

QUIZ GAMES: A MODEL FOR INFORMATION HIDING

Luis M. Pardo

University of Cantabria, Spain

luis.m.pardo@gmail.com

In this talk I introduce a model for information hiding in Elimination Theory. The model we call Quiz Game is an interactive protocol based on a single round two-players game, admitting exact and approximative models. The model extends existing models like robust algorithms, universal algorithms or software engineering models in Elimination Theory, shown in former outcomes of the same current of thought. The main outcome here is to show that a player with a winning strategy for Elimination Problems requires exponential size abstract data types and, hence, any winning strategy cannot be efficient. Similar results are shown for the evaluation of characteristic polynomials, interpolation of straight-line programs and elementary arithmetic neural networks. This is ongoing research written with B. Bank, J. Heintz, G. Matera and A. Rojas-Paredes.