Quantum games and SDPs

We first describe the idea behind Gutoski and Watrous' "General Theory of Entangled Games' [GW07] and show how it gives a very quick proof of Kitaev's strong coin flipping lower bound. We then briefly go over the different SDPs that have been proposed for quantum games.

1 Gutoski-Watrous proof of Kitaev's lower bound on strong coin flipping

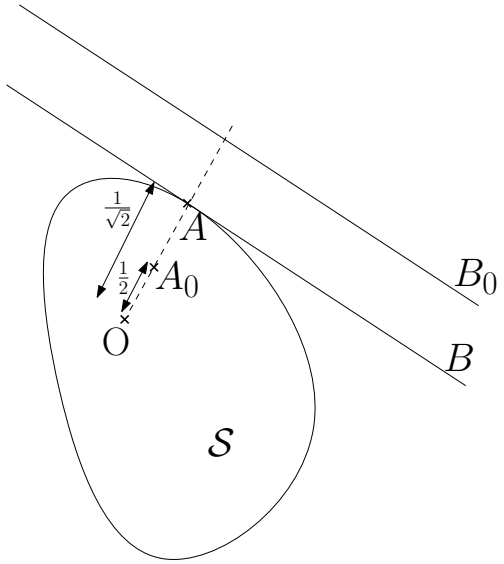

Figure 1: The point vs. hyperplane game: honest (resp. dishonest) strategies A_0, B_0 (resp. A, B) for Alice and Bob.

Consider a game in which Alice's strategies are matrices in a fixed convex subset $\mathcal{S} \subset \mathcal{H}_n(\mathbb{C})$ of the n-dimensional Hermitian matrices $\mathcal{H}_n(\mathbb{C})$ containing the origin, and Bob's strategies are hyperplanes $H_B = \{X \in \mathcal{H}_n(\mathbb{C}), \langle X, B\rangle = 1\}$ such that $\langle A, B\rangle \leq 1$ for all $A \in \mathcal{S}$ (i.e Bob can play any hyperplane that does not cut Alice's set of possible strategies). In this game, there is a fixed pair of "honest" strategies A_0 for Alice and B_0 for Bob. Alice's goal is to maximize $\langle A, B_0\rangle$, while Bob's is to maximize $\langle A_0, B\rangle$ (see Figure 1).

Suppose that $\langle A_0, B_0\rangle = 1/2$. Let $p = \max_{A\in\mathcal{S}}\langle A, B_0\rangle$ be the maximum payoff achievable by Alice. Then B_0/p is automatically a valid strategy for Bob, which earns him a payoff of $1/(2p)$. Hence at least one of Alice's or Bob's payoffs must be larger than $1/\sqrt{2}$: this is a simple consequence of the specific format of this game.

Gutoski and Watrous show that any two-player quantum game can be put in this format. The work is in showing the following two things:

1. Any fixed strategy for Alice (resp. for Bob) can be represented by a pair of Hermitian matrices $A_0, A_1 \in \mathcal{A}$ (resp. $B_0, B_1 \in \mathcal{B}$) such that $\langle A_x, B_y \rangle$ is the probability that the game ends with Alice outputting x and Bob outputting y. The matrices A and B are obtained from Alice and Bob's strategies as depicted in Figure 2.

2. The sets $\mathcal{S} = \{X,\ X \leq A\}$ for some $A \in \mathcal{A}\}$ and $\mathcal{T} = \{Y,\ Y \leq B$ for some $B \in \mathcal{B}\}$ are dual to each other, in the sense that $\mathcal{T} = \mathring{\mathcal{S}} = \{X,\ \langle X, Y \rangle \leq 1\ \forall Y \in \mathcal{T}\}$. This follows from an inductive characterization of the sets $\mathcal{A}$ and $\mathcal{B}$, together with the calculation of the duals of some simple sets (the key step being Lemma 10 in the paper).

Once these two properties are known to hold, it is straightforward to translate any game into the format described above, and hence to obtain Kitaev's lower bound. This gives a nice pictorial way to think about quantum games, and might even help in designing specific games. A difficulty with that however is that a priori not all matrices in the set $\mathcal{S}$ can be played by Alice — only the extreme points, together with some interior points. Are all interior points valid strategies? Can the geometry of the set $\mathcal{S}$ be understood more precisely? From the paper we know that it is a "cut" of the set of positive matrices, by a small number of simple hyperplanes (cf. Theorem 6).

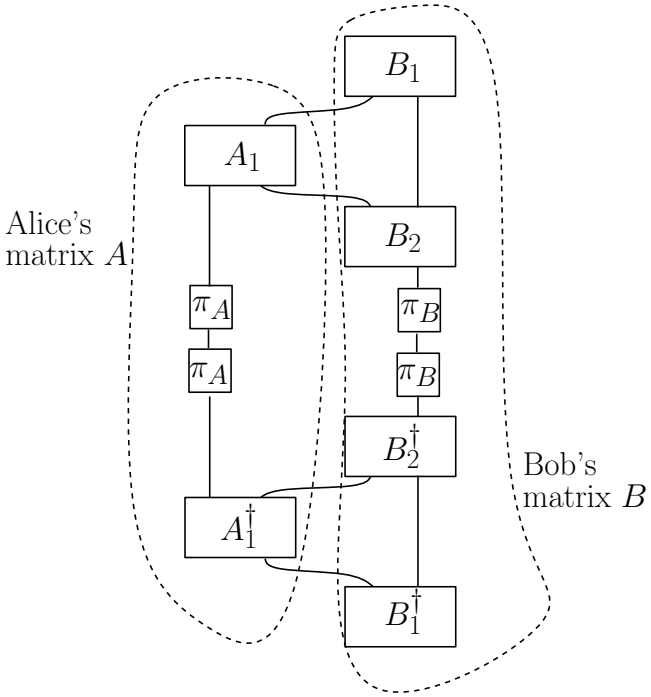

Figure 2: Constructing Alice's matrix A (resp. Bob's matrix B) from her strategy. Alice's matrix has the two top lines as "inputs" and the two bottom lines as "outputs".

2 Overview of the different SDP approaches to QIP

Broadly, SDPs for QIP can be classified in two groups: those which optimize over *messages* exchanged between the verifier and the prover during their interaction, and those which optimize over *the prover's actions*, i.e. its unitaries, themselves.

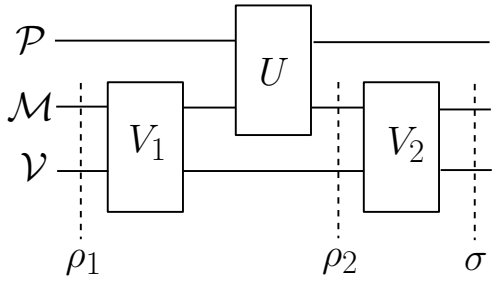

Figure 3: A QIP(3) protocol, together with the "snapshot states" optimized over by some of the SDPs

2.1 Optimization over messages

Let (V_1, V_2) be a 3-round QIP protocol (see Figure 3). Note that the initialization of the verifier's private qubits is part of V_1, while the projection of the output qubit on "accept" is part of V_2.

The Kitaev-Watrous SDP. The original SDP, due to Kitaev and Watrous [KW00], is based on the following observation:

- If there exists a prover which is accepted with probability 1, then there exists density matrices ρ_1 and σ such that $\mathrm{Tr}_{\mathcal{M}}(V_1\rho_1 V_1^\dagger) = \mathrm{Tr}_{\mathcal{M}}(V_2^\dagger \sigma V_2)$.
- If no prover is accepted with probability more than $1/3$, then for every density matrices ρ_1, σ, we have that $\|\mathrm{Tr}_{\mathcal{M}}(V_1\rho_1 V_1^\dagger) - \mathrm{Tr}_{\mathcal{M}}(V_2^\dagger \sigma V_2)\|_{\mathrm{tr}} \geq 2/3$.

Their idea was then to replace the trace norm with the operator norm, and write the problem of minimizing $\|\mathrm{Tr}_{\mathcal{M}}(V_1\rho_1 V_1^\dagger) - \mathrm{Tr}_{\mathcal{M}}(V_2^\dagger \sigma V_2)\|_\infty$ as a semi-definite program. Note that the switch from trace norm to operator norm means that we are forced to solve the SDP to high accuracy in order to distinguish between the two cases.

Kitaev's coin-flipping SDP. Kitaev takes a similar approach in his MSRI slides on coin flipping, except that he avoids the switch from trace to operator norm by using the following simpler SDP:

$$\begin{aligned} \max \quad & \mathrm{Tr}(V_2\rho_2 V_2^\dagger) \\ & \mathrm{Tr}_{\mathcal{M}}(V_1\rho_1 V_1^\dagger) = \mathrm{Tr}_{\mathcal{M}}\rho_2 \\ & \mathrm{Tr}(\rho_1) = \mathrm{Tr}(\rho_2) = 1 \\ & \rho_1, \rho_2 \geq 0 \end{aligned}$$

The QIP=PSPACE SDP. In their original proof that QIP $\subseteq$ PSPACE, Jain, Ji, Upadhyay and Watrous [JJUW09] use a SDP for QMAM, which is essentially the following (note that in that case the verifier can be described by a single procedure $V = |0\rangle\langle 0| \otimes V_1 + |1\rangle\langle 1| \otimes V_2$, where the first register is a control on the coin-flip):

$$\begin{aligned} &\max \mathrm{Tr}(V\rho) \\ \mathrm{Tr}_2(\rho) &= \mathrm{Id} \otimes \sigma \\ \mathrm{Tr}(\sigma) &= 1 \\ \rho, \sigma &\geq 0 \end{aligned}$$

Here, ρ is meant to represent the state $\rho = |0\rangle\langle 0| \otimes \rho_1 + |1\rangle\langle 1| \otimes \rho_2$, where ρ_1 (resp. ρ_2) is the message sent by the prover on a coin flip of 0 (resp. 1), and is on two registers 1 and 2, corresponding to the part that is sent as the first message (supposed to be independent of the coin, hence the σ in the SDP) and the part sent as the second message.

Xiaodi Wu's game. Finally, Xiaodi Wu [Wu] shows how the original Kitaev-Watrous SDP can easily be transformed in a min-max game, which can be solved using the multiplicative weights update method (leading to a simpler proof of QIP = PSPACE):

$$\max_{0 \leq \pi \leq \mathrm{Id}} \min_{\substack{\rho_1, \sigma \geq 0 \\ \mathrm{Tr}(\rho_1) = \mathrm{Tr}(\sigma) = 1}} \langle \Pi, \mathrm{Tr}_{\mathcal{M}}(V_1 \rho_1 V_1^\dagger) - \mathrm{Tr}_{\mathcal{M}}(V_2^\dagger \sigma V_2) \rangle$$

2.2 Optimizing over the prover's transformation

By using the Choi-Jamiolkowski isomorphism, one can optimize over the prover's transformation U through its representation $J(U)$, which is positive and satisfies some simple linear constraints whenever U is a valid transformation. This is the approach taken by Gutoski and Watrous [GW07] to study general games, and also by Jain, Upadhyay and Watrous [JUW09] in their proof of QIP(2) $\subseteq$ PSPACE.

References

[GW07] G Gutoski and J Watrous. Toward a general theory of quantum games. In *Proc. 39th ACM STOC*, pages 565–574, 2007.

[JJUW09] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Arxiv preprint arXiv:0907.4737*, pages 1–21, 2009.

[JUW09] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:534–543, 2009.

[KW00] A Kitaev and J Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proc. 32nd ACM STOC*, pages 608–617, 2000.

[Wu] Xiaodi Wu. Equilibrium Value Method for the Proof of QIP = PSPACE.