

The (quantum) moment problem: deriving bounds on (quantum) correlations



Stephanie Wehner

Joint work with:

- Andrew Doherty, Yeong-Cherng Liang, Ben Toner (0803.4373)
- Andreas Winter (0710.1185)
- Wim van Dam, Greg Ver Steeg (In preparation)

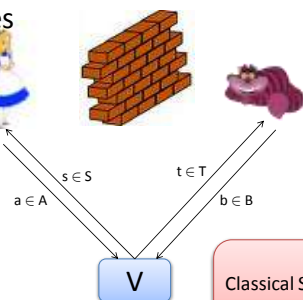


Outline

- **Games**
 - What is known?
 - What we will answer here
- **Tools**
 - Tensor product vs. commutation relations
 - Positivstellensatz
- **Finding bounds using SDPs**
 - The idea
 - A hierarchy of SDPs
 - An example
- **Generalizations**



Games

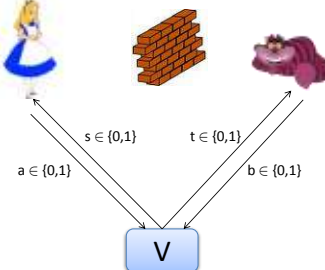


Classical Strategy:
• Shared randomness

- Sets of questions: S, T and answers A, B
- Probability distribution: $\pi: S \times T \rightarrow [0,1]$
- Predicate $V: A \times B \times S \times T \rightarrow \{0,1\}$
 - $V(a,b|s,t) = 1 \Leftrightarrow$ Alice and Bob win with answers a and b given questions s and t
- Winning probability
 - $\omega(G) = \max \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \Pr[\text{answer } a,b | \text{questions } s,t]$



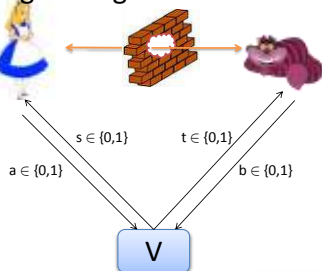
Games: CHSH



- $V(a,b|s,t) = 1 \Leftrightarrow s+t = a+b \pmod 2$
 $\Leftrightarrow$ Alice and Bob win iff $s+t = a+b \pmod 2$
- Classical value of the game
 - $\omega(\text{CHSH}) = 3/4$



Adding entanglement



- $V(a,b|s,t) = 1 \Leftrightarrow s+t = a+b \pmod 2$
 $\Leftrightarrow$ Alice and Bob win iff $s+t = a+b \pmod 2$
- Classical value of the game
 - $\omega(\text{CHSH}) = 1/2 + 1/(2\sqrt{2}) \approx 0.853$

Quantum Strategy:
• Shared state
• Measurements



Goal

- Given a description of a game (S,T,A,B,π,V) , what is the maximum probability that the players win the game?
- Compute

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



What is known?

- 2-player XOR games
 - Answers are single bits $A = B = \{0,1\}$
 - From answers $a \in A, b \in B$, the verifier bases his decision only on the XOR $c = a + b \bmod 2$
 - Can compute the optimal value in time polynomial in the number of questions using an SDP (Wehner, PRA '06)
- General games
 - Can obtain upper bounds on the optimal value of any game (Navascues, Pironio, Acin, PRL '07)
 - Not efficient
 - Not known whether the optimal value can be reached

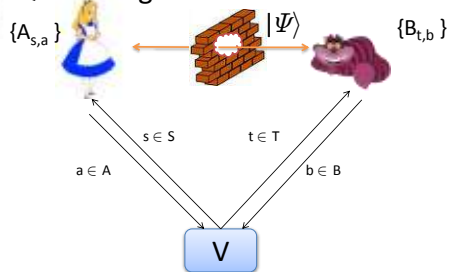


What is known?

- 2-prover games
 - Can approximate the value of a unique game to within a certain accuracy in polynomial time (Kempe, Regev, Toner, arxiv:0710.0655)
- General games
 - Here: can find the optimum value of any multi-player game using a hierarchy of SDPs that **converges** to the optimal value of the game. (arxiv:0803.4373, CCC'08)
 - Dual to the new work of Navascues, Pironio, Acin (arxiv:0803.4290).



Quantum games



$$\omega(G) = \max_{\sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) \langle \Psi | A_{s,a} B_{t,b} | \Psi \rangle}$$

Constraints:

- $|||\Psi\rangle|| = 1$
- $A_{s,a} \geq 0, B_{t,b} \geq 0$

- $\sum_a A_{s,a} = I, \sum_b B_{t,b} = I$
- **Tensor product form!**



Outline

- Games
 - What is known?
 - What we will answer here
- Tools
 - Tensor product vs. commutation relations
 - Positivstellensatz
- Finding bounds using SDPs
 - The idea
 - A hierarchy of SDPs
 - An example
- Generalizations



Tensor product vs. commutation relations

$$\omega_f(G) = \sup || \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_{s,a} B_{t,b} ||$$

- Replacing the tensor product constraint:
for all s, a and t, b , $[A_{s,a}, B_{t,b}] = 0$
- Gives an upper bound $\omega_f(G) \geq \omega(G)$
- How tight is this upper bound?



Tensor product vs. commutation relations

- By convexity, can assume that the for the optimal solution $A_{s,a}$ (and $B_{t,b}$) cannot be 'decomposed'.
- In finite-dimensions, the following two statements are equivalent:
 - For all s, a and t, b , $[A_{s,a}, B_{t,b}] = 0$
 - There exists a partitioning $H = H_A \cup H_B$ such that for all s, a $A_{s,a} \in B(H_A)$ and for all t, b $B_{t,b} \in B(H_B)$
- If the game is such that the optimum value can be achieved in finite dimensions, then $\omega_f(G) = \omega(G)$



The Positivstellensatz

- Consider $q_\nu = \nu I - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_{s,a} B_{t,b}$
- If q_ν is a sum of squares ($q_\nu = \sum_j r_j^\dagger r_j$), then $q_\nu \geq 0$
- But how about the converse?
- ...(almost) given by the Positivstellensatz!
- Variables: $A_{s,a} = A'_{s,a}{}^\dagger A'_{s,a}$ and $B_{t,b} = B'_{t,b}{}^\dagger B'_{t,b}$
- Set of polynomials P in such variables.
- Positivity domain
 - $D_P = \{A_{s,a}, B_{t,b} \mid \text{for } p \in P \text{ we have } p(A_{s,a}, B_{t,b}) \geq 0\}$



The Positivstellensatz

- Variables: $A_{s,a} = A'_{s,a}{}^\dagger A'_{s,a}$ and $B_{t,b} = B'_{t,b}{}^\dagger B'_{t,b}$
- Set of polynomials P in such variables.
- Positivity domain
 - $D_P = \{A_{s,a}, B_{t,b} \mid \text{for } p \in P \text{ we have } p(A_{s,a}, B_{t,b}) \geq 0\}$
- Helton&McCullough '03 (adapted to complex case):

Let $q_\nu = \nu I - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_{s,a} B_{t,b}$.

If $q_\nu > 0$ for variables in D_P , then there exist polynomials r_j and s_{ij} such that q_ν is a weighted sum of squares:

$$q_\nu = \sum_j r_j^\dagger r_j + \sum_{ij} s_{ij}^\dagger p_i s_{ij}$$

where $p_i \in P$



So what?

- Use the set P to represent the constraints:
 - Commutativity: $i[A_{s,a}, B_{t,b}] = 0$
 - Measurements: $\sum_a A_{s,a} - I = 0$ and $(A_{s,a})^2 - A_{s,a} = 0$
 - Orthogonality: for $a \neq a'$ $i[A_{s,a}, A_{s,a'}] = 0$ and $\{A_{s,a}, A_{s,a'}\} = 0$
- Let $P = \{\pm i[A_{s,a}, B_{t,b}], \pm (\sum_a A_{s,a} - I), \pm ((A_{s,a})^2 - A_{s,a}), \pm i[A_{s,a}, A_{s,a'}], \pm \{A_{s,a}, A_{s,a'}\}, \dots\}$
- operators $A_{s,a}, B_{t,b} \in D_P$ then they satisfy the constraints



The Positivstellensatz applied

Let $q_\nu = \nu I - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_{s,a} B_{t,b}$.

If $q_\nu > 0$ for variables satisfying our measurement constraints, then there exist polynomials r_j and s_{ij} such that q_ν is a weighted sum of squares:

$$q_\nu = \sum_j r_j^\dagger r_j + \sum_{ij} s_{ij}^\dagger p_i s_{ij}$$

where p_i is a constraint.

- If $q_\nu > 0$, then $\nu I > \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_{s,a} B_{t,b}$
- If $q_\nu > 0$ there exists no quantum strategy that attains ν

If there exists no strategy that attains q_ν , then there exist polynomials r_j and s_{ij} such that q_ν is a weighted sum of squares:

$$q_\nu = \sum_j r_j^\dagger r_j + \sum_{ij} s_{ij}^\dagger p_i s_{ij}$$

where p_i is a constraint.



Outline

- Games
 - What is known?
 - What we will answer here
- Tools
 - Tensor product vs. commutation relations
 - Positivstellensatz
- Finding bounds using SDPs
 - The idea
 - A hierarchy of SDPs
 - An example
- Generalizations



The idea

- Consider $q_\nu = \nu I - \sum_{s,t} \pi(s,t) \sum_{a,b} V(a,b|s,t) A_{s,a} B_{t,b}$
- If $q_\nu \geq 0$, then $\nu \geq \omega_f(G)$
- Goal: Minimize ν
 - Such that $q_\nu \geq 0$, and the constraints are satisfied.
- If q_ν is a SOS, then $q_\nu \geq 0$
- If $q_\nu > 0$, then
 - q_ν is a weighted SOS $q_\nu = \sum_j r_j^\dagger r_j + \sum_{ij} s_{ij}^\dagger p_i s_{ij}$
 - a SOS for operators satisfying the constraints
- Goal recast: Minimize ν
 - Such that q_ν is a weighted SOS



The idea

- Goal recast: Minimize ν
 - Such that q_ν is a weighted SOS $q_\nu = \sum_j r_j^\dagger r_j + \sum_{ij} s_{ij}^\dagger p_i s_{ij}$
- To cast as an SDP: Minimize ν
 - Such that $q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij}$ is a SOS
- Can be solved using an SDP (analogous Parrillo '00)
 - Fix the total degree of the polynomials
 - Can check whether we find a SOS decomposition for a fixed degree



A hierarchy of SDPs

- To cast as an SDP: Minimize ν
 - Such that $q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij} = \sum_j r_j^\dagger r_j$
- At level n :
 - Fix the degree of r_j to be n and s_{ij} to be $n-1$
 - Note that the total degree of p_i is at most 2, hence the total degree of q_ν is $2n$
 - Let $\omega_n(G)$ be the optimal value obtained at level n
 - If q_ν has a decomposition with degree n , then also with degree $n+1$
 - $\omega_n(G) \geq \omega_{n+1}(G)$



Reaching the optimal value

- Claim: $\lim_{n \rightarrow \infty} \omega_n(G) = \omega_f(G)$
- First, note that $\omega_n(G) \geq \omega_f(G)$.
 - Second, for $\nu = \omega_f(G) + \epsilon$ with $\epsilon > 0$ SOS

$$q_\nu = \sum_j r_j^\dagger r_j + \sum_{ij} s_{ij}^\dagger p_i s_{ij}$$
 - Let $2D$ be the maximum degree of the polynomials.
 - Hence at level D we have $\omega_D(G) \leq \omega_f(G) + \epsilon$
 - Let $\epsilon \rightarrow 0$, can get arbitrarily close



An example: CHSH

- Bell operators $B_{\text{CHSH}} = A_1 B_1 + A_1 B_2 + A_2 B_1 - A_2 B_2$
- Constraints
 - $(A_1)^2 = (A_2)^2 = (B_1)^2 = (B_2)^2 = I$
 - $[A_1, B_1] = [A_1, B_2] = [A_2, B_1] = [A_2, B_2] = 0$
- $q_\nu = \nu I - B_{\text{CHSH}}$
- Goal: minimize ν such that $q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij}$ is SOS
- Let $z = (A_1, A_2, B_1, B_2)$
- Look for Γ such that
 - $z^\dagger \Gamma z = q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij}$
 - $\Gamma \geq 0$



An example: CHSH

- $q_\nu = \nu I - (A_1 B_1 + A_1 B_2 + A_2 B_1 - A_2 B_2)$
- Goal: minimize ν such that $q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij}$ is SOS
- Let $z = (A_1, A_2, B_1, B_2)$, look for Γ such that
 - $z^\dagger \Gamma z = q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij}$
 - $\Gamma \geq 0$
 - If $q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij} = \sum_j r_j^\dagger r_j$ then we can find such a Γ
 - For such a Γ , $\Gamma = U^\dagger D U$ and $q_\nu = \sum_j d_j (Uz)_j^\dagger (Uz)_j$



An example: CHSH

- $q_\nu = \nu I - (A_1 B_1 + A_1 B_2 + A_2 B_1 - A_2 B_2)$
 - Goal: minimize ν such that $q_\nu - \sum_{ij} s_{ij}^\dagger p_i s_{ij}$ is SOS
 - Let $z = (A_1, A_2, B_1, B_2)$
 - Look for Γ such that

$$z^\dagger \Gamma z = \nu I - (A_1 B_1 + A_1 B_2 + A_2 B_1 - A_2 B_2) - \sum_j \gamma_{jj} (I - (A_j)^2) - \sum_j \gamma_{jj} (I - (B_j)^2)$$
- $$2\Gamma = \begin{bmatrix} 2\gamma_{11} & 0 & -1 & -1 \\ 0 & 2\gamma_{22} & -1 & 1 \\ -1 & -1 & 2\gamma_{33} & 0 \\ -1 & 1 & 0 & 2\gamma_{44} \end{bmatrix} \quad \text{with } \nu = \gamma_{11} + \gamma_{22} + \gamma_{33} + \gamma_{44}$$



An example: CHSH

$$2\Gamma = \begin{bmatrix} 2\gamma_{11} & 0 & -1 & -1 \\ 0 & 2\gamma_{22} & -1 & 1 \\ -1 & -1 & 2\gamma_{33} & 0 \\ -1 & 1 & 0 & 2\gamma_{44} \end{bmatrix}$$

$$\text{with } \nu = \gamma_{11} + \gamma_{22} + \gamma_{33} + \gamma_{44}$$

By solving this SDP, one gets
 $\gamma_{11} = \gamma_{22} = \gamma_{33} = \gamma_{44} = 1/\sqrt{2}$

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

Minimize $\nu = \text{Tr}(\Gamma)$

Such that $\Gamma \geq 0$

$$\begin{aligned} q_{2\sqrt{2}} &= 2\sqrt{2} I - B_{\text{CHSH}} - 1/\sqrt{2} \sum_j (I - (A_j)^2) - 1/\sqrt{2} \sum_j (I - (B_j)^2) \\ &= z^\dagger \Gamma z = 1/(2\sqrt{2}) (h_1^\dagger h_1 + h_2^\dagger h_2) \\ &\text{with } h_1 = A_1 + A_2 - \sqrt{2} B_1 \text{ and } h_2 = A_1 - A_2 - \sqrt{2} B_2 \end{aligned}$$



Further examples

- Yao's inequality
 - 3 players
 - 3 measurements, 2 outcomes
- I3322 inequality
 - 2 players
 - 3 measurements, 2 outcomes



General idea

- Let z be the vector of monomials up to degree n
- Find Γ such that $z^\dagger \Gamma z = \nu I - B - \sum_{ij} s_{ij}^\dagger p_i s_j$
- Piecewise
 - Choose F_0 such that $z^\dagger F_0 z = \nu I$
 - Choose F_1 such that $z^\dagger F_1 z = -B$
 - Implement constraints individually
 - Write $s_{ij} = \sum_k \alpha_{ijk} z_k$ and note $p_i = \sum_k \beta_{ik} z_k$
 - Can find k' such that $z_{k'} = z_k z_k$
 - Find matrix $F_{ijkk'}$ such that $z^\dagger F_{ijkk'} z = z_{k'}^\dagger p_i z_{k''} = \sum_k \beta_{ik} z_{k''}$
 - Minimize ν
 - Such that $F_0 + F_1 + \sum F_{ijkk'} \geq 0$



Outline

- Games
 - What is known?
 - What we will answer here
- Tools
 - Tensor product vs. commutation relations
 - Positivstellensatz
- Finding bounds using SDPs
 - The idea
 - A hierarchy of SDPs
 - An example
- **Generalizations**



The quantum moment problem

- Given measurements $\{A_{s,a}\}$ and $\{B_{t,b}\}$
 - Satisfying polynomials (in)equalities
 - With associated probabilities $p(a,b|s,t)$
- ..does there exist a state ρ_{AB} and measurements such that
 - $P(a,b|s,t) = \text{Tr}(\rho_{AB} (A_{s,a} B_{t,b}))$
 - for operators satisfying the (in)equalities
- Can find a certificate that such a state and measurement operators do *not* exist using the Positivstellensatz
- *Different from 'marginal problem': There is no restriction on the dimension*



Generalized theories

- Can do this for any theory for which there exists a corresponding 'Positivstellensatz'
- For example, for a theory described by probabilities $p(a,b|s,t)$, with additional constraints (eg GNST):
 - No-signaling, normalization, positivity...
 - For any state $\rho: \sum_j |E[M_j(\rho)]|^p \leq 1$
 - Note: Probabilities $p(a,b|s,t)$ are real commutative variables
 - Note: Constraints can be expressed by polynomials
- Using the real Positivstellensatz(Parrillo '00)
 - Find certificates certifying that a configuration can't be obtained.
 - Optimize



Motivating the constraint

For Hermitian $\Gamma_1, \dots, \Gamma_N$ satisfying

- $(\Gamma_j)^2 = I$
- for $i \neq j$: $\{\Gamma_i, \Gamma_j\} = 0$
- For any state ρ : $\sum_j \text{Tr}(\Gamma_j \rho)^2 \leq 1$ (Wehner, Winter '07)
- Leads to entropic uncertainty relations that are:
 - Maximally strong for the Shannon entropy
 - Nearly maximally strong for the collision and min-entropy



Motivating the constraint

For Hermitian $\Gamma_1, \dots, \Gamma_N$ satisfying

- $(\Gamma_j)^2 = I$
- for $i \neq j$: $\{\Gamma_i, \Gamma_j\} = 0$
- For any p-state ρ : $\sum_j |\text{Tr}(\Gamma_j \rho)|^p \leq 1$ (van Dam, Ver Steeg, Wehner, '08)
 - allow measurements of $\Gamma_1, \dots, \Gamma_N$
 - all operations preserving this condition (e.g. Clifford gates)
- Properties
 - Weaker uncertainty relations
 - Stronger non-locality (can have non-local box states for $p=\infty$)
 - ...



Summary and open questions

- Can compute the optimal value of a general multi-party quantum-game, but...
 - Rate of convergence?
 - How hard does it really have to be?
 - Can we say more about tensor products vs. commutation?
- Uncertainty relations for more outcomes?
- What would relaxations of such relations lead to?