Workshop on the Foundations of Randomness

Wallenberg Research centre

10 Marais Street, Stellenbosch, 7600

Monday 10/26		Tuesday 10/27		Wednesday 10/28	
9:15-9:30	Geyer	**9:15-10:15**	Zuckerman		
9:30-10:30	Scarani	**10:15-11:00**	Chattopadhyay	**9:30-10:30**	Dodis
10:30-11:00	*Coffee break*	**11:00-11:30**	*Coffee break*	**10:30-11:00**	*Coffee break*
11:00-12:00	Renner	**11:30-12:30**	Yuen	**11:00-12:00**	Fawzi
12:00-14:00	*Lunch break*	**12:30-14:00**	*Lunch break*	**12:00-14:00**	*Lunch break*
14:00-15:00	Hoefer	**14:00-15:00**	Schack	**14:00-15:00**	Pironio
15:00-15:30	*Coffee break*	**15:00-15:30**	*Coffee break*	**15:00-15:30**	*Coffee break*
15:30-16:30	Pawlowski	**15:30-16:30**	Miller	**15:30-16:30**	Acin
		16:30	Depart for conference dinner		

Titles & Abstracts

Speaker: Valerio Scarani (NUS & CQT, Singapore)

Title: Quantum randomness and the device-independent claim

Abstract: We have known (or believed) that quantum physics is intrinsically statistical for many decades; but I shall argue that only the idea of "device-independent certification" brought the generation of randomness at the same disruptive level as key distribution and computing. I'll introduce the notions needed in order to get there.

Speaker: Renato Renner (ETH Zurich, Switzerland)

Title: Is the existence of randomness an axiom of quantum theory?

Abstract: Within the usual formulation of quantum theory, the Born rule postulates that the outcomes of measurements are generally random. The existence of randomness is therefore often regarded as an axiom of quantum theory. In this talk, I will argue that the Born rule can be "decomposed" into more basic statements. The study of them can provide novel insights into the nature of quantum randomness and, in particular, the physical interpretations of the probabilities obtained from the Born rule.

Speaker: Carl Hoefer (UAB Barcelona, Spain)

Title: Irreducibly Probabilistic Laws and Quantum Randomness

Abstract: The laws of nature could be indeterministic, in the sense that they simply fail to be deterministic. There are numerous examples of determinism-failure even in classical physics. A different idea entirely is that of irreducibly probabilistic laws of nature: laws whose contents are, or entail, putative objective probabilities or chances for events. I will raise concerns about how well we understand the notion of an irreducible probabilistic law in general, arguing that we face an interpretive dilemma where both options are very problematic. And I will offer some comments on how we may be able to understand specifically quantum chances, the probabilities prescribed by the Born rule in QM.

Speaker: Marcin Pawlowski (KCIK, Poland)

Title: Relation of randomness and monogamy of nonlocal correlations

Abstact: Physical principles constrain the way nonlocal correlations can be distributed among distant parties. These constraints are usually expressed by monogamy relations that bound the amount of Bell inequality violation observed among a set of parties by the violation observed by

a different set of parties. I discuss how these relations are connected to the intrinsic randomness of quantum measurements and the meaning of this connection.

Speaker: David Zuckerman (UT Austin, USA)

Title: When is Randomness Extraction Possible?

Abstract: A randomness extractor is an efficient algorithm that extracts high-quality randomness from a low-quality random source. We examine when such randomness extraction is possible, surveying seedless and seeded extractors and their applications.

Speaker: Eshan Chattopadhyay (UT Austin, USA)

Title: Explicit Two-Source Extractors and Resilient Functions

Abstract: We explicitly construct an extractor for two independent sources on n bits, each with min-entropy at least log^C n for a large enough constant C. Our extractor outputs one bit and has error n^{-\Omega(1)}. The best previous extractor, by Bourgain, required each source to have min-entropy .499n.

A key ingredient in our construction is an explicit construction of a monotone, almost-balanced boolean function on n bits that is resilient to coalitions of size n^{1-delta}, for any delta>0. In fact, our construction is stronger in that it gives an explicit extractor for a generalization of non-oblivious bit-fixing sources on n bits, where some unknown n-q bits are chosen almost polylog(n)-wise independently, and the remaining q=n^{1-\delta} bits are chosen by an adversary as an arbitrary function of the n-q bits. The best previous construction, by Viola, achieved q=n^{1/2 - \delta}.

Our explicit two-source extractor directly implies an explicit construction of a 2^{(log log N)^{O(1)}}-Ramsey graph over N vertices, improving bounds obtained by Barak et al. and matching independent work by Cohen.

Joint work with David Zuckerman.

Speaker: Henry Yuen (MIT, USA)

Title: What are the minimal assumptions needed for infinite randomness expansion?

Abstract: Infinite randomness expansion is the tantalizing idea of classical beings using *finite* seed randomness to certify an *unbounded* amount of randomness generation from quantum processes. This was recently shown to be possible, as long as one believes that quantum

mechanics is correct, and that one can prevent different regions of space from signaling to each other.

In this talk I'll give an overview of infinite randomness expansion, and discuss what are the *minimal* assumptions needed for it. How much seed randomness do we need? Can general relativity help? Do we need to assume the validity of quantum mechanics, or can we only use the non-signaling principle? I will explore these possibilities and more.

Speaker: Ruediger Schack (Royal Holloway, University of London, UK)

Title: Randomness and laws of nature: the QBist perspective

Abstract: Randomness is a well understood and well defined field of study in mathematics and computer science. For instance, algorithmic information quantifies the amount of randomness in a bit string, and the theory of pseudorandom number generators gives bounds on the computational difficulty of guessing the next bit in a sequence. By contrast, it is much less clear what it means for a physical source to be ``truly random", e.g., for it to produce every possible output string with equal probability.

It might seem that quantum mechanics solves the problem. Quantum random number generators are often said to provide true randomness guaranteed by ``the laws of nature". The recent invention of device-independent protocols makes it possible to certify the randomness of the bits output by a quantum device even if the latter cannot be trusted. The theory of device independence has led to rigorous theorems about quantum random number generators, proving, e.g., strong randomness properties for the output given weak randomness assumptions for the input, or seed. These theorems are much stronger than their classical counterparts. At the same time, they are like the classical counterparts in that they assume a prior probability for the seed. The theory of device independence provides new and strong connections between the input and output probabilities, but does not put any constraints on the input probabilities.

In this talk I argue that this characteristic of the theory of device independence is actually a characteristic of the quantum formalism in general. That the role of quantum mechanics, and of the Born rule in particular, is not to set probabilities but to connect probabilities in different and typically incompatible measurements is one of the main tenets of QBism, an interpretation of quantum mechanics developed out of the earlier quantum Bayesianism.

By adopting a stricly personalist approach to probability in quantum mechanics, QBism takes the view that quantum states reflect an agent's personal degrees of belief about the consequences of his or her actions on the world. The quantum formalism enables agents to make better decisions in the light of their previous experiences, and thus has a normative character similar to the rules of probability theory. The QBist approach leads to a consistent picture which is free of interpretational difficulties such as the measurement problem.

Since according to QBism, quantum states, probabilities and thus randomness are not determined by properties of a physical system, but are personal to an agent, an agent's probability assignments does not put any constraints on what particular outcome will result from a quantum

measurement. Physical systems possess intrinsic freedom: quantum mechanics does not provide a mechanism, be it deterministic or stochastic, for the behaviour of a physical system. The fact that certified randomness necessarily depends on a prior probability assignment for an input seed thus may turn out to be the most fundamental insight gained from the study of device-independent quantum random number generators.

Speaker: Carl Miller

Title: The extremes of quantum random number generation

Abstract: Randomness can be certifiably generated using devices that exhibit Bell inequality violations -- that is, multi-part devices that score high at certain nonlocal games. The "rate curve" for a game identifies how the score is related to the amount of certified randomness. In this talk I will discuss how the extreme points of this curve illustrate two elegant principles. The first is the notion of "self-testing": the idea that the states and measurements of a device can sometimes be determined through classical means alone. The second is the notion of measurement disturbance: some quantum states are unavoidably changed by the mere act of measuring, and this disturbance generates true randomness.

Speaker: Yevggeniy Dodis (NYU)

Title: Randomness in Cryptography

Abstract: Unlike many other fields in computer science, randomness is essential for cryptography: secrets must have uncertainty to the attacker, and many cryptographic algorithms must be randomized (e.g., two stateless encryptions of the same message must look different). Traditionally, one assumes the existence of perfect randomness. However, this assumption is often unrealistic. In this talk I will survey what is know about basing cryptography of various (realistic) sources of randomness. We will ask the following questions:

1) Does Cryptography need nearly perfect ("extractable") sources of randomness, or is entropy sufficient?
2) What if the secret key is imperfect but "local" (or public) perfect randomness is available?

As we will see, the answer to the first question is largely negative, while the second questions leads to many positive answers, some of which found many applications beyond cryptography.

Speaker: Omar Fawzi (ENS Lyon, France)

Title: Exams

Abstract: In device-independent cryptography, the validity of protocols relies on a test of some property of the device (typically via a Bell test). The challenge in the security proof is to ensure that a device passing the test has the desired property. We ask a similar question in the setting of a student taking an exam. Suppose a student passed a test composed of randomly chosen question. Making no assumptions on the strategy used by the student to answer the questions, how can we quantify his knowledge?

Based on joint work with Norm Beaudry, Frederic Dupuis and Renato Renner.

Speaker: Stefano Pironio (ULB Brussels)

Title: Some open questions related to device-independent randomness generation

Abstract:

Speaker: Antonio Acin (ICFO, Spain)

Title: How much randomness can be certified in quantum and general non-signalling theories?

Abstract: The non-local correlations obtained by performing measurements on entangled quantum states certify the presence of randomness in the outputs. However, there exist non-local correlations that are (i) supra-quantum, in the sense that give an amount of non-locality higher than in quantum theory, but yet (ii) non-signalling, as they do not allow any form of communication. In the talk, we first compare randomness certification for quantum and general non-signalling correlations, proving that while maximal randomness can be certified in the first, it becomes impossible in the second. Then, we proceed to study the limits for randomness certification using quantum entangled states. We provide upper bounds on the amount of randomness certifiable from a quantum state of a given dimension in the standard Bell scenario involving destructive measurements, and present two strategies saturating the bound for qubits. Finally, we discuss how an unbounded amount of randomness can be certified using sequences of measurements.
