^2 = A_s^a \qquad \forall t, b \; (B_t^b)^2 = B_t^b$$

$$A_s^a A_s^{a'} = 0 \; \forall a \neq a' \forall s \qquad B_t^b B_t^{b'} = 0 \; \forall b \neq b' \forall t$$

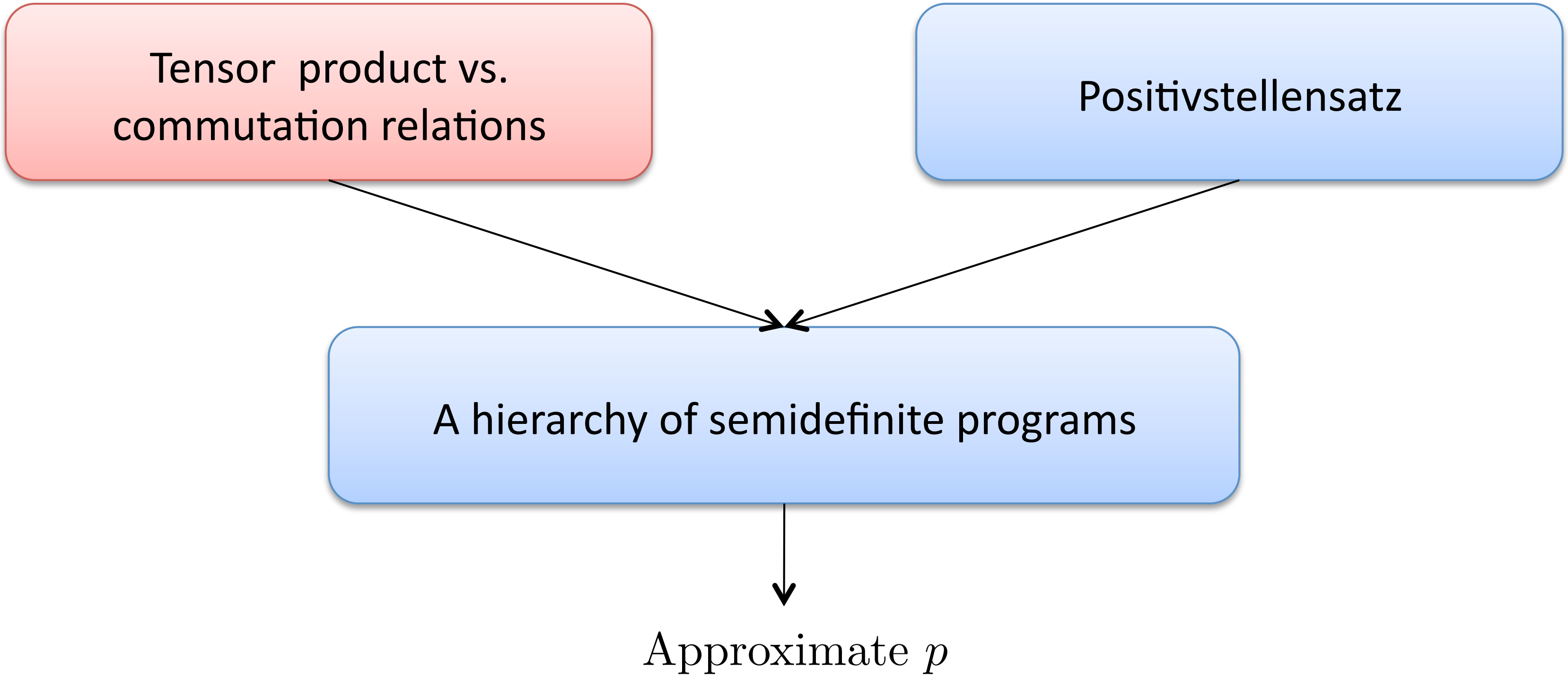
$$\forall s \; \sum_a A_s^a = \mathbb{I} \qquad \forall t \; \sum_b B_t^b = \mathbb{I}$$

Neumark's dilation theorem

Computing winning probability



Computing winning probability



Commutation relations

Lemma: If the space $\mathcal{H}_{AB}$ is finite dimensional, then the following are equivalent:

- Alice and Bob's measurement operators commute $\forall s,t \forall a,b \; [A_s^a, B_t^b] = 0$
- There exists a partitioning $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ such that

$$A_s^a = \tilde{A}_s^a \otimes \mathbb{I}_B \qquad \text{with } \tilde{A}_s^a \in \mathcal{B}(\mathcal{H}_A) \qquad \forall s, a$$

$$B_t^b = \mathbb{I}_A \otimes \tilde{B}_t^b \qquad \text{with } \tilde{B}_t^b \in \mathcal{B}(\mathcal{H}_B) \qquad \forall t, b$$

Not known in general!

Always equivalent if any strategy can be approximated in finite dimensions
Scholz, Werner 0812.4305

Related to Connes embedding problem
Scholz, Werner et al. 1008.1142

Goal

- Find upper bound on the winning probability

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_s^a \otimes B_t^b | \Psi \rangle$$

$$\text{minimize } \nu$$

$$\nu \mathbb{I} - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_s^a B_t^b \geq 0$$

Quantum measurements

$$\forall s,a \ (A_s^a)^2 = A_s^a \qquad \forall t,b \ (B_t^b)^2 = B_t^b$$

$$A_s^a A_s^{a'} = 0 \ \forall a \neq a' \forall s \qquad B_t^b B_t^{b'} = 0 \ \forall b \neq b' \forall t$$

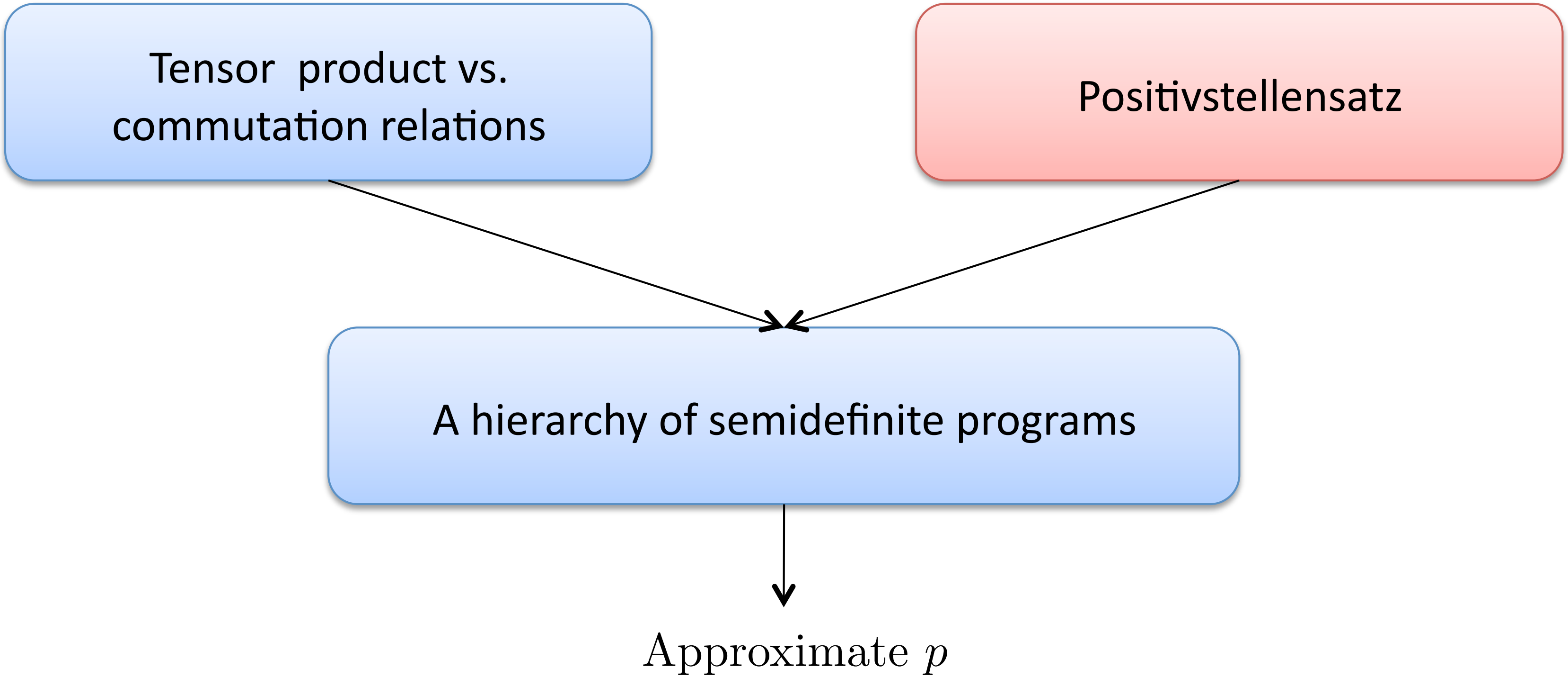
$$\forall s \ \sum_a A_s^a = \mathbb{I} \qquad \forall t \ \sum_b B_t^b = \mathbb{I}$$

$$A_s^a = (\tilde{A}_s^a)^\dagger \tilde{A}_s^a$$

$$B_t^b = (\tilde{B}_t^b)^\dagger \tilde{B}_t^b$$

$$\forall s,t \forall a,b \qquad i[A_s^a, B_t^b] = 0$$

Computing winning probability



Positivstellensatz

Non-commutative variables

$$V = \{A_s^a \mid a \in A, s \in S\} \cup \ \{B_t^b \mid b \in B, t \in T\}$$

Constraint polynomials

$$P_0 = \{\pm A_s^a A_s^{a'} \mid a \neq a' \in A, s \in S\} \cup \ \{\pm B_t^b B_t^{b'} \mid b \neq b' \in B, t \in T\}$$

$$P_1 = \{\pm((A_s^a)^2 - A_s^a) \mid a \in A, s \in S\} \cup \ \{\pm((B_t^b)^2 - B_t^b) \mid b \in B, t \in T\}$$

$$P_2 = \{\pm(\sum_a A_s^a - \mathbb{I}) \mid a \in A, s \in S\} \cup \ \{\sum_b B_t^b - \mathbb{I} \mid b \in B, t \in T\}$$

$$P_3 = \{\pm i[A_s^a, B_t^b] \mid a \in A, s \in S, b \in B, t \in T\}$$

$$P = P_0 \cup P_1 \cup P_2 \cup P_3$$

Positivity domain

$$D_P = \{M \in V \mid \forall p \in P \ p(M) \geq 0\}$$

Positivstellensatz

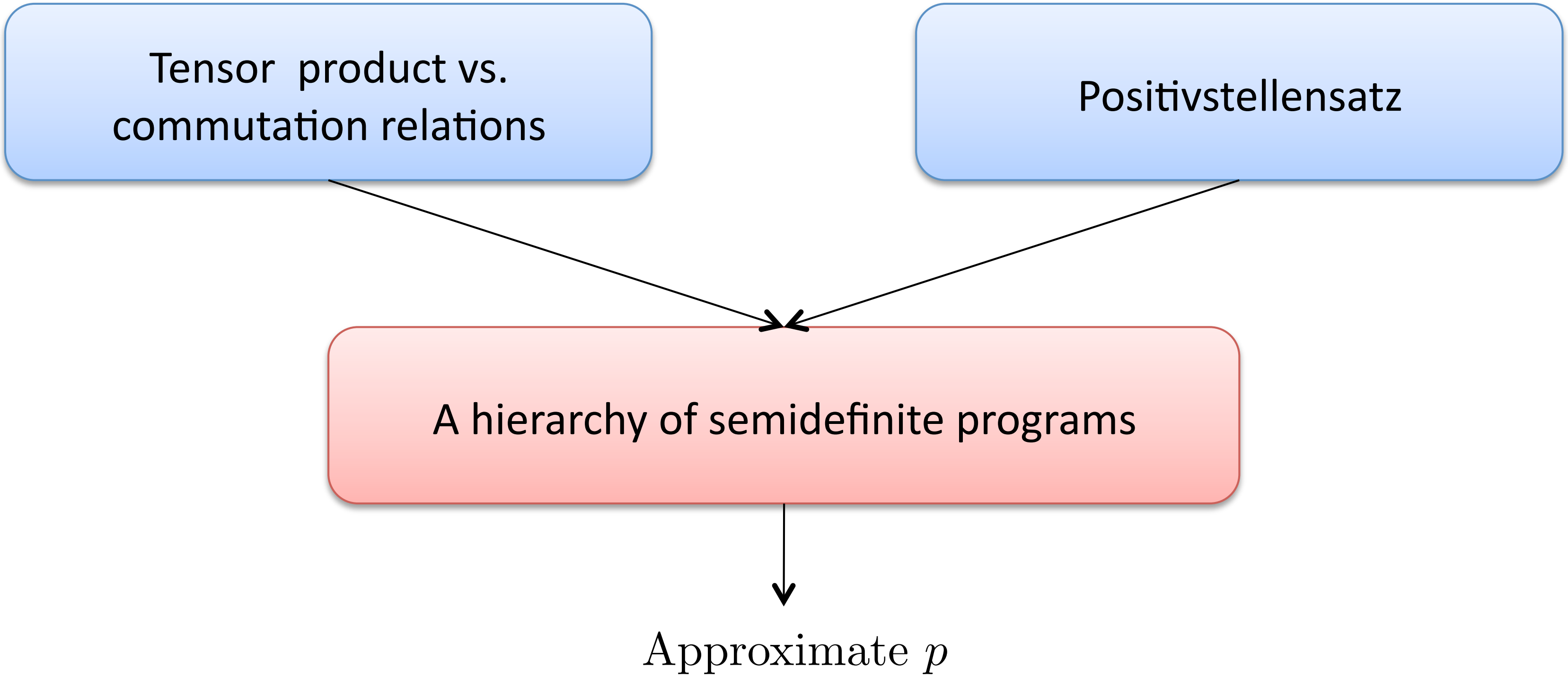
Game polynomial $$q_\nu = \nu \mathbb{I} - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_s^a B_t^b$$

Positivstellensatz by Helton & McCullough '03 (adapted to the complex case):
If $q_\nu > 0$ for variables in D_P, then there exist polynomials $\{r_j\}_j$ and $\{s_{ij}\}_{ij}$ such that q_ν is a weighted sums of squares

$$q_\nu = \sum_{j=1}^{N} r_j^\dagger r_j + \sum_{i=1}^{M} \sum_{j=1}^{L} s_{ij}^\dagger p_j s_{ij} \qquad \text{with } p_j \in P$$

If there do NOT exist measurements attaining winning probability ν
then q_ν can be written as a weighted sums of squares

Computing winning probability



SDP hierarchy

Minimize ν

s.t. $q_\nu \geq 0$

For variables satisfying the constraints

→ Positivstellensatz →

Minimize ν

s.t.

$$q_\nu = \sum_{j=1}^{N} r_j^\dagger r_j + \sum_{i=1}^{M} \sum_{j=1}^{L} s_{ij}^\dagger p_j s_{ij}$$

SDP hierarchy

Minimize ν

s.t. $q_\nu \geq 0$

For variables satisfying the constraints

Positivstellensatz

Minimize ν

s.t.

$$q_\nu - \sum_{i=1}^{M}\sum_{j=1}^{L} s_{ij}^{\dagger} p_j s_{ij} = \sum_{j=1}^{N} r_j^{\dagger} r_j$$

Sum of squares

Parrilo ‘00: At level n:

- Fix the degree of r_j to be n and s_{ij} to be n-1
- Since p_j has degree at most 2, q_ν has degree 2n

•Obtain a bound p_n on the winning probability $(p_n \geq p_{n+1})$

Theorem: $\lim_{n\to\infty} p_n = p$

Example: CHSH

$$A = B = S = T = \{0,1\} \qquad \pi(s,t) = \frac{1}{4} \qquad s \cdot t = a + b \mod 2$$

$$q_\nu = \nu \mathbb{I} - \frac{1}{8} \sum_{s,t} \sum_{c} V(c = a + b | s,t)(1 + (-1)^c A_s B_t)$$

$$= \nu \mathbb{I} - \frac{1}{2} \left(1 + \frac{\mathcal{B}ell}{4} \right)$$

$$A_s = A_s^0 - A_s^1$$
$$B_t = B_t^0 - B_t^1$$

$$Bell = A_0 B_0 + A_1 B_0 + A_0 B_0 - A_1 B_1$$

$$minimize\ \tilde{\nu} \qquad (A_0)^2 = (A_1)^2 = (B_0)^2 = (B_1)^2 = \mathbb{I}$$

$$q_{\tilde{\nu}} = \tilde{\nu} \mathbb{I} - \mathcal{B}ell \geq 0 \qquad \forall s,t\ [A_s, B_t] = 0$$

At level n = 1,

$$z^\dagger \Gamma z = \tilde{\nu} \mathbb{I} - \mathcal{B}ell - \lambda_0(\mathbb{I} - (A_0)^2) - \lambda_1(\mathbb{I} - (A_1)^2) - \lambda_2(\mathbb{I} - (B_0)^2) - \lambda_3(\mathbb{I} - (B_1)^2)$$

$$z = (A_0, A_1, B_0, B_1)$$

$\Gamma \geq 0$ ⟷ Sums of squares

Example: CHSH

$$p = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

$$minimize\ \tilde{\nu}$$

$$q_{\tilde{\nu}} = \tilde{\nu}\mathbb{I} - \mathcal{B}ell \geq 0$$

$$(A_0)^2 = (A_1)^2 = (B_0)^2 = (B_1)^2 = \mathbb{I}$$

$$\forall s, t\ [A_s, B_t] = 0$$

At level n = 1,

$$z^\dagger \Gamma z = \tilde{\nu}\mathbb{I} - \mathcal{B}ell - \lambda_0(\mathbb{I} - (A_0)^2) - \lambda_1(\mathbb{I} - (A_1)^2) - \lambda_2(\mathbb{I} - (B_0)^2) - \lambda_3(\mathbb{I} - (B_1)^2)$$

$$z = (A_0, A_1, B_0, B_1)$$

$\Gamma \geq 0$ ⟷ Sums of squares

$$\Gamma = \frac{1}{2}\begin{pmatrix} 2\lambda_0 & 0 & -1 & -1 \\ 0 & 2\lambda_1 & -1 & 1 \\ -1 & -1 & 2\lambda_2 & 0 \\ -1 & 1 & 0 & 2\lambda_3 \end{pmatrix}$$

$$\tilde{\nu} = \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3$$

$$minimize\ \mathrm{Tr}(\Gamma)$$

$$\Gamma \geq 0$$

$$\tilde{\nu} = 2\sqrt{2}$$

$$\lambda_j = \frac{\sqrt{2}}{2}$$

$$\lambda_j = \frac{\sqrt{2}}{2}$$

$$q_{2\sqrt{2}} = z^\dagger \Gamma z = \frac{1}{2\sqrt{2}}(h_1^\dagger h_1 + h_2^\dagger h_2)$$

$$h_1 = A_0 + A_1 - \sqrt{2}B_0$$

$$h_2 = A_0 - A_1 - \sqrt{2}B_1$$

Convergence

If there exists a strategy that achieves the optimal winning probability dimension d, then we can stop at level d

(dual: Navascues, Pironio, Acin 0803.4290)

Is the optimal strategy finite dimensional? (finite number of measurements and outcomes)

Numerical evidence suggests not! (Pal, Vertesi 1006.3032)

Bounds on how much entanglement is needed:
From information theory: Christandl, Doherty, Wehner 0808.3960
From quantum evolution: Perez-Garcia, Wolf 0901.2542

Some games need a large amount of entanglement:
Perez-Garcia, Wolf, Palazuelos, Villanueva, Junge quant-ph/0702189 and 0910.4228
Briet, Buhrman, Toner/Briet, Olivera Filho, Vallentin 0901.2009/0910.5765

Outline

- Motivation: non-local games
- What was known
- Optimization and non-local games
- The general quantum moment problem
- Open questions

Generalizations

- Other questions involving non-commutative variables
- .. With similar constraints, questions involving quantum measurements

- The quantum moment problem

Measurements labeled $s \in S$
Outcomes $a \in A$

Measurements labeled $t \in T$
Outcomes $b \in B$

Given distributions $p(a, b|s, t)$ does there exists a shared state and measurements realizing this distribution?

Outline

- Motivation: non-local games
- What was known
- Optimization and non-local games
- The general quantum moment problem
- Open questions

Open questions

- Convergence? Already interesting for special classes of games

- Dimension bounds?

- Improved stopping conditions? Mod p games?

$$a + b \mod p \qquad a, b \in \{0, \ldots, p-1\}$$

- Can the optimal strategy be approximated in much lower dimension? (true for XOR games)

Open questions

- Generic structure of states and measurements?
- Powe of MI
- Classical vs.

$$p = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t)\langle\Psi|A_s \otimes B_t|\Psi\rangle$$

Conditions on when there is no quantum advantage

Thank you!