DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF SOUTHERN DENMARK, ODENSE

COMPUTER SCIENCE COLLOQUIUM

SAT-based Synthesis of Shortest Linear Straight-Line Programs over GF(2)

Carsten Fuhs
LuFG I2
RWTH Aachen University, Germany

Wednesday, 09 February, 2011 at 12:15
U145

Abstract:

Non-trivial linear straight-line programs over the Galois field of two elements occur frequently in applications such as encryption or high-performance computing. Finding the shortest linear straight-line program for a given set of linear forms is known to be MaxSNP-complete, i.e., there is no epsilon-approximation for the problem unless P = NP.

We present a non-approximative approach for finding the shortest linear straight-line program. In other words, we show how to search for a circuit of XOR gates with the minimal number of such gates. The approach is based on a reduction of the associated decision problem ("Is there a program of length k?") to satisfiability of propositional logic. Using modern SAT solvers, optimal solutions to interesting problem instances can be obtained. In particular, we prove optimality of an implementation of a part of the AES.

Host: Peter Schneider-Kamp