Lecture 1: Introduction to Quantum Games

The theory of quantum games has roots in both computer science and quantum physics. We start this module by introducing the background and motivations from both sides.

1.1 Classical Games

The classical analog of the games this module studies is the following particular model. In the game, there are two or more players called Alice, Bob and so on. There is also a referee who communicates with the players and decides whether the players win the game or not. Sometimes, the players are also called provers and the referee is called a verifier. For simplicity, we assume in the following discussions that there are only two players A and B. The case of more players can be defined similarly.

The referee will ask questions to the players A and B from some finite question sets S and T respectively. The players reply cooperatively to the referee with answers from some finite answer sets A and B respectively. The referee will then decide either to accept or reject based on the questions asked and the answers replied. The players win the game if and only if the referee accepts. It is important to note that A and B are *not allowed to communicate* once the game starts although they can talk to each other and agree upon some strategy that they will use in the game. See an illustration of the game in Figure. 1.1. Such games are sometimes called *two-player one-round (2P1R) games* in the literature.

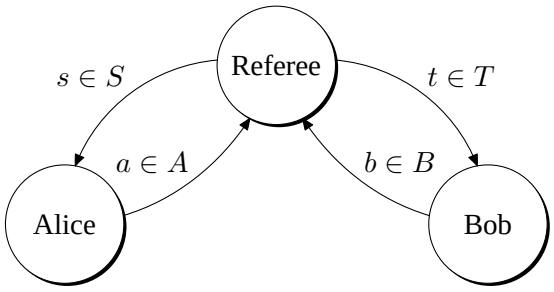

FIGURE 1.1: Two-player one-round game

More formally, the referee will sample a pair of questions $(s,t) \in S \times T$ according to some probability distribution μ on the set $S \times T$. The decision of the referee is characterized by a predicate $V : A \times B \times S \times T \to \{0,1\}$. It is understood that $V(a,b|s,t) = 1$ when the referee accepts upon getting answers a,b for questions s,t. The distribution μ and the predicate V completely describe the game and are publicly known to all the players.

Given a particular game defined by (μ, V), how well can the players do in this game? Let λ, taking values in some set Λ, to denote the random variable that represents the agreement or shared randomness between A and B before the game starts. The strategy for Alice is then a function $a : S \times \Lambda \to A$. Similarly, Bob's strategy is a function $b : T \times \Lambda \to B$. Alice and Bob's strategy can then be described by the tuple (π, a, b) where π is the distribution of λ Alice and Bob choose before the game starts.

The probability that Alice and Bob win the game if they use strategy (π, a, b) is

$$\omega(\pi, a, b) = \mathop{\mathbb{E}}_{\lambda} \mathop{\mathbb{E}}_{(s,t)} V(a(s,\lambda), b(t,\lambda), s, t), \tag{1.1}$$

where the expectation over λ is with respect to π and the second expectation over (s,t) is with respect to the distribution μ. The maximal winning probability of a game is therefore the maximization of the above quantity over all distributions of λ on Λ and all functions a, b. By a simple convexity argument, there is a particular $\lambda_0 \in \Lambda$ that is optimal for the maximization. Fixing λ_0, the functions a, b are now functions from the question sets S, T to answer sets A, B respectively, $a : S \to A$, $b : T \to B$. Therefore, the maximal winning probability of a game, also called the *classical game value*, is

$$\omega = \max_{a,b} \mathop{\mathbb{E}}_{(s,t)} V(a(s), b(t), s, t). \tag{1.2}$$

It is worth emphasizing that, by the above argument, the use shared randomness ($\lambda \in \Lambda$) won't help the players to achieve a higher game value.

It is easy to imagine that the quantum variant of a game will allow the players to use shared entanglement and thus make the multi-player case interesting as opposed to the single-player case. But why is multi-player games interesting already in the classical setting? This is usually explained intuitively by the advantage of interrogations of criminals in separate rooms. In the following, we discuss an important use of an additional prover in the setting of interactive proof verification.

Take any **NP**-complete constraint satisfaction problem, say `3-SAT`, as an example. An instance of a `3-SAT` problem of n variables $x_1, x_2, \ldots, x_n$ is a collection of disjunctive clauses $C_1, C_2, \ldots, C_m$ of at most three variables or negation of variables. For example, C_1 could be of the form $x_1 \vee x_3 \vee \neg x_4$. A `3-SAT` instance is said satisfiable if and only if there is an assignment to the variables $x_1, x_2, \ldots, x_n$ of values in $\{0, 1\}$ so that each clause is satisfied.

Motivated by the proof-verification definition of **NP**, one can define a single-prover game for each `3-SAT` instance. The verifier asks the prover, say Alice, for a satisfying assignment of the instance. He then verify that the reply indeed satisfies all clauses and reject otherwise. This defines a proof system for the `3-SAT` problem and the following *completeness* and *soundness* conditions hold. For any satisfiable instance, Alice can always reply the assignment and win the game (Completeness). For any non-satisfiable instance, there is no reply that Alice can give to convince the verifier (Soundness). This model, however, requires the prover to communicate n bits of information to the verifier.

Is there a proof system for the `3-SAT` problem that has less communication costs? Ideally, if the prover is non-adaptive and acts like an oracle that has stored an assignment of the variables, the verifier can randomly choose a clause C_j, query the prover the values for the three variables in C_j and check if the clause is satisfied or not. The communication cost is therefore $O(\log n)$, an exponential saving compared to the previous setting. The price is that the soundness is not perfect. A non-satisfying instance may be accepted with some positive probability (called the soundness probability) less than 1. We content ourselves with the compromise as long as the probability is strictly bounded away from 1. But how can we enforce the non-adaptive behavior of a prover?

Fortnow, Rompel and Sipser[1] gave a solution. They showed that, by adding a second prover Bob, who is asked the value for one of the three variables sent to the first prover Alice, Alice is

[1] Lance Fortnow and John Rompel and Michael Sipser. "On the power of multi-prover interactive protocols". In: *Theoretical Computer Science* 134.2 (1994), pp. 545–557.

forced to either behave like a non-adaptive oracle or be caught with positive probability. The important point here is that Bob does not have any information about the other queries Alice receives and cannot answer the queries in an adaptive manner. This is called the oracularization technique, and for a 3-SAT instance, it motivates the definition of the 3-SAT game as in Figure 1.2. The questions are of length $O(\log n)$ and answers have constant sizes. The exponential saving of question and answer size is one of the key reasons for the unexpected power of multi-player games and multi-prover interactive proofs. One can check that the 3-SAT game give rise to a proof system that is perfect complete (any satisfiable instance is accepted with probability 1) and soundness probability at most $1 - 1/3m$, as one of the $3m$ question pair must be rejected.

3-SAT Game

1. The referee selects a clause C_j and a variable x_i in C_j uniformly at random.
2. The referee sends j to Alice and i to Bob.
3. Receives assignment to all variables in C_j from Alice and an assignment to x_i from Bob.
4. Accepts if and only if (1) Alice's reply satisfies C_j, and (2) Alice and Bob agree on the value for x_i.

FIGURE 1.2: A two-prover one-round game for 3-SAT

We remark that multi-prover one-round games have played an important role in theoretical computer science. It grows out of the study of multi-prover interactive proofs and also has crucial application in the development of the celebrated PCP theorem[2]. The PCP theorem can be naturally stated as a theorem in terms of multi-prover games although it is usually stated in terms of probabilistic proof verification. Moreover, the parallel repetition theorem by Raz[3] for two-prover one-round games provides a power tool in the analysis of interactive proofs and constructions of PCPs.

1.2 Bell Inequalities

On the physics side, several interesting quantum games were studied for a long time even though they were usually presented in a different form known as Bell inequalities. The framework of quantum games provides a modern viewpoint of quantum non-locality and Bell inequalities.

Back in the 30's, many physicists were puzzled by the weird nature of quantum mechanics and quantum entanglement. For example, in the famous 1935 paper of Einstein, Rosen and Podolsky[4],

[2] Sanjeev Arora and Shmuel Safra. "Probabilistic Checking of Proofs: A New Characterization of NP". In: *J. ACM* 45.1 (1998), pp. 70–122; Sanjeev Arora et al. "Proof Verification and the Hardness of Approximation Problems". In: *J. ACM* 45.3 (1998), pp. 501–555. ISSN: 0004-5411.

[3] R. Raz. "A Parallel Repetition Theorem". In: *SIAM Journal on Computing* 27.3 (1998), pp. 763–803.

[4] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Phys. Rev.* 47 (10 1935), pp. 777–780.

the three authors questioned the completeness of quantum theory after observing the correlation behavior of local measurements on the singlet state

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{1.3}$$

Suppose Alice has the first qubit and measures the observable $\vec{u}\cdot\vec{\sigma}$ where $\vec{u} = (u_x, u_y, u_z) \in S^2$ is a unit vector in $\mathbb{R}^3$ and the $\vec{\sigma}$ is the vector of the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Bob measures his half of the state along the direction $\vec{v}\cdot\vec{\sigma}$ for some unit vector $\vec{v} \in \mathbb{R}^3$. The quantum mechanical expectation value on the singlet state is

$$Q(\vec{u}, \vec{v}) \stackrel{\text{def}}{=} \langle (\vec{u}\cdot\vec{\sigma})_A (\vec{v}\cdot\vec{\sigma})_B \rangle = -\vec{u}\cdot\vec{v}. \tag{1.4}$$

The value of $Q(\vec{u}, \vec{v})$ quantifies the correlation of the two outcomes. In fact,

$$Q(\vec{u}, \vec{v}) = 2\Pr\big[A \textit{ and } B \textit{ have the same outcome}\big] - 1.$$

In particular, if Alice measures σ_x and Bob measures σ_z, Bob will see a random ± 1 outcome. While if Alice measures σ_z and Bob measures σ_z, Bob's outcome is already determined (the opposite of Alice's outcome) even before the measurement of Bob. The puzzle here is that operations done on Alice's side seem to have influenced Bob's system right away, causing Bob's particle to behave differently. It is therefore argued by some physicists that there are hidden parameters not described in the quantum theory that help Bob's particle to choose the right behavior, either being random or deterministic.

In a local hidden variable model motivated by the above discussion, the result a of measuring $\vec{u}\cdot\vec{\sigma}$ on Alice's side is determined by $\vec{u}$ and some hidden variable λ. Similarly, the result b of measuring $\vec{v}\cdot\vec{\sigma}$ on Bob's side is determined by $\vec{v}$ and λ. The corresponding expectation value as in (1.4) for the hidden variable model is therefore

$$P(\vec{u}, \vec{v}) = \mathop{\mathbb{E}}_{\lambda} a(\vec{u}, \lambda) b(\vec{v}, \lambda).$$

Indeed, several commonly discussed features of $Q(\vec{u}, \vec{v})$ can be realized with a hidden variable model. These include (1) A and B give the opposite result if they measure along the same direction, namely $Q(\vec{u}, \vec{u}) = -1$, and (2) A and B give uncorrelated random outcome if they measure along two orthogonal directions, $Q(\vec{u}, \vec{v}) = 0$ if $\vec{u}\cdot\vec{v} = 0$. Both (1) and (2) can be realized by choosing λ to be a uniform random unit vector and

$$\begin{aligned} a(\vec{u}, \lambda) &= \quad \operatorname{sign} \vec{u}\cdot\lambda, \\ b(\vec{v}, \lambda) &= -\operatorname{sign} \vec{v}\cdot\lambda. \end{aligned}$$

However, John Stewart Bell showed in 1964 that there is no local hidden variable model that can fully reproduce the correlation in Eq. (1.4). His solution is quite simple and is now known as the Bell inequalities. It is interesting to note that John Bell worked almost exclusively as a theoretical particle physicist and only studied quantum foundations as his "hobby". If it were not for his unexpected death in 1990, he might receive a Nobel Prize for this fundamental work.

The importance of Bell's inequality is that it provides a way to tell apart the quantum theory and the classical theories, such as the local hidden variable models. Experiments have been done with results in favor of the quantum theory.

We will discuss an improvement to the original Bell's inequality called the CHSH inequality proposed by John Clauser, Michael Horne, Abner Shimony and Richard Holt. The CHSH inequality is as follows

$$-2 \le E \le 2, \tag{1.5}$$

where

$$E = P(\vec{u}_0, \vec{v}_0) + P(\vec{u}_0, \vec{v}_1) + P(\vec{u}_1, \vec{v}_0) - P(\vec{u}_1, \vec{v}_1).$$

The proof follows easily by the following argument. By definition of $P(\vec{u}, \vec{v})$,

$$\begin{aligned} |E| &= \Big| \mathop{\mathbb{E}}_{\lambda} a(\vec{u}_0, \lambda)\big[b(\vec{v}_0, \lambda) + b(\vec{v}_1, \lambda)\big] + a(\vec{u}_1, \lambda)\big[b(\vec{v}_0, \lambda) - b(\vec{v}_1, \lambda)\big] \Big| \\ &\le \mathop{\mathbb{E}}_{\lambda} \Big| a(\vec{u}_0, \lambda)\big[b(\vec{v}_0, \lambda) + b(\vec{v}_1, \lambda)\big] + a(\vec{u}_1, \lambda)\big[b(\vec{v}_0, \lambda) - b(\vec{v}_1, \lambda)\big] \Big| \\ &\le 2. \end{aligned}$$

The last step follows as either $b(\vec{v}_0, \lambda) + b(\vec{v}_1, \lambda)$ or $b(\vec{v}_0, \lambda) - b(\vec{v}_1, \lambda)$ must be 0.

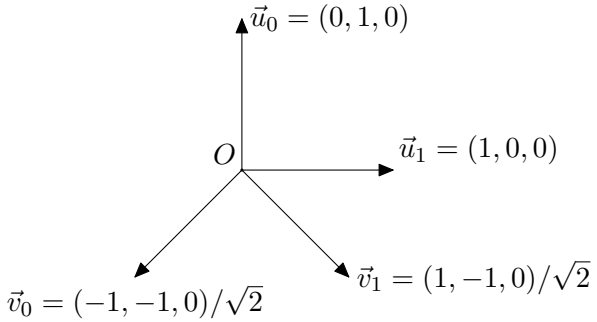

FIGURE 1.3: Vectors of u_s and v_t that achieve the value $2\sqrt{2}$

Quantum mechanically, however, it is possible to choose vectors $\vec{u}_s$ and $\vec{v}_t$ (see Figure 1.3 for example) such that

$$Q(\vec{u}_s, \vec{v}_t) = -\vec{u}_s \cdot \vec{v}_t = (-1)^{st} \frac{\sqrt{2}}{2},$$

which gives a corresponding value of $E = 2\sqrt{2}$, a violation by a factor of $\sqrt{2}$.

Here is how the CHSH inequality naturally gives rise to a two-player one-round game. The CHSH inequality is equivalent to

$$-\frac{1}{2} \le \mathop{\mathbb{E}}_{s,t} (-1)^{st} P(\vec{u}_s, \vec{v}_t) \le \frac{1}{2},$$

which, by the definition of $P(\vec{u}, \vec{v})$, is

$$\Big| \mathop{\mathbb{E}}_{\lambda} \mathop{\mathbb{E}}_{s,t} (-1)^{st} a(\vec{u}_s, \lambda) b(\vec{v}_t, \lambda) \Big| \le \frac{1}{2}.$$

Comparing it with the classical value of a game in Eq. (1.1), it is obvious that the above is simply a bound on the classical winning probability of a game in which the referee uses a ± 1-valued function instead of a predicate. The value 1 indicates the acceptance of the verifier and -1 indicates rejection. The condition for the verifier to accept is given in the following table.

s	t	a b
0	0	$=$
0	1	$=$
1	0	$=$
1	1	$\neq$

Shifting the domain, we obtain the CHSH game as in Figure 1.4. The parity $a \oplus b$ is used instead of the product ab since the game works with answers in $\{0,1\}$ instead of $\{\pm 1\}$.

CHSH Game

1. The referee samples two uniformly random bits $s, t \in \{0,1\}$.
2. The referee sends s to Alice and t to Bob.
3. Receives one bit a from Alice and b from Bob.
4. Accepts if and only if $a \oplus b = st$.

FIGURE 1.4: The CHSH Game

There is a subtle difference in the original statement of the CHSH inequality and the formulation in terms of two-prover one-round games. In CHSH inequalities, real vectors $\vec{u}$ and $\vec{v}$ are given directly to the players to specify the measurements they need to perform. In the game language, however, the referee only sends the indices of the measurement settings to the players. But this doesn't make much difference as the CHSH inequality holds for any choices of measurement settings.

By a simple calculation, the game value is related to the quantity E as follows

$$\omega = \frac{1}{2} + \frac{E}{8}. \tag{1.6}$$

Hence, the CHSH inequality is simply a statement that the value of the game is at most $3/4$. If the players can share entangled state, the above discussion tells that the bound no longer applies and the players can achieve a high winning probability $1/2 + \sqrt{2}/4 \approx .85$. In other words $\omega^* \geq 1/2 + \sqrt{2}/4$ and we will see later that this value is optimal and equals to the quantum game value of the CHSH game.

1.3 Quantum Games

Having discussed both the two-prover one-round games from computer science background and the Bell inequalities from the physics background, we are ready to introduce the main subject of this module, quantum games, by combining the ideas from both sides.

A quantum game is the same as a classical game except that the players are now allowed to share quantum entanglement and use quantum strategies. The study of the effect of nonlocal strategies on multi-prover interactive proof systems was initiated by Cleve, Høyer, Toner and Watrous[5] in 2004. The motivation for such quantum variants is twofold. First, as we have seen it gives a nice and clean framework for the study of nonlocality and Bell's inequality from the computer science perspective. Second, it is also natural to consider quantum strategies in the context of interactive proof systems where the provers are usually assumed to be "all powerful".

A quantum strategy is described by a shared quantum state ρ and POVMs $\{X_s^a\}$ for each question $s \in S$ to Alice and $\{Y_t^b\}$ for each $t \in T$. We sometimes use the tuple $(\rho, \{X_s^a\}, \{Y_t^b\})$ to denote the strategy. Fixing any such strategy, the corresponding value achieved is

$$\omega^*(\rho, \{X_s^a\}, \{Y_t^b\}) = \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} V(a,b|s,t) \operatorname{tr}(X_s^a \otimes Y_t^b \rho), \tag{1.7}$$

where ρ is a shared state on $\mathscr{H}_A \otimes \mathscr{H}_B$, Alice and Bob's state space, and $\{X_s^a\}$, $\{Y_t^b\}$ are POVMs.

The maximal winning probability for quantum players with shared entanglement is therefore

$$\begin{aligned} \omega^*(\rho, \{X_s^a\}, \{Y_t^b\}) &= \sup_{(\rho, \{X_s^a\}, \{Y_t^b\})} \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} V(a,b|s,t) \operatorname{tr}(X_s^a \otimes Y_t^b \rho) \\ &= \sup_{(\rho, \{X_s^a\}, \{Y_t^b\})} \mathop{\mathbb{E}}_{(s,t)} \sum_{a \sim b} \operatorname{tr}_\rho(X_s^a \otimes Y_t^b \rho), \end{aligned} \tag{1.8}$$

where in the last line, the summation $\sum_{a \sim b}$ is the shorthand notion of $\sum_{a,b:V(a,b|s,t)=1}$ and $\operatorname{tr}_\rho(A)$ denotes $\operatorname{tr}(A\rho)$. By a convexity argument, we can assume that the shared state ρ is a pure state. Hence, the game value can also be written as

$$\omega^* = \sup_{(|\Psi\rangle, \{X_s^a\}, \{Y_t^b\})} \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} V(a,b|s,t) \langle \Psi | X_s^a \otimes Y_t^b | \Psi \rangle.$$

For any two-player one-round game, we have defined the classical value ω and the quantum value ω^*. We also learn from the study of CHSH inequalities that there are games whose quantum values are strictly larger than their classical values, $\omega^* > \omega$. Indeed, any such game gives rise to a Bell-type inequality, which states that the classical value is at most ω. Yet, this inequality is violated by some quantum strategy as $\omega^* > \omega$.

Other than the relation to Bell inequalities, the fact that the quantum value can be strictly larger than the classical value also has implications in quantum multi-prover interactive proofs. This is most clearly illustrated by the example of the magic square game that we will discuss in the next lecture.

[5] Richard Cleve et al. "Consequences and Limits of Nonlocal Strategies". In: *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*. CCC '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 236–249.