ATELIER « INFORMATION QUANTIQUE : CODES, GÉOMETRIE ET STRUCTURES ALÉATOIRES »
24–26 OCTOBRE 2011

WORKSHOP ON QUANTUM INFORMATION: CODES, GEOMETRY AND RANDOM STRUCTURES
OCTOBER 24–26, 2011

Random quantum circuits are approximate polynomial-designs

Fernando Brandao *
fgslbrandao@gmail.com

An approximate unitary t-design is a distribution of unitaries that mimic properties of the Haar measure for polynomials (in the entries of the unitaries) of degree up to t. It is a conjecture in the theory of quantum pseudo-randomness that polynomial sized random quantum circuits form an approximate unitary poly(n)-design. Unfortunately, up to now, the best result known is that polynomial random quantum circuits are unitary 3-designs. In this talk I will discuss recent work in this direction that settles the conjecture, showing that poly(n) random circuits are indeed approximate unitary poly(n)-designs. The proof combines three techniques that might show useful elsewhere. The first is a result of Nachtergaele for obtaining lower bounds on the spectral gap of certain frustration-free local Hamiltonians. The second is a version to the unitary group of the path-coupling method of Bubley and Dyer for bounding the convergence time of random walks. The third, explained in the talk by Aram Harrow, is an approximately orthogonality property of permutation matrices. Time permitting I'll discuss two applications of the result, one concerned with hiding data from a computationally bounded adversary, and another with linking the time of equilibration of local quantum systems to the diagonalisation complexity of the system Hamiltonian.

This is based on joint work with Aram Harrow and Michal Horodecki..

*Instituto de Ciencias Exatas, Departamento de Fisica, Universidade Federal de Minas Gerais, Av. Antonio Carlos, 6627, 31270-901 Belo Horizonte, MG, BRAZIL.