Research Statement

The discovery of the combined power of *randomness* and *interaction* is at the origin of some of the most important developments in theoretical computer science over the past quarter century, including interactive proof systems, the PCP theorem and hardness of approximation. Celebrated breakthroughs in quantum computing, the possibility for unconditionally secure key distribution [BB84] and a polynomial-time algorithm for factoring [Sho97], rely at their heart on *entanglement*, the quintessential quantum mechanical resource. My research is situated at the intensely active interface between these two areas: what is the *combined* power of interaction and entanglement?

Studying this question opens the way for many profound consequences. It makes it possible to generate certifiably random numbers [VV12a], a desirable task impossible to achieve classically. My work on this topic has already generated interest from NIST, which announced a plan to experimentally implement a randomness generation protocol. Building upon this work, very recently I proved security of a simple protocol for realizing device independent quantum key distribution [VV12b], a holy grail of quantum cryptography over the last 15 years. Both these works required the development of new tools to study a fundamental property of entanglement, its *monogamy*.

The combination of interaction and entanglement also raises deep questions in complexity theory. The complexity of multiplayer games, which are interactive games played between a trusted referee and two or more collaborating but non-communicating players, is a major theme in modern computational complexity theory. Its study has led to the PCP theorem and applications ranging from combinatorial optimization to cryptography. The complexity of games with entangled players has been one of the most challenging questions in quantum complexity theory. Resolving it [IV12] required the development of new insights into the power of entanglement (and its limits) to coordinate the actions of non-communicating provers. It also leads to a new perspective on a fundamental building block of probabilistically checkable proofs, the linearity test.

Over the last few years there is a growing connection between quantum information theory and “classical” theoretical computer science. This is manifest in the deep relationship between semidefinite programming (now a, if not the, central technique in both algorithms and complexity theory) and quantum information. Indeed, quantum interpretations of semidefinite programs are increasingly proving to be the “right way” to interpret and gain insight on the latter (just as probability theory in the context of counting arguments). My research has exploited such insight to develop new algorithms for purely classical problems [NRV12] as well as to give new proofs of important results in functional analysis [RV12a, BBLV12]. This “quantum connection” plays a fundamental role in my research, as outlined below, and can only be expected to intensify with time.

**Linearity testing with entangled provers and NEXP \( \subseteq \text{MIP}^* \)**

One of the central questions in complexity theory concerns the power of a polynomially bounded verifier interacting with multiple provers who are not allowed to communicate with each other. The proof that the associated complexity class MIP contains NEXP [BFL91] led to the PCP theorem and many of the most important developments in modern complexity theory. How is this computational power affected if
the provers are allowed to share entanglement? Intuitively, the resulting class MIP$^*$ captures how effectively non-communicating provers can use entanglement to coordinate their actions. (MIP$^*$ is the class of languages that can be decided by a classical randomized polynomial-time verifier, who interacts with a constant number of all-powerful but untrusted provers allowed to share entanglement.) The exploration of this question in a non-interactive setting played a pivotal role in the development of quantum mechanics, starting with the formulation by Einstein, Podolsky and Rosen of the famous EPR paradox [EPR35]. The extension is significant: examples of games are known in which classical provers must fail with constant probability but entangled provers have a perfect winning strategy [Ara02].

In [IV12] I proved that NEXP $\subseteq$ MIP$^*$. The crux of the proof lies in establishing that the multilinearity test of Babai, Fortnow and Lund works even against entangled provers. Like its predecessor, the Blum-Luby-Rubinfeld linearity test [BLR93], and subsequent low-degree tests, the multilinearity test is designed to robustly check for a global property by only making local queries. Entanglement provides a unique challenge to this local-global connection, and generalizing the linearity test to the quantum setting brings new insights on the nonlocal properties of this famously counterintuitive phenomenon.

The starting point for our entangled-prover linearity test is Hastad’s Fourier analysis-based proof of the linearity test [Hås01], which can be adapted to the broader operator-based mathematical framework of quantum mechanics. Indeed, one might even say that quantum mechanics is the natural setting for Fourier-analytic proofs, and this generalization leads to a deeper understanding of the techniques. Multilinearity testing poses further challenges, which we tackle by introducing a new self-correction procedure based on the use of a semidefinite program. Once again, quantum mechanics provides the most natural setting for understanding semidefinite programming, as we discuss in more detail in the next section.

The traditional variant of the linearity test makes three queries to a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and accepts if and only if $f$ is close to a linear function $x \mapsto u_1 x_1 + \cdots + u_n x_n$. In the quantum setting, it is most natural to think of each query as being made to non-communicating provers sharing entanglement. In this setting the uncertainty principle implies that it is in general impossible to translate the provers’ strategy into a consistent list of answers to all possible queries, even a probabilistic one. This poses a serious difficulty for the linearity test: since quantum provers do not necessarily provide answers consistent with any given function, what does it even mean to test them for linearity? To formulate an answer, recall that the crux of Hastad’s argument consists in showing that the distribution defined by the squared Fourier coefficients of $f$ is highly peaked. The same reasoning applied to the quantum setting yields the following. Success in the linearity test implies that the provers’ strategy is equivalent to one in which each prover first, applies a global, query-independent measurement defined from the the operator-valued Fourier coefficients associated to its original strategy and second, answers its query by evaluating the function obtained as the outcome of his measurement. The peaked distribution in the classical setting translates to this new strategy for the provers being consistent: with high probability applying the same global measurement will produce the same linear function for all provers. This elegant reformulation of the meaning of being close to linear is adapted to both the classical and quantum settings, as neither the statement nor its proof require one to refer to an underlying function.

The techniques developed in my work on entangled-prover interactive proofs only scrape the surface of the wide range of questions that can be asked in this context. The biggest outstanding question is arguably that of proving an upper bound on the class MIP$^*$. The difficulty is that quantum provers may a priori benefit from larger and larger amounts of shared entanglement, and the problem of deciding between a maximum success probability of $1/3$ and $2/3$ is not even known to be decidable. Could the presence of entanglement between the provers even be beneficial to verify larger classes of languages? These question are connected to classical problems in dimension reduction, and studying them could yield new insights in high-dimensional
One of the key properties of entanglement is that it is monogamous \cite{Ter04}. Intuitively, this means that a quantum state that exhibits maximal entanglement in-between two parties cannot be extended, or shared, with a third party. Monogamy is one of the most distinguishing features of entanglement, and it is also one of the hardest to quantify; many information-theoretic measures have been proposed for its study. Multiprover interactive proofs provide a new setting in which to study the consequences of this phenomenon. For instance, in \cite{KKM11} we exploited monogamy to obtain the first hardness results on entangled games. My result NEXP ⊆ MIP* seems to require the use of three provers: is three-prover MIP* a different class from two-prover MIP*? (In the section on cryptography below I discuss a different type of application of monogamy.)

Quantum games and semidefinite programming

The maximum success probability of classical players in a two-player game can be cast as a quadratic optimization problem, and the natural semidefinite relaxation often provides a good (and under the Unique Games Conjecture (UGC) optimal) polynomial-time approximation. Allowing entanglement between the players leads to a rich set of questions and new techniques. To begin with, the entangled value of the game (the maximum success probability of players sharing entanglement) lies between the classical and semidefinite values. For certain classes of games the entangled value turns out to be equal to, or closely approximated by, the semidefinite value \cite{CHTW04,KRT10}. In \cite{RV12b} we introduced a new class of games, called quantum XOR games, in which questions to the players are quantum messages. Using a non-trivial connection with deep inequalities in functional analysis (the non-commutative and operator space Grothendieck inequalities \cite{Pis12}) we gave two semidefinite programs (SDPs) whose optimum is within a constant factor of the unentangled and entangled values respectively. These semidefinite programs have a somewhat unusual form, and an intriguing open question is whether they can lead to a better approximation factor for some classical games than permitted by the UGC. The quantum connection has already fed back into functional analysis, leading us to a new, quantitative proof \cite{RV12a} of the aforementioned extensions of Grothendieck’s inequality based on tools from quantum information theory.

The optimization problem solved by the players in a quantum XOR game turns out to capture a surprisingly broad class of problems from learning theory. As a consequence of the semidefinite programs mentioned above, in \cite{NRV12} we obtained constant-factor approximation algorithms for variants of robust principal component analysis \cite{DZH06,Kwa08} and the orthogonal Procrustes problem \cite{GD04}. The best previous polynomial-time algorithms for these problems had approximation guarantees with a logarithmic dependence on the input size \cite{MT12,Nem07,So11}.

Multiplayer games illustrate that the connection between semidefinite programs and quantum information goes much deeper than the observation that positive semidefinite matrices can be interpreted as quantum states (and their dual object, Hermitian operators, as quantum measurements). Thinking in terms of games and strategies is often easier than reasoning about matrices, and this explains why quantum multiplayer games are taking an increasingly central role in classical complexity theory. Very recently, a problem on computing tensor norms closely connected with the Lasserre hierarchy was shown NP-hard by adapting a result on the class QMA(2) of languages having two unentangled quantum proofs \cite{BBH12}. Going in the other direction, integrality gaps for semidefinite relaxations can sometimes be translated back to separations between classical and entangled players \cite{BRSJW11}, possibly leading to convincing experiments demonstrating quantum nonlocality.

Thinking about semidefinite programs through the lens of quantum information theory will likely lead
to further insights. It played an important role in the discovery of the matrix multiplicative weights update (MMWU) method \cite{TRW05, Kal07}, which gives the fastest primal-dual implementations of SDP-based approximation algorithms and is central to the celebrated proof of QIP=PSPACE \cite{JJUW11}. A possible direction I am particularly interested in would be to exploit the connection between SDPs and entangled players in the context of rounding algorithms: is it possible to devise a rounding procedure that performs provably better when applied to quantum strategies than when applied to a vector solution from the basic semidefinite relaxation? This might lead to the UGC-based hardness of approximating the entangled value, as well as give new insights on the strength and limitations of SDP relaxations.

**Device-independent cryptography and quantum-proof extractors**

We already encountered a most striking limitation of entanglement, its *monogamy*: the presence of strong correlations between two parties all but guarantees that no space-like separated third party can be correlated with either of the first two. This property, shared to some extent by all correlations that do not allow for signaling \cite{BLM05}, takes on many guises and is notoriously hard to quantify. In \cite{VV12a, VV12b} we developed tools to harness monogamy in the so-called *device-independent* scenario. Here the idea is that the quantum mechanical apparatus (or *devices*) used to perform a certain cryptographic task are completely untrusted, and may have been handed out by an adversary (for instance, a manufacturer with malicious intentions). The goal is to design protocols that either successfully use the devices to accomplish the task, or reject overly suspicious devices. The following two far-reaching applications entailed a deepening of our understanding of monogamy:

- Given two non-communicating devices, a simple statistical test can guarantee the presence of supra-classical correlations in the devices’ input/output behavior. By definition, any such test certifies that the devices must be generating randomness \cite{Col06}. In \cite{VV12a} we devised the first protocol for randomness expansion that guarantees that the bits are unpredictable even by a quantum adversary, making them suitable for use in cryptography. The only assumption required is that no information is exchanged between the devices throughout the protocol. This work has generated interest from various experimental groups; however, to be fully practical the noise tolerance of our protocol needs to be drastically improved. Achieving this may require further insights, and constitutes an exciting prospect for further work.

- Proving security of quantum key distribution in the device-independent setting has been a tantalizing possibility ever since the pioneering work of Mayers and Yao \cite{MY98}. In \cite{VV12b} we resolved this question by establishing the security of a simple protocol for quantum key distribution (in fact very closely related to Ekert’s original proposal \cite{Eke91}). Although the context here is more complex than for randomness expansion (in part because the protocol involves public communication on which the adversary may eavesdrop), we again exploited monogamy to rule out the possibility for the adversary to gain information about the key.

The proofs of both results rely on a crucial connection with the theory of randomness extractors, a cornerstone of modern cryptography. The advent of quantum attacks on classical cryptosystems requires the introduction of “quantum-proof” extractors: extractors able to produce near-uniform random bits even in the presence of an adversary holding quantum side information about the source. The proper formalization of the notion of quantum side information started an ongoing revolution in quantum information theory, from the introduction of the quantum bounded storage model \cite{DFSS05} to the development of a framework of conditional entropies \cite{Ren05}. 

4
In [DV10, DPVR12] we established that any extractor based on Trevisan’s construction paradigm [Tre01] is automatically quantum-proof, with virtually no loss in parameters. This answered the long-standing open question of whether it was even possible to obtain quantum-proof extractors with poly-logarithmic seed length. Adapting Trevisan’s proof technique, known as the reconstruction paradigm, to the quantum setting was challenging because it involves repeated “measurements” of the adversary’s side information, a very sensitive task in the context of quantum information. We introduced a “quantum reconstruction paradigm” which exploits properties of the so-called pretty-good measurement (first used in the analysis of extractors by König and Terhal [KT08]) to surmount this difficulty. This powerful technique plays a key role in the aforementioned results in quantum cryptography.

Questions revolving around interaction and the nature of entanglement are currently among the most exciting and promising directions for research in quantum computing. Recent advances in experimental implementations suggest that the first small-scale quantum computers may soon be built. It is unlikely that these computers will have the ability to factor impressively large numbers; instead they will be custom-made to solve a particular task. This raises the following question: given a device purported to exhibit “truly quantum” behavior, is there a way by which a classical observer can verify this claim? The study of this problem has already prompted exciting theoretical [ABOE10, BFK09, RUV12] as well as practical [BKB+12] research. I would very much like to explore the question further; in addition to it being a fundamental challenge for quantum computing it seems to provide a promising direction in which to extend some of my work on device independence and interactive proofs.

The possibility for a “quantum PCP theorem” has in recent years focused the attention of researchers in quantum complexity theory [AALV11] as well as condensed matter physics [Has07], from where the problem originates. At its heart lie deep questions about the nature of entanglement and its localization in quantum states, and on the complexity of simulating quantum mechanical processes. The fact that computer science may provide the ideal perspective and set of techniques to study such problems is, to my mind, one of the most stimulating current prospects for scientific discovery. The quantum PCP conjecture can be phrased as a problem on gap amplification: is approximating the ground state energy of a gapped local Hamiltonian up to a constant factor as hard as approximating it to within an inverse polynomial? Finding a convergence between techniques employed to achieve a similar gap amplification in the context of multi-prover interactive proofs and previous approaches to this question could lead to new advances.

References


