Part 1. **Warm-up**

001H

PAULI BRAIDING

Contents

001J

1. Multiplayer games

A multiplayer game is a single-round interaction between a *referee* and multiple *players*. The game specifies the actions of the referee: with what distribution she selects the questions to the players, and what tuples of answers are valid for each tuple of questions. The players, traditionally referred to as Alice, Bob, Charlie, etc., are always assumed to attempt to maximize their probability of winning (i.e. providing valid answers) in the game. The probability is over both the referee's and the players' randomness. This quantity, the players' maximum winning probability, is usually called the *value* of the game.

Multiplayer games play an important role in theoretical computer science. Their study ca be motivated from at least two vantage points:

- *Hardness of approximation for constraint satisfaction problems.* The most famous game in this context is the 3SAT "clause-vs-variable" game. In this game there are two players, Alice and Bob. Both players and the referee are given access to the same 3SAT formula φ. Moreover, the players can agree on a strategy after having seen the formula and before the game starts. Once the game starts, the referee selects a clause $C = x \vee y \vee z$ (some of the variables may be negated) uniformly at random, as well as a variable $w \in \{x, y, z\}$ appearing in C, again uniformly at random. She sends the triple $\{x, y, z\}$ to Alice, and the single variable w to Bob. Each player is expected to return an assignment to the variables he or she was asked about. The players win if and only if Alice's assignment satisfies the clause C, and Bob's assignment is consistent with Alice's on the variable they were asked in common.
  It is not hard to verify that the maximum success probability in this game is directly related to the largest number of clauses of φ that can be simultaneously satisfied by any assignment. Since 3SAT is NP-hard, it follows that the value of a game specified explicitly (in matrix form, i.e. a table specifying explicitly the distribution on questions and the truth table for valid answer tuples) is NP-hard to compute.
  In fact, it follows from the PCP theorem that the value is not only hard to compute exactly, but even to approximate within a sufficiently small constant factor. The language of games plays an important role in Dinur's

proof of the PCP theorem [**?**], and it has been instrumental in many reductions deriving hardness of approximation for combinatorial problems. It can also be a useful perspective when studying rounding techniques for linear programming (LP) or semidefinite programming (SDP) relaxations of constraint satisfaction problems.

- *Interactive protocols in cryptography.* In cryptography, games often play a role as building blocks in *interactive protocols*, where the players are usually referred to as *provers*. A famous game in this context is the two-prover commitment protocol by Ben-Or et al. [**?**]. This protocol was introduced to show that all languages in NP have two-prover interactive proofs with perfect zero-knowledge. Technically the protocol gives rise to a two-round game: the referee first interacts with the first prover (commit phase), and then with the second prover (reveal phase). Many kinds of games arise in cryptography, with the players sometimes exchanging messages between themselves, some players being trusted ("oracles") and others not, etc.

Quantum information introduces an exciting twist in the theory of multiplayer games: what if the players are allowed to use entanglement? The game is the same, but the set of allowed strategies has been broadened. While entanglement does not allow the players to communicate, it could in principle allow them to increase their odds of winning, and indeed this is the case: you already saw this in the example of the CHSH game, and we will see many more examples as we go.

Remark 1.1. One can ask, why stop at quantum? The most general strategies that respect the no-communication assumption are aptly called *non-signaling strategies*. We will not discuss them in this lecture, but aside from being a nice extension of quantum strategies they have recently become very relevant in designing efficient (single-prover) classical delegation protocols; see e.g. [**?**].

Interestingly, many games have the property that the optimal quantum strategy for the players is essentially unique. This property, called *rigidity*, can be leveraged to devise classical tests that verify that arbitrary quantum devices (the players) perform very specific operations. This opens up a whole new world of possibilities, from the certification of information-theoretic randomness to "device-independent" security proofs in cryptography to protocols for delegated computation; we will touch on some of these topics in a subsequent lecture.

Resources. A great introduction to complexity-theoretic questions about non-local games is the paper by Cleve et al. [**?**]. The lecture notes by Ji (see module 5 here) cover CHSH, the Magic Square game, linearity testing (using a slightly different analysis than the one we will give here), and graph-based games.

Notation. In this lecture we use the non-standard notation 001K

$$|\phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle \tag{1.1.1}$$

for the maximally entangled state in d dimension. In particular, $|\phi_2\rangle$ denotes an EPR pair.

2. Chapters

Preliminaries (1) Introduction