A Classical Leash for a Quantum System: 
Command of Quantum Systems 
via Rigidity of CHSH Games

Ben W. Reichardt 
University of Southern California

Falk Unger 
Knight Capital Group

Umesh Vazirani 
UC Berkeley

ABSTRACT

Can a classical experimentalist command an untrusted quantum system to realize arbitrary quantum dynamics, aborting if it misbehaves? If so, then we could realize the dream of device-independent quantum cryptography: using untrusted quantum devices to establish a shared random key, with security based on the correctness of quantum mechanics. It would also allow for testing whether a claimed quantum computer is truly quantum.

We prove a rigidity theorem for the famous Clauser-Horne-Shimony-Holt (CHSH) game, first formulated to provide a means of experimentally testing the violation of the Bell inequalities. The theorem shows that the only way for the two non-communicating quantum players to win many games played in sequence is if their shared quantum state is close to the tensor product of EPR states (Bell states) and their measurements are the optimal CHSH measurements on successive qubits. This theorem may be viewed as analogous to classical multi-linearity testing, in the sense that the outcome of local checks gives a characterization of a global object.

The rigidity theorem provides the basis of a technique by which a classical system can certify the joint, entangled state of a bipartite quantum system, as well as command the application of specific operators on each subsystem. This leads directly to a scheme for device-independent quantum key distribution. Control over the state and operators can also be leveraged to create more elaborate protocols for realizing general quantum circuits. In particular, it allows us to establish that a quantum interactive proof system with a classical verifier is as powerful as one with a quantum verifier, or QMIP = MIP∗.

Categories and Subject Descriptors
F.1 [Computation by Abstract Devices]: Miscellaneous

General Terms
Theory

Keywords
CHSH game; quantum computing; device independence; quantum key distribution; property testing; multi-prover interactive proof systems

1. REFERENCES

[1] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems via rigidity of CHSH games. 2012, arXiv:1209.0449 [quant-ph].
[2] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. 2012, arXiv:1209.0448 [quant-ph].

An extended abstract for this paper, including proof sketches, is available at [1]. A full version of this paper, including all proofs, is available at [2].