FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, edificio norte, piso 7
Santiago, CHILE
CP 837 0456

tel +56 2 2978 4870

AGCO Seminar

Author: Ivan Rapaport, DIM-CMM, U de Chile.

Where: Av República 701, Sala 33.

When: Wednesday, July 24, 14:30.

Title: On Distributed Merlin-Arthur Decision Protocols

Abstract:
In a distributed locally-checkable proof, we are interested in checking the legality of a given network configuration with respect to some Boolean predicate. To do so, the network enlists the help of a prover — a computationally-unbounded oracle that aims at convincing the network that its state is legal, by providing the nodes with certificates that form a distributed proof of legality. The nodes then verify the proof by examining their certificate, their local neighborhood and the certificates of their neighbors.

In this talk we examine the power of a randomized form of locally-checkable proof, called distributed Merlin-Arthur protocols, or dMA for short. In a dMA protocol, the prover assigns each node a short certificate, and the nodes then exchange random messages with their neighbors. We show that while there exist problems for which dMA protocols are more efficient than protocols that do not use randomness, for several natural problems, including Leader Election, Diameter, Symmetry, and Counting Distinct Elements, dMA protocols are no more efficient than standard nondeterministic protocols. This is in contrast with Arthur- Merlin (dAM) protocols and Randomized Proof Labeling Schemes (RPLS), which are known to provide improvements in certificate size, at least for some of the aforementioned properties.

Joint work with Pierre Fraigniaud, Pedro Montealegre, Rotem Oshman and Ioan Todinca.

CONICYT
Ministerio de Educación
Gobierno de Chile

cnrs