Kitaev's lower bound on strong coin flipping

Presentation by Anand Bhaskar, notes by Thomas Vidick

Consider a game in which Alice and Bob interact in order to output a random bit. Let $p_{x,y}$ be the probability that Alice outputs a x, and Bob a y, at the end of the game. Then this game is a coin-flipping protocol if $p_{1,1} = p_{0,0} = 1/2$. Moreover, let p_{1*} be the probability that Alice outputs a 1, maximized over all possible (cheating) strategies for Bob. Define p_{*1} symmetrically. We say that the protocol is a *strong coin-flipping protocol with bias* ε if both $p_{1*}, p_{*1} \in [1/2 - \varepsilon, 1/2 + \varepsilon]$.

Theorem 1 (Kitaev)**.** *For any strong coin-flipping game, we have* $p_{1*}p_{*1} \geq \frac{1}{2}$.

Corollary 2. *Any strong coin-flipping protocol has bias at least* $1/2 - 1\sqrt{2}$.

Kitaev's theorem applies to both classical and quantum games. We'll see the proof for classical games first, and then move to the quantum setting. Both proofs have the same structure: Bob's best cheating strategy can be expressed as a LP (or SDP in the quantum case), and similarly for Alice's. Any feasible solution to the duals of each LP will provide an upper bound on the probability of success of the cheating strategy. The crucial insight is that the cheating probabilities need to be considered *together*, through the quantity $p_{1*}p_{*1}$: a good upper bound on this expresses the fact that, either Alice can force Bob to output a 1, or, if she can't, then it must mean that Bob can force her into outputting a 1. Kitaev obtains a bound on this bias by taking the product of some of the dual LP (or SDP) constraints.

1 The bound on classical protocols

Let's fix a classical protocol. See it as a tree, where each node is indexed by a variable u representing the transcript that led to this node: if we are in node u, and Alice plays by sending a message a, then we arrive in node (u, a). The honest protocol is given by probabilities $p_A(a|u)$, $p_B(b|u)$, which are Alice's (resp. Bob's) transition probabilities. Given that Alice is honest, Bob's maximum cheating probability can be expressed as a linear program LP_B, in which the variables $p_B(u)$ represent the probability of reaching node u, when Alice is honest and Bob cheats. Bob's goal is to maximize the probability of reaching a leaf labeled with a 1; denote this set L_1. Constraints express the fact that Bob can choose any distribution on edges when it is his turn to play, but he has to follow Alice's distribution when it is her turn.

$$
\begin{aligned}
(\text{LP}_B,\ \text{primal}) \qquad & \max \sum_{u \in L_1} p_B(u) & \\
& p_B(u)p(a|u) = p_B(u,a) & \forall a,\ \forall u \text{ node for Alice} \\
& p_B(u) = \sum_b p_B(u,b) & \forall u \text{ node for Bob} \\
& p_B(0) = 1 & \\
& p_B(u) \geq 0 & \forall u
\end{aligned}
$$

To write the dual of this LP, introduce variables $Z^A(u,a)$ for the first set of constraints, and $Z^A(u)$ for the second set. The dual is[1]

$$\begin{aligned}
(\mathrm{LP}_B,\ \text{dual}) \qquad & \min \quad Z^A(0) \\
& Z^A(u) \geq \sum_a p(a|u) Z^A(u,a) && \forall u \text{ node for Alice} \\
& Z^A(u) \geq Z^A(u,b) && \forall b,\ \forall u \text{ node for Bob} \\
& Z^A(u) \geq 1 && \forall u \in L_1
\end{aligned}$$

$Z_A(u)$ can be interpreted[2] as the maximum probability with which Bob can cheat, starting at node u. We can consider another linear program LP_A, this time for a cheating Alice, which is completely symmetrical. The interpretation of the variables Z^A, Z^B motivates the introduction of the quantity

$$F_\ell = \mathrm{E}_{u\sim\ell}\left[Z^A(u) Z^B(u)\right] \tag{1}$$

where $u \sim \ell$ is shorthand for u being taken according to the probability distribution on states at level ℓ which arises from the honest game. In this expression, $Z^A(u)Z^B(u)$ should be interpreted as the bias that cheating players can achieve, if any of them starts cheating at state u.

Let Z^A, Z^B be optimal solutions to the duals of LP_B and LP_A respectively. The last constraint of the dual implies that without loss of generality we can assume that both Z^A and Z^B will be exactly 1 at all leaves labeled with a 1 (as if they were larger, a better solution to the LP could be obtained by scaling). Hence if n is the last level of the game, then $F_n = p_{1,1} = 1/2$. Moreover, strong duality implies that $F_0 = p_{1*}p_{*1}$. Finally, by multiplying out the constraints of the two duals one easily gets that $F_\ell \geq F_{\ell+1}$, which proves Theorem 1 for the case of classical protocols.

2 The bound on quantum protocols

For quantum protocols, the bound follows analogously, with a few minor tweaks. A game is modeled by a series of unitary operations A_i for Alice, B_i for Bob. The players are assumed to start in the all 0 state. At the end of the interaction, they measure using π_A, π_B respectively and obtain their outcome. The coin-flipping requirement is that

$$p_{1,1} = \|(\pi_A \otimes \mathrm{Id}_M \otimes \pi_B) B_n A_n \cdots B_1 A_1 |0\ldots0\rangle\|^2 = 1/2$$

and $p_{0,0}$, defined symmetrically using $(\mathrm{Id} - \pi_A), (\mathrm{Id} - \pi_B)$ as the measurements, is also $1/2$. The following SDP, analogous to the one Kitaev and Watrous used for QIP, captures the maximum cheating probability for Bob:

$$\begin{aligned}
(\mathrm{SDP}_B,\ \text{primal}) \qquad & \max \quad \langle \pi_B \otimes \mathrm{Id}, \rho_n \rangle \\
& \mathrm{Tr}_M(\rho_{i+1}) = \mathrm{Tr}_M(A_i \rho_i A_{i+1}^\dagger) \forall i \\
& \rho_0 = |0\rangle\langle 0|_{A\otimes M} \\
& \rho_i \geq 0 && \forall i
\end{aligned}$$

[1] The actual black-box dual is slightly different, but is easily seen to be equivalent to the one given here.

[2] This interpretation can be made rigorous by considering (p_B, Z^B) an optimal primal/dual solution and expressing the complementary slackness conditions.

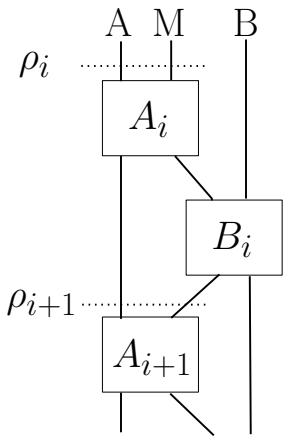

Figure 1: Step i in the coin-flipping protocol

Here ρ_i represents the state of Alice's and the message's registers, right before Alice performs her i-th action (see Figure 1). The dual of this SDP is

$$\begin{aligned}
(\text{SDP}_B,\ \text{dual}) \qquad & \min \quad \langle 0|Z^A(0)|0\rangle \\
& Z^A(i) \otimes \mathrm{Id}_M \geq A_{i+1}^\dagger (Z^A(i+1) \otimes \mathrm{Id}_M) A_{i+1} && \forall i \\
& Z^A(n) = \pi_A \\
& Z^A(i) = (Z^A(i))^\dagger && \forall i
\end{aligned}$$

Let $|\Psi_\ell\rangle$ be the state of the whole system at the ℓ-th round, assuming honest play. Then the analogue of (1) is

$$F_\ell = \langle \Psi_\ell | Z^A(\ell) \otimes \mathrm{Id}_M \otimes Z^B(\ell) | \Psi_\ell \rangle \tag{2}$$

By strong duality, it is easily seen that $F_0 = p_{1*}p_{*1}$, while $F_n = 1/2$. The relation $F_\ell \geq F_{\ell+1}$ follows from the dual constraints, and we are done.

Interpretation. Kitaev gives an interpretation of the matrices $Z^A(i)$ as "objectives" for Bob; i.e. at step i Bob is trying to perform a unitary which will maximize the inner product $Z^A(i) \cdot \mathrm{Tr}_M(\rho_i)$. For the case of an optimal primal/dual solution (ρ, Z), the complementary slackness conditions imply that this quantity is constant, equal to the maximum probability $p_{1\cdot}$ with which Bob can cheat.