Lecture 4: Quantum Constraint Satisfaction Games

In this last lecture, we revisit several quantum constraint satisfaction games. As explained in previous lectures, these games do not give rise to sound proof systems for the corresponding constraint satisfaction problems (CSP). Seen from a different angle, however, they do give definitions and say something interesting about a quantum variant of the constraint satisfaction problems. We will discuss how to do reductions between these quantum CSPs and thus provide a nonlocal theory of **NP**-completeness.

4.1 Graph Constraint Satisfaction Games

Let us start with the graph coloring problem. For a graph $G = (V, E)$, a k-coloring of G is an assignment of k colors to each of the vertices of the graph G such that for any edge $e = (u, v)$, the vertices u and v have different colors. If a graph G has a k-coloring, it is said to be k-colorable. Given a graph G, the problem k-COLORING of deciding whether it is k-colorable is a well-known **NP**-complete problem for all $k \geq 3$. There is a natural way to define a two-player one-round game for the graph k-coloring problem as in Figure 4.1. In the game, case 2a is called the coloring check and case 2b is called the consistency check. Consistency check is necessary here as otherwise Alice can always reply color 1 and Bob can always reply color 2 and they always win the game even if the graph is not k-colorable. It is easy to see that, for any graph not k-colorable, the players cannot always win the corresponding game and the winning probability is at most $1 - \Omega(1/|E|)$.

Graph Coloring Game

1. The referee randomly select an edge $e = (u, v) \in E$.
2. The referee do the following two checks each with probability 1/2:
   (a) Sends u to Alice and v to Bob, and accepts if he receives from Alice and Bob two different colors in $\{1, 2, \ldots, k\}$.
   (b) Sends u to both Alice and Bob, and accepts if he receives the same color in $\{1, 2, \ldots, k\}$.

FIGURE 4.1: A two-prover one-round game for the graph coloring problem

As in the magic square game, there are graphs whose coloring games have no perfect classical strategy, but do have a perfect quantum strategy. This means that the game does not give a sound interactive proof for k-COLORING against quantum players. Yet, the quantum coloring game is not totally irrelevant or trivial. It is more naturally related to a quantum variant of the coloring problem defined as follows.

Definition 4.1. *A graph G is said quantum k-colorable if players with shared entanglement can always win the graph coloring game. The smallest number k such that G is quantum k-colorable*

*is called the quantum chromatic number $\chi^*(G)$. Given a graph G, the quantum graph k-coloring problem k-*COLORING** is the decision problem asking whether G is quantum k-colorable or not.*

As the graph coloring game treats Alice and Bob symmetrically, we can assume that they use the same strategy on a symmetric pure state.

Theorem 4.2. *Let $(\rho, \{X_v^a\})$ be a symmetric quantum strategy of the graph coloring game that has value $1-\epsilon$. Then,*

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big[X_u^a - (X_u^a)^2\big] \le O(\epsilon), \tag{4.1}$$

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\Big[\sqrt{X_v^a} X_u^a \sqrt{X_v^a}\Big] \le O(\epsilon). \tag{4.2}$$

Proof. The first inequality follows by a similar argument as the proof of Lemma 3.5 of Lecture 3. We prove the second inequality only.

By the assumption that the strategy $(\rho, \{X_v^a\})$ has quantum value $1-\epsilon$, it must holds that both the coloring check and the consistency check succeed with probability at least $1-2\epsilon$. Namely, we have

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(X_u^a \otimes X_v^a\big) \le 2\epsilon,$$
$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_{a\neq b} \mathrm{tr}_\rho\big(X_u^a \otimes X_u^b\big) \le 2\epsilon.$$

With these two conditions, one can show

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(X_u^a \otimes X_v^a\big) \approx_\epsilon \mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(\sqrt{X_v^a} X_u^a \otimes X_v^a\big).$$

The trick is again the adding and removing of operators by consistency. To prove the above approximation, compute the difference of the two sides

$$\begin{aligned}
&\left|\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\Big[\big(1-\sqrt{X_v^a}\big) X_u^a \otimes X_v^a\Big]\right| \\
\le\ & \mathop{\mathbb{E}}_{e=(u,v)} \sum_a \left|\mathrm{tr}_\rho\Big[\big(1-\sqrt{X_v^a}\big) X_u^a \otimes X_v^a\Big]\right| \\
\le\ & \mathop{\mathbb{E}}_{e=(u,v)} \sum_a \sqrt{\mathrm{tr}_\rho\Big[\big(1-\sqrt{X_v^a}\big)^2 \otimes X_v^a\Big] \cdot \mathrm{tr}_\rho\big[\big(X_u^a\big)^2 \otimes X_v^a\big]} \\
\le\ & \sqrt{\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big[(1-X_v^a) \otimes X_v^a\big] \cdot \mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho(X_u^a \otimes X_v^a)} \\
\le\ & O(\epsilon).
\end{aligned}$$

Following a similar argument as in the proof of Lemma 3.3 of Lecture 3, we can add another $\sqrt{X_v^a}$ and get

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(X_u^a \otimes X_v^a\big) \approx_\epsilon \mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(\sqrt{X_v^a} X_u^a \sqrt{X_v^a} \otimes X_v^a\big).$$

We complete the proof by removing the X_v^a from the second subsystem

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(\sqrt{X_v^a} X_u^a \sqrt{X_v^a} \otimes X_v^a\big) \approx_\epsilon \mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho\big(\sqrt{X_v^a} X_u^a \sqrt{X_v^a}\big).$$

Taking the difference, the above approximation follows directly from the fact that $X_u^a \leq I$ and the self-consistency of X_v in expectation. □

We get the following characterization of the quantum graph k-coloring problem, by taking ϵ to be 0 in the above theorem.

Theorem 4.3. *Graph G is quantum k-colorable if and only if there exists projections $\{X_v^a\}$ for each vertex $v \in V$ and color $a \in \{1,2,\ldots,k\}$ such that*

$$\sum_a X_v^a = I, \text{ for all } v \in V,$$
$$X_u^a X_v^a = 0, \text{ for all } (u,v) \in E.$$

Proof. Suppose first that G is quantum k-colorable and by definition there exist a perfect quantum strategy $(\rho, \{X_v^a\})$ for the graph coloring game. Without loss of generality, one can assume that ρ is a full rank state. Taking $\epsilon = 0$ in Theorem 4.2, we have

$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho \left[X_u^a - (X_u^a)^2 \right] = 0,$$
$$\mathop{\mathbb{E}}_{e=(u,v)} \sum_a \mathrm{tr}_\rho \left[\sqrt{X_v^a} X_u^a \sqrt{X_v^a} \right] = 0.$$

By the first identity, $X_u^a = (X_u^a)^2$ for all u and a, proving that X_u^a is a projection. By the second identity, we have

$$\sqrt{X_v^a} X_u^a \sqrt{X_v^a} = 0,$$

which is equivalent to $X_u^a X_v^a = 0$ for all $(u,v) \in E$ and all a.

Conversely, if there is a set of projections satisfying the equations in the theorem, it is easy to construct a perfect strategy for the graph coloring game using the maximally entangled state. □

We remark that one can prove the above theorem more directly[1] without using Theorem 4.2. However, Theorem 4.2 says more about the game and its proof makes it clear to see the importance of the consistency check in the game. The consistency check enforces rich structures on the strategy in the game and makes the game more manageable.

The quantum k-coloring game discussed above has a natural generalization, called the graph homomorphism quantum game[2] as in Figure 4.2. The quantum chromatic number $\chi^*(G)$ of a graph G is the smallest number k such that there is a quantum homomorphism from G to the complete graph of k vertices.

In addition to the well-studied quantum chromatic number, the concept of quantum homomorphism between graphs gives rise to natural definitions of several other quantum graph parameters, such as the quantum independence and clique numbers[3]. For a graph G, its quantum clique (independence) number is defined to be the maximum number k such that there is a quantum homomorphism from the complete graph of k vertices to G (or the complement of G respectively). We will use $\alpha^*(G)$ to denote the quantum independence number of G. Given a graph G and an integer m, we use $\texttt{CLIQUE}^*$ ($\texttt{INDEPENDENCE}^*$) to denote the problem of deciding whether the quantum clique number (quantum independence number, respectively) is larger than or equal to m.

[1] See e.g. Peter J. Cameron et al. "On the Quantum Chromatic Number of a Graph". In: *Electronic Journal of Combinatorics* 14 (2007), R81.

[2] David E. Roberson and Laura Mančinska. *Graph Homomorphisms for Quantum Players*. arXiv:1212.1724. 2012.

[3] Ibid.

(G,H)-Homomorphism Game

1. The referee randomly selects an edge $e=(u,u')$ in G.
2. The referee does the following with 1/2 probability each:
   (a) Sends u to Alice and u' to Bob, receive $v,v' \in V(H)$ from Alice and Bob respectively and accept if and only if $(v,v') \in E(H)$
   (b) Sends u to both Alice and Bob, accept if and only if $v=v'$.

FIGURE 4.2: Graph Homomorphism Game of Graphs G and H.

4.2 Binary Constraint System Games

Binary constraint system games[4] are quantum games defined by a system of constraints of binary variables using the oracularization technique. We have seen special examples such as the magic square game or the 3-SAT game in previous lectures.

A binary constraint system (BCS) is a collection of binary constraints $C_1, C_2, \ldots, C_m$ over binary variables $x_1, x_2, \ldots, x_n \in \{0,1\}$. A BCS is classically satisfiable if there exists a truth assignment to the variables that satisfies all constraints. For each BCS, one can define a two-prover game as in Figure 4.3.

Before analyzing the game, we introduce several notions. For each constraint C_j, let V_j be the set of variables in C_j. Assume for simplicity that each constraint has the same arity k, the number of different variables in it. Also assume that no two constraints share the same set of variables. For any strategy $(\rho, \{X^a_{V_j}\}, \{Y^b_i\})$, where $a: V_j \to \{0,1\}$ is an assignment of variables in V_j and $b \in \{0,1\}$, define the following induced POVMs as

$$X^b_{i|j} = \sum_{a:a(i)=b} X^a_{V_j}, \quad X^b_i = \mathop{\mathbb{E}}_{j:i\in V_j} X^b_{i|j}. \tag{4.3}$$

It is easy to verify that they are indeed POVMs. For a set of k POVMs $X_i = \{X^b_i\}$, let $\hat{X}_{i_1,i_2,\ldots,i_k}$ to be the POVM that measures X_{i_l} sequentially,

$$\hat{X}^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} = \sqrt{X^{b_1}_{i_1}} \cdots \sqrt{X^{b_{k-1}}_{i_{k-1}}} X^{b_k}_{i_k} \sqrt{X^{b_{k-1}}_{i_{k-1}}} \cdots \sqrt{X^{b_1}_{i_1}}.$$

First note that Alice has no intention to give an answer a that doesn't satisfy the constraint. Hence, without loss of generality, one can assume that $X^a_{V_j} = 0$ if $C_j(a)$ fails. Then, the only way Alice and Bob will fail is that they give inconsistent answers. The quantum game value of a strategy $(\rho, \{X^a_{V_j}\}, \{Y^b_i\})$ is therefore

$$\mathop{\mathbb{E}}_j \mathop{\mathbb{E}}_{i\in V_j} \sum_a \mathrm{tr}_\rho(X^a_{V_j} \otimes Y^{a(i)}_i). \tag{4.4}$$

[4] Richard Cleve and Rajat Mittal. *Characterization of Binary Constraint System Games*. arXiv:1209.2729. 2012.

BCS Game

1. The referee selects a constraint 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 4.3: Binary Constraint System Games

Theorem 4.4. *For any strategy* $(\rho, \{X^a_{V_j}\}, \{Y^b_i\})$ *of value* $1-\epsilon$ *for a BCS game, the following holds*

$$\mathop{\mathbb{E}}_j \mathrm{tr}_\rho\big(X^b_{j_l} - (X^b_{j_l})^2\big) \le O(k\epsilon), \text{ for all } l = 1,2,\ldots,k,$$
$$\mathop{\mathbb{E}}_j F_\rho\big(X_{V_j}, \hat{X}_{j_1,j_2,\ldots,j_k}\big) \ge 1 - O(k\sqrt{k\epsilon}),$$

where $j_1, j_2, \ldots, j_k$ *is any ordering of indices in* V_j.

Proof. The first inequality is easy and we prove the second as follows. By Eqs. (4.4), (4.3) and the assumption on the game value,

$$\mathop{\mathbb{E}}_j \mathop{\mathbb{E}}_{i\in V_j} \sum_a \mathrm{tr}_\rho(X^a_{V_j} \otimes Y^{a(i)}_i) \ge 1-\epsilon,$$

we have

$$\mathop{\mathbb{E}}_i \sum_b \mathrm{tr}_\rho(X^b_i \otimes Y^b_i) \ge 1-\epsilon.$$

The index i of a variable is sampled by the verifier who first samples a constraint C_j, and uniformly selects one of the k variables in the constraint. Hence, we have

$$\mathop{\mathbb{E}}_j \mathop{\mathbb{E}}_{1\le l\le k} \sum_b \mathrm{tr}_\rho(X^b_{j_l} \otimes Y^b_{j_l}) \ge 1-\epsilon,$$

where we slightly abuse the notion and use j_l to denote the l-th variable in constraint C_j. This implies that, for all $1 \le l \le k$,

$$\mathop{\mathbb{E}}_j \sum_b \mathrm{tr}_\rho(X^b_{j_l} \otimes Y^b_{j_l}) \ge 1-k\epsilon.$$

This establishes the consistency of the average POVMs X_{j_l} and Bob's measurement Y_{j_l} in expectation of j.

Next, we use a hybrid argument and denote

$$S_l = \mathop{\mathbb{E}}_j \sum_a \mathrm{tr}_\rho\Big(\sqrt{X^a_{V_j}}\sqrt{X^{a_k}_{j_k}}\cdots\sqrt{X^{a_l}_{j_l}} \otimes \hat{Y}^{a_{l-1},\ldots,a_1}_{j_{l-1},\ldots,j_1}\Big),$$

where $\hat{Y}_{j_{l-1},\ldots,j_1}$ is the POVM repeatedly measuring Y_i's. We claim that the approximation $S_l \approx_{\sqrt{k\epsilon}} S_{l+1}$ holds. To see this, first note that, by the consistency of X_{j_l} and Y_{j_l},

$$\begin{aligned} S_l &\approx_{\sqrt{k\epsilon}} \mathop{\mathbb{E}}_j \sum_a \mathrm{tr}_\rho\Big(\sqrt{X^a_{V_j}}\sqrt{X^{a_k}_{j_k}}\cdots\sqrt{X^{a_l}_{j_l}} \otimes \sqrt{Y^{a_l}_{j_l}}\hat{Y}^{a_{l-1},\ldots,a_1}_{j_{l-1},\ldots,j_1}\sqrt{Y^{a_l}_{j_l}}\Big), \\ &= \mathop{\mathbb{E}}_j \sum_a \mathrm{tr}_\rho\Big(\sqrt{X^a_{V_j}}\sqrt{X^{a_k}_{j_k}}\cdots\sqrt{X^{a_l}_{j_l}} \otimes \hat{Y}^{a_l,\ldots,a_1}_{j_l,\ldots,j_1}\Big). \end{aligned}$$

Again by the consistency of $X^{a_l}_{j_l}$ and $Y^{a_l}_{j_l}$, we can continue the above approximation by removing the $\sqrt{X^{a_l}_{j_l}}$ operator,

$$S_l \approx_{\sqrt{k\epsilon}} \mathop{\mathbb{E}}_j \sum_a \mathrm{tr}_\rho\Big(\sqrt{X^a_{V_j}}\sqrt{X^{a_k}_{j_k}}\cdots\sqrt{X^{a_{l+1}}_{j_{l+1}}} \otimes \hat{Y}^{a_l,\ldots,a_1}_{j_l,\ldots,j_1}\Big) = S_{l+1}.$$

Therefore, we have $S_1 \approx_{k\sqrt{k\epsilon}} S_{k+1}$. Notice further that

$$S_{k+1} \geq \mathop{\mathbb{E}}_j \sum_a \mathrm{tr}_\rho\big(X^a_{V_j} \otimes \hat{Y}^a_{j_k,\ldots,j_1}\big) \approx_{k\sqrt{k\epsilon}} 1,$$

where the last step uses the consistency of X_{V_j} and Y_i to remove the Y_i measurements sequentially. The proof completes by noting that $S_1 = \mathbb{E}_j F_\rho\big(X_{V_j}, \hat{X}_{j_1,j_2,\ldots,j_k}\big)$. □

Theorem 4.5. *A BCS game has a perfect quantum strategy if and only if there exists an assignment of projection operators X_i to each variable x_i such that*

1. *The operators satisfy the constraint (represented as polynomials) when substitute variables x_i's with operators X_i's,*

2. *For any two variables x_i, x_j occurring in the same constraint, operators X_i and X_j commute.*

Any assignment of projection operators satisfying the above two conditions is called a *quantum satisfying assignment*. The theorem therefore claims that the BCS game has a perfect quantum strategy if and only if the corresponding BCS has a quantum satisfying assignment. The second condition on the operators is important to us and we name it the *locally commutative condition*.

Proof. The theorem follows easily from Theorem 4.4. Suppose the BCS game has a perfect strategy $(\rho, \{X^a_{V_j}\}, \{Y^b_i\})$ such that the shared state is a pure state whose reduced state is full rank and $X^a_{V_j} = 0$ for a fails C_j. Consider the induced POVMs X_i's. By the first inequality of Theorem 4.4, each X^b_i operator must be a projection. By the second inequality in the theorem, $X^a_{V_j} = \Pi_l X^{a_l}_{j_l}$. Summing over all indices in V_j other than j_l and $j_{l'}$, the commutativity of variables $X^a_{j_l}$ and $X^a_{j_{l'}}$ follows from the fact that the ordering of j_l's is arbitrary. Finally, the set of operators $X_i = X^1_i$ must satisfy the constraints C_j by the assumption that $X^a_{V_j} = 0$ for all a fails C_j for all j. This is most easily seen, for example, by diagonalizing the operators X_{j_l}.

Conversely, given a quantum assignment, one can construct a corresponding game using the maximally entangled state and $X^a_{V_j} = \Pi_l X^{a_l}_{j_l}$ and $Y^b_i = \overline{X}^b_i$ where $X^1_i = X_i$ and $X^0_i = I - X_i$. □

BCS games provide a versatile framework for quantum constraint satisfaction problems. The quantum 3-SAT game and the magic square game are special examples of BCS games. The quantum 3-SAT game defines a quantum variant of 3-SAT denoted as 3-SAT*, the decision problem about the existence of quantum satisfying assignments. The quantum graph k-coloring game and the quantum graph homomorphism game can also be described in the BCS framework. For the graph k-coloring game for example, the following BCS with variables $x_{v,\alpha}$ for each vertex v and color α and constraints

$$\begin{aligned} x_{v,1} + x_{v,2} + \cdots + x_{v,k} &= 1, \text{ for all } v \in V, \\ x_{v,\alpha} x_{w,\alpha} &= 0, \text{ for all } (v,w) \in E, \end{aligned}$$

describes the quantum k-coloring problem.

Another important concept that fits well in the BCS framework is the Kochen-Specker sets. Generally, a Kochen-Specker set is a set of projections $S = \{P_j\}$ such that there is no 0,1-valued function $h : S \to \{0,1\}$ satisfying the condition: $\sum_{P_j \in B} h(P_j) = 1$ for any subset B of S such that $\sum_{P_j \in B} P_j = I$. Most of the examples of Kochen-Specker sets consist solely of rank-one projections, in which case the set can also be described by a set of unit vectors. A set $S = \{u_i\}$ of unit vectors in $\mathscr{H}$ is a Kochen-Specker set if there is no function $h : S \to \{0,1\}$ such that for any subset B of S forming an orthonormal basis of $\mathscr{H}$, $\sum_{u \in B} h(u) = 1$. The first finite construction of Kochen-Specker set consists of 117 vectors in $\mathbb{R}^3$, but this number has been reduced to 31 by Conway and Kochen.

To describe Kochen-Specker sets in the BCS framework, let us consider the following linear constraint system of a set S of binary variables x_j

$$\sum_{x_j \in B_k} x_j = 1, \text{ for some } B_1, B_2, \ldots, B_m \subset S. \tag{4.5}$$

The classical assignment of the constraint system corresponds exactly to the 0,1-valued function h in the definition of Kochen-Specker sets. Therefore, for any BCS in Eq. (4.5) that has a quantum assignment but no classical assignment, the quantum assignment for the BCS forms a Kochen-Specker set. On the other hand, any Kochen-Specker set of projections defines a magic constraint system of the above form where B_j's are chosen to be all the subsets of projections summing to I.

For later references, we denote KOCHEN-SPECKER* to be the quantum CSP defined by binary constraint systems whose constraints are all of the form $\sum_{x_j \in B} x_j = 1$ as in Eq. (4.5).

4.3 Locally Commutative Reductions

We have seen several interesting examples of games defined by constraint satisfaction problems. In the following, we will show that they are problems of the same difficulty. A particular form of reductions, called the locally commutative reductions, is employed for this purpose.

The idea of the locally commutative reductions is most clearly illustrated by the reduction from 3-SAT* to 1-in-3-SAT* defined below. The problem 1-in-3-SAT is a variant of 3-SAT that requires one and only one of three literals to be true in each clause. It is shown to be **NP**-complete by Schaefer[5]. In fact, the monotone version of it (where no negative literals occur) remains **NP**-complete. The constraint that exactly one of the three variables is true can be described by a

[5]Thomas J. Schaefer. "The complexity of satisfiability problems". In: *Proceedings of the tenth annual ACM symposium on Theory of Computing*. STOC '78. New York, NY, USA: ACM, 1978, pp. 216–226.

linear equation of the form $x_1 + x_2 + x_3 = 1$, where the addition is over real numbers. Therefore, 1-in-3-SAT* is a special KOCHEN-SPECKER* problem, and the following theorem also implies that 3-SAT* is reducible to KOCHEN-SPECKER*.

Theorem 4.6. 3-SAT* *is polynomial-time (Karp) reducible to* 1-in-3-SAT*.

Proof. We start with the classical reduction given by Schaefer[6]. Let R be a polynomial such that $R(x, y, z) = 1$ if and only if exactly one of x, y, z is 1. For example, one can take $R(x, y, z) = x + y + z$ as discussed above. For each clause $C = x \vee y \vee z$, the classical reduction uses six new variables $u_1, u_2, \ldots, u_6$, and introduces five clauses

$$R(x, u_1, u_4) = 1, R(y, u_2, u_4) = 1, R(u_1, u_2, u_3) = 1, R(u_4, u_5, u_6) = 1, R(z, u_5, 0) = 1. \tag{4.6}$$

The claim is that these five clauses can all be satisfied if and only if clause C is satisfied. (Negative literals such as $\neg x$ can be dealt with by introducing a variable x' and a constraint $x + x' = 1$.)

Now suppose that the 3-SAT* instance has a quantum satisfying assignment. It is easy to see that the resulting 1-in-3-SAT* instance of the above reduction also has a quantum satisfying assignment, by choosing certain operators for the variables u_i.

Conversely, however, if the 1-in-3-SAT* instance has a quantum satisfying assignment, it is not always the case that the operators X, Y and Z will satisfy the 3-SAT* clause and they are not even guaranteed to be locally commutative as required by a quantum satisfying assignment for 3-SAT*. To solve the problem, we need some gadget that enforces the commutativity of the operators. In order to reuse the classical reduction, we will also require that commutativity is the *only* constraint that the gadget enforces. This is possible for 1-in-3-SAT* as Lemma 4.7 states. Once we have this new construction and use it for any two variables for which we want to enforce the commutativity, the proof of the reduction completes easily. □

Lemma 4.7. *The binary constraint system*

$$x \ + u_1 + u_4 = 1, \tag{4.7a}$$
$$y \ + u_2 + u_4 = 1, \tag{4.7b}$$
$$u_1 + u_2 + u_3 = 1, \tag{4.7c}$$

forms a commutativity gadget of x, y *for* 1-in-3-SAT*.

Proof. By the first two constraints, the commutator

$$[x, y] = [1 - u_1 - u_4, 1 - u_2 - u_4] = [u_1 + u_4, u_2 + u_4] = [u_1, u_2],$$

where in the last step we used the local commutativity conditions of the first two constraints. Finally, by the local commutativity condition of the last constraint, we have $[x, y] = 0$, proving the commutativity of x, y.

To see that the commutativity is the only condition for x, y, it suffices to show that for any classical assignment to x, y, the constraint system always has an assignment that extends the assignment to x, y. This can be easily verified case by case. □

[6] Ibid.

Similarly, by a constructing a commutativity gadget for the 3-COLORING*, one can show that 3-SAT* is reducible to 3-COLORING*. The gadget is the following simple prism graph in Figure 4.4. The proof that this is indeed a commutativity gadget for 3-SAT* is more complicated and we won't discuss it in class. We also mention without proof that there is a natural reduction from 3-COLORING* to INDEPENDENCE* where the classical reduction suffices without the help of commutativity gadgets.

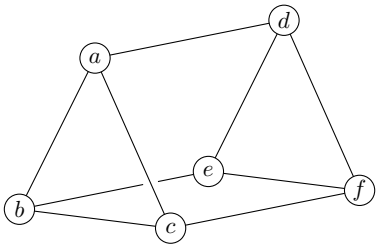

FIGURE 4.4: Triangular prism as a commutative gadget for 3-COLORING*

Sometimes, the commutativity gadget is very easy to construct. For example, if we want to reduce some problem to 3-SAT*, the commutativity gadget of x, y is simply a new clause $x \vee y \vee z$ where z is a new variable not occurring in the classical reduction. In this example, commutativity follows from the local commutativity condition, and extendibility is guaranteed by the nature of these constraints.

Theorem 4.8. *k-SAT* is polynomial-time (Karp) reducible to* 3-SAT*.

Proof. Following the classical reduction, transform each clause of the form $C = \bigvee_{j=1}^{k} x_j$ to a conjunction of $k-2$ clauses

$$(x_1 \vee x_2 \vee y_1) \wedge (\neg y_1 \vee x_3 \vee y_2) \wedge \cdots \wedge (\neg y_{k-4} \vee x_{k-2} \vee y_{k-3}) \wedge (\neg y_{k-3} \vee x_{k-1} \vee x_k),$$

where $y_1, y_2, \ldots, y_{k-3}$ are new variables. To recover commutativity lost from the reduction, add a new clause $x \vee y \vee z$ for each pair of variables x, y from $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_{k-3}$ not occurring in the same clause. □

The commutativity gadget can also be used to prove **NP**-hardness of many $*$-problems. For example, by applying the commutativity gadget of 3-SAT* globally, we have the following theorem stating the **NP**-hardness of 3-SAT*. It also implies the **NP**-hardness of many other problems including 3-COLORING*, 1-in-3-SAT*, and INDEPENDENCE* as simple corollaries.

Theorem 4.9. 3-SAT* *is* **NP***-hard.*

Proof. We prove the result by reducing 3-SAT to 3-SAT*. Let the 3-SAT instance of n variables $x_1, x_2, \ldots, x_n$ be $\bigwedge_{j=1}^{m} C_j$. For each pair of variables x_i, x_j that do not occur in the same clause, introduce a new clause $x_i \vee x_j \vee x'$, the commutativity gadget, where x' is a new variable. It is then easy to see that the resulting instance has quantum satisfying assignment if and only if the original instance has a classical satisfying assignment. □

The commutativity gadget for 3-SAT* can be thought as the dummy question check in Ito et al[7] embedded right in the problem instance. Following the analysis there and using Theorem 4.4, one can show that the following theorem that has an inverse polynomial gap.

Theorem 4.10. *There is a constant c such that, for* 3-SAT *instance ϕ of n variables and the* 3-SAT *game G_ϕ it defines, it is* **NP***-hard to distinguish between $\omega(G_\phi) = 1$ and $\omega^*(G_\phi) \le 1 - O(1/n^c)$.*

Lemma 4.11. *For any sequence $S = (i_1, i_2, \dots i_m)$ of indices of POVMs, Let π_S be the distribution defined by*

$$\pi_S(b) = \mathrm{tr}_\rho\big[\hat{X}^{b_1,b_2,\dots,b_m}_{i_1,i_2,\dots,i_m}\big].$$

For sequence $S' = (i_r, i_1, \dots, i_{r-1}, i_{r+1}, \dots, i_m)$,

$$D(\pi_S, \pi_{S'}) \le O\Big[\sum_{s=1}^{r-1} \mathrm{INC}(X_{i_s}, Y_{i_s}) + \sum_{s=1}^{r-1} D_\rho(\hat{X}_{i_s,i_r}, \hat{X}_{i_r,i_s})\Big].$$

We skip the proof of the lemma, which follows by a hybrid argument as in the proof of Theorem 4.4.

Proof of Theorem 4.10. We only sketch the proof, the main part of which is a rounding algorithm from a good quantum strategy $(\rho, \{X^a_{V_j}\}, \{Y^b_i\})$ to a randomized classical strategies[8].

For any classical 3-SAT instance, use the commutativity gadget $x_i \vee x_{i'} \vee x'$ as in Theorem 4.9 for each pair of variables x_i, $x_{i'}$. Call the resulting instance ϕ and relabel the n variables, including the auxiliary variable x', as $x_1, x_2, \dots, x_n$. Let $(\rho, \{X^a_{V_j}\}, \{Y^b_i\})$ be a quantum strategy for G_ϕ with value $1-\epsilon$. Define $\mu(i)$ as the marginal probability of $\mu(j,i)$, the distribution of questions. Assume without loss of generality that $\mu(1) \ge \mu(2) \ge \cdots \ge \mu(n)$.

Consider the probabilistic classical strategy π_S for $S = (1, 2, \dots, n)$. For each constraint C_j, define $S_j = (j_1, j_2, \dots, j_k, 1, \dots, n)$ to be the reordering of S moving j_r's to the front of the sequence. By Lemma 4.11, we have

$$D(\pi_S, \pi_{S_j}) \le \sum_{l=1}^{k} O\Big[\sum_{i=1}^{j_l-1} \mathrm{INC}(X_i, Y_i) + \sum_{i=1}^{j_l-1} D_\rho(\hat{X}_{i,j_l}, \hat{X}_{j_l,i})\Big].$$

Consider the difference of the classical value achieved by π_S and the quantum value related to π_{S_j}

$$1 - \mathop{\mathbb{E}}_j \sum_{a \text{ fails } C_j} \mathrm{tr}_\rho(\hat{X}^a_{j_1,\dots,j_k}) \approx_{k\sqrt{k\epsilon}} 1 - \mathop{\mathbb{E}}_j \sum_{a \text{ fails } C_j} \mathrm{tr}_\rho(X^a_{V_j}) = 1.$$

[7] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. "Oracularization and Two-Prover One-Round Interactive Proofs Against Nonlocal Strategies". In: *Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity*. CCC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 217–228. ISBN: 978-0-7695-3717-7.

[8] Our proof closely follows idem, "Oracularization and Two-Prover One-Round Interactive Proofs Against Nonlocal Strategies"; See also Julia Kempe et al. "Entangled Games Are Hard to Approximate". In: *Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*. FOCS '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 447–456.

The difference is bounded by a constant times

$$\begin{aligned}
&\mathop{\mathbb{E}}_{j}\Big[\sum_{l=1}^{k}\sum_{i=1}^{j_l-1}\mathrm{INC}(X_i,Y_i)+\sum_{l=1}^{k}\sum_{i=1}^{j_l-1}D_\rho(\hat{X}_{i,j_l},\hat{X}_{j_l,i})\Big]\\
&\le k\sum_{i,i':i<i'}\big[\mu(i')\,\mathrm{INC}(X_i,Y_i)\big]+k\sum_{i,i':i<i'}\big[\mu(i')D_\rho(\hat{X}_{i,i'},\hat{X}_{i',i})\big]\\
&\le k\sum_{i,i':i<i'}\big[\mu(i)\,\mathrm{INC}(X_i,Y_i)\big]+k\sum_{i,i':i<i'}\big[\sqrt{\mu(i)\mu(i')}D_\rho(\hat{X}_{i,i'},\hat{X}_{i',i})\big]\\
&\le kn\mathop{\mathbb{E}}_{i}\big[\mathrm{INC}(X_i,Y_i)\big]+kn^2\mathop{\mathbb{E}}_{i,i'}\big[D_\rho^2(\hat{X}_{i,i'},\hat{X}_{i',i})\big].
\end{aligned}$$

For each of the new gadget constraint $x_i \vee x_{i'} \vee x'$, Alice can always answer 1 to x' and the constraint is always satisfied. The second approximation in Theorem 4.4 then implies

$$\mathop{\mathbb{E}}_{i,i'} D_\rho^2\big[\hat{X}_{i,i'},\hat{X}_{i',i}\big] \le O(\epsilon^{1/2}), \tag{4.8}$$

assuming without loss of generality that the number of gadget clauses is roughly some constant fraction of all clauses.

The above analysis shows that the classical strategy of π_S has value at least $1-O(n^2\epsilon^{1/2})$. For $\epsilon = O(\frac{1}{n^4m^2})$ where m is the number of clauses, the instance must be classically satisfiable as G_ϕ has classical value at least $1-O(1/m)$ in this case. So the 3-SAT problem is reduced to decide whether $\omega(G_\phi)=1$ or $\omega^*(G_\phi)\le 1-\epsilon$. □