Informatik-Kolloquium

Rheinisch-Westfälische Technische Hochschule Aachen
Lehrstuhl für Informatik I

EINLADUNG

Zeit: Donnerstag, 07. Juni 2001, 17.00 Uhr

Ort: Raum AH I, Ahornstr.55

Referent: Prof. Dr. Matthias Krause, Uni Mannheim

Thema: Komplexität Boolescher Funktionen, Lernbarkeit und Kryptographie

Abstract:

Die Komplexitätstheorie Boolescher Funktionen beschäftigt sich mit der Analyse der Ausdruckskraft und mit algorithmischen Eigenschaften geeignet beschränkter Schaltkreis- und BDD Modelle. Dabei geht es nicht nur um die effiziente Darstellbarkeit bzw. Nichtdarstellbarkeit grundlegender Hardwareoperationen (logische und arithmetische Operationen, Adress- und Sortierfunktionen), sondern auch um die Eignung als Datenstruktur zur Minimierung und Manipulation Boolescher Funktionen bzw. zum Lernen Boolescher Konzeptklassen.

Ein weitere interessante Frage ist die nach der effizienten Darstellbarkeit kryptographischer Grundoperationen wie pseudozufälliger Bit- und Funktionsgeneratoren, Einweg- oder Hashfunktionen. In diesem Vortrag werden zunächst einige grundlegende Beziehungen und Resultate zu den Begriffen effiziente Darstellbarkeit Boolescher Funktionen, Untere-Schranken-Beweise gegen vorgegebene Modelle, Lernbarkeit Boolescher Funktionen und Fähigkeit eines Modells zur Generierung von Pseudozufälligkeit präsentiert. Danach werden neuere Resultate zu den Themen Lernbarkeit und Ausdruckskraft von Entscheidungslisten, minimale Hardwarekomplexität von pseudozufälliger Funktionsgeneratoren und Flusschiffrierer, sowie offene Problemevorgestellt und diskutiert.

Es laden ein: Die Dozenten der Informatik