Mathematics, Statistics, and Computer Science **@ UIC**

Departmental Colloquium

Quantum correlations: from foundations to security against post-quantum eavesdropper

Pawel Horodecki (Gdańsk University of Technology)

Abstract: Quantum mechanics allows quantum correlations – also called quantum entanglement – that are stronger than all the correlations we know from our daily lives. Their enigma has already troubled fathers of Quantum Mechanics. Einstein's ingenious skepticism about this theory gave rise to the fundamental philosophical question - formalized mathematically by John Bell - about the objective existence of properties of quantum particles before measurement. We shall discuss the related Bell inequalities tests from the perspective of randomness and stress that while quantum mechanical statistics look completely random, it may allow for a contribution of determinism, if we look at them from the perspective of possible future physical theories. This rises an interesting problem of certification of randomness and cryptographic security in hypothetical situations where eavesdropper has a post-quantum power.

The two most natural post-quantum frameworks are the ones of no-signaling boxes and no- signaling assamblages. We discuss quantum correlations from the perspectives of the two frameworks. This includes on the one hand some no-go theorems and on the other hand some positive results concerning randomness amplification and generation of secure bits.

[1] J. Barrett, L. Hardy, A. Kent, Phys. Rev. Lett. 95, 010503 (2005) [2] R. Renner. R. Collbeck, Nat. Phys. 8, 450

Friday, October 6 at 3:00 PM in 636 SEO

(2012) [3] F. G.S.L. Brandao, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. H., T. Szarek, H. Wojewodka, Nat. Comm. 7, 11345 (2016) [4] P. Horodecki and R. Ramanathan, Nat. Comm. 10,1701 (2019) [5] R. Ramanathan, M. Banacki, R. Ravel Rodrigues, P. Horodecki, npj Quantum Information, 8, 119 (2022). [6] M. Banacki, P. Mironowicz, R. Ramanathan, P. Horodecki, New J. Phys. 24, 083003 (2022) [7] A. B. Sainz, N. Brunner, D. Cavalcanti, P. Skrzypczyk, T. Vertesi, Phys. Rev. Lett. 115, 190403 (2015) [8] M. Banacki, R. Ramanathan, P. Horodecki, Multipartite channel assemblages, arXiv:2205.05033 (2022).

Please reach out to Shmuel Friedland <friedlan@uic.edu> if you want to join the speaker for lunch or dinner, or have a meeting during their visit.

Friday, October 6 at 3:00 PM in 636 SEO