The quantum moment problem

Stephanie Wehner

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

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

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

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

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

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

Distribution \( \pi(s, t) \)

Any non-signaling distribution is allowed

\( \forall a, s \forall t, t' \quad \Pr[a|s, t] = \Pr[a|s, t'] \)

\( \forall b, t \forall s, s' \quad \Pr[b|s, t] = \Pr[b|s', t] \)

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

Linear program!
Example: The CHSH game (no-signaling)

- \( s \in S = \{0, 1\} \)
- \( t \in T = \{0, 1\} \)
- \( a \in A = \{0, 1\} \)
- \( b \in B = \{0, 1\} \)

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

\[ s \in S \]
\[ t \in T \]
\[ a \in A \]
\[ b \in B \]

Distribution \( \pi(s, t) \)

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

\[ a_r : S \rightarrow A \]
\[ b_r : T \rightarrow B \]
Example: The CHSH game (classical)

$s \in S = \{0, 1\}$

$t \in T = \{0, 1\}$

$a \in A = \{0, 1\}$

$b \in B = \{0, 1\}$

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

1. Shared quantum state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$
2. Quantum measurements
   
   $A_s = \{A^a_s \in \mathcal{B}(\mathcal{H}_A)\}_{a \in A}$ \hspace{1cm} $\forall s, a \ A^a_s \geq 0$ \hspace{1cm} $\forall s \ \sum_a A^a_s = \mathbb{I}$
   
   $B_t = \{B^b_t \in \mathcal{B}(\mathcal{H}_B)\}_{b \in B}$ \hspace{1cm} $\forall t, b \ B^b_t \geq 0$ \hspace{1cm} $\forall t \ \sum_b B^b_t = \mathbb{I}$

p = \max \sum_{s,t} \pi(s, t) \sum_{a,b} V(a, b|s, t) \langle \Psi|A^a_s \otimes B^b_t|\Psi\rangle

Pr[a, b|s, t] = \langle \Psi|A^a_s \otimes B^b_t|\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,

$\text{\ ?}$

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

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

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

($> \frac{3}{4}$ classical)
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

Prover 1 \rightarrow V \rightarrow Prover 2

Unbounded

Poly-time bounded

- 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

\[ s \in S \]
\[ t \in T \]
\[ a \in A = \{0, 1\} \]
\[ b \in B = \{0, 1\} \]

Distribution \( \pi(s, t) \)

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

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

\[
= \max \frac{1}{2} \sum_{s,t} \pi(s, t) \sum_{c} V(c|s, t)(1 + (-1)^c a_s \cdot b_t)
\]

\( a_s, b_t \in \mathbb{R}^{\min |T|, |S|} \)

\( a_s \|_2, \| b_t \|_2 = 1 \)

Optimal solution is easy to find!

Wehner, quant-ph/0510076
What is known

- $\oplus\text{MIP}^* \subseteq \text{QIP}$  
  (Wehner quant-ph/0508201)

- $\text{QIP} = \text{PSPACE}$  
  (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

\[ p = \max \sum_{s,t} \pi(s, t) \sum_{a,b} V(a, b|s, t) \langle \Psi | A^a_s \otimes B^b_t | \Psi \rangle \]

minimize \( \nu \)

\[ \nu \mathbb{I} - \sum_{s,t} \pi(s, t) \sum_{a,b} V(a, b|s, t) A^a_s \otimes B^b_t \geq 0 \]

Quantum measurements

\[ \forall s, a \ A^a_s \geq 0 \quad \forall t, b \ B^b_t \geq 0 \]

\[ \forall s : \sum_a A^a_s = \mathbb{I} \quad \forall t : \sum_a B^b_t = \mathbb{I} \]
Goal

Find upper bound on the winning probability

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

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

\[ \forall s, a \ (A_s^a)^2 = A_s^a \]
\[ \forall t, b \ (B_t^b)^2 = B_t^b \]
\[ A_s^a A_s^{a'} = 0 \ \forall a \neq a' \ \forall s \]
\[ B_t^b B_t^{b'} = 0 \ \forall b \neq b' \ \forall t \]
\[ \forall s \ \sum_a A_s^a = \mathbb{I} \]
\[ \forall t \ \sum_b B_t^b = \mathbb{I} \]

Neumark’s dilation theorem
Computing winning probability

- Tensor product vs. commutation relations
- Positivstellensatz
- A hierarchy of semidefinite programs

Approximate $p$
Computing winning probability

Tensor product vs. commutation relations

A hierarchy of semidefinite programs

Positivstellensatz

Approximate $p$
Commutation relations

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

- Alice and Bob’s measurement operators commute $\forall s, t \forall a, b \ [A^a_s, B^b_t] = 0$

- There exists a partitioning $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ such that
  
  \begin{align*}
  A^a_s &= \tilde{A}^a_s \otimes \mathbb{I}_B \quad &\text{with } \tilde{A}^a_s \in \mathcal{B}(\mathcal{H}_A) \quad \forall s, a \\
  B^b_t &= \mathbb{I}_A \otimes \tilde{B}^b_t \quad &\text{with } \tilde{B}^b_t \in \mathcal{B}(\mathcal{H}_B) \quad \forall t, b
  \end{align*}

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

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

minimize \( \nu \)

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

Quantum measurements

\[
\forall s, a \ (A_s^a)^2 = A_s^a \quad \forall t, b \ (B_t^b)^2 = B_t^b
\]

\[
A_s^a A_s^{a'} = 0 \ \forall a \neq a' \forall s \quad B_t^b B_t^{b'} = 0 \ \forall b \neq b' \forall t
\]

\[
A_s^a = (\tilde{A}_s^a)^\dagger \tilde{A}_s^a \quad \forall s \ \sum_a A_s^a = I
\]

\[
B_t^b = (\tilde{B}_t^b)^\dagger \tilde{B}_t^b \quad \forall t \ \sum_b B_t^b = I
\]

\[
\forall s, t, \forall a, b \quad i[A_s^a, B_t^b] = 0
\]
Computing winning probability

- Tensor product vs. commutation relations
- Positivstellensatz

A hierarchy of semidefinite programs

Approximate $p$
Positivstellensatz

Non-commutative variables
\[ V = \{ A^a_s \mid a \in A, s \in S \} \cup \{ B^b_t \mid b \in B, t \in T \} \]

Constraint polynomials
\[ P_0 = \{ \pm A^a_s A^{a'}_s \mid a \neq a' \in A, s \in S \} \cup \{ \pm B^b_t B^{b'}_t \mid b \neq b' \in B, t \in T \} \]
\[ P_1 = \{ \pm ((A^a_s)^2 - A^a_s) \mid a \in A, s \in S \} \cup \{ \pm ((B^b_t)^2 - B^b_t) \mid b \in B, t \in T \} \]
\[ P_2 = \{ \pm (\sum_a A^a_s - \mathbb{I}) \mid a \in A, s \in S \} \cup \{ \sum_b B^b_t - \mathbb{I} \mid b \in B, t \in T \} \]
\[ P_3 = \{ \pm i[A^a_s, B^b_t] \mid a \in A, s \in S, b \in B, t \in T \} \]
\[ P = P_0 \cup P_1 \cup P_2 \cup P_3 \]

Positivity domain
\[ D_P = \{ M \in V \mid \forall p \in P \ p(M) \geq 0 \} \]
Positivstellensatz

Game polynomial

\[ q_\nu = \nu \mathbb{1} - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_s^a B_t^b \]

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 \( q_\nu \) is a weighted sums of squares

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

If there do NOT exist measurements attaining winning probability \( \nu \) then \( q_\nu \) can be written as a weighted sums of squares
Computing winning probability

Tensor product vs. commutation relations

Positivstellensatz

A hierarchy of semidefinite programs

Approximate $p$
Minimize $\nu$
\[ q_\nu \geq 0 \]
\[ q_\nu = \sum_{j=1}^{N} r_j^\dagger r_j + \sum_{i=1}^{M} \sum_{j=1}^{L} s_{ij}^\dagger p_j s_{ij} \]
For variables satisfying the constraints
Minimize $\nu$

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

For variables satisfying the constraints

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, $q_\nu$ 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

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

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

\[ = \nu \mathbb{I} - \frac{1}{2} \left( 1 + \frac{\text{Bell}}{4} \right) \]

\[ \text{Bell} = A_0 B_0 + A_1 B_0 + A_0 B_1 - A_1 B_1 \]

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

At level \( n = 1 \),

\[ z^\dagger \Gamma z = \nu \mathbb{I} - \text{Bell} - \lambda_0 (\mathbb{I} - (A_0)^2) - \lambda_1 (\mathbb{I} - (A_1)^2) - \lambda_2 (\mathbb{I} - (B_0)^2) - \lambda_3 (\mathbb{I} - (B_1)^2) \]

\[ z = (A_0, A_1, B_0, B_1) \quad \Gamma \geq 0 \quad \text{Sums of squares} \]
Example: CHSH

\[ p = \frac{1}{2} + \frac{1}{2\sqrt{2}} \]

\[ \begin{align*}
\text{minimize } \tilde{\nu} \\
q_{\tilde{\nu}} = \tilde{\nu} \mathbb{I} - \text{Bell} \geq 0
\end{align*} \]

At level \( n = 1 \),

\[ z^{\dagger} \Gamma z = \tilde{\nu} \mathbb{I} - \text{Bell} - \lambda_0 (\mathbb{I} - (A_0)^2) - \lambda_1 (\mathbb{I} - (A_1)^2) - \lambda_2 (\mathbb{I} - (B_0)^2) - \lambda_3 (\mathbb{I} - (B_1)^2) \]

\[ z = (A_0, A_1, B_0, B_1) \quad \Gamma \geq 0 \quad \text{Sums of squares} \]

\[ \begin{align*}
\Gamma &= \frac{1}{2} \begin{pmatrix}
2\lambda_0 & 0 & -1 & -1 \\
0 & 2\lambda_1 & -1 & 1 \\
-1 & -1 & 2\lambda_2 & 0 \\
-1 & 1 & 0 & 2\lambda_3
\end{pmatrix} \\
\tilde{\nu} &= \lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 \\
\text{minimize } & \text{Tr}(\Gamma) \\
& \Gamma \geq 0
\end{align*} \]

\[ \begin{align*}
\tilde{\nu} &= 2\sqrt{2} \\
\lambda_j &= \frac{\sqrt{2}}{2} \\
q_{2\sqrt{2}} &= z^{\dagger} \Gamma z = \frac{1}{2\sqrt{2}}(h_1^{\dagger} h_1 + h_2^{\dagger} h_2) \\
&= h_1 = A_0 + A_1 - \sqrt{2}B_0 \\
&= h_2 = A_0 - A_1 - \sqrt{2}B_1
\end{align*} \]
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:
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?

  \[ a + b \mod p \quad a, b \in \{0, \ldots, p - 1\} \]

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

- Generic structure of states and measurements?
- Power of MIP*?
- Classical vs.

\[ p = \max_{s,t} \sum_{a,b} \pi(s, t) \sum_{u} V(u|s, t) \langle \Psi | A_s \otimes B_t | \Psi \rangle \]

Conditions on when there is no quantum advantage

Thank you!